



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

Zoo working with Army Corps to prepare for changes in 2011. Currently, the U.S. Army Corps of Engineers is working with Wahpeton and Chahinkapa Zoo in North Dakota to make changes in the zoo's features for a levee project, moving fences and some exhibits. "We have to get our stuff done prior to them putting in some work they're doing with the drain," said the zoo director. They will have to move some of the animal exhibits. "This is not something that we have a choice in, so we're going to work the best we can with them, and we are going to try to plan it in a way that's good and healthy for our animals," she said. These changes, which will not be made until the conclusion of the zoo's regular season in the fall, are not being funded by the zoo. Source:

<http://www.wahpetondailynews.com/articles/2010/12/27/news/doc4d18a51fde51d133009483.txt>

REGIONAL

(Minnesota) Minnesota sues 3M over chemical disposal. The state of Minnesota is suing 3M Co. over its disposal of chemicals previously used to make Scotchgard and other products. The lawsuit filed December 30 in Hennepin County alleges 3M damaged the state's natural resources, as well as ground and surface water, by disposing of perfluorochemicals, or PFCs. Maplewood, Minnesota-based 3M has produced PFCs since the 1940s, and legally disposed of them in landfills until the 1970s. 3M stopped making PFCs in 2002. In 2004, traces of the chemicals were found in groundwater from Lake Elmo to Hastings. The state's lawsuit seeks unspecified damages. Source:

<http://www.bloomberg.com/news/2010-12-30/minnesota-sues-3m-over-chemical-disposal.html>

(Minnesota) Mankato Clinic laptop with patient data is stolen. The Mankato Clinic in Mankato, Minnesota reported that a laptop with information on nearly 3,200 patients was stolen from a nurse's car last month. The clinic chief executive said it is unlikely anyone has accessed the password-protected information. The records included patients' full names, dates of birth, medical record numbers, and diagnosis information. The clinic chief also said the records did not include financial information, Social Security numbers, or home addresses. The theft occurred about November 1. Clinic officials sent letters to all affected patients December 23. The clinic chief executive said the delay in notification came about because the clinic was performing an internal investigation to understand the extent of the situation. The clinic notified federal officials about the security breach as required. The Free Press of Mankato reported the laptop has not been recovered. Source:

<http://washingtonexaminer.com/news/2010/12/mankato-clinic-laptop-patient-data-stolen>

NATIONAL

2.3 million Americans reentered without proper documents. Despite new travel requirements, more than 2.3 million Americans reentering the country by land or sea from Mexico or Canada failed to produce a passport, birth certificate, or other secure document to establish identity and nationality, according to a report by the Inspector General for the Department of Homeland Security. Most

UNCLASSIFIED

people, including about 500,000 in California, were allowed to pass through ports of entry without the approved documents or without being sent to a secondary inspection post for a more in-depth examination. Many travelers were allowed to pass after undergoing extensive questioning and producing at least a driver's license, the report found. Overall, 96 percent of travelers arriving at the 39 busiest land ports were in compliance with the new law, which took effect in June 2009. The audit concluded that if all those who skirted the rules were sent for a secondary inspection, the agency would not have the necessary staffing and infrastructure to handle the resulting increase in workload. U.S. Customs and Border Protection agreed with the report's findings and plans to follow the Inspector General's recommendations, an agency spokeswoman said. Source: <http://articles.latimes.com/2010/dec/28/local/la-me-customs-audit-20101228>

(Nevada) 8,000 still without power in storm at Lake Tahoe. A winter storm in the Sierra Nevada left more than 10,000 homes and businesses without power around Lake Tahoe, Nevada most of December 29, and about 8,000 were still in the dark at nightfall. A NV Energy spokesman said crews were working to repair power lines that were downed overnight by high winds and tree limbs snapping under the weight of heavy snow. The biggest outage affected about 10,000 customers at South Lake Tahoe and the Meyers area. The spokesman said power was restored to about 2,000 customers December 29. Numerous smaller outages were reported around the lake, from Stateline, Nevada, to Tahoma on the west shore and near Tahoe City in the north. Power was restored earlier December 29 to 3,300 customers on the north shore between Tahoe City and Kings Beach. Source: http://www.mercurynews.com/breaking-news/ci_16973373?nclick_check=1

INTERNATIONAL

Broken dam floods home. A swollen Australian dam containing 2.1 million gallons of water has burst near Stanthorpe, flooding neighboring properties. A Stanthorpe Police detective senior constable said the dam wall, measuring 10 meters in height, collapsed at the Applethorpe property at 1 p.m. December 27. The mass of water flooded a house, destroyed a farm shed, and flattened an orchard at a nearby Kelly Road farm. A family on Kelly Road saw the wall of water coming and were able to get to safety just before their property was hit. The hole in the dam wall measured 33 feet by 33 feet. The water traveled 4.3 miles to Stanthorpe where it caused minor flooding of multiple residential garages and sheds. Source: <http://www.thechronicle.com.au/story/2010/12/29/broken-dam-water-stanthorpe-flood/>

Pirates: Ship released, another taken. As Somali pirates in the Indian Ocean released a German oil tanker with 19 Indians aboard, other pirates captured another ship with a crew that included seven Filipinos. Pirates in the Gulf of Aden set free the German-owned Marida Marguerite and its crew, held for almost 9 months, the European Union's naval force operating in the Indian Ocean, Navfor, said. The crew of the 13,168-ton, Marshall Islands-flagged vessel also included two Bangladeshis and one Ukrainian. Pirates, armed with rocket-propelled grenades, boarded the ship, bound for Holland, May 8, 2010 around 120 nautical miles south of the port of Salalah, close to the Gulf of Aden and on the southern coast of Oman on the Arabian Peninsula. There are reports that the ship's owners paid ransom of \$5.5 million. The day before the release of the Marida, pirates seized another German ship, the 5,200-ton general cargo vessel Ems River, flagged in Antigua and Barbuda, along with its crew of seven Filipinos and one Romanian. The ship carrying petroleum coke was boarded around 175 nautical miles northeast of Salalah. The Ems River was on its way to San Nicolas, Greece, from

UNCLASSIFIED

UNCLASSIFIED

Jebel Ali in the United Arab Emirates when the attack happened. Source:

http://www.upi.com/Top_News/Special/2010/12/29/Pirates-Ship-released-another-taken/UPI-46991293621840/

Somali Islamist insurgents threaten US attack A leader of Somalia's Islamist insurgency threatened to attack America during a speech broadcast Monday. Tweet Be the first to Tweet this! Yahoo! Buzz ShareThis "We tell the American President Barack Obama to embrace Islam before we come to his country," said Fuad Mohamed "Shongole" Qalaf. Al-Shabab has not yet launched an attack outside Africa but Western intelligence has long been worried because the group targeted young Somali-Americans for recruitment. About 20 have traveled to Somalia for training and at least three were used as suicide bombers inside Somalia. Al-Shabab holds most of southern and central Somalia and has the support of hundreds of foreign fighters, mostly radicalized East Africans. It seeks to overthrow the weak U.N.-backed government, which is protected by 8,000 Ugandan and Burundian African Union peacekeepers. The al-Shabab militia launched coordinated suicide attacks in Uganda in July that killed 76 people. It has also announced its allegiance to al-Qaida and is believed to be harboring a mastermind of the twin 1998 bombings of U.S. embassies in Kenya and Tanzania that killed 224 people. The radio message was recorded in the town of Afgoye, near the Somali capital, during a meeting of Shongole and Sheik Hassan Dahir Aweys, formerly the leader of insurgent group Hizbul Islam. The two insurgent groups had clashed several times previously but announced a merger last week. Aweys said his group will fight under al-Shabab's command. "We have united for the sake of our ideology and we are going to redouble our efforts to remove the government and the African Union from the country," said Aweys on Monday. In an unrelated development, the Somali information minister said the new Cabinet had approved the use of a private security contractor to train forces in the capital of Mogadishu and the program would start "soon." Saracen International would train forces for VIP protection, said Abdulkareem Jama. He said he did not know exactly when training would start, what the men's duties would include or how many men would be trained but he said the program included the renovation of a hospital and government buildings. Somali officials are frequently killed by insurgents, both in single assassinations and en masse in suicide bombings and attacks. The Somali ambassador in Kenya previously said that up to 1,000 men could be trained in the capital for an anti-piracy force and 300 for a presidential guard. Saracen is already training 1,000 men for an anti-piracy force in the semiautonomous northern region of Puntland. The program has been criticized by U.S. officials who say it is unclear who is funding it, what its objectives are and whether it breaks a U.N. arms embargo. Jama said the Somali cabinet had discussed those issues and were satisfied the embargo was not being broken but he did not say who was funding the program. "There is a need for training," he said. "There was an effort to slow down the project (in Mogadishu) because of those concerns." The arid Horn of Africa nation has not had a functioning government since a socialist dictatorship collapsed in 1991. Its position on the Horn of Africa means pirates can use its long coastline to capture shipping. Analysts fear that al-Qaida linked insurgents are also gaining ground across the Gulf of Aden in the unstable nation of Yemen. If Yemen fell, that would mean failed states on either side of the shipping route leading into the strategically vital Suez Canal, the route taken by a substantial portion of the world's oil shipments.

http://www.boston.com/news/world/africa/articles/2010/12/27/somali_islamist_insurgents_threaten_us_attack/

Terror threat to Narmada dam, security up. Security of the Narmada dam has been strengthened after a terror alert in Gujarat, India, December 27. The Central Industrial Security Force and state

UNCLASSIFIED

UNCLASSIFIED

police were deployed in the dam area and all passing vehicles were being searched. The access of tourists to the area was also restricted. The Intelligence Bureau (IB) alerted the Gujarat government on terror threats to sensitive locations, including the Narmada dam. Ahmedabad and Gandhinagar were also possible targets. IB sources said 12 men from the Lashkar-e-Taiba and the Indian Mujahideen have entered Gujarat. Three of them have been identified, but no arrests have been made. Source: <http://indiatoday.intoday.in/site/Story/124761/India/terror-threat-to-narmada-dam-security-up.html>

Explosives found in parcel at Rome embassy. A suspicious parcel found December 27 outside the Greek embassy in Rome, Italy contained explosives, police said only days after two parcel bombs went off injuring two staffers at two foreign missions in Rome. “Bomb disposal experts are currently working to defuse it and determine whether it is similar to those who exploded last week or whether it is the work of someone trying to emulate it,” a police spokesman said. On December 23, two parcel bombs exploded at the Chilean and Swiss embassies in Rome, injuring two. The blasts were claimed by an Italian anarchist group calling itself the Informal Federation of Anarchy (FAI). Investigators said the claim was “reliable” and backed by “objective” checks. Since then, diplomatic missions in the Italian capital have been put on alert. The spokesman said suspicious parcels were reported at the embassies of Monaco and Venezuela December 27, but police who rushed to the scene in each case determined they were “false alarms”. Source: <http://news.smh.com.au/breaking-news-world/explosives-found-in-parcel-at-rome-embassy-20101228-198ol.html>

BANKING AND FINANCE INDUSTRY

54 banking breaches in 2010. There have been 54 reported banking-related data breaches so far in 2010, according to the Identity Theft Resource Center (ITRC) — slightly fewer than the total of 62 breaches in 2009. But it is possible that additional 2010 breaches will be reported after the new year. Of the 54 breaches tracked by the ITRC: 9 are related to insider theft; 6 are related to missing paper documents; 8 were linked to card skimming attacks; 5 resulted from stolen or missing hardware; 8 are blamed on cyberattacks or outside network intrusions; 4 are related to the exposure of data on the Web; 6 are linked to an accidental breach; and 3 were of unknown origin. While some breaches were accidental or related to sloppy security, such as the improper disposal of paper files and documents, many involved a malicious or criminal element. Whether linked to an insider, a cyberattack or an ATM skimming device, the incidents prove criminals continue to target financial institutions. Source: http://www.bankinfosecurity.com/articles.php?art_id=3220

Anonymous attacks Bank of America. Anonymous has launched a distributed denial of service attack (DDoS) against Bank of America (BoA), after the U.S.-based financial giant banned transactions destined for WikiLeaks. About 2 weeks ago, BoA joined the list of companies boycotting WikiLeaks by announcing it would block all transactions related to the whistleblower organization. All of the firms became targets of coordinated DDoS attacks by Anonymous, a notorious group of hacktivists. The holiday delayed the attack, but it launched December 27. However, as some previously predicted, a lack of organization failed to cause major problems for Bank of America. Infosec Island reported the primary impediment was technical issues with the “hive mind” feature of the LOIC DDoS tool, which normally forces the user’s computer to join a voluntary botnet. Users had to resort to filling in the target details manually and not all of them managed to do it. Even so, the BoA Web site experienced slowdowns and even went offline for short periods of time. The force of the attacks is expected to

UNCLASSIFIED

UNCLASSIFIED

increase as the hive mind problem gets resolved and more members return from the Christmas holiday to join the effort. Source: <http://news.softpedia.com/news/Anonymous-Cell-Attacks-Bank-of-America-174930.shtml>

Online stores insure against cyber-hacking after Wikileaks protest. Online retailers will be offered insurance against cyber-hacking following the recent attack by supporters of Wikileaks. IMRG, a trade body in England, will provide protection against politically-driven “denial of service” attacks that threaten Britain’s 57.8 billion pound online shopping industry. It follows the targeting of payment services PayPal, Visa and Mastercard earlier in December by “hacktivists” who accused them of bowing to U.S. pressure to hinder the release of embarrassing diplomatic cables. Amazon was also attacked because it had removed Wikileaks information from its servers. Christmas shopping was not disrupted, but the movement behind the attacks, calling itself Anonymous, said it would mount similar campaigns in the future. A member of the online security organization ISACA and chief executive of security consultants First Base Technologies, said: “Politically-motivated denial of service is a new threat to online retail because previously the threat has only been from criminals.” Source: <http://www.telegraph.co.uk/finance/newsbysector/retailandconsumer/8224968/Online-stores-insure-against-cyber-hacking-after-Wikileaks-protest.html>

Chip and PIN security hack prompts censorship rebuke from researchers. Cambridge University has refused to censor a masters student’s thesis on the security flaws in the Chip and PIN security system, rebuking calls from the UK Cards Association trade body to bury the research after allegations it “breaches the boundary of responsible disclosure.” According to a security group researcher, not only is the paper lawful and already in the public domain, it will soon be followed by a similarly-detailed paper on the subject. The Association claimed the loophole utilized has already been fixed when using Barclays bank cards at a Barclays merchant, though that still leaves Chip and PIN systems managed by other banks open to attack. The research had led to the creation of a card-sized monitoring device that can track transactions and flag up — among other things — cases where illegally modified card-readers show one value on-screen and then charge a higher amount to the card. Source: <http://www.slashgear.com/chip-and-pin-security-hack-prompts-censorship-rebuke-from-researchers-27121248/>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

U.S. nuclear output little changed as plants operate at 97%. U.S. nuclear output was little changed from December 29, the Nuclear Regulatory Commission (NRC) reported. Production fell 63 megawatts to 98,058, or 97 percent of capacity, according to the report December 30 from the commission and data compiled by Bloomberg. Three of the 104 U.S. power reactors were offline. FirstEnergy Corp. slowed the 1,261-megawatt Perry reactor in Ohio to 95 percent of capacity from 100 percent December 29, according to the commission. Source: <http://www.bloomberg.com/news/2010-12-30/u-s-nuclear-output-little-changed-as-plants-operate-at-97-.html>

Stuxnet possibly responsible for 1,000 broken centrifuges at Natanz. A new report from the Institute for Science and International Security (ISIS) suggested Stuxnet might be responsible for 1,000 broken IR-1 centrifuges replaced at Iran’s Natanz Fuel Enrichment Plant (FEP). It is a known fact Stuxnet was designed to target industrial SCADA systems, in particular those with frequency converter drives

UNCLASSIFIED

UNCLASSIFIED

attached. According to an analysis of its code, Stuxnet looks only for such drives produced by two companies, one located in Finland and one in Tehran. Furthermore, the malware checks if the equipment operates at frequencies between 807 Hz and 1210 Hz for long periods of time. One of the few applications for converter drives operating at such high frequencies is uranium enrichment centrifuges. Now, ISIS reports 1,000 centrifuges were decommissioned at Natanz in late 2009, early 2010, noting that “Iran’s IR-1 centrifuges often break, yet this level of breakage exceeded expectations and occurred during an extended period of relatively poor centrifuge performance.” Stuxnet hides the attack by sending commands to disable the frequency converters’ warning and safety controls that would normally alert operators. ISIS ends its assessment with a warning. “Countries hostile to the United States may feel justified in launching their own attacks against U.S. facilities, perhaps even using a modified Stuxnet code.” Source:

<http://news.softpedia.com/news/Stuxnet-Possibly-Responsible-for-1-000-Broken-Centrifuges-at-Natanz-174842.shtml>

COMMERCIAL FACILITIES

Danish court charges 3 men with attempted terrorism. Three men suspected of planning a deadly attack on a Danish newspaper were charged with an attempted act of terrorism and possession of weapons December 30. Police detained four men in Denmark and one in Sweden, December 29, on suspicion of plotting an assault by January 1 on the office block on Copenhagen’s city hall square that houses Jyllands-Posten — the Danish daily that published cartoons of the Prophet Mohammad in 2005 — and another newspaper. The three — one Tunisian and two Swedish citizens — pleaded not-guilty to the charges, officials said. The Danish security police chief said the arrests prevented an “imminent terror attack” that aimed “to kill as many as possible” of the people present at the Copenhagen offices of the newspaper. A court in Glostrup ordered the suspects be held in custody for 4 weeks pending more investigations. A fourth man detained in Denmark, a 26-year-old Iraqi asylum-seeker, was released but remains a suspect, though police did not have evidence to hold him further. The fifth detainee, a 37-year-old Swedish citizen, was scheduled to appear before a court in Sweden December 30, and was also expected to be remanded in custody, a Swedish court official said. The men came to Denmark from Sweden the night of December 28. Police found plastic strips that could be used as handcuffs, a machine gun, a pistol, and more than 100 cartridges. Source:

<http://www.reuters.com/article/idUSTRE6BT1QV20101230>

(Arizona) Arizona strip club shooter fired at random. A man accused of opening fire in a Phoenix, Arizona strip club, killing two people and injuring three others, told police he had planned the crime and chose the victims at random, according to a court document released December 28. The 28-year-old man, of Scottsdale, is accused of shooting four people with a .38-caliber revolver and physically attacking a fifth person at the Great Alaskan Bush Company shortly before midnight December 26. Patrons tackled and beat him after he ran out of ammunition. He remained held in the Maricopa County jail’s psychiatric unit on a \$2 million cash bond, and it was unclear whether he has a lawyer. Police wrote that the man said he knew what he did was wrong “but stated he felt compelled to commit this offense.” Source: <http://www.msnbc.msn.com/id/40830682>

(Florida) 5 teenagers found dead in Florida motel carbon monoxide poisoning. Fire officials said five friends are dead likely from carbon monoxide poisoning caused by a running car in a closed garage underneath their South Florida motel room. A Hialeah police spokesman said it is believed to be an

UNCLASSIFIED

UNCLASSIFIED

accident. A Hialeah fire spokesman said a maid at Presidente Motel called 911 December 27 after looking through a window and seeing several of the teens unconscious. Police said they had rented the room December 26 to celebrate one of teens' 19th birthday. A car that had needed a jump-start earlier was left running in the garage. A door leading to a staircase up to the room had been left open, and high levels of carbon monoxide were found inside. Officials said no alcohol, illegal drugs, or other suspicious items were found inside the room. Source:

http://www.huffingtonpost.com/2010/12/28/5-teenagers-found-dead-in_n_801816.html

(California) Robbery suspect nabbed after claiming he had C-4 explosive. A San Francisco, California man is in custody December 27 after he and an accomplice allegedly robbed at least one electronics store by threatening he had a powerful explosive, police said. A police spokesman said a man entered a Radio Shack store at 1799 Lombard St. in the Marina District at 2:50 p.m. December 24, gathered a bunch of items, walked up to the register, and, claiming he had the powerful plastic explosive C-4, demanded money. The man then fled and was arrested by officers nearby who found no C-4, he said. The 19-year-old man was booked for robbery. A second male suspect believed to be his accomplice was not found. Police believe the robbery may be connected to a similar crime on December 23, when a man walked into an electronics store at Market and Fifth streets at 3:45 p.m. and made a similar threat. Source: <http://www.ktvu.com/news/26295993/detail.html>

COMMUNICATIONS SECTOR

FBI looking for possible victims of phone scam. The FBI is looking for people who may have been victimized by a phone bill scam. The scam involves charges on phone bills for services related to Alternate Billing Corp., 24078 Greenway Road, Forest Lake, Minnesota, or any of the following: 800VMailbox; BusinessSEOPro; Digital VMail; Durham Technology; eProtectID; eSafeld; Identity Holdings; InfoCall; Instant 411; InstantSEOPro; Matchgamepro; Mobile 411 Plus; My411Connect; MyIDSafe; MyIProducts; NeedTheInfo; ProIdentityProtect; Safeguard My Credit; Streaming Flix; Streaming Flix-FamilyWebSafety; Streaming Flix-Iconz of Rock VIP; Streaming Flix-Mobile; Streaming Flix-National Lampoon; Streaming Flix-No Good TV Digital; Streaming Flix-UBD; Studio 127; Uvolve; VolCoff. According to a statement from the Springfield office, no further information can be released because of an ongoing inquiry. The FBI does want to contact people who believe they were improperly billed. Source: http://www.pantagraph.com/news/local/article_1509582a-1153-11e0-a2ba-001cc4c03286.html

Verizon, RIM investing in mobile security to protect phones from attackers. Carriers, developers, and phone makers are rolling out new services and features to protect mobile devices from malicious attacks and data breaches. As people increase their use of smartphones to check e-mail, do their banking, and access documents, the wireless industry is addressing mobile device security. The effort is not limited to IT administrators within the enterprises, as carriers and phone makers are deploying new features and services to bring security to the mobile devices, according to the Wall Street Journal. "Everyone is realizing that this is an uncontrolled environment. We don't want to have the same problems that we had with PCs," the chief security officer of AT&T, told the Wall Street Journal. Several security vendors have raised the alarm, predicting that various types of mobile threats will appear in 2011. Researchers at Panda Security said there will be new attacks on mobile devices, "but not on a massive scale," which will target Symbian- and Android-based phones. In many cases, some of the security features are already available within the smartphone operating system. For example,

UNCLASSIFIED

UNCLASSIFIED

one of the most frequently touted mobile security features for preventing data breaches, remote wipe, is available in the latest version of the Android operating system, as well as for the BlackBerry and iPhone. Source: <http://www.eweek.com/c/a/Security/Verizon-RIM-Investing-in-Mobile-Security-to-Protect-Phones-from-Attackers-391875/>

CRITICAL MANUFACTURING

Attackers walk with 4.9 million customer records in Honda breach. American Honda Motor Company recently discovered that 2.2 million customers were impacted by a data breach exposing the Owner Link e-mail list maintained by outsourced vendor Silverpop. In addition, a further 2.7 million records were lost when the My Acura list was hit. In a letter to customers, American Honda Motor Company said it recently became aware of “unauthorized access to an e-mail list used by a vendor to create a welcome e-mail to customers who have an Owner Link or My Acura vehicle account.” The Owner Link e-mail list contained customer names, email addresses, user names, and Vehicle Identification Numbers. The compromised My Acura list only contained e-mail addresses. Source: <http://www.thetechherald.com/article.php/201052/6623/Attackers-walk-with-4-9-million-customer-records-in-Honda-breach>

FAA seeks fixes to midair collision warning devices. Federal aviation regulators are proposing fixes to midair collision warning devices installed on nearly 9,000 U.S. airliners and business aircraft, after uncovering a safety problem during a test flight. The Federal Aviation Administration’s (FAA) proposed directive, made public December 27, seeks to mandate software upgrades to widely used devices manufactured by a unit of L-3 Communications Holdings Inc. The FAA said that during a flight test over a busy airport’s airspace, airborne collision warning systems manufactured by the unit, Aviation Communication & Surveillance Systems LLC, failed to properly keep track of all nearby planes. The agency said one aircraft disappeared for at least 40 seconds from cockpit displays, which “could lead to possible loss of separation of air traffic and possible mid-air collisions.” Despite the proposal’s broad sweep, regulators apparently concluded the problem does not pose an imminent safety threat because they want to give airlines and operators of business aircraft up to 4 years to complete the upgrades. An FAA spokeswoman said the company’s TCAS devices are installed on more than 7,000 U.S. airliners, and more than 1,800 business aircraft registered in the United States. Less than 100 U.S. military aircraft also use the affected TCAS devices, which provide pilots with computer-generated alerts and emergency instructions to avoid nearby aircraft. Source: http://online.wsj.com/article/SB10001424052970203513204576047303349520540.html?mod=google_news_wsj

GM to recall almost 100,000 vehicles. General Motors (GM) announced it would recall about 100,000 vehicles to fix problems with airbags and rear axles. The recalled lineups will include Cadillac, Chevrolet, and GMC. The first recall involves 96,000 units of Cadillac CTS of model years 2005 and 2007. The vehicles suffer from problems with passenger-side airbags, leading to non-deployment and increasing the risk of injury in crashes. The second recall impacts 1,200 units of Cadillac Escalades, Chevrolet Avalanches, Chevrolet Silverados, and GMC Sierras. It is related to manufacturing defects of the rear axle cross pin, which could possibly fracture and get displaced. GM also announced that it will recall 111,136 units of some of its mid-size crossover lineups in January 2011 related to a problem with the anchor of the seat-belt buckle, leading to injury in a crash. The recalled lineups include Chevrolet Equinox (67,805 units), GMC Terrain (29,926 units), and Cadillac SRX (13,405 units)

UNCLASSIFIED

UNCLASSIFIED

from the 2011 model year. As many as 97,843 units of these vehicles were sold in the United States, and the rest were sold in Canada and Mexico. Since the beginning of 2010, GM has recalled about 3 million vehicles in the United States, Canada, Mexico, and South Korea. Source:

<http://www.zacks.com/stock/news/45174/GM+To+Recall+Almost+100,000+Vehicles>

DEFENSE/ INDUSTRY BASE SECTOR

Report: Cyber-spies to wage non-stop assaults on defense firms in 2011. Defense companies should expect to come under non-stop attack by countries engaging in cyberespionage in 2011, experts at McAfee Labs predicted. January 2010's Operation Aurora helped coin a new term, the advanced persistent threat (APT). Aurora, believed to have originated in China, successfully infiltrated dozens of U.S. companies with the goal of stealing source codes and other data. "Companies of all sizes that have any involvement in national security or major global economic activities — even peripherally, such as a law firm advising a corporate conglomerate starting business in another country — should expect to come under pervasive and continuous APT attacks that go after email archives, document stores, intellectual property repositories, and other databases," the report said. Source:

<http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=277>

EMERGENCY SERVICES

(New York) Hazmat team responds to suspicious substance. Around noon December 29, a hazmat team was called to Albany, New York's police headquarters on Henry Johnson Boulevard after a man brought in a container with small ampules filled with liquid. The man said his son found them in a safe and thought they may contain a hazardous substance. The state police bomb squad believes the liquid may be phosgene, a chemical gas used in World War I. No one was injured. Source:

http://www.fox23news.com/news/local/story/Hazmat-team-responds-to-suspicious-substance/i2YDMXGw80Wanadf_FuWKQ.csp

(Texas) Man admits to intentionally driving through P.A.P.D. front lobby. A driver managed to tear apart a section of the Port Arthur Police Station in Texas, December 26, around 9:30 p.m. Officers said the man wanted to hurt himself. The 53-year-old man drove his Crown Victoria straight through the building. He was taken to a hospital and that is where he admitted to police that he intentionally drove through the front lobby. The crash forced the department to board up the lobby and close it to the public all day December 27. It reopened December 28, but windows are covered with thick plywood. The Port Arthur Police Department is taking steps to prevent this from happening again.

The department estimated it is going to cost several thousand dollars to fix the damage. Police charged the suspect with felony criminal mischief. Source: <http://www.kfdm.com/news/police-40782-department-through.html>

(New Mexico) 911 goes dead again. For the second time in 2 weeks, 911 callers were unable to get through to the emergency dispatch center in Las Cruces, New Mexico. The December 27 and 28 telephone outage, apparently caused by effects of the first outage 2 weeks ago, knocked out emergency telephone service for Las Cruces and Do-a Ana Counties in New Mexico for more than 3 hours. The director of the Mesilla Valley Regional Dispatch Authority said the 911 emergency dispatch system started experiencing problems about 10 p.m. December 27 and completely went down about 12:30 a.m. December 28. Only cellular telephone calls could be placed to 911 until 3:30 a.m. He said

UNCLASSIFIED

UNCLASSIFIED

Qwest Communications told him the loss of service was blamed on a computer routing configuration of telephone line circuits that were modified during a December 14 outage that knocked out telephone service throughout much of southern New Mexico and a small portion of Arizona. No major problems were reported due to the loss of emergency dispatch communications. The latest outage came as the New Mexico Public Regulation Commission (PRC) was investigating the cause of the December 14 outage. The PRC commissioner said initial findings showed that a cut fiber-optic cable south of Socorro apparently happened because the Army Corps of Engineers did not obtain a permit from the PRC to conduct core sample digging. Source: http://www.lcsun-news.com/las_cruces-news/ci_16962917

Police fatalities jump 37 percent in 2010. Deaths of U.S. law enforcement officers in the line of duty jumped 37 percent to about 160 from 117 the year before, according to numbers as of December 28 compiled by the National Law Enforcement Officers Memorial Fund. There also was a spike in shooting deaths. Fifty-nine federal, state, and local officers were killed by gunfire in 2010, a 20 percent jump from last year's figures, when 49 were killed. The total does not include the death of a Georgia State Patrol trooper shot twice in the face December 27 in Atlanta as he tried to make a traffic stop. And 73 officers died in traffic incidents, a rise from the 51 killed in 2009, according to the data. Last year's toll of 117 officers killed was a 50-year low that encouraged police groups. But this year's total is more the norm than an anomaly: The number of police deaths has topped 160 five times since 2000, including 240 in 2001. The deaths were spread across more than 30 states and Puerto Rico — with the most killings reported in Texas, California, Illinois, Florida, and Georgia. Source:

http://news.yahoo.com/s/ap/us_police_deaths;_ylt=AkzVIPpw_bbGIXrVvf0wlnSs0NUE;_ylu=X3oDMTNrbHNqOGZ1BGFzc2V0A2FwLzlwMTAxMjI4L3VzX3BvbGljZV9kZWFOaHMEY2NvZGUDbW9zdHBvcHVzYXIEY3BvcwM2BHBvcwMzBHB0A2hvbWVfy29rZQRzZWMW5faGVhZGxpbmVfbGlzdARzbGsDcG9saWNIZmFOYWxp

ENERGY

EPA plans to tighten power plant, oil refinery emissions standards. The U.S. Environmental Protection Agency (EPA) has announced plans to tighten greenhouse gas emission standards for coal-fired power plants and oil refineries. The agency, which is taking the action under the Clean Air Act in 2011, said "fossil fuel power plants" and petroleum refineries are two of the largest industrial sources of greenhouse gas emissions. EPA said those sources emit nearly 40 percent of the GHG pollution in the United States. "The schedule issued in the December 23 agreements provides a clear path forward for these sectors and is part of EPA's common-sense approach to addressing GHGs from the largest industrial pollution sources," the agency said in a news release. The EPA said several states, local governments and environmental organizations have sued EPA over the agency's failure to update the pollution standards. EPA said it will propose standards for power plants in July 2011 and for refineries in December 2011. It plans to issue final standards in May 2012, and November 2012, respectively. The agency said the Clean Air Act requires it to set industry-specific standards for new sources that emit significant quantities of harmful pollutants. Source:

<http://wowktv.com/story.cfm?func=viewstory&storyid=91601>

(Louisiana) Outage caused by wire theft. An overnight theft of copper wire December 22, resulted in nearly 4,000 Livingston Parish homes and businesses in Louisiana losing power December 23 a Dixie

UNCLASSIFIED

UNCLASSIFIED

Electric Membership Corporation (DEMCO) official said. The outage affected DEMCO customers in the Watson and Walker areas. The utility system became overloaded and shut down. The theft occurred at the company's Watson substation near the intersection of Louisiana highways 1023 and 1019, a spokesman said. The thieves appeared to have used bolt cutters to enter the fence around the substation, cut the copper from ground wires, and left through some nearby woods, said the Livingston Parish Sheriff's Office spokesperson. It took DEMCO technicians about 4 hours to restore power. Livingston Parish sheriff's detectives were in the initial stages of the investigation, along with the FBI. In August, DEMCO reported thefts from four substations in East Baton Rouge and Livingston parishes. Source: <http://www.theadvocate.com/news/police/112417134.html?c=1293171727243>

FOOD AND AGRICULTURE

(California) Product recalls: beef jerky. About 3,874 pounds of teriyaki beef jerky products have been recalled by Bach CÃ© Beef Jerky, Inc., of South El Monte, California, because they contain an undeclared allergen, wheat, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced. The products have been distributed nationwide. FSIS and the company have received no reports of adverse reactions due to consumption of these products. Source: <http://www.bloomberg.com/news/2010-12-30/product-recalls-beef-jerky.html>

FSIS unveils nutrition labeling rule. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) December 29 unveiled a final rule, Nutrition Labeling of Single-Ingredient Products and Ground or Chopped Meat and Poultry Products. The rule, which has been 10 years in the making, will be published in the Federal Register December 29 and will take effect January 1, 2012. The rule amends federal meat and poultry product regulations to require nutrition labeling of the major cuts of single ingredient, raw meat and poultry products on labels or at point-of-purchase (POP), and to require nutrition labels on all ground or chopped meat and poultry products, with or without added seasonings, unless the products are exempted. Specifically, the rule requires retailers to provide nutrition information for "major" cuts of meat and poultry either on the label or at POP. "Nonmajor" cuts of single-ingredient, raw products are not required to bear nutrition labeling, but if plants or retailers voluntarily provide nutrition information for nonmajor cuts, that information will have to comply with the requirements for the major cuts. Source: <http://www.cattlenetwork.com/FSIS-Unveils-Nutrition-Labeling-Rule/2010-12-29/Article.aspx?oid=1294889&fid=>

(Illinois) CDC: Salmonella outbreak spreads to 16 states. An outbreak of salmonella that was tied to tainted alfalfa sprouts has grown to at least 94 cases in 16 states. The U.S. Centers for Disease Control and Prevention December 28 said the case count had risen from 89 cases in 15 states in the past week, with California joining the list. More than half the cases have been in Illinois. There have been no deaths. The U.S. Food and Drug Administration advised the public not to eat alfalfa sprouts produced by the Tiny Greens Organic Farm in Urbana, Illinois, because of possible salmonella contamination. The warning issued December 27 also includes a mix called spicy sprouts, which contains radish and clover sprouts. Source: http://www.salon.com/food/food_business/?story=/news/feature/2010/12/28/us_sprouts_salmonella

UNCLASSIFIED

UNCLASSIFIED

(Florida) Florida freeze costs farmers \$115M so far. Florida farmers have lost at least \$115 million in this winter's cold blast. And it is not over yet. According to the St. Petersburg Times, reports show the losses through December 20 affected fruits, vegetables, citrus, foliage, and aquaculture. Almost 9,000 acres of farmland was deemed a total loss. A Florida Department of Agriculture spokeswoman said \$115 million is a conservative figure that will likely rise. The report said peppers, squash, endive, eggplant, cucumbers, sweet corn, cabbage, and string beans suffered the worst damage. Strawberries seem to have escaped major harm, but the freeze probably will delay the harvest. Source: <http://www.cbsnews.com/stories/2010/12/29/national/main7194424.shtml>

(Texas) Parsley-cilantro recall expanded to include other vegetables. J&D Produce, Inc., a Texas distributor, has expanded a recall already involving thousands of cases of produce over fears of salmonella cross-contamination in its processing facility, the company said. The company is also recalling 19 other types of produce that were run on the same packing lines, because the salmonella may have spread to those products as well. The case is one of two apparently unrelated outbreaks that have sickened nearly 100 people in the United States and Canada. The company had previously announced the recall of nearly 7,000 cases of cilantro and curly parsley after samples in Quebec, Canada, and Michigan tested positive for the bacteria, the company said December 27. The company's products are sold retail as well as to wholesalers, who may then distribute them to restaurants and other establishments, according to a public relations consultant for the company. The recall involves 2,498 cases of the parsley — which have expiration dates 12 days after being packed — that went out to the Canadian provinces of Quebec and Ontario, and the U.S. states of Connecticut, Massachusetts, Michigan, Missouri, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, Texas, Washington, and Wisconsin. The 4,411 recalled cases of cilantro, carrying the same packing and expiration dates, were distributed in Colorado, Illinois, Massachusetts, Michigan, New Jersey, New York, Ohio, Pennsylvania, Texas, Washington, and Wisconsin, as well as Quebec and Ontario. A complete listing of the other recalled produce will be available on the company's Web site. Source: <http://www.cnn.com/2010/HEALTH/12/29/salmonella.produce/index.html?hpt=T2>

(Texas; Michigan) Salmonella found in U.S., Canada prompts cilantro, parsley recall. J&D Produce, Inc., a Texas produce distributor, has recalled nearly 7,000 cases of cilantro and curly parsley after samples in Quebec, Canada, and Michigan tested positive for salmonella, the company said December 27. The latest recall comes days after dozens of people fell sick after consuming bacteria-tainted alfalfa sprouts in an apparently unrelated situation. The "precautionary, voluntary recall" pertains to cilantro and parsley packed between November 30 and December 6, the Edinburg, Texas-based company said in a statement. Cilantro and parsley processed and branded as Little Bear between those dates can be taken to retailers for a full refund. No one has reported getting sick from eating the vegetables, according to J&D Produce. Source: <http://www.cnn.com/2010/HEALTH/12/28/salmonella.produce/index.html?hpt=T2>

Assessing the risk of intentional contamination. In the United States, DHS is responsible for analyzing risks associated with intentional food contamination and for communicating the threat levels to local governments. As part of this charge, the Food and Drug Administration (FDA), through the Center for Food Safety and Applied Nutrition (CFSAN), has developed a working framework for local and state governments to use as a means to assess potential threats to food. This framework consists of identifying the three components necessary to lead to intentional contamination: the aggressor (whether a disgruntled employee or an agent working for a terrorist organization), the routes of

UNCLASSIFIED

UNCLASSIFIED

gaining access to food, and food-endangering pathogens or poisons. A recent study published in The Journal of Public Health Management Practice developed a standard survey to diagnose the status of food defense in the restaurant industry. Funded by grants from the Centers for Disease Control and Prevention and the FDA, the survey's aim is to identify potential gaps in food defense and also to raise awareness among hospitality industry workers about possible points of vulnerability within their own establishments. Source: <http://www.foodsafetynews.com/2010/12/assessing-the-risk-of-intentional-contamination/>

CDC reports salmonella outbreak affects 15 states. The Centers for Disease Control and Prevention (CDC) announced December 24 it was investigating a multi-state outbreak of salmonella in alfalfa sprouts, with 89 reports of a matching strain across 15 states and the District of Columbia. Preliminary results of the CDC investigation indicate a link to eating alfalfa sprouts at a national sandwich chain, the agency said. The CDC said there were reports of 50 cases in Illinois, 14 in Missouri, and 9 in Indiana. Among the 81 people for whom information was available, the CDC said the start of their illnesses ranged from November 1 to December 14, and ranged in age from 1 to 75 years old, with a median age of 28. Of the information available, the CDC said 23 percent of the people affected were hospitalized, with no deaths reported. The CDC said because the pattern associated with this salmonella type commonly occurred in the U.S., some cases currently identified might not be related to the outbreak. The outbreak first was reported December 17 when the Illinois Department of Public Health (IDPH) reported more than 40 people said they had become ill after eating alfalfa sprouts at Jimmy John's restaurants. The IDPH's update December 23 raised the count to 50 confirmed Illinois residents, and one Wisconsin resident, with reports stretching over 11 counties in the state. The CDC said the investigation was ongoing, and the agency would continue to monitor new cases, along with the Food and Drug Administration, and state and local public health partners. Source: <http://www.nwherald.com/2010/12/23/cdc-reports-salmonella-outbreak-affects-15-states/agxgy43/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Pentagon revamps security in wake of Wikileaks. There are 2.2 million people in the United States with access to one or more levels (confidential, secret, and top secret) of classified information; there are 854,000 people with top secret clearances — of which 265,000 are contractors; the 9/11 Commission recommended more sharing of information among agencies — but critics say too much sharing is as risky as too little sharing. The two massive Wikileaks releases in June and November 2010, as well as threats from the organization to force a major bank executive to resign, shows Wikileaks is far from relenting. This news has brought the U.S. federal government's safeguards and method of data sharing into question. The Department of Defense (DoD) has taken steps to increase security since documents were first disclosed by Wikileaks. They conducted an internal 60-day review of security procedures with recommendations sent to the Secretary of Defense. Some combatant commanders have taken individual measures for their commands. Removable storage media have been restricted or disabled as well as the capability to write or burn removable media on DoD classified computers. This is a temporary technical solution to mitigate future risks of personnel moving classified data to unclassified systems. Source: <http://homelandsecuritynewswire.com/pentagon-revamps-security-wake-wikileaks>

UNCLASSIFIED

UNCLASSIFIED

US says it may evacuate Ivory Coast embassy. The United States has started planning for the possible evacuation of its embassy in Ivory Coast amid concerns postelection violence could escalate into full-blown conflict, the State Department said December 29. A spokesman said a team of eight Pentagon officials is now in Abidjan to weigh options, including evacuating embassy personnel, and to assess the damage caused by an errant rocket-propelled grenade that hit the outer wall of the compound the week of December 20. He said the military team arrived December 28. He also repeated U.S. calls for the Ivory Coast president to step down, and said he should control his supporters. The leader has refused to accept the results of the November 28 election that tallies show he lost to the opposition leader. Shortly after the rocket incident, the State Department ordered non-essential embassy personnel and the families of all American employees to leave Ivory Coast. Source:

<http://www.npr.org/templates/story/story.php?storyId=131937323>

McAfee: Coming cyber threats to target mobile devices, official secrets. The biggest cyber threats in 2011 are expected to include malicious applications on mobile devices and attacks aimed at stealing government secrets and sabotaging business operations, according to McAfee. The computer security firm annually issues a list predicting what will be the biggest cyber scares during the coming year. New for 2011 is the projection that perpetrators will target social media communications on mobile devices — a means of interaction that businesses, including agencies, increasingly depend on for work. The societal shift from desk-based e-mail communications to mobile instant messaging and Twitter insta-blogging has transformed the threat landscape, the report said. McAfee anticipates attackers will hide malicious software in programs that look like legitimate applications, including federal data apps, the study's co-author and McAfee's vice president for threat research said in an interview. According to the threat list, "friendly fire" malware, which appears to come from contacts on social networks, will grow. The motivation of attackers also is changing, according to the study. Instead of carrying out attacks to steal money or to send a political message, some groups, including nation-states and corporations, increasingly are interested in stealing intelligence. Source:

http://www.nextgov.com/nextgov/ng_20101228_6846.php?oref=topnews

FBI: 236 congressional threats in 10 years. At least 236 death threats were made against U.S. congressional members in the past decade, an analysis of cases by Politico revealed. Politico said its review of documents — obtained through the Freedom of Information Act — indicated serious death threats against lawmakers dropped in the past 10 years, along a pattern similar to Congress's overall public approval. "It's interesting that specific events and legislation can trigger death threats," said the vice president and director of governance studies at the Brookings Institution. "The popular image is that these people are crazy, not that they have policy motivations behind their anger. It's interesting to see that connection." The documents indicated death threats investigated by the FBI hit a yearly high of 42 cases in 2001, the same year as the terrorist attacks on the United States and when 56 percent of people approved of the job Congress was doing. Source:

<http://www.investors.com/NewsAndAnalysis/Newsfeed/Article/124090269/201012280826/FBI-236-congressional-threats-in-10-years.aspx>

U.S. says embassy was target of attack. The U.S. Embassy in London was a target of a group of men arrested last week in Britain and charged with conspiracy to cause explosions and preparing acts of terrorism, the U.S. State Department said December 27. Twelve men were arrested December 20 in what British police said were counter-terrorism raids essential to protect the public from the threat of attack. Three were later released without charges, leaving nine who appeared in court December 27

UNCLASSIFIED

UNCLASSIFIED

to face the charges. The suspects were from London, the Welsh capital of Cardiff, and the central English city of Stoke. A British police statement said the men had conspired to cause “explosions of a nature likely to endanger life or cause serious injury to property.” It added they had been downloading material from the Internet, researching and discussing potential targets, carrying out reconnaissance, and “igniting and testing incendiary material.” The police statement did not specify what the potential targets were. Source:

<http://www.thepeterboroughexaminer.com/ArticleDisplay.aspx?e=2906963>

(New York) Bomb threat closes Lockport street. East Avenue in Lockport, New York was closed to traffic for more than 30 minutes December 23 as officers from three local law enforcement agencies searched the department of social services building, 24 East Ave., for a bomb after receiving a phoned-in threat. A report filed by the Lockport Police Department said an “unidentified male voice was laughing and then stated that there was a bomb in the building. He then continued laughing and hung up.” The Lockport Police Department, Niagara County Sheriff’s Department, and New York State Police searched the building with the help of building security. Meanwhile, the Lockport Fire Department was put on standby and stayed near the Ulrich City Center in case they were needed, according to a Lockport detective. The security officer at the social services building said he searched the building with the help of the deputy commissioner of social services. When no bomb was found and police felt it was safe to allow employees to return to work, the building was re-opened, the Lockport detective said. Source: <http://tonawanda-news.com/local/x2018343365/Bomb-threat-closes-Lockport-street>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Old apps can pose privacy risks for Facebook users and their friends. People who own a Facebook account since before April 2010 should remove older apps and install new versions, because they still have unrestricted access to a wealth of information about them and their friends. Back in April, Facebook announced a new data control system where users would be notified at install of how an application needs to interact with their account and information in order to work properly. This allows people to weigh the privacy versus functionality trade-off of certain apps, and was part of the company’s work with the Canadian privacy commissioner. The new permissions dialog became mandatory starting June 1, 2010, but it did not affect the access granted to already installed apps. While Facebook was clear about this aspect with developers, it failed to include it in their announcement to users. Source: <http://news.softpedia.com/news/Old-Apps-Can-Pose-Privacy-Risks-for-Facebook-Users-and-Their-Friends-175370.shtml>

Android mobile malware has botnet-like traits. Hackers are aiming for users of Google’s Android mobile operating system with a malicious application that harvests personal information and sends it to a remote server. The malware, which has been named “Geinimi,” appears to be the first one that has botnet-like capabilities targeted at the Android platform, said the chief technology officer for Lookout Mobile Security, which develops mobile security software. Geinimi appears to target Chinese-speaking users of Android, and Lookout was tipped off to Geinimi after a user wrote a post concerned about it on a forum, he said. Lookout researchers, which posted a writeup on Geinimi, have found it has been wrapped into legitimate free and paid games for Android users with games’ developers unaware their applications were being used as a lure. Those tampered applications are appearing on third-party Web sites offering Android applications that have not been vetted for

UNCLASSIFIED

UNCLASSIFIED

security. Some programs have apparently been downloaded thousands of times. The company is still analyzing Geinimi, and it is not clear what its creators are aiming to do with a victim's phone. Source: http://www.computerworld.com/s/article/9202778/Android_mobile_malware_has_botnet_like_traits

Skype blames buggy Windows software, swamped servers for outage. Skype December 29 blamed the previous week's outage on a combination of overloaded instant messaging servers, buggy software, and the failure of its "supernode" infrastructure. In a lengthy blog entry December 29, Skype's chief information officer provided more details on the outage that kept the instant message, Internet telephone, and video chat service offline for much of December 22 and parts of December 23. Previously, Skype had tapped its supernodes — the systems running Skype that also act as directories — for the outage. He said a bug in an older version of the Windows Skype client was at the root of the failure, although the flaw did not trigger the blackout. The bug in version 5.0.0152 caused Windows clients to crash when they received a delayed response from "a cluster of support servers responsible for offline instant messaging" that had been overloaded, he said. About 50 percent of all Skype users were running the buggy 5.0.0152 version of the Windows client the week of December 20. He did not explain how or why those servers — which triggered the Windows client crashes, and thus, the outage — became unresponsive December 22. When the Windows clients began crashing — at the peak, about 4 out of every 10 copies of version 5.0.0152 failed — they also took down as many as 30 percent of Skype's supernodes, which were also running the problem-plagued edition. The downfall of those supernodes eventually took all the rest offline as well, as users swamped the remaining supernodes with requests after experiencing a crash. Source: http://www.computerworld.com/s/article/9202729/Skype_blames_buggy_Windows_software_swamped_servers_for_outage

PlayStation 3 code signing cracked. Hardware hackers claim to have uncovered the private key used by Sony to authorize code to run on PlayStation 3 systems. The hackers uncovered the hack in order to run Linux or PS3 consoles, irrespective of the version of firmware the game's console was running. By knowing the private key used by Sony, the hackers are able to sign code so a console can boot directly into Linux. Previous approaches to running the open source OS on a game console were firmware specific and involved messing around with USB sticks. The same code-signing technique might also be used to run pirated or counterfeit games on a console. That is not the intention of the hackers even though it might turn out to be the main practical effect of the hack. The group, fail0verflow, who also run the Wii's Homebrew Channel, gave more information about the crack and a demo during the annual Chaos Communication Conference hacker congress in Berlin. Sony's weak implementation of cryptography was exploited by fail0verflow to pull off the hack. Source: http://www.theregister.co.uk/2010/12/30/ps3_jailbreak_hack/

Apple sued over applications giving information to advertisers. Apple Inc., maker of the iPhone and iPad, was accused in a lawsuit of allowing applications for those devices to transmit users' personal information to advertising networks without customers' consent. The complaint, which seeks class action, or group, status, was filed December 23 in federal court in San Jose, California. The suit claims Cupertino, California-based Apple's iPhones and iPads are encoded with identifying devices that allow advertising networks to track what applications users download, how frequently they are used, and for how long. Apple iPhones and iPads are set with a Unique Device Identifier, or UDID, which cannot be blocked by users, according to the complaint. Apple claims it reviews all applications on its App

UNCLASSIFIED

UNCLASSIFIED

Store and does not allow them to transmit user data without customer permission, according to the complaint. Source: <http://www.businessweek.com/news/2010-12-29/apple-sued-over-applications-giving-information-to-advertisers.html>

Geolocation, mobile devices and Apple top the list of emerging threats. McAfee unveiled its 2011 Threat Predictions report, outlining the top threats that researchers at McAfee Labs foresee for the coming year. The list comprises 2010's most buzzed about platforms and services, including Android, iPhone, foursquare, Google TV, and the Mac OS X platform, which are all expected to become major targets for cybercriminals. McAfee also predicts that politically motivated attacks will be on the rise, as more groups are expected to repeat the WikiLeaks paradigm. The report outlines the following top threats: Exploiting Social Media: URL-shortening services; Exploiting Social Media: Geolocation services; Mobile: Usage is rising in the workplace, and so will attacks; Apple: No longer flying under the radar; Applications: Privacy leaks — from your TV; Sophistication Mimics Legitimacy: Your next computer virus could be from a friend; Botnets: The new face of Mergers and Acquisitions; Hacktivism: Following the WikiLeaks path; Advanced Persistent Threats: A whole new category. Source: <http://www.net-security.org/secworld.php?id=10374>

Trojan distributed in new mass injection attack via Java downloader. Security researchers warn a new mass injection attack is underway directing the visitors of hundreds of Web sites to a malicious Java applet which downloads a Trojan. According to the creator of the Unmask Parasites Web scanner, the malicious code is added at the end of HTML pages on compromised Web sites and takes the form of an obfuscated JavaScript function. When parsed by the browser, this function adds a rogue IFrame to the HTML document, which loads a new(dot)htm page from aubreyserr(dot)com, medien-verlag(dot)de or yennicq(dot)be. According to statistics from Google's Safe Browsing service, around 2,000 Web sites link to these domains, giving a rough estimation of the attack's impact so far. The page called by the IFrame loads a Hidden.jar applet deceptively titled "Java Update." This is a Java OpenConnection-type downloader whose only purpose is to download and execute a file called host.exe. Source: <http://news.softpedia.com/news/Trojan-Distributed-in-New-Mass-Injection-Attack-via-Java-Downloader-174971.shtml>

NATIONAL MONUMENTS AND ICONS

(California) Border Patrol investigates beached boat. The U.S. Customs and Border Patrol is investigating an incident December 28 where 8 to 10 people reportedly came ashore at Crystal Cove State Park in Newport Beach, California in a small boat, then shed their life jackets and some clothes as they scattered about the area. As of the late afternoon that day, authorities still were looking for these people. Border patrol officials said the group was aboard a panga boat, a type of open-hulled Mexican fishing boat frequently used in coastal smuggling. About 7 a.m., a visitor at Crystal Cove called police to report the incident. The person said that the boat pulled ashore and people ran in several different directions. Immigration authorities received a report of a second boat seen motoring back southward from the beach minutes after the first boat was found on the sand, a Border Patrol spokesman said. An Orange County Sheriff Harbor Patrol boat and helicopter converged on the area but did not find anyone, a sheriff's department lieutenant said. The incident is part of a new trend authorities are seeing in human and drug smuggling from Mexico and points farther south, a representative of San Diego County's Immigration and Customs Enforcement office said. Source: <http://www.dailypilot.com/news/tn-dpt-1229-boat-20101228,0,6280813.story>

UNCLASSIFIED

UNCLASSIFIED

(Utah) Reward offered for suspect who shot park ranger. On December 23, the FBI Salt Lake City Division, the United States Marshals Service, and the Utah Department of Natural Resources announced a reward of up to \$30,000 for information leading to the apprehension and/or recovery of the person who shot a Utah State Parks Ranger. Each agency is contributing up to \$10,000 toward the \$30,000 reward offer. The public is asked to contact the Grand County Sheriff's Office with tips about the case. The shooting happened November 19 southwest of Moab. Several law enforcement agencies responded and assisted the Grand County Sheriff's Office in its search for the suspect. He remains at-large and should be considered armed and dangerous. A state arrest warrant has been issued for the suspect. According to the warrant, filed in the Seventh District Court for the State of Utah, the suspect shot the ranger multiple times. He faces one count of attempted aggravated murder, a first degree felony. On the wanted poster issued by the Grand County Sheriff's Office, the suspect is described as 6 feet one inch tall, weighing 165 pounds, with long black hair and hazel eyes. His date of birth is April 30, 1970. Source: <http://stgnews.com/archive/485>

POSTAL AND SHIPPING

Cargo that flies over the United States doesn't get screened to federal standards. As the Presidential Administration works to harden domestic defenses against terrorism, some experts point to a potential vulnerability from thousands of flights that pass over the United States each week. Although the United States regulates overflights, the cargo aboard them is not screened to federal standards and passenger lists are not matched to names on the terrorist watch list maintained by the Transportation Security Administration (TSA). The TSA said other countries "have their own cargo security protocols that apply to those aircraft." The TSA has not implemented the new Secure Flight program to scrutinize passengers boarding overflights. That behind-the-scenes operation is designed to ferret out potential terrorists through a process that begins with airlines collecting detailed information when someone buys a ticket. Security experts are divided about the severity of the risk. Scanning all the cargo that flies over the country "is totally unrealistic," said the director of the Center for Transportation and Logistics at Massachusetts Institute of Technology. "We have tens of millions of packages flying almost every night. We can't stop the huge flow of packages from all over the world. There has to be a balance between acceptable risk and the economy." But a longtime U.S. intelligence operative who teaches counterterrorism courses at Embry-Riddle Aeronautical University in Arizona said a terrorist could "explode a plane with a dirty bomb or a biological weapon or an actual nuclear weapon on board, and that material will spread wherever it crashes." Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/26/AR2010122601795.html>

PUBLIC HEALTH

Arrow Intra-Aortic Balloon (IAB) catheter products: Class 1 recall - catheters can become stuck in the sheath. The Arrow Ultra 8 Intra-Aortic Balloon Catheters (IABS) 8 FR 30CC and 40CC Universal and Arrow Intra-Aortic Balloon (IAB) Catheter with a Fiber Optic Sensor and a Measurement System were recalled by the U.S. Food and Drug Administration because the catheters can become stuck in the sheath. When the IAB catheter becomes stuck, the user is unable to move it forward or backward, causing delay in therapy, bleeding, or arterial injury. The Arrow IAB products are used in the treatment of a variety of cardiac conditions, including heart failure, septic shock, and myocardial

UNCLASSIFIED

UNCLASSIFIED

infarction. They are also used to support and stabilize high-risk patients undergoing diagnostic and non-surgical procedures. Source:

<http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm238408.htm>

FDA recalls glucose test strips sent to military hospitals. Military medical officials in the Pacific are trying to reach some 700 patients who might be using faulty glucose test strips to measure their blood sugar levels. Abbott Diabetes Care glucose test strips sent by the Defense Department to hospitals in the Pacific were among the 359 million strips identified in a recall announced December 22 by the U.S. Food and Drug Administration (FDA). About 200 patients at U.S. Naval Hospital Yokosuka clinics, 457 patients at Okinawa bases, and 47 patients at Misawa Air Base were among those affected by the recall, officials said December 28. The hospitals are calling patients and distributing recall information. The recall was issued after results showed that the strips might report inaccurately low blood glucose levels, according to the FDA. "False results may lead patients to try to raise their blood glucose unnecessarily, or they may fail to treat elevated blood glucose because of a false, low reading," according to the FDA statement. "Both scenarios pose risks to a patient's health." The recall affects Abbott's Precision Xtra, Precision Xceed Pro, MediSense Optium, Optium, Optium EZ, and ReliOn Ultima blood glucose strips. Source: <http://www.stripes.com/news/fda-recalls-glucose-test-strips-sent-to-military-hospitals-1.130109>

Global flu warning after UK hit. Northern hemisphere countries are being told by health experts to brace themselves for flu outbreaks. There has been a well-publicized surge of cases in the United Kingdom during December with swine flu appearing to be the dominant of the three strains circulating. The European Center for Disease Prevention and Control warned much of the rest of Europe was also beginning to see increases too. Meanwhile, parts of the United States and Canada have reported higher levels. Many of those being infected are younger age groups. In the United Kingdom, the number of people who have died with all types of flu this winter hit 27. The volume of patients going to their doctor with flu-like illnesses also rose, more than doubling to 87.1 per 100,000 in the week of December 20-24. Cases have been highest in children aged between 5 and 14, followed by children under 4 and then those aged between 15 and 44. But the UK's Health Protection Agency said a very large outbreak was "not likely". Source: <http://www.bbc.co.uk/news/health-12074786>

U.S. facing largest hospital drug shortage in decades. Many hospital patients are being turned away for potentially life-saving injection treatments in what may be the largest U.S. hospital drug shortage in over two decades. Most drugs in short supply are known as injectables and include sedation medication such as propofol, the popular blood thinner heparin, and hard-hitting chemotherapy drugs like doxorubicin. Limited manufacturing, lagging production time, and lack of profits from these drugs are contributing to the shortage, according to an August 2010 editorial published in the New England Journal of Medicine. The production cost outweighs the profits for some companies. Since many firms would rather produce cheaper generic drugs, manufacturers are shunning some costly brands. Doctors at local hospitals are frustrated and many times they are not even informed of the shortage, according to survey results released in September by the Institute for Safe Medication Practices. Of those surveyed, 85 percent said they were given little to no information on how long the shortages would last. And since these medications are mainly housed in hospitals, most patients will not know it might not be available until they really need it. Some medications in short supply offer an

UNCLASSIFIED

UNCLASSIFIED

equivalent substitute, but in some cases insurance companies do not reimburse patients for the substituted therapies. Source:

<http://abcnews.go.com/Health/CancerPreventionAndTreatment/largest-hospital-drug-shortage-decades/story?id=12452389&page=1>

TRANSPORTATION

Northeast blizzard could cost airlines \$150 million. The blizzard that shook the Northeastern United States and put a halt to air travel in the region could cost the airline industry close to \$150 million, reports USA Today. Some industry experts, however, said it is too soon to assign a price tag. Analysts predicted cancellations and delays caused by the December 26 storm could continue for several days as airlines tried to rebook and regroup. According to the Federal Aviation Administration, more than 6,000 flights were canceled as a result of the storm. Airports in and around New York City were the hardest hit. Source: <http://www.670kboi.com/rssItem.asp?feedid=114&itemid=29614974>

U.S. proposes new rest rules for truckers. The Presidential Administration favors giving truckers more rest, but for now is leaving open the question of whether drivers should spend fewer hours each day behind the wheel. The Transportation Department December 23 proposed a new rule designed to end a years-long effort to rewrite driver rules for the first time in more than 60 years. “We are committed to an hours-of-service rule that will help create an environment where commercial truck drivers are rested, alert and focused on safety while on the job,” the Transportation Secretary said in a statement. The trucking industry, represented by the American Trucking Associations trade group, said the planned changes were too complex, would reduce industry productivity, and would be “enormously expensive for trucking and the economy.” Some large firms covered by the rule include FedEx Corp, UPS Inc, and YRC Worldwide. Trucking companies are concerned any reduction in hours would drive up costs. A central point of contention revolves around the maximum time a driver can spend behind the wheel each day and the length of “off duty” time. The current rule allows a daily driving maximum of 11 hours, and a 34-hour gap between the end of one week and the start of another. The Transportation Department favors a 10-hour daily limit, but sought public comment on whether 11 would be acceptable if other rest requirements were in place. The work day could not exceed 14 hours, which includes a 1-hour break. Source: <http://www.reuters.com/article/idUSTRE6BM3Z720101223>

Can trains, subways be protected from terrorists? The government’s top security officials said they are upgrading subway and rail defenses against terrorist attacks throughout the country, but a USA TODAY examination finds gaping holes, including many that may not be possible to plug. The holes in security leave travelers more vulnerable on the more than 4 billion trips they take by subway and rail each year than in the sky, where airlines carried fewer than 700 million passengers from U.S. airports last year. Six terrorist plots targeting U.S. subway and rail systems have been exposed since the September 11th attacks, and the systems remain a target, transit authorities, security expert, and members of Congress agree. They noted that about 15 million passengers board subway cars and trains unscreened each weekday. “Mass transit systems are much less secure than the aviation sector or certain key government buildings,” said DHS’s former inspector general. Source: http://www.usatoday.com/money/industries/travel/2010-12-27-railsecurity27_CV_N.htm

UNCLASSIFIED

UNCLASSIFIED

Napolitano: New TSA methods ‘objectively safer’. The Homeland Security Secretary is not giving any ground when it comes to the use of full-body scanners and pat-downs at airports around the United States. While some travelers do not like them, the Secretary in an interview broadcast December 26 insisted the practices will not change for the “foreseeable future.” The new technology and the pat-downs are “objectively safer for our traveling public,” the Secretary said, adding she is always looking to improve the security systems in place. The Secretary also dismissed a recent news report about major airports failing secret tests designed to get contraband such as guns and knives past security screeners. The report said some airports had a 70 percent failure rate. “Many of them are very old and out of date, and there were all kinds of methodology issues with them. Let’s set those aside,” she said on “State of the Union” on CNN. “We pick up more contraband with the new procedures and the new machinery.” Source: <http://www.cbsnews.com/stories/2010/12/27/politics/main7188394.shtml>

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 ; 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, 701-328-8168



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED