



**UNCLASSIFIED**



# **North Dakota Homeland Security Anti-Terrorism Summary**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

**UNCLASSIFIED**

**NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

**QUICK LINKS**

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools and Universities\)](#)

[International](#)

[Information Technology and Telecommunications](#)

[Banking and Finance Industry](#)

[National Monuments and Icons](#)

[Chemical and Hazardous Materials Sector](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security Contacts](#)

[Emergency Services](#)

## **NORTH DAKOTA**

**North Dakota to continue monitoring pesticide levels found in Red.** The North Dakota Department of Agriculture said it will continue to monitor three pesticides found in 2010 in the Red River in concentrations approaching at-risk levels for fish and other aquatic life to see if the results repeat themselves. Results of a statewide survey of streams and rivers were largely positive, but the detection of three pesticides — atrazine, bifenthrin, and metolachlor — was noted as an area of concern that may warrant “risk mitigation measures” if pesticide levels persist. The state health department and U.S. Geological Survey conducted the survey, taking water samples from 33 sites from April through October. Overall, the survey found North Dakota’s rivers and streams contained only trace amounts of nine commonly used products, an agriculture commissioner said. Of the 43 detections, 29 were in the intensely farmed Red River Valley. Source:

<http://www.inforum.com/event/article/id/306281/>

## **REGIONAL**

**(Colorado; Wyoming; South Dakota) Bark beetle epidemic has infested 4 million acres in Colorado, Wyoming.** The bark beetle epidemic has infested 4 million acres in Colorado and southern Wyoming, and it is spreading into the Black Hills of South Dakota, U.S. Forest Service officials said. The figures released from an annual aerial survey of the U.S. Forest Service and the Colorado State Forest Service showed the bark beetle epidemic that started in 1996 spread to 400,000 new acres last year, according to the Associated Press. The hardest hit forests are the Arapaho, White River, Roosevelt, and Routt national forests in Colorado, and the Medicine Bow National Forest. Aerial survey results also showed the size of the infestation doubled in 2010 in the Black Hills of South Dakota and Wyoming. The epidemic has spread to 44,000 acres, up from 22,000 in 2009. Mitigation projects in the Laramie Ranger District of Medicine Bow include fuels reduction treatments, watershed protection treatments, hazardous tree removal and more, a Laramie district forester said. Source: <http://www.laramieboomerang.com/articles/2011/01/26/news/doc4d3fbdd0b26a5364197223.txt>

**(Minnesota) Man accused of arson for Ada, Minn., seniors’ center blaze appears in court.** Police said the man charged with arson in a fire January 22 at a seniors’ center in Ada, Minnesota, wore a jacket smelling like gasoline when arrested while leaving the burning building. The 31-year-old Ada man is accused of starting the fire at the activity center for seniors, which was damaged badly enough it has not reopened, the Ada police chief said. Court records filed January 24 allege the police found the suspect exiting the center holding a pair of coolers, wearing a jacket that smelled of fuel. He said the coolers had food in them, and that the suspect was also taking a television from the center. He made his first appearance in Norman County District Court on the arson charge January 25. Unconditional bail was set at \$250,000 cash. With conditions — including staying at least a block away from the senior center — bail was set at \$500,000 bond or \$50,000 cash. Court records said the blaze appeared to have started on a basement cabinet. An earlier fire the same morning at a residence 2 blocks away

## UNCLASSIFIED

from the senior center might be linked and is being investigated as a potential arson, the police chief said. Source: <http://www.inforum.com/event/article/id/306191/group/News/>

**(Wyoming) Yellowstone has bulged as magma pocket swells.** Yellowstone National Park's supervolcano in Wyoming just took a deep "breath," causing miles of ground to rise, scientists reported. The simmering volcano has produced major eruptions — each a thousand times more powerful than Mount St. Helens's 1980 eruption — three times in the past 2.1 million years. Yellowstone's caldera, which covers a 25- by 37-mile swath of Wyoming, is an ancient crater formed after the last big blast, some 640,000 years ago. Beginning in 2004, scientists saw the ground above the caldera rise upward at rates as high as 2.8 inches per year. The rate slowed between 2007 and 2010 to a centimeter per year or less. Still, since the start of the swelling, ground levels over the volcano have been raised by as much as 10 inches in places. Source: <http://news.nationalgeographic.com/news/2011/01/110119-yellowstone-park-supervolcano-eruption-magma-science/>

## NATIONAL

**Napolitano announces end of color coded terror alert system.** The U.S. Homeland Security Secretary announced January 27 a new targeted terror alert system that will replace the current structure which uses coded colors to represent varying threat levels. The new, two-tiered system will inform specific groups or sectors of threats and will have definitive end dates, she said during her inaugural State of the Homeland Security address. The Department of Homeland Security (DHS) will work with federal agencies to issue "formal, detailed alerts" about specific, credible threats, she said. The United States will begin its transition to the new system over a 90-day period beginning January 27. Source: <http://www.myfoxdc.com/dpp/news/napolitano-announces-end-of-color-coded-terror-alert-system-ncxdc-012811>

**(Ohio) FBI Hazmat teams called to Coventry Township home for suspected ricin.** Federal agents in special protective gear entered a Coventry Township, Ohio, home January 25 to remove a "hazardous substance." For most of the day, federal agents, Summit County sheriff's deputies, and firefighters from three area departments gathered outside of the home for the arrival of a special FBI hazardous materials teams from Pittsburgh, Pennsylvania, and Quantico, Virginia. Local law enforcement and the FBI personnel received a tip January 24 about the substance, which authorities would not identify on the record. "The substance told to us is hazardous to humans," an FBI spokesman said. "We're not going to speculate because we don't know what it is." A law enforcement official at the scene cited ricin as a possibility. The spokesman said the material inside of the home was only a small amount. Authorities sealed off the large brick house and property after receiving the tip around 4 p.m. The International Brotherhood of Electrical Workers facility next door was used as a staging area. A special FBI team dressed in hazmat gear and carrying a metal box entered the home around 3 p.m. By 3:41 p.m., the extraction was complete. The FBI dispatched a plane to fly the material to a special laboratory in Maryland for analysis. Source: [http://www.ohio.com/news/break\\_news/114580384.html](http://www.ohio.com/news/break_news/114580384.html)

**Cruise ships canceling Mazatlan stop, citing crime.** Some cruise ship companies are canceling stops in the Pacific port of Mazatlan, Mexico, and others are considering it due to crime against tourists.

UNCLASSIFIED

## UNCLASSIFIED

Disney Wonder has dropped calls to Mazatlan from its seven-night Mexican Riviera tour and replaced them with an additional stop in Cabo San Lucas on the Baja, California peninsula. "Safety is very important to us and we believe this change is necessary to provide the best family vacation experience for our guests," a spokeswoman said January 26. Mazatlan officials had touted Disney's decision in 2010 to resume stops at the port as a sign of growing confidence in the city. The Disney Wonder had planned 27 port calls in Mazatlan in 2011, according to the Mazatlan port authority Web site. Mazatlan has continued to thrive as a tourist destination despite drug-gang violence in other parts of Sinaloa state, where it is located. The state is the cradle of several Mexican cartels and has one of the highest homicide rates in the country. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5jiLSAb-AuT9vaLkUCnclNPKUT5AQ?docId=32c5f75c42d449d5b8b7e88170d75915>

**Experts say Moscow airport attack may cause security rethink worldwide.** The suicide attack on Moscow's Domodedovo airport may prompt a re-evaluation of how to protect airport terminals, but is unlikely to result in tougher security measures, pilots, and aviation security, experts said January 24. Analysts warned that the large crowds that gather at airports' public areas are an easy target for terrorists. But it is virtually impossible to screen them because many airports have been turned into commercial centers, with shops, food courts, train stations, and other facilities. "Like any crowded public space, be it a subway station or a shopping mall or a football stadium, an airport will always have inherent vulnerabilities," a commercial airline pilot and aviation author said. Most airports in the West do not restrict access to the terminals, which are considered public areas. Security screening only takes place once the passengers enter the departure areas. Analysts said the Domodedovo attack appeared to be the first time terrorists have tried to exploit unrestricted public access to the terminals since the failed bombing of an airport in Glasgow, Scotland, in 2007. Attackers there tried to crash a Jeep loaded with explosives through the entrance doors, but the bomb did not go off. Source:

<http://www.google.com/hostednews/canadianpress/article/ALeqM5jvipVBI6VcC0LMk82MceKloWQzFg?docId=5753423>

**(California) Pipeline explosion caused by bad welding.** An inferior weld caused a San Bruno, California, gas pipeline explosion that killed eight people and destroyed 38 homes in September 2010, officials said. The metallurgical report released January 22 by federal transportation safety officials identified for the first time a particular seam weld as the cause of the rupture in the September 9, 2010, explosion, the San Francisco Chronicle reported. The weld was just half as thick as it should have been, the report said. Experts said the flaw would have been exposed during high-pressure water testing inspections the utility, Pacific Gas & Electric, had ruled out as expensive and burdensome. The utility company's records, found by investigators to be wrong, indicated the pipeline carrying the gas was seamless. Instead, the San Bruno site was part of a cobbled assortment of potentially inferior 4-foot seamed pipes of possibly unknown origin. The January 22 report by the National Transportation Safety Board said the pipe developed a crack "consistent with ductile overstress from the root of the weld." Source:

[http://www.upi.com/Top\\_News/US/2011/01/22/Pipeline-explosion-caused-by-bad-welding/UPI-44931295723585/](http://www.upi.com/Top_News/US/2011/01/22/Pipeline-explosion-caused-by-bad-welding/UPI-44931295723585/)

UNCLASSIFIED

## UNCLASSIFIED

**(Ohio) Gas line pressure increase causes 9 house fires in Ohio village.** At least nine homes in the Ohio village of Fairport Harbor caught fire January 24 after an increase in gas line pressure, the mayor's office said. Authorities scrambled to shut off gas service amid reports of gas fumes in the air. A Lake County sheriff said that as of about 8:40 a.m., gas service had been shut off and all the fires were believed to be out. Police initially had said they would attempt to evacuate up to 3,000 people in the village. However, a police major called off the evacuation, saying it would be too chaotic to get residents out of the village through only three exits. Residents were asked to turn off their gas from the outside and remain in their homes, the statement said. Gas began flowing at a higher rate than normal because of a problem in the pressure line, and that caused the fires, the mayor's office said in a written statement. There were no immediate reports of injuries. All 17 of the county's fire departments were called out. The initial call came in about 7 a.m., the major said. Source: <http://www.cnn.com/2011/US/01/24/ohio.fire.evacuations/index.html?hpt=T2>

## INTERNATIONAL

**Kabul supermarket bomb kills 9, foreigners target.** A suicide attack on a supermarket in Kabul's upmarket embassy district on January 28 killed at least nine people, including three foreign women and a child, in the first major Taliban assault on civilians in the capital for nearly a year. Gunfire rattled through the area — home to the British, Canadian, Pakistani and other missions — at the start of the assault. The Taliban said they had carried out the attack. It was aimed at foreigners, but the primary target was the head of security firm Xe Services, formerly known as Blackwater, a spokesman told Reuters by telephone. Police said there were no security employees among the dead. Source: <http://ca.reuters.com/article/topNews/idCATRE70R1UJ20110128>

**Japan evacuates homes, cancels flights as volcano spews ash mile into sky.** Japan's government issued alerts after a volcano on the southern island of Kyushu erupted for the first time in 52 years, causing the evacuation of homes and cancellation of more than 60 flights. Shinmoedake, in the Kirishima range, erupted January 27, spewing ash as high as 8,200 feet into the air, Japan's Meteorological Agency said. A second eruption occurred January 28 at about 1 p.m. local time, national broadcaster NHK reported. Ash from the volcano reached Miyazaki city, 30 miles to the east, according to the broadcaster. Japan Airlines Corp. canceled 37 flights to or from nearby Miyazaki airport, according to its website January 28. Three additional flights will be scrapped January 29, it said. All Nippon Airways Co., Asia's largest listed carrier, canceled 24 flights affecting 3,350 people, spokeswoman said by phone January 28. Source: <http://www.bloomberg.com/news/2011-01-28/kyushu-volcano-spews-mile-high-ash-causing-evacuations-canceled-flights.html>

**Swiss police: blast at Davos hotel, no injuries.** A small blast shattered two windows but caused no injuries at a hotel used by top business and political leaders attending the World Economic Forum, Swiss police said January 27. The incident occurred on the day the French president, British deputy prime minister, and a former U.S. President were due to take the stage at the annual gathering in the Swiss Alpine town of Davos. Forum organizers said in a statement the explosion was caused by a firework. An anonymous posting on the Web site indymedia.ch claimed responsibility for the attack on the Posthotel Morosani, saying it was directed at Swiss government officials and senior executives of Swiss bank UBS staying at the hotel. Its authenticity could not immediately be confirmed. Swiss federal prosecutors office said in a statement that it is investigating the incident but provided no further information "for tactical reasons." The explosion happened in a hotel storage room shortly

UNCLASSIFIED

## UNCLASSIFIED

after 9 a.m., a regional police spokesman told the Associated Press. The anonymous claim of responsibility said “two pyrotechnical devices and sugar” were used to cause the blast. There was little disruption to the hotel and its activities beyond an increased security presence at the hotel’s entrance. There is tight security at the World Economic Forum as left-wing groups plan to hold a protest against the annual meeting of political and business leaders and social activists. Source: [http://news.yahoo.com/s/ap/eu\\_davos\\_forum\\_explosion;\\_ylt=Ap9KQdF6w.cZlpUK398wM3Cs0NUE;\\_ylu=X3oDMTNzM2doNGQyBGFzc2V0A2FwLzlwMTEwMTI3L2V1X2Rhdm9zX2ZvcnVtX2V4cGxvc2lvbgRiY29kZQNtb3N0cG9wdWxhcGRjcG9zAzQEcg9zAzEEcHQDaG9tZV92tIBHNIYwN5bl9oZWFKbGluZV9saXNOBHNs](http://news.yahoo.com/s/ap/eu_davos_forum_explosion;_ylt=Ap9KQdF6w.cZlpUK398wM3Cs0NUE;_ylu=X3oDMTNzM2doNGQyBGFzc2V0A2FwLzlwMTEwMTI3L2V1X2Rhdm9zX2ZvcnVtX2V4cGxvc2lvbgRiY29kZQNtb3N0cG9wdWxhcGRjcG9zAzQEcg9zAzEEcHQDaG9tZV92tIBHNIYwN5bl9oZWFKbGluZV9saXNOBHNs)

**Paris airport evacuated over suspected explosive.** The Roissy Charles De Gaulle Airport in Paris, France, was briefly evacuated January 24 after authorities received a report of suspected explosive, police said. A bomb disposal expert was called to a terminal where an unclaimed baggage was found and reckoned to be an explosive, a policeman told Xinhua. The operation lasted about 20 minutes before the police lifted the evacuation order. “He (the expert) made no declaration,” the policeman said, refusing to give further details. An unconfirmed earlier report said the explosive was successfully defused. Source: <http://www.sify.com/news/paris-airport-evacuated-over-suspected-explosive-news-international-lbzkudajhg.html>

**Explosion on Philippine bus kills 4, wounds 14.** A powerful blast from a suspected bomb ripped through a bus in the financial district of Manila, Philippines, January 25, tearing a huge hole in the vehicle and spraying shrapnel at the passengers. Four people were killed and 14 wounded. The force of the explosion, believed to have come from a remotely detonated mortar round, also punched fist-size holes in a concrete wall of a nearby upscale compound in Makati City, officials said. The Philippine president and other officials have not named any specific suspects but suggested they included al-Qaida-linked militants, who have been blamed in past attacks on passenger buses.

Source:

<http://www.google.com/hostednews/ap/article/ALeqM5iOX3m3niQ4t2q67nKCf4pVxzmVlg?docId=c9cd62db781b4827bebeb2dc10468bf3>

**Terror cells suspected in Canada.** A professor said most terrorist activity uncovered in Canada involves raising money there for operations overseas. The professor said in some cases, extremists will infiltrate legitimate charitable groups and skim money from them, then launder the cash through shady overseas banks in places like Cyprus or Russia. If there was one terrorist plying his trade in the city of Edmonton in Alberta, Canada, there are likely more where he came from, the local professor said. “Terrorist cells typically have four to seven people in them,” said the former Mountie who now teaches at Grant MacEwan University. The professor said the Canadian Security Intelligence Service suspects every major city in Canada likely has a couple of cells working for a variety of terrorist causes around the world. After the Royal Canadian Mounted Police arrested a suspect earlier the week of January 17 on suspicion of orchestrating deadly suicide bombings in Iraq in 2009, they were quick to say the accused posed no threat to anyone in Edmonton. Source:

<http://www.torontosun.com/news/canada/2011/01/22/16990841.html>

**One dead, 7 injured in Mexico explosions.** A police commander was killed, and seven others – four officers and three teenage boys – were injured in two separate explosions in different parts of Mexico, officials said January 22. The three boys were injured by a grenade hurled during a clash

UNCLASSIFIED

## UNCLASSIFIED

between army soldiers and suspected cartel hit men in the northern industrial city of Monterrey. The gun battle erupted when a military convoy came upon several SUVs carrying at least five armed men. The clash left one gunman dead and two soldiers wounded, officials said. The other four suspected cartel enforcers were wounded but managed to flee on foot. Separately, a car exploded January 22 in the central town of Tula. That state's public safety secretariat, which is still investigating the blast, said the police were alerted to the presence of an abandoned vehicle and that it exploded upon their arrival. A police commander died of injuries suffered in the blast at a hospital in Hidalgo's capital, Pachuca. Four other officers were wounded in the blast, but their injuries are not serious. Source: <http://www.laht.com/article.asp?ArticleId=384820&CategoryId=14091>

**Officials: 35 dead in Moscow bomb blast.** An explosion ripped through the arrivals hall at Domodedovo airport in Moscow, Russia, January 24, killing 35 people and wounding about 130, officials said. An analyst told NBC News the blast was "almost certainly" the work of Islamist militants from Russia's North Caucasus region. The state-run news agency RIA Novosti said preliminary reports suggest a bomb was detonated by a suicide bomber as people emerged from the international arrivals zone. The bomb was packed with metal objects to cause maximum damage, according to law enforcement authorities. Planes from London, Brussels, Greece, Ukraine and Egypt had landed in the 30 minutes before the attack, RIA Novosti reported. Russian investigators told the Associated Press that two British citizens were among the dead. The Russian Emergency Ministry said 51 people were hospitalized after the blast with 35 of those in serious condition, NBC News reported. International flights continued to arrive at Domodedovo after the blast at first, but were later diverted to Sheremetyevo airport, Interfax reported. Moscow police were checking the city's subway and other places where large numbers of people gather to try to avert possible follow-on attacks, the news agency said. Interfax also said security had been stepped up at Sheremetyevo and Vnukovo airports. Domodedovo is generally regarded as Moscow's most up-to-date airport, but its security procedures have been called into question. Source: [http://www.msnbc.msn.com/id/41231668/ns/world\\_news-europe/?gt1=43001](http://www.msnbc.msn.com/id/41231668/ns/world_news-europe/?gt1=43001)

## **BANKING AND FINANCE INDUSTRY**

**(Maryland) ATM skimmer investigated in Md.** A 48-year-old woman discovered what appeared to be an ATM skimmer while using an ATM at a Bank of America in Anne Arundel County, Maryland on January 22, police said. At approximately 5:26 p.m., officers responded to a call from to the Bank of America in the 600 block of Annapolis Boulevard in Severna Park, for a recovered ATM skimmer affixed to the ATM machine. The woman told police she observed what appeared to be a fraudulent device attached to the machine for the purpose of scanning the ATM cards of customers. She had pried the device from the machine before the suspect could return to retrieve the device and obtain customer data. This appeared to be an isolated incident and no personal account information has been compromised for individuals that used the ATM, police said. The case is being investigated by the United States Secret Service with the assistance of the Anne Arundel County Police Department. Source: <http://voices.washingtonpost.com/crime-scene/baltimore/atm-skimmer-investigated.html>

**Hedge funds unprepared for cyber attack.** With details trickling in about how the sophisticated Stuxnet computer worm derailed years of work on Iran's nuclear program, many seasoned observers are left to wonder what might happen if such a powerful weapon were ever turned against the nearly \$2 trillion hedge fund industry. On January 26, Alphaserve Technologies, IT advisor to many of the

UNCLASSIFIED

## UNCLASSIFIED

world's largest hedge funds, offered potential solutions to an industry it perceives as ill-prepared when compared to big banks and other financial institutions. Most hedge funds have protected themselves from external security breaches for years, but today's managers must protect themselves not only from the outside in, but rather from the inside out, contends the CEO and CTO of Alphaserve Technologies. The everyday, internal activities of employees accessing the Internet, e-mail, Skype, and other information provide ideal channels for worms, malicious software and dishonest employees to siphon off confidential information and do harm. New technologies like Digital Loss Prevention (DLP) software and deep packet inspection firewalls can look inside the Internet channel for any corporate data leaving the company and stop intentional or unintentional illicit transfers of information. Surprisingly though, many marquee names in the hedge fund industry do not have this essential protection even though some are in the process of adopting it, the CEO said. Source:

<http://www.net-security.org/secworld.php?id=10491>

**Numerous phishing emails with HTML attachments in circulation.** Security researchers from Websense warn of several new phishing campaigns that instruct recipients to open rogue HTML files attached to the fake e-mails. Some of them are taking advantage of the U.K. and U.S. tax seasons and spoof the taxation authorities in those countries. A wave of e-mails purporting to come from the HM Revenue & Customs masquerade as tax refund alerts. The e-mails are similar to the common tax return phishing scams, but instead of directing recipients to a malicious page, they instruct them to open the attached HTML form. A separate tax refund phishing campaign spoofs the IRS and tells recipients they are eligible to receive stimulus payments. These fake IRS e-mails also carry a form and instruct people to open it in a JavaScript-enabled browser. Other recent phishing attacks target the customers of several banks and have rogue HTML documents attached to them. Source:

<http://news.softpedia.com/news/Flurry-of-Form-Based-Phishing-Emails-in-Circulation-180322.shtml>

**Govt may soon force banks to impose new online authentication steps.** The Federal Financial Institutions Examination Council (FFIEC) could soon release new guidelines for banks to use when authenticating users to online banking transactions. The new guidelines will clarify the FFIEC's existing guidelines on the subject and more explicitly inform banks about what they need to do to bolster online authentication, an analyst at Gartner said. The analyst recently met with the FFIEC's IT subcommittee to discuss the updates. The FFIEC is an interagency council that develops standards for the federal auditing of financial institutions by bodies such as the Federal Reserve System and the Federal Deposit Insurance Corp. (FDIC). In 2005, it issued a set of guidelines, titled "Authentication in an Internet Banking Environment." They called on banks to upgrade their single-factor authentication processes — typically based on user name and passwords — with a stronger, second form of authentication by the end of 2006. The guidance left it largely up to the banks to choose whatever second form of authentication that they felt was the most appropriate for their needs. The FFIEC listed several available authentication technologies that banks could choose from, including biometrics, one-time passwords and token-based authentication. Source:

[http://www.pcworld.com/article/217637/govt\\_may\\_soon\\_force\\_banks\\_to\\_impose\\_new\\_online\\_authentication\\_steps.html](http://www.pcworld.com/article/217637/govt_may_soon_force_banks_to_impose_new_online_authentication_steps.html)

**4 banks closed on Jan. 21.** United Western Bank, Denver, Colorado, was the largest of four institutions closed by federal and state regulators January 21. The \$2.05 billion bank was acquired by First-Citizens Bank & Trust Company, Raleigh, North Carolina, which assumes all deposits of United Western. The eight branches of United Western will reopen January 24 as branches of First-Citizens.

## UNCLASSIFIED

## UNCLASSIFIED

These latest announcements of failed institutions raise the total to 7 so far in 2011. The latest failures: The Bank of Asheville, Asheville, North Carolina, was closed by the North Carolina Office of Commissioner of Banks, which appointed the Federal Deposit Insurance Corporation (FDIC) as receiver. FDIC entered into an agreement with First Bank, Troy, North Carolina, to have it assume all deposits. The five branches of the Bank of Asheville will reopen as branches of First Bank. FDIC estimates the cost to the Depositors Insurance Fund (DIF) will be \$56.2 million. The CommunitySouth Bank and Trust, Easley, South Carolina was closed by the South Carolina State Board of Financial Institutions, which appointed FDIC as receiver. FDIC entered into an agreement with CertusBank, National Association, Easley, South Carolina to have it assume all deposits. The six branches of CommunitySouth will reopen as branches of CertusBank. FDIC estimates the cost to the DIF will be \$46.3 million. The Enterprise Banking Company, McDonough, Georgia was closed by the Georgia Department of Banking and Finance, which appointed FDIC as receiver. FDIC created the Deposit Insurance National Bank of McDonough to protect depositors. The new institution will remain open until January 28 to allow depositors access to their insured deposits and time to open accounts at other insured institutions. Source: [http://www.bankinfosecurity.com/articles.php?art\\_id=3289](http://www.bankinfosecurity.com/articles.php?art_id=3289)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**NRC to adopt safety culture policy.** The Nuclear Regulatory Commission (NRC) is considering adopting a policy on safety culture designed to minimize human error and managerial problems at reactors. The NRC chairman said the federal agency's draft, 3 years in the making, irons out key issues. It is not, however, an enforceable regulation, but rather a guide to "expectations" about how reactor employees should conduct themselves to enhance safety and security, he said. The draft is available at [http://www\(dot\)nrc.gov/reading-rm/doc-collections/commission/secys/2011/2011-0005scy.pdf](http://www(dot)nrc.gov/reading-rm/doc-collections/commission/secys/2011/2011-0005scy.pdf). The proposed policy defines safety culture as "the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and the environment." Source: <http://www.theday.com/article/20110126/BIZ02/301269926/1044>

**(Washington) Nuclear cleanup plant questioned.** A costly U.S. environmental project, meant to deal with millions of gallons of nuclear waste, is over budget and faces technical and safety issues, critics said. The Department of Energy (DOE) is building a facility at the Hanford, Washington, nuclear reservation to clean up 53 million gallons of radioactive waste left over from 40 years of nuclear weapons production currently stored in aging, leaking tanks, but cost estimates have nearly tripled to \$12.2 billion and its builders have yet to settle some vexing problems with design, the Seattle Times reported January 23. Some critics said they worry the final plant may be dangerous and will not be able to treat as much waste as expected, could pose environmental dangers, and might take billions of more dollars to get right. The plant is being built even though details of the final design have yet to be worked out, they said. The government's own tests show equipment might fail or pipes might clog in parts of the facility so radioactive with nuclear waste no human or machine could ever get in and make repairs. The plant is scheduled to begin operating in 2019, a decade behind schedule. Source: [http://www.upi.com/Science\\_News/2011/01/23/Nuclear-cleanup-plant-questioned/UPI-52391295813251/](http://www.upi.com/Science_News/2011/01/23/Nuclear-cleanup-plant-questioned/UPI-52391295813251/)

UNCLASSIFIED

## **COMMERCIAL FACILITIES**

**(Washington) Fourth suspicious package found in Spokane within a week is harmless.** Police investigating a suspicious package left at a Spokane, Washington, gas station determined it was harmless. Officers blocked off part of Highway 2 January 23 while they investigated the backpack left at a Chevron station near Holland. The highway was shut down for about an hour while crews set up a command center nearby. After careful inspection, police said there was nothing dangerous in the backpack. The backpack was the fourth suspicious package reported in Spokane within the last week. On January 21, a suspicious device was reported near Sprague and Washington. It turned out to be a false alarm. Authorities said it was a tall metal coffee mug. A suitcase was spotted January 19 in downtown Spokane. It was full of women's clothing. But January 17, a backpack with wires poking out of it was found along the Martin Luther King Jr. parade route. That bag did in fact contain a bomb. The FBI is investigating that device. Source:

<http://www.nwcn.com/home/?fId=114470734&fPath=/news/local&fDomain=10222>

**(Washington) 2 injured, 2 dead in Walmart shooting.** Two people died and two Kitsap County sheriff's deputies were wounded January 23 after a shootout in a Walmart parking lot in Port Orchard, Washington. A third deputy shot and killed the man who unexpectedly opened fire on the deputies, a sheriff's spokesman said. Witnesses said a woman apparently tried to run to the man's aid – and directly into the line of fire – and was struck. It is unclear whether the deputies or the gunman shot the woman. She died at Tacoma General Hospital. The wounded deputies were shot in the torso and listed in stable condition. Deputies were called about 3:40 p.m. to the Walmart at 3497 Bethel Road S.E. after someone reported a suspicious man. Two deputies approached the man, who was standing outside the store, and began talking to him. Witnesses said the man was walking with them to their patrol car and was about to be put in handcuffs when he broke free and began sprinting across the parking lot toward the woods. A witness said the man did not turn around when he fired several rounds, striking both deputies. A third deputy coming around the south side of the building fired at the fleeing gunman after seeing her colleagues were down, the spokesman said. Witnesses said dozens of people ran into the store seeking cover. Walmart employees immediately placed the store on lockdown. Walmart reopened its doors shortly after 7:30 p.m. Source:

<http://www.thenewstribune.com/2011/01/24/1514865/2-injured-2-dead-in-walmart-shooting.html>

**(Michigan) Details on Kroger store evacuation after shopper said he had a bomb and demanded Vicodin.** A shopper at the Kroger supermarket in Independence Township, Michigan, demanded the prescription painkiller Vicodin and told a clerk he had a bomb January 20. The Oakland County Sheriff's Office released images January 21 of the man taken from store security video. The images show the man pushing a shopping cart. Investigators said the man dropped a package, which was made to look like a bomb on the pharmacy counter. It had wires, spark plugs, and duct tape. A clerk threw a bottle of Vicodin at the man and he left. The store was then evacuated. The bomb squad determined the package was not a bomb. Businesses in the same busy shopping center were not evacuated. Source: [http://www.wxyz.com/dpp/news/region/oakland\\_county/details-on-kroger-store-evacuation-after-shopper-said-he-had-a-bomb-and-demanded-vicodin](http://www.wxyz.com/dpp/news/region/oakland_county/details-on-kroger-store-evacuation-after-shopper-said-he-had-a-bomb-and-demanded-vicodin)

## **COMMUNICATIONS SECTOR**

**Comcast to broadcast info on missing children.** Starting January 27, a missing child's story and photo will be available to nearly 20 million Comcast cable customers in more than 25 cities in partnership with the National Center for Missing & Exploited Children. "Somebody knows where this child is," says center President. "If we reach that one person, we increase the likelihood that we'll get that one lead that will bring the child home." The public service campaign comes a day before Comcast closes its deal with General Electric for 51 percent of a joint venture that includes NBC Universal. The deal makes Comcast the nation's most powerful media, entertainment and news company. Comcast created the missing kids videos after having some success with its Police Blotter program, which features fugitives. Police credit the crime videos with generating tips that led to 90 arrests, said vice president of entertainment services for Philadelphia-based Comcast. Twenty, 2-minute video profiles are available. The videos include the child's name, description, photo, possible whereabouts, and a narrative of the disappearance. Each month, the missing children's center and Comcast will rotate new videos into the lineup. Each video will be available for at least 12 weeks. Source:

[http://www.usatoday.com/news/nation/2011-01-27-missingkids27\\_ST\\_N.htm](http://www.usatoday.com/news/nation/2011-01-27-missingkids27_ST_N.htm)

**Half of federal Web sites fail DNS security test.** Half of U.S. government Web sites are vulnerable to commonplace denial of service (DNS) attacks because they have not deployed a new authentication mechanism that was mandated in 2008, a new study shows. The Office of Management and Budget issued a mandate requiring federal agencies to deploy an extra layer of security — called DNS Security Extensions (DNSSEC) — on their .gov Web sites by December 31, 2009. However, an independent study conducted in January 2010 shows that 51 percent of agencies are out of compliance with the requirement to deploy DNSSEC, which is also necessary for high marks in agency report cards under the Federal Information Security Management Act. Source:

<http://www.networkworld.com/news/2011/012711-dns-security-test.html>

**Verizon struggles with BlackBerry data traffic.** Some Verizon Wireless customers using BlackBerrys have been limited to making voice calls on Research In Motion's (RIM) smartphone for as long as a week, but Verizon said January 26 the issue was fully resolved. Contributors to a BlackBerry support forum said they had trouble connecting to the Internet, using Internet-based apps and had delayed e-mail delivery since January 25. RIM routes BlackBerry data traffic through its own servers via a carrier's network, a method not replicated by other smartphones. The company said its service has been operating normally. "There is no outage, and there hasn't been one," a Verizon Wireless spokesman said. "Our engineers discovered that a small number of customers in a limited geographic area had technical glitches that resulted in their e-mail being delayed up to an hour," he said. The Verizon glitch was fully resolved January 25, he said, declining to provide further technical details or say how many customers were affected or where they were located. Source:

<http://www.reuters.com/article/idUSTRE70P9N120110126>

**Smartphones get more airwaves.** The Federal Communications Commission (FCC) approved a request January 26 to allow a satellite broadband start-up funded by investment firm Harbinger Capital Partners to lease its airwaves for traditional mobile phones. The agency approved a request by LightSquared to drop a requirement that airwaves set aside for satellite-phone use aren't primarily

## UNCLASSIFIED

used instead for ground-based phone networks. The FCC's action means LightSquared can lease its airwaves to companies that offer normal smartphones such as the iPhone, and not pricier satellite-enabled phones. Source:

<http://online.wsj.com/article/SB10001424052748703293204576106293753233196.html>

### **CRITICAL MANUFACTURING**

**Parts shortage idles Chrysler plant.** A parts shortage will halt production at Chrysler Canada's minivan plant in Windsor, Canada, for a week. A Chrysler spokesperson said January 27 that the company will halt operations beginning January 31, but anticipates production will resume February 7. The spokesperson said the shortage involves "an external supplier" but would not identify the source or the parts. One report indicated that the shortage originated in China. Chrysler would not estimate how much the stoppage means in lost vehicle production but said the company would make it up over time. Source: <http://www.thestar.com/business/auto/article/929586--parts-shortage-idles-chrysler-plant>

**Ford recalls more than 400,000 minivans.** Ford Motor Co. recalled more than 400,000 Windstar minivans in cold-weather states January 26 to fix brackets and mounts that could separate from the vehicle's subframe and cause a driver to lose control. The recall, the latest quality issue to afflict older Windstars, covered 425,288 minivans from the 1999-2003 model years sold or registered in 22 states and the District of Columbia. Ford said there had been seven crashes and five minor injuries connected to the recall. Source: <http://www.msnbc.msn.com/id/41290763/ns/business-autos/>

**Toyota recalls 1.7 million vehicles for fuel leaks.** Toyota recalled nearly 1.7 million cars worldwide January 26 for fuel leaks. The recalls are mostly in Japan, but they also include the IS and GS Lexus luxury models in North America. There were no accidents suspected of being related to the latest recall, according to Toyota. Source: <http://www.foxnews.com/world/2011/01/26/toyota-recalls-nearly-million-vehicles-1956580065/>

### **DEFENSE/ INDUSTRY BASE SECTOR**

**(Utah) Missing vial of nerve agent triggers Dugway shutdown.** An overnight lockdown, triggered when a vial of the deadly VX nerve agent went temporarily missing, was lifted January 27 at Utah's sprawling, 801,000-acre Dugway Proving Ground. Officials at the remote Army installation, 90 miles southwest of Salt Lake City, ordered gates closed at 5:24 p.m. January 26. Up to 1,500 employees of Dugway — military personnel, contractors and civilian workers — were forced to stay the night. A Dugway spokeswoman said the lockdown was ordered after a "routine inventory of sensitive material in the chemical laboratory ... discovered a discrepancy between the records and the agent on-hand. As a precaution, the commander immediately locked down the installation and began efforts to identify the cause of the discrepancy." The vial was located, uncompromised, at 3 a.m. January 27 within the facility. Dugway officials did not specify exactly where the vial, containing less than 1 milliliter, or roughly a quarter-teaspoon of the agent, was found — nor did they detail how the vial had gone missing in the first place, or whether anyone was being disciplined as a result of the incident. Dugway houses small amounts of various chemical and biological warfare agents for defense testing purposes; it also is a prime Army base for testing of an array of conventional military

UNCLASSIFIED

## UNCLASSIFIED

weaponry and ammunition. Source: <http://www.sltrib.com/sltrib/home/51134945-76/dugway-vial-agent-thursday.html.csp>

**China's new stealth fighter may use US technology.** Chinese officials recently unveiled a new, high-tech stealth fighter that could pose a significant threat to American air superiority — and some of its technology may well have come from the U.S. itself. Balkan military officials and other experts told the Associated Press that in all probability the Chinese gleaned some of their technological know-how from an American F-117 Nighthawk shot down over Serbia in 1999. “At the time, our intelligence reports told of Chinese agents crisscrossing the region where the F-117 disintegrated, buying up parts of the plane from local farmers,” said a man who was Croatia’s military chief of staff during the Kosovo war. “We believe the Chinese used those materials to gain an insight into secret stealth technologies ... and to reverse-engineer them,” he said. A senior Serbian military official confirmed pieces of the wreckage were removed by souvenir collectors, and that some ended up “in the hands of foreign military attaches.” Source:

<http://www.google.com/hostednews/ap/article/ALeqM5iE3jMTTaEhm5I8l63W9OzWiji0-Q?docId=e8f4fe6f3cc042d8af123a99e96b2a96>

**Sentencing due in China military secrets case.** A former B-2 stealth bomber engineer convicted of selling military secrets to China is due to be sentenced in federal court in Honolulu, Hawaii, January 24. The man faces up to life in prison for his conviction on 14 counts, including conspiracy, communicating national defense information to aid a foreign nation, and violating the arms export control act. He has been in custody without bail since his 2005 arrest. Prosecutors said the engineer helped China design a stealth cruise missile, and demonstrated how its design would be effective against U.S. air-to-air missiles. They said he was paid at least \$110,000 from the sale of military secrets. Source: <http://www.militarytimes.com/news/2011/01/ap-china-military-secrets-case-sentencing-012311/>

## **EMERGENCY SERVICES**

**Formidable Footprint exercise series an opportunity to assess neighborhood preparedness.** A series of virtual tabletop exercises between January and June will test the capacity of neighborhood groups to prepare for, respond to, and recover from a natural disaster. A January 29 earthquake exercise will address the response to an earthquake. Disasters to be taken up in succeeding months are floods, wildfires, tornadoes, a flu pandemic, and a hurricane scenario. The Web-based Formidable Footprint exercises ask participants to answer a series of questions about their capacity to respond to a variety of situations they may be faced with following a disaster. The exercises also prompt the teams to consider what information they should report to their local emergency management officials, how to do that, and what to do in other instances, such as if a member is injured. At the end of the exercise, each of the teams completes a Web-based review and receives a copy of its responses to the prompts. The questions lead teams to develop incident action plans (IAP) even though the exercise is written in plain language. There is no cost to community groups to participate in the exercises, but registration is required so participants may receive exercise materials beforehand. So far groups representing sectors from across the economy in 38 states have registered to take part in the upcoming exercise series, according to the Formidable Footprint Web site. Source:

<http://www.emergencymgmt.com/training/Formidable-Footprint-Exercise-Series.html>

UNCLASSIFIED

## UNCLASSIFIED

**Justice Dept settles over faulty Zylon body armor.** A Justice Department (DOJ) investigation into the use of defective Zylon fiber in bulletproof vests has led to a settlement with a Japanese importer. The body armor company now will cooperate in the probe of the material's manufacturer, Toyobo Co. Ltd. of Japan. The United States will collect \$1.5 million from N.I Teijin Shoji Co. Ltd and an American subsidiary. DOJ said the two Teijin companies were aware the Zylon fiber would degrade quickly, rendering bulletproof vests unfit for use. The government has sued Toyobo and several vest manufacturers, and has settled previously with eight other body armor companies for more than \$59 million. DOJ's civil division chief said providers of defective material in the vests have jeopardized the lives of law enforcement officers. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2011/01/25/AR2011012505216.html>

**(Michigan) Four Detroit police injured in department shootout.** Four police officers were slightly wounded and their assailant killed January 23, after a man walked into the 6th police precinct in Detroit, Michigan, and "began shooting indiscriminately," a spokeswoman for the mayor said. She said the incident began about 4:30 p.m. when the man opened fire with a pistol-grip shotgun. The man was able to shoot four officers before one or more officers returned fire, killing him. The most seriously injured police officer was the precinct's commander, who was hit in the lower back, she said. He underwent surgery at Sinai Grace Hospital January 23. "His condition is critical, but he is expected to pull through," the spokeswoman said. Two other male officers were hospitalized but expected to be released January 24. A female officer was hit in the chest, but the bulletproof vest she was wearing prevented her from being injured. Police said it was unclear whether the gunman had previous contact with the precinct or was targeting any specific officers. The police station is one of the department's eight district offices. Members of the public who enter the station do not pass through metal detectors or otherwise undergo a security screening. Source: <http://www.nytimes.com/2011/01/24/us/24detroit.html?src=twrhp>

## **ENERGY**

**(Oklahoma) Two men injured in Pawhuska from explosive device.** Three men were injured January 27 when some sort of explosive device went off outside of the National Oilwell Service Co., about a mile southeast of downtown Pawhuska, Oklahoma, according to the Osage County Sheriff's Office. The undersheriff said investigators were still at the scene, trying to determine if the explosion was caused by a pipe bomb or some other type of device. She said the explosion injured three of the company's workers, and they were taken to the local hospital for treatment. The undersheriff said their injuries did not appear life-threatening. The explosion also started a grass fire, "and that's how we first learned about it," she said. Source: [http://www.tulsaworld.com/news/article.aspx?subjectid=12&articleid=20110127\\_12\\_0\\_PAWHUS195969](http://www.tulsaworld.com/news/article.aspx?subjectid=12&articleid=20110127_12_0_PAWHUS195969)

**(California) PG&E can't find crucial pipeline pressure records.** Pacific Gas and Electric Co.'s (PG&E) president told a Bay Area congresswoman that the utility company cannot find records that support pressure levels on nearly a third of its natural-gas transmission system in populated areas, the congresswoman said January 27. The Representative said the utility president reported that PG&E has been unable to produce key manufacturing and installation documents for 30 percent of its pipelines in and around urban areas in Northern and Central California. The revelation that PG&E had

UNCLASSIFIED

## UNCLASSIFIED

erroneous documents about the pipeline that exploded in San Bruno on September 9, killing eight people, prompted the California Public Utilities Commission to order the state's utilities to produce reliable records for their gas transmission lines by March 15. If no reliable records can be found, utilities face the prospect of having to shut down a pipeline for days and run expensive tests that use high-pressure water to detect weaknesses. Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/01/28/MN6M1HFE6G.DTL>

### **FOOD AND AGRICULTURE**

**USDA fully deregulates roundup ready alfalfa.** The U.S. Agriculture Secretary said January 27 that USDA will allow genetically engineered (GE) Roundup Ready alfalfa to be planted without restriction. The announcement bucked expectations that the department's Animal and Plant Health Inspection Service (APHIS) would likely introduce a partial deregulation of the crop, which is engineered to withstand Monsanto's Roundup herbicide. Partial deregulation would have imposed geographic restrictions on planting in an effort to prevent GE contamination of non-GE and organic alfalfa. The Agriculture Secretary's recent statements about "coexistence and cooperation" between GE and non-GE agriculture led many to believe partial deregulation of the crop was in the pipeline. Source: <http://www.foodsafetynews.com/2011/01/usda-fully-deregulates-ge-roundup-ready-alfalfa/>

**(Rhode Island; Massachusetts) Recall news.** Salad mixes produced by State Garden of Chelsea, Massachusetts, were recalled because of Listeria concerns. The recall involves all salad products produced in the company's plant January 4 which correspond to trace back codes 45693 and 45703. No Listeria illnesses have been linked to the products. Health officials in Rhode Island notified the company that a sample of Northeast Spring Mix Salad at a retail store in the state tested positive for Listeria. Source: <http://www.myfoxa.com/Global/story.asp?S=13911462>

**Recalls: slimming capsules, gluten-free products.** The following recalls have been announced: An undisclosed number of Celerite Slimming Capsules from Shaping Beauty Inc. of Southampton, Pennsylvania, because the weight loss dietary supplement contains an undeclared drug ingredient, Sibutramine, used as an appetite suppressant for weight loss. The Food and Drug Administration said the product poses a threat to consumers because Sibutramine is known to substantially increase blood pressure, pulse rate or both in some patients and may present a significant risk for patients with a history of coronary artery disease, congestive heart failure, arrhythmias, or stroke. The product was sold nationwide via the Internet. Another recall involves 492 8-ounce boxes of Ian's Natural Foods wheat free, gluten free mac and no cheese and wheat free, gluten free French bread pizza because they may be contaminated with Listeria monocytogenes. Source: <http://www.kivity.com/Global/story.asp?S=13900844>

**More evidence of non-O157 STEC in ground beef.** Tests conducted on commercial ground beef identified disease-causing E. coli that could be considered significant food safety threats, according to the authors of a new study. Results of these latest tests support earlier studies that have shown the presence of non-O157 Shiga toxin-producing E. coli (STEC) in the retail meat supply, particularly in ground beef. According to estimates by the Centers for Disease Control and Prevention, these non-O157 STEC cause more than 160,000 illnesses each year. Only E. coli O157:H7 has been classified as an adulterant in U.S. beef, but these non-O157 STEC also can harm human health and have become an increasing concern, the study noted. "The data clearly show that clinical and public health

UNCLASSIFIED

## UNCLASSIFIED

laboratories should routinely screen human and environmental specimens for the presence of non-O157," the scientists conclude. Currently most labs do not. The study, by researchers from the U.S. Department of Agriculture's Agriculture Research Service and the College of Food and Agriculture at King Saud University, was published January 21 in the American Society for Microbiology's Applied and Environmental Microbiology journal. Source:

<http://www.foodsafetynews.com/2011/01/another-study-shows-stec-contamination-of-beef/>

**(Maryland) Researchers find virus plaguing soft-crab businesses.** Scientists with the University of Maryland's Institute of Marine and Environmental Technology and a worker in the crab business have found a virus in Chesapeake Bay blue crabs that they believe routinely kills a quarter or more of all soft crabs produced baywide before the premium seafood can get to market. They hope the discovery will lead to a way to spot and screen out infected animals, making soft-crab businesses more profitable while easing harvest pressure on the bay's iconic crustacean. Published in the December issue of the journal Diseases of Aquatic Organisms, the findings go a long way toward explaining the significant die-off seen in soft-crab shedding operations, a research assistant professor with UM's Center for Environmental Science at the Inner Harbor institute said. The researcher said the virus appears to affect only blue crabs, and there is no evidence it poses any hazard to humans. In any case, he pointed out, pathogens would be eliminated when the crabs are cooked. Until now, most watermen had written off the crabs' demise to poor water quality or the stress and injuries they get in being caught, handled, and kept in captivity. Source:

<http://www.baltimoresun.com/features/green/bs-gr-soft-crab-virus-20110124,0,4994579.story>

**(Oregon) Australian apple moth found in Oregon.** Oregon Department of Agriculture officials said a light brown apple moth has been trapped at a Polk County nursery, the first time it has been found in the state. The Salem Statesman Journal said the bug is a native of Australia that can harm orchards, trees, and ornamental plants. The department said it likely came to Oregon on imported nursery stock. The moth has the potential to be a highly destructive pest. A spokesman from the Oregon Agriculture Department said there is no indication a breeding population of the moth is in the state. The state will put out more traps in Polk County in February. Source:

<http://www.mycentraloregon.com/news/state/ap/523242/Australian-apple-moth-found-in-Oregon.html>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**(Missouri) Facebook bomb threat gets student suspended.** A comment posted on a Facebook account January 23 by a special education student at West Platte High School in Weston, Missouri, led to an out-of-school suspension. Weston police said the principal called them January 24 to report the comment a freshman had posted. Police would not quote the comment, but said the report characterized it as a bomb threat. The Weston School Board president said the district needs to treat seriously anything construed as a potential threat. The editor of the Platte County Citizen said the superintendent acknowledged the child was a special-education student who was suspended for 5 days after posting that he intended to blow himself up. Source:

<http://www.kctv5.com/news/26629095/detail.html>

UNCLASSIFIED

## UNCLASSIFIED

**(Michigan) Shots fired outside Detroit school.** Police in Detroit, Michigan, were searching January 26 for the person who fired shots outside Westside Christian Academy. Police said a young man went into the school on Bramell Street looking for a student, with whom he has a child, but was turned away when the school said the student was absent. Police said the man, who is not a student, then went outside of the school and fired several shots into the air. The school was put on lockdown as a precaution, but parents were allowed to pick up their children. Police said they know the identity of the shooter and are trying to locate him. Source:

<http://www.clickondetroit.com/news/26624424/detail.html>

**(Texas) Sen. John Cornyn's Dallas office evacuated for suspicious packages.** At least one of a Republican Senator's Dallas, Texas-area offices was evacuated January 26, his staff confirmed to CBSNews.com, after two suspicious packages arrived in the mail. Bomb squad technicians detonated the two devices. An FBI official in Dallas told CBS News the Dallas Police Department "disrupted" the package, but there were no explosives, nor was there any threat. The Senator's office said his staff has been given the all-clear. Source: [http://www.cbsnews.com/8301-503544\\_162-20029695-503544.html](http://www.cbsnews.com/8301-503544_162-20029695-503544.html)

**(Massachusetts) Brockton District Court evacuated after second bomb scare in a week.** A bomb threat phoned into Brockton District Court in Brockton, Massachusetts January 25 forced the second evacuation of the building in a week as police cordoned off surrounding streets downtown. Firefighters responded to the courthouse after receiving a 911 call at 2:50 p.m. from a courthouse employee, a deputy fire chief said. An unknown number of courthouse employees, and nine prisoners awaiting court hearings, were evacuated from the building at 215 Main St. about 3 p.m. Authorities called the state police bomb squad unit, which responded to the courthouse with a bomb-sniffing K-9 unit, and no suspicious packages or devices were found. Police cordoned off portions of streets around the courthouse. The nine prisoners were transported to a corrections facility. Source:

<http://www.enterpriseneews.com/news/x362546211/Brockton-District-Court-evacuated-after-second-bomb-scare-in-a-week>

**(Indiana) Congressman's staff threatened.** A 46-year-old Granger, Indiana man has been arrested and accused of threatening the staff of a U.S. Representative. A man allegedly called the Representative's South Bend office January 24 and claimed the staff was "backstabbing him." He told an employee, "I am going to come and backstab you, I mean literally come down and stab you," according to a criminal complaint filed in the Northern Indiana District of U.S. District Court. The employee who answered the phone is familiar with the caller because of frequent calls to the Representative's office, according to the complaint. The employee hung up on the caller and claims he made three more calls but did not make further threats. The man was arrested without incident at his residence in St. Joseph County January 24. The FBI and the St. Joseph County Sheriff's Department arrested the man, and he is being held in the county jail in South Bend pending a detention hearing January 28. He is accused of assault on a person engaged in official duties and two counts of assault on an internationally protected person. Source:

<http://www.journalgazette.net/article/20110126/LOCAL08/301269943/1044/LOCAL08>

**(California) County studies evacuation routes.** San Diego County, California is spending \$250,000 to study how easily some East County residents can evacuate in the event of an emergency. The study

UNCLASSIFIED

## UNCLASSIFIED

will focus on Valley Center where there are just a few roads offering 18,000 residents a way out in a hurry, according to the North County Times. The paper reported a local company, Fehr & Peers, has been hired to complete the study. The transportation consultants have identified 14 corridors across Valley Center where new roads would help residents get out of the area in the event of a fast-moving brush fire or other emergency. The next step is for the consultants to report on how difficult it would be to acquire land and build a new road in each of the 14 corridors, according to the paper. That portion of the study is expected by March. Source: <http://www.nbcsandiego.com/news/local-beat/County-Studies-Evacuation-Routes-114494424.html>

**(Pennsylvania) Police arrest student for online threats, false reports.** A 16-year-old Clearview Regional High School student in New Jersey was arrested January 23 for allegedly making online threats and falsely reporting incidents to police. Investigators said the teen, who lives in Harrison Township, New Jersey, first created a fake facebook page for himself on October 8. The student allegedly claimed that he was a new Clearview student while making physical threats toward other students and teachers in the school. Investigators said he encouraged others to make racially abusive remarks online toward different individuals. The Harrison Township Police Department first became aware of the fake account October 18. They contacted the Gloucester County Prosecutor's Office High-Tech Crimes Unit for assistance. The Mantua Township Police Department also investigated separate incidents involving the same student. Police said he made three calls to Gloucester County's 911 center using Voice Over Internet Protocol while concealing his identity. The calls all required a police response while one falsely reported a shooting at the Telford Inn in Mantua Township. Authorities said the student made the false report October 16 and that it required a response from five municipal police departments. The FBI assisted in the investigation of the student, which took more than 3 months. The teen is charged with bias intimidation, two counts of causing false public alarms, two counts of harassment, disorderly conduct, and conspiracy. Source: <http://www.nbcphiladelphia.com/news/local-beat/Police-Arrest-Student-for-Online-Threats-False-Reports--114512764.html>

**(Texas) Multiple bomb threats prompt evacuation of middle school in La Feria.** Police in La Feria, Texas, are tracing the origin of multiple bomb threats phoned into W.B. Green Middle School January 21. Police responded to the campus shortly after the calls came in around 2:30 p.m., the police chief said. Police officers worked with school employees to secure the students before conducting a room-by-room search for any evidence of explosives. None were found. Investigators are working with the phone company to see where the calls were made from. Students were picked up from a field next to the school. Source: <http://www.valleycentral.com/news/story.aspx?id=570790>

**Hacker selling access to government, military and education sites.** The security firm Imperva has uncovered a hacker selling access to U.S. government, military, and education Web sites on the cheap. "The victims' vulnerabilities were probably obtained by SQL injection vulnerability automatic scanner and exploited in automatic manner, as the hacker published his methods in a post in some hacker forum," the company explained. The unknown hacker is offering access to U.S. and European government, military, and education sites for anything between \$55 to \$499. Access to the U.S. Army and National Guard Web sites is up for sale for around \$499 each, while those belonging to the U.S. Department of Defense are accessible for \$399 per site. The hacker is also offering whole databases of personal user data, complete with names, telephone numbers, and addresses, for as low as \$20

## UNCLASSIFIED

## UNCLASSIFIED

per 1,000 names. Other services include a \$2 full Web site vulnerabilities scan, hacking of a “normal” Web site for \$10, hacking of a “high-profile” site for \$10+ and 3MB of information taken from random hacked user accounts for \$65. Source: <http://www.itproportal.com/2011/01/24/hacker-selling-access-government-military-and-education-sites/>

**(Illinois) Threatening letter sent to driver’s license office.** Police are investigating a threatening letter sent to employees at an Illinois Secretary of State’s driver’s license office. The unsigned letter was sent January 10 to the Chicago Heights Secretary of State’s Office. Investigators said the writer threatened to do harm to those who work at the facility, but did not single anyone out by name. Source: <http://abclocal.go.com/wls/story?section=news/local&id=7914540>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**UK.gov braces for Anonymous hacklash.** U.K. government websites have been warned to brace themselves for website attacks in the wake of the arrest of five Britons as part of an investigation into Anonymous the week of January 23. Members of the Anonymous hacking collective condemned the arrests, arguing that denial of services attacks are a legitimate protest tactic, comparable with staging a sit-in or picketing. In a statement, the group criticized the police operation as disproportionate, describing it as “a serious declaration of war from yourself, the U.K. government, to us, Anonymous, the people.” Information security agency GovCertUK has taken this implied threat seriously, issuing an advisor urging government websites to prepare defenses against possible attack. Source: [http://www.theregister.co.uk/2011/01/28/anonymous\\_hacklash\\_warning/](http://www.theregister.co.uk/2011/01/28/anonymous_hacklash_warning/)

**Eight-character password bug identified on Amazon.** A password bug has been identified on Amazon, where the casing and everything after the first eight characters is ignored for older access codes. The discussion about this problem was started on Reddit by a user who noticed that Amazon’s system would authenticate him even if he mistyped the ending of his password. Apparently, the issue exists only for access codes longer than eight characters. And, after analyzing the implications, that the impact is quite limited — if an attacker would decide to hack a user whose password is common eight-letter word, they would still need to find out their e-mail addresses. Giving the sheer size of Amazon and the likely protection against brute force attacks, finding even a single match would probably take a lot of time, even with lists of already harvested e-mail addresses. In addition, the password must not have been changed in a long time, because this trick does not appear to work with newer access codes, probably because the source of the bug is an old password hashing algorithm. Source: <http://news.softpedia.com/news/Eight-Character-Password-Bug-Identified-on-Amazon-181109.shtml>

**50 million viruses and rising.** IT security lab AV-Test registered the 50 millionth new entry into its malware repository January 27. The malware in question is a PDF file which exploits a security hole in Adobe Reader to infect Windows systems. It has not been given a name yet because it has not been fully identified. So far, only the heuristics of Authentium, Eset, F-Prot, Kaspersky, and McAfee have issued a generic message such as: “HEUR:Exploit.Script.Generic.” This new item of malware confirms the trend that attackers trying to infect PCs no longer use mainly the security holes in operating systems or browsers as their point of entry. Instead, malware authors are focusing on third party

UNCLASSIFIED

## UNCLASSIFIED

applications. Source: <http://www.h-online.com/security/news/item/50-million-viruses-and-rising-1178664.html>

**Low-cost SSL proxy could bring cheaper, faster security; defeat threats like Firesheep.** Researchers have found a cheaper, faster way to process SSL/TLS with off-the-shelf hardware, a development that could let more Web sites shut down cyber threats posed by the likes of the Firesheep hijacking tool. The technology, dubbed SSLShading, shows how SSL proxies based on commodity hardware can protect Web servers without slowing down transactions, according to a presentation scheduled at the USENIX Symposium on Networked Design and Implementation in Boston March 30 through April 1, 2011. SSL/TLS — the cryptographic protocols used to protect online Web transactions — encrypts traffic from visitors' machines all the way to Web servers. That makes it impossible to pick up data such as session cookies by preying on unencrypted wireless networks, which is what Firesheep does. Based on an algorithm devised by researchers in Korea and the United States, SSLShading is software that directs SSL traffic being proxied either to a CPU or a graphics processing unit, whichever is most appropriate to handle the current load. The researchers will discuss the algorithm in their paper "SSLShader: Cheap SSL Acceleration with Commodity Processors." Source: [http://www.computerworld.com/s/article/9206482/Low\\_cost\\_SSL\\_proxy\\_could\\_bring\\_cheaper\\_faster\\_security\\_defeat\\_threats\\_like\\_Firesheep](http://www.computerworld.com/s/article/9206482/Low_cost_SSL_proxy_could_bring_cheaper_faster_security_defeat_threats_like_Firesheep)

**Multiple vulnerabilities in Symantec products.** Multiple vulnerabilities have been reported in Symantec products, which can be exploited by malicious people to cause a Denial of Service attack and compromise a vulnerable system, according to Secunia. The first is an error in the Intel AMS2 component when processing certain messages can be exploited to cause a buffer overflow via specially crafted packets sent to TCP port 38292. The second is an error in the Intel AMS2 component when processing certain messages can be exploited to run arbitrary commands via specially crafted packets sent to TCP port 38292. The third is an error in the Intel AMS2 component when processing certain messages can be exploited to create arbitrary events (e.g. launch a program or send an e-mail) via specially crafted messages sent to TCP port 38292. Successful exploitation of the vulnerabilities may allow execution of arbitrary code. The fourth is an error in the Intel AMS2 component when processing certain messages can be exploited to crash the Intel Alert Handler service via specially crafted packets sent to TCP port 38292. The vulnerabilities are reported in Symantec AntiVirus Corporate Edition Server 10.x. and Symantec System Center 10.x. Source: <http://www.net-security.org/secworld.php?id=10503>

**Facebook fake photo links lead to malware.** A simplistic but effective bait leading to malware has been circling on Facebook for the past few weeks. Users are sent messages from friends' accounts saying Foto :D apps(dot)facebook(dot)com/photobf/index(dot)php. If the user fails to find it strange or suspicious, a click on the link will take him to a page where the photo was allegedly posted prior to being moved. The next click on the "View Photo" button triggers the download of what looks at first glance like a .png file because of its icon, but it is actually an executable. According to GFI, many rogue application pages were involved in the malware run, but have been deactivated by Facebook one by one. The external sites that have been serving the malware have also been taken offline. The malicious file is a generic Trojan, and is currently being detected by more than two thirds of the AV solutions used by VirusTotal. Source: [http://www.net-security.org/malware\\_news.php?id=1607](http://www.net-security.org/malware_news.php?id=1607)

UNCLASSIFIED

## UNCLASSIFIED

**Intel developing security 'game-changer'.** Intel's chief technology officer said the chip maker is developing a technology that will be a security game changer. He told Computerworld January 25 that scientists at Intel are working on security technology that will stop all zero-day attacks. And, while he would give few details about it, he said he hopes the new technology will be ready to be released in 2011. He noted the technology will not be signature-based. Signature-based malware detection is based on searching for known patterns within malicious code. The problem, though, is that zero-day, or brand-new, malware attacks are often successful because they have no known signatures to guard against. Intel is working around this problem by not depending on signatures. Source:

[http://www.computerworld.com/s/article/9206366/Intel\\_developing\\_security\\_game\\_changer](http://www.computerworld.com/s/article/9206366/Intel_developing_security_game_changer)

**Fedora infrastructure hacked – no damage done.** The Fedora Project has confirmed there was an intrusion into its infrastructure January 22, but investigations have shown “no impact on product integrity.” The Fedora Project is a general purpose collection of free and open software including an operating system based on the Linux kernel, sponsored by Red Hat. The announcement of the intrusion by a Fedora Project leader states the project became aware of a problem when a contributor received an e-mail from the Fedora Accounts System, saying his account details had been changed. The Fedora Infrastructure Team investigated and confirmed the account had been compromised. After locking down systems, snap-shotting file systems, and auditing logs, it was found the account, which was only authorized for SSH to fedorapeople.org, push packages into Fedora's SCM, and perform builds of Fedora packages, had only changed the account's SSH key and logged into fedorapeople.org. Source: <http://www.h-online.com/security/news/item/Fedora-infrastructure-hacked-no-damage-done-1176358.html>

**Twitter flooded with free iPhone survey scams.** Security researchers warn that waves of spam messages offering free iPhones and iPads have been flooding Twitter recently and lead users to various online scams. According to the GFI Software researchers who analyzed the attacks, the spam messages appear to be sent from both fake and compromised accounts. At their peak, the spam messages were coming in at a rate of over 1,300 per hour and read “want to find out how to get a free iphone? [link]” or “I just won a free iphone and ipad! [link].” Some of the rogue links are displayed in full, while others are shortened via bit.ly. The links take users to pages inviting them to a trial program, which involves testing an iPhone and getting to keep it. In order to sign up for the alleged program, the site asks users to disclose their e-mail address and personal information. Source: <http://news.softpedia.com/news/Twitter-Flooded-with-Free-iPhone-Survey-Scams-179756.shtml>

**Twitter scareware wave.** An apparently large number of links leading to scareware sites were spread via Twitter January 20. The page links were disguised using short URLs from goo.gl and advertised as “Cool”, “Very Nice,” or “Google's search page has done it again” in varying tweets by different users. Clicking on the link transferred users to a Web site that pretended to find numerous viruses after performing a bogus scan on a Windows PC. According to the Internet Storm Center, one of the files offered to solve the alleged problem contained in the SecurityShieldFraud scareware. Once installed, the malware contacted other servers; no further functional details have become available yet. It remains unknown how many Windows users have fallen victim to the attack. Whether the attackers used hacked accounts or stolen access data to send out the links via Twitter, or exploited existing

## UNCLASSIFIED

## UNCLASSIFIED

Twitter accounts on infected PCs, is yet unclear. All scareware sites discovered in connection with this attack have now been shut down. Source: <http://www.h-online.com/security/news/item/Twitter-scareware-wave-1174562.html>

**'Guy Kills Girlfriend' scams spread virally on Facebook.** Security researchers warn of several Facebook scams that lure users onto deceptive survey pages via fake news headlines about a man killing his girlfriend. The links take users to pages promoting rogue Facebook apps. In one case, the page promotes a fake news application and displays a message reading "She had forgotten to close her session on the world's biggest social network. Her boyfriend came back home early and found this message in her inbox..." This is meant to peak the user's interest and is followed by a "Click here to read the story" link. Doing so prompts a permission dialog from the rogue application asking for permission to post on their wall. The apps are the propagation mechanisms behind these scams and will spam the victim's friends without their knowledge. Users who end up installing them are then asked to complete surveys, usually under the pretense of security verifications, in order to see the promised content. Source: <http://news.softpedia.com/news/Guy-Kills-Girlfriend-Scams-Spread-Virally-on-Facebook-180115.shtml>

**VLC Media Player 1.1.6 fixes critical vulnerabilities.** VideoLAN project developers have announced the release of version 1.1.6 of their VLC Media Player. The seventh release of the 1.1.x branch of VLC is a maintenance and security update that includes various bug fixes and improvements. VLC 1.1.6 addresses security issues in the Real demuxer, the subtitle decoder, and two previously reported critical heap corruption vulnerabilities; these are in the relatively rarely used CDG format decoder. Using VLC to play manipulated video in this format could cause heap corruption, which could in turn be exploited to inject and execute malicious code. Source: <http://www.h-online.com/security/news/item/VLC-Media-Player-1-1-6-fixes-critical-vulnerabilities-1175821.html>

## **NATIONAL MONUMENTS AND ICONS**

**(Washington) Study ties pine beetle to severe Wash. wildfires.** A new study mapping the mountain pine beetle outbreak in north-central Washington State showed infested areas were more likely to experience larger, more destructive forest fires. The study, which was a collaboration between NASA and the U.S. Forest Service, aimed to detect bark beetle infestations and to evaluate the link between them and forest fires in the Okanogan-Wenatchee National Forest. Satellite data showed regions of the forest experiencing water and vegetation stress, and analysis tied these regions to beetle infestations. Additional review showed highly infested areas that subsequently burned had more intense forest fires than areas without infestations. The forest has experienced severe wildfires in recent years, including the Tripod Fire, which burned on more than 273 square miles. Source: [http://seattletimes.nwsourc.com/html/localnews/2014042718\\_apwafirefires.html](http://seattletimes.nwsourc.com/html/localnews/2014042718_apwafirefires.html)

**(Hawaii) Arson damages tour boat used for shark tours.** Honolulu, Hawaii fire investigators have determined a fire that heavily damaged a 30-foot shark tour boat January 24 at Haleiwa Harbor was intentionally set. It was the second suspicious fire involving a North Shore Shark Adventures boat in January. The fire occurred at 12:11 a.m., and firefighters extinguished the fire within 10 minutes, fire officials said. The blaze damaged the front end and cabin of the boat. No one was on board the boat or in the area when firefighters arrived. Damage was estimated at \$225,000. The case was turned

UNCLASSIFIED

## UNCLASSIFIED

over to police. There were no arrests as of January 24, according to a police spokeswoman. The fire came 3 weeks after an intentionally set fire destroyed another shark tour boat owned by North Shore Shark Adventures. That blaze occurred at about 12:40 a.m. January 7. Heat from the fire also damaged a nearby vessel. Damage to the shark tour boat was also estimated at \$225,000. The company's two damaged boats, Kailolo and Kolohe, were dry-docked on the Waimea side of the harbor. Source:

[http://www.staradvertiser.com/news/hawaii/news/20110125\\_Arson\\_damages\\_tour\\_boat\\_used\\_for\\_shark\\_tours.html](http://www.staradvertiser.com/news/hawaii/news/20110125_Arson_damages_tour_boat_used_for_shark_tours.html)

## **POSTAL AND SHIPPING**

**(Pennsylvania) Powder prompts hazmat at state police barracks.** Hazmat crews, along with police and fire officials, were called out to the state police barracks in the Wynnefield Heights section of Philadelphia, Pennsylvania January 23. According to police sources, a Pennsylvania State Trooper opened up a threatening letter at the Troop K barracks on Belmont Avenue. Also inside the envelope was a white powder. At 1 p.m., hazmat crews were called to the barracks to identify the powder. The investigation determined the powder to be cornstarch. There is no word on if police plan to press charges against anyone. Source: <http://abclocal.go.com/wpvi/story?section=news/local&id=7913979>

## **PUBLIC HEALTH**

**International counterfeit drugs supplier arrested in New Zealand.** New Zealand Police announced the arrest of a Chinese national suspected of serving as an international supplier of counterfeit pharmaceuticals. The 32-year-old man was arrested following a three-year long investigation into the international trade of counterfeit drugs. The suspect was taken into custody in Wellington January 25 by the Auckland Metro Crime and Operations Support (AMCOS) officers. A Wellington District Court judge set bail and ordered him to appear at a hearing next month where his extradition to the United States will be considered. The U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations and the U.S. Food and Drug Administration's Office of Criminal Investigations cooperated with New Zealand authorities in the investigation. "Counterfeit pharmaceuticals include those used as sexual stimulants, heart medications, pain killers and other medications which Police believe have been sourced from China and distributed internationally via the internet," the AMCOS field crime manager, said. These operations are closely tied to the pharma spam that plagues people's email inboxes and the countless rogue online pharmacy websites. According to recent statistics from Symantec, 64 percent of the entire spam traffic in December fell into the pharmaceutical category. Source: <http://news.softpedia.com/news/International-Counterfeit-Drugs-Supplier-Arrested-in-New-Zealand-180818.shtml>

**(North Carolina) Bio-threat system being showcased.** The North Carolina Bio-Preparedness Collaborative (NCB) is showcasing a bio-surveillance system for early outbreak threat detection. When complete, the NCB-Prepared system will integrate data from sources as disparate as the environment, animal, and human clinical services and food production, processing and distribution to detect emerging health threats more quickly and effectively. Examples of data used in the system include ambulance calls, emergency room visits, hospitalizations, reports of tainted food, and veterinary records. NCB-Prepared will allow public health experts to differentiate between normal

UNCLASSIFIED

## UNCLASSIFIED

health patterns, environmental changes, and natural or man-made bio-threats. The North Carolina Bio-Preparedness Collaborative is a public-private partnership that includes the University of North Carolina at Chapel Hill, North Carolina State University and SAS, with support from the U.S. Department of Homeland Security. The system is being presented January 27 at the North Carolina State Health Director's Conference. Source: [http://www.upi.com/Business\\_News/Security-Industry/2011/01/26/Bio-threat-system-being-showcased/UPI-64331296065272/](http://www.upi.com/Business_News/Security-Industry/2011/01/26/Bio-threat-system-being-showcased/UPI-64331296065272/)

**(Massachusetts) Massachusetts man is diagnosed with cholera.** A 30-year-old Massachusetts man who traveled to the Dominican Republic for a wedding has been diagnosed with cholera after returning to Boston, state disease trackers confirmed January 27. The man is recovering, and doctors said there is no evidence he spread the intestinal infection to anyone in the state. The patient went to the emergency room at Massachusetts General Hospital January 25. The man had attended a wedding from January 20 to 23 at a resort in the Dominican Republic, where more than 400 guests feasted on lobster. Dozens, including some who had returned to Venezuela, fell violently sick in the days after the celebration. Tests show that the ill are infected with the same strain of cholera that has killed more than 3,000 in Haiti since October and spread to the Dominican Republic, said the director of the Division of Epidemiology and Immunization at the Massachusetts Department of Public Health. Preliminary testing conducted at Massachusetts General suggested that the man contracted cholera; a confirmatory test will be performed at the U.S. Centers for Disease Control and Prevention in Atlanta. Source: [http://www.boston.com/news/local/massachusetts/articles/2011/01/28/massachusetts\\_man\\_is\\_diagnosed\\_with\\_cholera/](http://www.boston.com/news/local/massachusetts/articles/2011/01/28/massachusetts_man_is_diagnosed_with_cholera/)

**FDA wants stricter testing for defibrillators.** The Food and Drug Administration (FDA) is recommending stricter safety measures for heart-zapping defibrillators after years of increasing problems with the emergency medical devices. Under the agency's proposal posted online January 21, makers of external defibrillators would need to submit more data and undergo manufacturing inspections before launching a new product. The tighter regulation is aimed at curbing design and manufacturing flaws with the devices, which are found everywhere from hospitals to schools to airports. Medical device manufacturers have issued 68 recalls of defibrillators in the last 5 years, the FDA said. The agency has received more than 23,000 reports of device malfunctions, "including some where the device failure occurred during a rescue attempt and may have contributed to patient harm or death." On January 25, the FDA will ask an expert panel to provide recommendations. Currently, makers of defibrillators are approved through an accelerated approval pathway designed for low-risk devices. The so-called 510(k) system allows speedy approval of devices similar to products already on the market. But the FDA argues stricter measures are needed because defibrillator makers have failed to fix problems that have led to the recall of hundreds of thousands of devices. Source: <http://www.google.com/hostednews/ap/article/ALeqM5jDGQ1wCSEPxGeJPsBAmTTGjYO4Dw?docId=feeb9f285446412c98b5a6d1a20aba05>

**WHO board backs retention of smallpox strains.** The executive board of the World Health Organization January 20 supported the U.S. and Russian argument the two nations should be allowed to retain their smallpox strains for biodefense research purposes, the Wall Street Journal reported. Gathering in Geneva, the 34-member board agreed more study is needed of the highly virulent disease before the last known smallpox cultures are destroyed. Moscow and Washington asserted

UNCLASSIFIED

## UNCLASSIFIED

their work would produce new vaccines and other countermeasures against an act of biological terrorism or an outbreak caused by a previously unknown supply of the virus, according to informed sources. The U.S. and Russian position received backing from African and European states, sources said. The board's recommendation will be considered by the entire World Health Assembly for a final decision in May on whether to establish a deadline for the smallpox strains to be destroyed. There are worries some states might have retained illicit samples of the deadly smallpox virus, Radio Free Europe/Radio Liberty reported. However, there is intense debate within the international community over whether these fears are overblown and whether the real danger lies in the accidental release of a U.S. or Russian-held strain. The United States stores 451 specimens with the Atlanta-based Centers for Disease Control and Prevention, while Russia houses 120 different strains at its Vector laboratory in Siberia. Source: [http://gsn.nti.org/gsn/nw\\_20110121\\_5430.php](http://gsn.nti.org/gsn/nw_20110121_5430.php)

**Hacker attacks Defense pharmacy site.** One or more hackers attacked the Web site and Internet domain of the Defense Department's prescription drug database, the PharmacoEconomic Center, the security firm Imperva reported January 21. The site and domain remained inaccessible into January 24. Attempts to reach the site resulted in the message: "www.pec.ha.osd.mil is temporarily unavailable; We're working to resolve this issue." Programs on the PharmacoEconomic Center site and domain include the Prescription Medication Analysis and Reporting Tool, which maintains a medication profile for troops slated for deployment. It also includes a version of that tool developed to track drugs prescribed for soldiers in warrior transition units. Both programs remained inaccessible January 24. The PharmacoEconomic Center, in partnership with the Veterans Affairs Department (VA) and the Defense Supply Center-Philadelphia, manages national pharmaceutical contracts for Defense and VA as well as a prescription formulary describing the types of drugs that can be prescribed to active-duty military personnel, retirees, and their families. The PharmacoEconomic Center maintains the U.S. Central Command Central Nervous System Drug Formulary. Imperva said the hacker offered full control and root access to the domain for \$399. A security blogger reported the hacker also offered to sell personally identifiable information from the sites hacked for \$20 per 1,000 records. Source: [http://www.nextgov.com/nextgov/ng\\_20110124\\_7617.php?oref=topstory](http://www.nextgov.com/nextgov/ng_20110124_7617.php?oref=topstory)

**Investigation shows fraud plagues health fund.** A \$21.7 billion development fund backed by celebrities and hailed as an alternative to the bureaucracy of the United Nations sees as much as two-thirds of some grants eaten up by corruption, the Associated Press has learned. Much of the money is accounted for with forged documents or improper bookkeeping, indicating it was pocketed, investigators for the Global Fund to Fight AIDS, Tuberculosis, and Malaria said. Donated prescription drugs wind up being sold on the black market. The fund's newly reinforced inspector general's office, which uncovered the corruption, cannot give an overall accounting because it has examined only a tiny fraction of the \$10 billion the fund has spent since its creation in 2002. Sixty-seven percent of money spent on an anti-AIDS program in Mauritania was misspent, the investigators told the fund's board of directors. So was 36 percent of the money spent on a program in Mali to fight tuberculosis and malaria, and 30 percent of grants to Djibouti. The fund is pulling or suspending grants from nations where corruption is found, and demanding recipients return millions of dollars of misspent money. To date, the United States, the European Union, and other major donors have pledged \$21.7 billion to the fund, the dominant financier of efforts to fight the three diseases. The fund finances programs in 150 nations. Source: <http://www.deseretnews.com/article/700103392/Investigation-shows-fraud-plagues-health-fund.html>

UNCLASSIFIED

## **TRANSPORTATION**

**Terrorists look to unprotected parts of airports.** The suicide bombing at a busy international airport outside Moscow, Russia, exposes the vulnerable underbelly of airports in this country and around the world, several security experts and former anti-terrorist government officials said. Terrorists have long sought to disrupt aviation through hijackings and bombings. Since many of those recent attempts have failed at least partly because of heightened security, experts said, it makes sense that terrorists would launch attacks on the unprotected zones of an airport: baggage claim areas, ticket counters, security check-in lines, and curbside areas where passengers are picked up and dropped off. “The situation in the United States is even more dangerous” than at Domodedovo International Airport, said a former chief of U.S. aviation security. In this country, anyone can walk up to a baggage claim area, which during peak hours can be a chaotic sea of travelers and their baggage the former chief said. Source: [http://www.usatoday.com/news/world/2011-01-26-airportterror26\\_ST\\_N.htm?csp=34news&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+UsatodaycomWorld-TopStories+\(News+-+World+-+Top+Stories\)](http://www.usatoday.com/news/world/2011-01-26-airportterror26_ST_N.htm?csp=34news&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+UsatodaycomWorld-TopStories+(News+-+World+-+Top+Stories))

**Pilots union targets laser threats to planes.** The Air Line Pilots Association has stepped up the campaign against people on the ground intentionally pointing lasers at airliners, by calling on lawmakers, regulators, and industry officials to prevent such hazards. The union’s proposal — unveiled 1 week after the government announced heightened dangers from lasers — includes calls for a sweeping public awareness effort and expansion of “laser-free zones” around airports. The union, which represents nearly 53,000 commercial pilots in North America, also wants new air-traffic-control safeguards and pilot procedures when laser threats emerge. Lasers can temporarily blind or incapacitate pilots, and even cause permanent eye damage in some cases. Source: [http://online.wsj.com/article/SB10001424052748703293204576105950154162410.html?mod=google\\_news\\_wsj](http://online.wsj.com/article/SB10001424052748703293204576105950154162410.html?mod=google_news_wsj)

**DHS and TSA offer parking anti-terrorism training.** Terrorists often use parked cars or trucks to carry, conceal, or serve as bombs, so the U.S. Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) are offering a free parking-specific training program for local government officials. The training comes in the form of DHS and TSA’s First Observer software module. The First Observer training program, which is entirely funded by the federal government, trains parking professionals to address five critical security areas: on-street, surface parking lots, garages/decks, special events, and shuttle operations. First Observers recognize and report potential threats using a concise, accurate, and simple communications process. First Observer was developed with the help of the Fredericksburg, Virginia-based parking industry trade association International Parking Institute (IPI). “Since the program was launched, more than 2,000 parking professionals have earned First Observer certificates, and we expect this number to increase significantly,” said IPI’s Executive Director. The program supports DHS’s National Preparedness Guidelines. It is available three ways: as an online training module; as an onsite classroom-style training session; or as a train-the-trainer workshop. Source: <http://americacityandcounty.com/pubsafe/parking-terrorism-training-20110121/>

## UNCLASSIFIED

**FAA issues aircraft GPS disruption advisory because of DOD testing.** The Federal Aviation Administration (FAA) has issued a warning to pilots to expect unreliable performance from Global Positioning System (GPS) instruments in the Southeast and Southwest United States, resulting from tests being done by the Defense Department. The Register, a news outlet in the United Kingdom, reported the Notice To Airmen (NOTAM) advisories about the impending tests. The Southeast will have two series of tests, the first from January 20 to February 11, and another round from February 15 to 22. Pilots are being told that GPS may be unreliable or unavailable during the testing periods. "Several test events will be conducted and will be active for 45 minutes, followed by 15 minutes of off time," the FAA NOTAM states. "These tests may not be concurrent so pilots are advised to check NOTAMs frequently for possible changes prior to operating in the area." The test is based off the coast of Georgia, centered at coordinates N304906 by W0802811 and has a radius of 370 nautical miles. A spokesperson at the FAA said there will be "no impact to ground vehicle GPS." That means that smart phones, automobile guidance systems and other civilian GPS functions will not be affected by the tests. Source: <http://gcn.com/articles/2011/01/24/faa-gps-aircraft-warning-dod-testing>

**(Michigan) Part of Detroit airport evacuated after box found.** Authorities said part of a terminal at Detroit Metropolitan Airport in Michigan was evacuated after a suspicious box was found at an area for loading cargo and luggage onto planes. An airport spokesman said the box was found about 7:15 a.m. January 25, and passengers were removed from part of Concourse B at the McNamara Terminal. The concourse at the airport in Romulus primarily is used by regional aircraft. The spokesman said details about why security officials determined the box to be suspicious were not immediately available. Source: <http://www.wfrv.com/news/michigan/114562314.html>

**London-bound flight diverted after threat.** British authorities said a Heathrow Airport-bound flight from Abu Dhabi was diverted and given a fighter escort after a passenger began making threats. Britain's military said two Royal Air Force jets were scrambled to accompany the Etihad flight as it was diverted to Stansted airport, north of London. Police said a 37-year-old British man was arrested January 24, but gave no further details. Source: [http://www.washingtonpost.com/wp-dyn/content/article/2011/01/24/AR2011012401947.html?nav=ft\\_world](http://www.washingtonpost.com/wp-dyn/content/article/2011/01/24/AR2011012401947.html?nav=ft_world)

## WATER AND DAMS

Nothing Significant to Report

## NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov) ; Fax: 701-328-8175  
**State Radio:** 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455  
**US Attorney's Office Intel Analyst:** 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168

UNCLASSIFIED

**UNCLASSIFIED**



**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**