



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

Nothing Significant to Report

REGIONAL

(Wyoming; Montana) Wyoming cow found with brucellosis. The Wyoming Livestock Board announced February 9 it had received notice from animal health officials in Montana that a Wyoming cow at a Montana auction had serological evidence of brucellosis. The adult beef cow was from a ranch in Park County. State animal health officials are investigating the case, and making plans for further testing of the cow, as well as the herd she was from. Source:

<http://www.wyomingbusinessreport.com/article.asp?id=56010>

(Montana) Backcountry avalanche warning in effect for Bozeman area mountains. A backcountry avalanche warning was issued February 7 for the Bridger and northern Gallatin Range and the mountains outside Cooke City, Montana, according to the Gallatin National Forest Avalanche Center (GNFAC). "Heavy snowfall since Saturday has been deposited on a weak snowpack. Strong winds at all elevations are loading slopes further. Continued and intense snow through tonight will create very unstable conditions through February 8," according to a GNFAC news release. The avalanche danger is rated high on all slopes with dangerous avalanche conditions in these ranges. Travel in avalanche terrain is not recommended, and avalanche runout zones should be avoided. The warning will either terminate or be updated by 6:30 a.m. February 9. Source: <http://www.kbzk.com/news/backcountry-avalanche-warning-in-effect-for-bozeman-area-mountains/>

(Montana) Man arrested after alleged threats at Bozeman hospital. Law enforcement checked out reports of a man with a gun who was threatening to harm someone at Bozeman Deaconess Emergency Room in Bozeman, Montana, February 7. Officers took a man in a wheelchair out and put him in a police car at around 7:30 p.m. A Bozeman police sergeant said the man has been arrested on a disorderly conduct charge, plus criminal mischief charges for allegedly damaging some fire sprinklers at the detention center after he was taken in from the hospital. There may be more charges filed. According to officers, they were called out on a male who had gone to the emergency room with a gun threatening to harm people. Police said it appears the man had been in possession of a firearm earlier and the investigation is continuing. No firearm was found on him when he was arrested, but he did have ammunition on him. Officers from the Bozeman Police Department, Gallatin County Sheriff's Department, and Montana State University Police responded. Source:

<http://www.kaj18.com/news/man-arrested-after-alleged-threats-at-bozeman-hospital/>

NATIONAL

Military radar sought for northern drug crackdown. U.S. Senators from states along and near the nation's northern border requested February 10 that the Department of Defense provide military

UNCLASSIFIED

radar to crack down on drug trafficking by low-flying aircraft. Drug smuggling across the border with Canada is much more prevalent than indicated by the number of cases where drugs have been seized, according to a federal report from November 2010 and recent media stories, a New York Senator said. Less than 1 percent of the 4,000 mile border is considered under the operational control of U.S. border officials, according to a General Accountability Office (GAO) report released in February. Most areas of the northern border are remote and inaccessible by traditional patrol methods. Customs and Border Protection believes it can detect illegal entries, respond, and deal with them on only about 32 miles of the northern border. The Border Patrol was aware of all illegal border crossings on only 25 percent of the border, or 1,000 out of 4,000 miles, the GAO report said. Source: http://www.forbes.com/feeds/ap/2011/02/10/general-us-border-security-northern-border_8301578.html

UCI: ‘Green’ LED bulbs full of lead, arsenic. The LED bulbs sold as safe and eco-friendly can contain high levels of lead, arsenic, and other hazardous substances, a new University of California, Irvine (UCI) study showed — the same bulbs widely used in headlights, traffic lights, even holiday lights. The toxic material could increase the risk of cancer, kidney disease, and other illnesses, although the risks are more long-term than immediate; a single exposure to a broken bulb is unlikely to cause illness. “I wouldn’t worry about an immediate release of vapor,” said a UCI public health and social ecology professor, the principal investigator and an author of the study. “But still, when these residues hang around the house, if not cleaned up properly they could constitute an eventual danger.” The lights should be treated as hazardous materials, and should not be disposed of in regular landfill trash, he said, because of the risk of the materials leaching into soil and groundwater. Source: <http://www.oregister.com/news/bulbs-287781-ogunseitan-lights.html>

‘Rude awakening’ for central U.S.: 2 blizzards in a week. A second powerful blizzard in a week roared through parts of the nation’s midsection February 9, bringing biting winds and dumping up to 2 feet of snow on areas still digging out from last week’s major storm. As the system barreled through the Plains toward the Deep South, it blanketed parts of northeastern Oklahoma and northwestern Arkansas. At least two traffic deaths were blamed on the system. And more than 1,200 flights were canceled, the tracking service FlightAware(dot)com said. In South Dakota, a 50-mile section of Interstate 29 north from Watertown was closed down overnight from February 8 into February 9 because snowdrifts blocked a section where up to 200 vehicles had been stranded last week, officials said. Source: <http://www.msnbc.msn.com/id/41486321/ns/today-weather/>

INTERNATIONAL

Coyotes endangering airport’s runways. The airport at Canada’s oil patch capital in Calgary, Alberta, is being plagued by roaming coyotes that threaten landing and take-off safety, regulators said. Since June, airport officials have filed 26 incident reports of the feral coyotes straying onto runways and prompting diversionary measures. This year alone, there have been four incidents, the Calgary Sun reported. A federal transportation safety board spokesman told the newspaper a 30-pound coyote was capable of doing “significant damage” to large aircraft. The airport’s director of environmental service said attempts in Calgary and other airports to devise coyote-proof fences did not work, so his staff patrols the entire perimeter four times a day. He said a backhoe smashes coyote dens and holes under the fences are filled. However, the director said having some coyotes around is actually a

UNCLASSIFIED

UNCLASSIFIED

benefit, as they help kill rabbits that attract large birds of prey, also a deadly danger to aircraft, the report said. Source: http://www.upi.com/Top_News/World-News/2011/02/09/Coyotes-endangering-airports-runways/UPI-45721297255241/

Thieves dig tunnel to steal water treatment gear. Thieves in Hamilton City, New Zealand, dug a tunnel under concrete to steal tens of thousands of dollars worth of equipment from the Hamilton City Council's water treatment plant. The city deployment manager said thieves cut through a neighboring fence and dug a tunnel under concrete to get past an electrified security fence as they broke into the plant to steal 10 bronze water pump impellers. "I'm not going to go into other security arrangements in place at the plant other than to say they were more than adequate. This appears to have been a professional burglary that was well planned," she said. Two of the larger impellers, valued at \$60-80,000, were taken, while three medium and five smaller devices were missing as well as the castings. She said the water pump impellers were very distinctive and were only used in the specific pumps operated by the city council. "To that end we're not ruling out the items may have been stolen for scrap metal value so we are liaising with scrap metal dealers not only in Hamilton but across the country." While the theft of such specialized equipment was a disappointment, the city council's general manager of works and services said the loss had not affected their ability to deliver high quality water to the city. Source: <http://tvnz.co.nz/national-news/thieves-dig-tunnel-steal-water-treatment-gear-4018714>

Mexico pipeline thieves trigger big fuel spill. Thieves tapping into a Mexican fuel pipeline triggered a large diesel fuel spill south of the border city of Tijuana in Baja California state February 9, authorities said. A senior source at the state emergencies agency, which has dealt with a number of fuel spills in recent years due to criminal activity, described the incident as serious. "There cannot be less than 50,000 liters (13,000 gallons) spilled," the official said. "We've never seen anything like this." A Reuters witness saw a 3-foot stream of fuel flowing on hilly ranch land a few miles from Rosarito, Mexico. Police prevented people from approaching the pipeline but bulldozers could be seen working to build huge piles of earth to contain and absorb the flow of fuel. The odor of petroleum was strong. Gangs of fuel thieves regularly tap into Pemex pipelines to steal gasoline, diesel fuel, and even crude oil. The lucrative trade has attracted Mexico's drug cartels, which earn money protecting fuel thieves and helping them smuggle oil out of the country. State oil monopoly Pemex said in a press release it was responding to the spill and that it posed no risk to bodies of waters or urban areas. The 10-inch diameter pipeline carries fuel from a Pemex terminal in Rosarito to the city of Mexicali. Source: http://news.yahoo.com/s/nm/20110209/wl_nm/us_mexico_oil_spill

Australian terrorist threat to airports. A group of Australians who are believed to be at terrorist training camps in Yemen pose a threat to airport security in Australia, a security expert has warned. ABC Television's Foreign Correspondent has reported that 22 Australians have gone missing in Yemen and are believed to be at al-Qaeda training camps. Heading up the al-Qaeda regime in Yemen is an American citizen. The suspect has been allegedly involved in a number of terrorist attacks and in his Internet sermons — delivered in perfect English — he preaches contempt for non-believers. The 22 Australians are believed to be receiving training at these camps where their value is their Australian passports and the access they can gain with them. "The authorities know who these people are," the homeland security asia pacific director said. All people who work in airports should be briefed on terrorist threats, according to the director of homeland security. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.theaustralian.com.au/news/breaking-news/australian-terrorist-threat-to-airports/story-fn3dxity-1226002550567>

Pirates hijack U.S.-bound oil tanker off Oman. Armed pirates seized a U.S.-bound oil tanker off Oman carrying around \$200 million worth of crude February 9 in one of the biggest raids in the area to date, escalating the threat to vital shipping lanes. The 333-meter crude carrier, the Irene SL, was carrying about 2 million barrels of crude oil, estimated to be nearly 20 percent of daily U.S. crude imports, a day after an Italian tanker was snatched by Somali pirates. A spokeswoman for the multinational Combined Maritime Forces fighting piracy in the area, said the tanker was hijacked 220 nautical miles off Oman and was likely attacked by Somali pirates. Ship industry associations have warned that more than 40 percent of the world's seaborne oil supply passing through the Gulf of Aden and the Arabian Sea was at high risk from well-equipped Somali pirates, who are able to operate ever further out at sea and for longer periods using mother ships. Source: <http://www.baltimoresun.com/sns-rt-international-us-omatre7182q2-20110209,0,5572781.story>

Sri Lanka: Over one million affected in further wave of deadly flooding. Another wave of severe flooding has wreaked havoc in the Eastern, North and North Central Provinces of Sri Lanka where heavy monsoon rains have caused 11 deaths and affected more than 1.2 million people. During the first week of February, more than 2,000 people were displaced in Dutuwewa, after a dam in the Kiwulkadawela tank in Polonnaruwa burst, unleashing 55,000 cubic acres of water. Coconut trees in the area were uprooted by the water gushing from the broken dam. By February 6, almost 250,000 people had been displaced from their homes. Families are being housed in more than 600 temporary evacuation centers established by the government in 11 districts across the island. Since December, heavy and persistent rains have deluged roads, agricultural lands and towns. So far 18 of Sri Lanka's 25 districts have been affected by what some are calling the worst floods that the country has experienced in the past 100 years. Several major tanks (reservoirs) have overflowed causing extensive flooding of downstream villages with over 8,000 homes reportedly damaged or destroyed. Source: <http://www.reliefweb.int/rw/rwb.nsf/db900sid/EDIS-8DUL8D?OpenDocument>

Police comb Moscow railway stations for explosives. Moscow, Russia police February 6 were combing city's nine railway stations for explosives after receiving a telephoned bomb threat 2 weeks after a suicide bomber killed 36 people at a Moscow airport. AFP reported an unidentified man called police saying bombs had been laid at three of Moscow's nine railway stations and they would soon go off, a transport police spokeswoman said. She said police were also searching the other six stations for explosives. Moscow has been on edge since a suicide bomber wreaked carnage at its biggest airport Domodedovo killing 36 and wounding more than 150 January 24, the second bombing attack with heavy casualties in the capital in less than a year. Authorities called on Muscovites to be vigilant and Agapova said transport police had been receiving bomb threats nearly daily in the past 2 weeks. But February 6 was the first time since the airport attack that police had to check all nine railway stations simultaneously, the spokeswoman said. Source: <http://www.eturbonews.com/20982/police-comb-moscow-railway-stations-explosives>

BANKING AND FINANCE INDUSTRY

Credit score checking app triggers Trojan download. The main reason people get scammed and/or their computer infected online is because they can not contain their curiosity, and that is precisely

UNCLASSIFIED

UNCLASSIFIED

the thing on which the peddlers of a small application for checking credit scores and criminals records of Brazilian citizens count on. The application is offered for download on a public forum and is simple — it only presents the information harvested from public sites in a tidy manner: But unbeknownst to the user, the application also downloads a banking Trojan. That is why, Trend Micro researchers said, users should always keep in mind that a certain level of trust should be involved when it comes to installing and utilizing applications, and that they should download and install software only from verified sources. Source: http://www.net-security.org/malware_news.php?id=1628

Credit crunch pushes US ID fraud to 8 year low. U.S. identity fraud losses fell sharply in 2010, bucking a long-running trend. The number of fraud victims decreased 28 percent in 2010 from 11 million to 8.1 million. The total value of fraudulent losses also fell from \$56 billion in 2009 to \$37 billion in 2010, according to an annual study by Javelin Strategy & Research. Javelin reports the figures for losses are the lowest it has seen in the 8 years it has run the study. The average fraudulent losses per victim also declined from \$5,000 in 2009 to \$4,600 in 2010. Javelin reckons a significant drop in reported data breaches goes some way toward explaining the decline in identity fraud. More stringent checks by lenders to “authenticate users and determine credit risk” as well as improved consumer awareness of ID fraud risks and the use of account monitoring tools, are also credited in the decline. “Economic conditions also appear to have contributed to this year-over-year decline, as well as increased security measures and some significant law enforcement successes,” the president and founder of Javelin said. Source: http://www.theregister.co.uk/2011/02/09/id_fraud_slump/

Zeus development might continue as source code offered for sale. The source code of the Zeus banking trojan is being offered for sale on the underground market suggesting the malware might continue to be developed independently from SpyEye. Security researchers from Trend Micro found some of the first versions of the new SpyEye which borrows several components from Zeus, earlier in February. An independent security reporter, revealed the week of January 30 that the source of the Zeus crimeware toolkit is being offered for sale by someone calling themselves “nem” on an underground trading forum. “Full Zeus Source code of last v2.0.8.9 (includes everything). Requires MSVC++ 2010. You can create your own HWID licenses and much more,” the sales pitch reads. Looking at the seller’s forum stats it appears he is a member since mid-2009 and has a very good reputation, which makes it likely the offer is legitimate. The price is not shown and is probably up for negotiation. Source: <http://news.softpedia.com/news/ZeuS-Development-Might-Continue-as-Source-Code-Offered-for-Sale-182791.shtml>

Russian hacker steals \$10 million. A 27-year old Russian hacker pleaded guilty to stealing \$10 million from a former Royal Bank of Scotland division back in 2008, and he’s awaiting a verdict and sentencing at the end of this week or at the beginning of the week of February 14. The trial is being held in Novosibirsk in Siberia, and the man has admitted that he was part of the international hacking ring that executed the cyber heist. According to Reuters, the ring hacked into the accounts of the bank’s customers, raised the limit that regulated the maximum withdrawal of funds that could be executed in one day, and organized a simultaneous withdrawal of the funds from ATMs located in Europe, the United States, and Asia. Source: <http://www.net-security.org/secworld.php?id=10543>

(New York) Nasdaq hackers reportedly penetrated computer network multiple times. Hackers broke into a Nasdaq service that handles confidential communications for about 300 corporations, the company said February 5 — the latest vulnerability exposed in the computer systems Wall Street

UNCLASSIFIED

UNCLASSIFIED

depends on. The intrusions did not affect Nasdaq's stock trading systems, and no customer data was compromised, Nasdaq OMX Group Inc. said. Nasdaq is the largest electronic securities trading market in the United States, with more than 2,800 listed companies. A federal official told Associated Press the hackers broke into the service repeatedly over a period of more than 1 year. Investigators are trying to identify the hackers, the official said. The FBI and Secret Service are investigating. The targeted service, Directors Desk, helps companies share documents with directors between scheduled board meetings. It also allows online discussions and Web conferencing within a board. Since board directors have access to information at the highest level of a company, penetrating the service could be of great value for insider trading. A Nasdaq OMX spokesman said the Justice Department had requested the company keep silent about the intrusion until at least February 14. However, the Wall Street Journal reported the investigation on its Web site February 4, prompting Nasdaq to issue a statement and notify its customers. Source:

http://www.huffingtonpost.com/2011/02/05/nasdaq-hackers-reportedly_n_819068.html

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Japan, U.S. plan nuclear counterterrorism 'road map'. Japan and the United States are preparing a "road map" for cooperative efforts to prevent atomic site workers from stealing potential ingredients for an act of nuclear terrorism, a top White House counterterrorism official told Kyodo News February 4. The plan would address the development of "security-by-design concepts" for facilities such as nuclear energy stations and atomic fuel processing sites, said the National Security Council senior director for WMD terrorism and threat reduction. The blueprint is slated for completion ahead of the second Global Nuclear Security Summit, slated to take place in Seoul in 2012. Source:

http://www.globalsecuritynewswire.org/gsn/nw_20110207_5734.php

(New Jersey) Pa. man brings pistol, hollow-point bullets to Oyster Creek power plant. Authorities in New Jersey said a Pennsylvania man had a pistol and hollow-point bullets when he drove through the front gate of the nation's oldest nuclear power plant. Lacey Township police said the suspect was visiting the Oyster Creek nuclear plant on business. A police official told the Asbury Park Press that security personnel found a loaded .32-caliber pistol and hollow-point bullets while inspecting the vehicle. The police official said the man's gun permit had expired. The man was charged with unlawful possession of a weapon, and possession of hollow-point bullets. Source:

http://www.nj.com/news/index.ssf/2011/02/pa_man_brings_pistol_hollow-po.html

(Texas) West Texas facility ready for nuclear waste. A new landfill in West Texas is allowed to accept radioactive waste from 36 other states, and a Dallas, Texas, billionaire is behind the project. But opponents worry about the long-term effects of burying low-level radioactive waste in the Lone Star State. If there is such a thing as a "good" place to build a massive radioactive waste landfill, it might be 30 miles outside of Andrews, Texas. This comes pretty close to the middle of nowhere. "It's a very safe facility, and it should last for tens of thousands of years," the president of Waste Control Specialists said. Opponents of burying nuclear waste in Texas point out that this a long time to keep a promise. In January, the Texas commission regulating radioactive material voted to let the site accept low-level waste shipped in from 36 states. Source: <http://www.wfaa.com/news/texas-news/West-Texas-facility-ready-for-nuclear-waste-115543929.html>

UNCLASSIFIED

COMMERCIAL FACILITIES

(Oregon) Van slams into Tualatin gas station, driver claims bomb. A man drove a van into a Shell gas station at I-5 and Nyberg Road in Tualatin, Oregon, February 7, and told police there was a bomb in his rig. The Portland Police Bureau sent a bomb squad but found nothing. The man, 33, of Lakewood, Washington, was arrested and held on accusations of criminal mischief, reckless endangerment, and DUI, a Tualatin police lieutenant said. He said alcohol and other drugs may be a factor in the incident. The gas station at 7090 Nyberg Road reopened several hours after the incident. The mostly glass storefront in the market area had been shattered. Source: <http://www.kgw.com/news/Van-slams-into-Tualatin-gas-station-driver-claims-bomb-115557069.html>

(New York) Harsh winter triggers New York City manhole explosions. Record snowfall is turning the New York City's mean streets even meaner, with 65 manholes exploding or catching fire since January 1, a utility spokesman said February 4. In the most recent serious case, a fireball erupting from a manhole in Brooklyn engulfed an SUV that had been parked over the opening moments before. It was one of three explosions on the same block that day. On New Years Day, a manhole blew in Manhattan's West Village, sending a 15-foot column of flames into the air. On January 3, a pair of East Harlem manhole fires spiked carbon monoxide levels at the Shield Institute, a center for people with developmental disabilities, forcing an evacuation, and closing several blocks. About 75 handicapped clients waited it out on buses before being transferred to another facility. On January 18, manhole fires forces evacuations of homes in Queens, Brooklyn, and the Bronx. Consolidated Edison (ConEd), which supplies power to the five boroughs of New York City and Westchester, pointed to a mix of salt, spread on the roads during storms, and melting snow or ice as the culprit. When salty water contacts a corroded cable or underground utility box, fire or explosion can result. "There's a direct correlation between the volume that goes onto the city streets and these incidents," a ConEd spokesman said. ConEd said it is converting some of its 264,000 manhole covers, currently solid, to vented ones, so gasses can escape and pressure is lessened. Source: <http://www.reuters.com/article/2011/02/04/us-weather-manholes-idUSTRE71374I20110204>

COMMUNICATIONS SECTOR

Cellphone security threats rise sharply: McAfee. In its fourth-quarter threat report, released February 8, McAfee said the number of pieces of new cellphone malware it found in 2010 rose 46 percent over 2009's level. "As more users access the Internet from an ever-expanding pool of devices — computer, tablet, smartphone or Internet TV — Web-based threats will continue to grow in size and sophistication," the report said. McAfree attributed the trend to Adobe's greater popularity in mobile devices and non-Microsoft environments, coupled with the ongoing widespread use of PDF document files to convey malware. Source: <http://www.reuters.com/article/2011/02/08/us-security-mobile-idUSTRE7170LO20110208>

iPhone attack reveals passwords in six minutes. Researchers in Germany say they have been able to reveal passwords stored in a locked iPhone in just 6 minutes and they did it without cracking the phone's passcode. The attack, which requires possession of the phone, targets keychain, Apple's password management system. Passwords for networks and corporate information systems can be revealed if an iPhone or iPad is lost or stolen, said the researchers at the state-sponsored Fraunhofer

UNCLASSIFIED

Institute Secure Information Technology. It is based on existing exploits that provide access to large parts of the iOS file system even if a device is locked. The attack works because the cryptographic key on current iOS devices is based on material available within the device and is independent of the passcode, the researchers said. This means attackers with access to the phone can create the key from the phone in their possession without having to hack the encrypted and secret passcode. Using the attack, researchers were able to access and decrypt passwords in the keychain, but not passwords in other protection classes. Source:

http://www.computerworld.com/s/article/9208920/IPhone_attack_reveals_passwords_in_six_minutes

Copper prices and incidences of copper theft rise. From Hawaii to Florida, copper thieves have electrocuted themselves and caused electrical and telephone failures and street light blackouts. Many municipalities, which have been hard hit by budget deficits, have been unable to afford repairs. "We believe this is a national security issue," said the executive director of the Coalition Against Copper Theft, an advocacy group in Washington D.C. that includes telecommunications firms, power companies, and railroads. "The only thing keeping it from being an epidemic is that scrap yards are now scrutinizing the material. But theft is still rampant." Copper is near an all-time high, which has translated into \$4-per-pound prices for scrap copper at salvage yards. The price in 2009 was about \$1.25 per pound. "If you watch the price of copper, you notice a correlation between the price and the rate of theft," said the security director for Frontier Communications, which has seen an increase in thefts of its power and broadband lines in the 27 states it serves. Last month, the FBI said it was planning to update a 2008 report that called theft of copper wire a threat to the nation's "critical infrastructure." The American Electrical Power Company in Ohio said it had begun to replace its copper wire with wire that contains less copper and is also more difficult to cut through. The company has also put up signs letting prospective thieves know the new brand of wire is not worth stealing. Source: <http://www.nytimes.com/2011/02/08/us/08theft.html>

G broadband may jam GPS. The GPS industry warned that a proposed broadband Internet network could effectively jam GPS signals. Further, it said it has data showing that any of the anticipated 40,000 transmitters can make a Garmin 430 go dark at a range of 5 miles. GPS World calls the proposal by LightSquared "disastrous" and warns of major problems for all kinds of GPS-reliant devices. The publication said a study by GPS-industry stakeholders, including Garmin, determined the LightSquared network "will create a disastrous interference problem for GPS receiver operation to the point where GPS receivers will cease to operate (complete loss of fix) when in the vicinity of these transmitters." That, says the report, "will deny GPS service over vast areas of the United States." The industry told the Federal Communications Commission (FCC) of the potential problem but the FCC approved the multibillion-dollar effort, which will carry 4G broadband throughout the country. Source: http://www.avweb.com/avwebflash/news/4G_Broadband_May_Jam_GPS_204069-1.html?

F.C.C. to propose expanding broadband service to underserved areas. The Federal Communications Commission (FCC) February 8 will propose the first steps toward converting the \$8 billion fund that subsidizes rural telephone service into one for helping pay to provide broadband Internet service to underserved areas, according to commission officials. The chairman of the FCC was expected to call for a consolidation of existing methods of supporting rural phone service into a new pool of funds. The chairman was expected to outline the proposal in a February 7 speech. Most of the money under

UNCLASSIFIED

UNCLASSIFIED

discussion involves a longstanding subsidy known as the Universal Service Fund, which is paid for through fees tacked onto most consumers' phone bills and distributed among telephone companies to subsidize the high costs of providing service to rural areas. The chairman will propose phasing out the payments between phone companies, which he said create "inefficiencies and perverse incentives" that result in waste in the fund. The FCC will also propose consolidating existing methods of paying for rural phone service into a new pool to be called the Connect America Fund, to be used for helping pay for making broadband available to underserved areas. Source:

http://www.nytimes.com/2011/02/07/business/07fcc.html?_r=1&partner=rss&emc=rss

CRITICAL MANUFACTURING

AmerTac recalls night lights due to fire and burn hazard. American Tack and Hardware Co. Inc. (AmerTac) of Saddle River, New Jersey, issued a recall February 9 for about 261,000 LED night lights. An electrical short circuit in the night light can cause it to overheat and smolder or melt, which can burn consumers or result in fire. AmerTac has received 18 reports of the night lights smoking, burning, melting, and/or charring, including 3 reports of minor property damage and 1 of a minor burn injury. The night lights were sold at hardware stores, lighting showrooms, and home centers nationwide from March 2009 through January 2011. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml11/11123.html>

Hoover recalls WindTunnel canister vacuums due to fire and shock hazards. Hoover Inc. of Glenwillow, Ohio, issued a recall February 9 for about 142,000 WindTunnel canister vacuums. The power cord between the power nozzle and the wand connector can short-circuit posing fire and shock hazards to consumers. This condition can occur even if the vacuum has been turned off but left plugged in. Hoover has received 69 reports of overheating or electrical malfunction, including 1 report of fire and smoke damage, and 2 reports of carpet damage. There has been one report of a minor injury. The vacuums were sold at mass merchandisers, department stores, and independent vacuum retailers nationwide and online from March 2003 to December 2008. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml11/11124.html>

Toyota trying to move beyond safety concerns. The results of a government investigation into Toyota safety problems released February 8 has found no electronic flaws to account for reports of sudden, unintentional acceleration in the auto manufacturer's vehicles. Transportation officials and engineers with NASA said two mechanical safety defects previously identified by the government — sticking accelerator pedals and gas pedals that can become trapped in floor mats — are the only known causes for the reports of runaway Toyotas. Both issues were the subject of large recalls. The Department of Transportation Secretary said the agency's 10-month study concluded there is no electronic-based cause of unintended high-speed acceleration. Toyota has recalled more than 12 million vehicles globally since fall 2009 for a series of safety issues. The company has denied that electronics are to blame. Source:

http://hosted.ap.org/dynamic/stories/U/US_TOYOTA_RECALLS?SITE=NCASH&SECTION=HOME&TEMPLATE=DEFAULT

Lasko recalls portable electric heaters due to fire hazard. Lasko Products Inc., of West Chester, Pennsylvania, issued a recall February 8 of about 107,500 portable electric heaters. The Lasko Model 5540 and Air King Model 8540 are subject to the recall. An electrical connection in the base of the

UNCLASSIFIED

UNCLASSIFIED

unit can overheat, causing it to melt and expose the electrical connection, posing a fire hazard to consumers. Lasko received 36 reports of the electrical connection overheating with no reports of injury. There were 18 reports of minor burn damage to floors or carpets. The Lasko Model 5540 was sold at Sam's Club and other retailers from September 2002 through early 2004. The Air King Model 8540 was sold primarily through the maintenance, repair, and operating products supply company, W.W. Grainger Inc. from late 2002 to 2004. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml11/11121.html>

Portable space heaters recalled by PD Sixty Distributor due to fire hazard. PD Sixty Distributor Inc., of Norcross, Georgia, issued a recall February 8 of about 3,000 portable space heaters. The heaters can overheat due to loose electrical connections, posing a fire hazard. The firm has received one report of the heater overheating, resulting in the unit catching fire and causing minor property damage. No injuries have been reported. The space heaters were sold at Hancock Fabrics stores nationwide and by America's Sewing Machine Company, of Augusta, Georgia, through nationwide direct marketing from October 2008 through March 2009. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml11/11720.html>

Simplex fire alarm control panels recalled by Tyco Safety Products Westminister due to failure to alert monitoring centers. Tyco Safety Products Westminister of Westminister, Massachusetts, issued a recall February 8 of about 540 Simplex fire alarm control panels. The recalled panels can fail to send a signal to alert monitoring centers of fires. The firm has received two reports of alarms failing to alert monitoring centers. No injuries have been reported. The panels were distributed by SimplexGrinnell from May 2010 to September 2010. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml11/11721.html>

DEFENSE / INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Justice department remains lacking on WMD response, official says. The U.S. Justice Department's (DOJ) efforts to prepare for a potential weapons of mass destruction (WMD) attack have been "uncoordinated and fragmented," the acting Inspector General said February 9. She said while the FBI had made adequate preparations for dealing with the fallout of a WMD assault, other branches of DOJ and the organization in total had not put in place appropriate measures, the Washington Times reported. DOJ has not selected an office or individual as a core supervisor for WMD response operations, she said in testimony before a U.S. House of Representatives subcommittee. With the exception of the FBI, department subunits have supplied zero or nearly zero applicable training and generally avoid taking part in WMD drills. Source:

http://www.globalsecuritynewswire.org/gsn/nw_20110210_1106.php

(Delaware) DE Homeland Security wants to increase 911 dispatchers. The Delaware Department of Homeland Security has released its fiscal year 2012 budget request as it asks for \$154 million before the joint finance committee. The state homeland security secretary said the state faces a critical

UNCLASSIFIED

UNCLASSIFIED

staffing shortage in 911 centers. “We’ve had a 40 percent increase in the calls for service, yet we have not increased the number of dispatchers since 1996. In addition, the population of Delaware has gone up, and the total number of calls has gone up,” the secretary said. In his budget request, he is asking for the money to hire 12 new dispatchers. The secretary is also seeking to replace the buildings for Troops 3 and 7 in Camden and Lewes, respectively, citing costly ongoing maintenance. Source: <http://www.wdel.com/story.php?id=32255>

FCC sets stage for nationwide presidential alerts. The Federal Communications Commission (FCC) took the first steps in implementing the first-ever presidential alert for the national Emergency Alert System (EAS), when it voted the week of January 30 to run a full test of the system and to provide rules for its use. The concept of a presidential alert system has been hampered by the lack of an official test of the system, which FCC said now will happen. “The primary goal is to provide the president with a mechanism to communicate with the American public during times of national emergency,” a deputy chief of FCC’s public safety and homeland security bureau said. The revamped alert system will allow presidential announcements to be transmitted from Washington, D.C., to television and radio broadcasters nationally. The test will help the FCC, the Federal Emergency Management Agency, and the National Weather Service, to assess the current system and determine what improvements must be undertaken. No official date for the test has been set. The FCC said the national test will require cable and satellite providers that participate in the EAS program to transmit a live code that includes a presidential alert message. Source: <http://www.executivegov.com/2011/02/fcc-sets-stage-for-nationwide-presidential-alerts/>

(California) Border police nab migrants with dive scooters. U.S. border police nabbed two wet-suit clad illegal immigrants from Mexico February 2, who used self-propelled underwater “dive scooters” to enter California, authorities said. The two males, aged 38 and 16, were spotted by a U.S. Customs and Border Protection helicopter crew as they walked up Imperial Beach, California, a few miles south of San Diego, clutching the dive scooters, the border patrol said. “These devices can be used to come north along the coastline and steer into shore ... where they can meet someone who will pick them up in a vehicle and further their entrance into the United States,” a border patrol agent said. Agents arrested the two men as they tried to hide in the sand, and took them to a local Border Patrol station for processing. Source: <http://www.reuters.com/article/2011/02/04/us-usa-mexico-immigrants-life-idUSTRE7134LU20110204>

(Arizona) Phoenix DPS building evacuated after bomb threat. The Arizona Department of Public Safety’s (DPS) headquarters in Phoenix, Arizona has been deemed safe after being evacuated because of a bomb threat February 6. A DPS spokesman said the Phoenix police dispatch center received the threatening call around 9 p.m. Police said the call came from a cell phone. The complex was evacuated, and the agency’s 911 calls were diverted to Phoenix police. Tucson and Flagstaff dispatch centers took over DPS dispatch responsibilities for the Phoenix metro area until 10:30 p.m. The spokesman said DPS’ explosive and ordinance disposal team conducted a sweep of the complex, and “all was found safe and secure.” Source: <http://www.kswt.com/Global/story.asp?S=13980717>

UNCLASSIFIED

ENERGY

EPA outlines how it will study fracking. Even though there is mounting public pressure on the natural gas industry to rein in potential dangers associated with hydraulic fracturing, the practice is largely exempt from federal environmental regulation. The U.S. Environmental Protection Agency (EPA) has never investigated the process industry engineers use to extract gas trapped underneath shale deposits deep below the earth's surface — even though environmentalists allege fracking pollutes supplies of drinking water throughout the nation. A recent congressional inquiry found natural gas drillers had dumped more than 32 millions of diesel — one of several potentially hazardous byproducts of the fracking process — into the ground over a 5-year period. But now EPA is preparing a review aimed at possibly extending its oversight of fracking — and it has released an outline of how it will carry out its investigation. Under the preliminary version of the overhaul, EPA will investigate water contamination at three to five sites, as a sample from the far wider number of troubled fracking sites across the country. EPA investigators would also conduct two or three full case studies to examine the environmental effects of fracking over the full course of a cycle of gas extraction. Source: http://news.yahoo.com/s/yblog_thelookout/20110209/ts_yblog_thelookout/epa-outlines-how-it-will-study-fracking

Report: Hackers in China hit Western oil companies. Hackers operating from China stole sensitive information from Western oil companies, McAfee Inc. reported February 10. The report did not identify the companies but said the “coordinated, covert and targeted” attacks began in November 2009 and targeted computers of oil and gas companies in the United States, Taiwan, Greece, and Kazakhstan. It said the attackers stole information on operations, bidding for oil fields, and financing. “We have identified the tools, techniques, and network activities used in these continuing attacks — which we have dubbed Night Dragon — as originating primarily in China,” the report said. The Chinese government has denied it is involved. Security consultants said China's military or other government agencies might be stealing technology and trade secrets to help Chinese state companies. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/10/AR2011021001051.html>

Senate bill would improve pipeline safety. Two U.S. Senators introduced legislation February 3 to boost pipeline safety in an effort to avoid the kind of major pipeline accidents last year that destroyed homes, killed people, and polluted the environment. The bill would increase fines for reckless pipeline operators, hire more federal safety inspectors, and require automatic shut-off valves to prevent oil spills and natural gas explosions. The United States has about 2.5 million miles of pipelines that move oil, natural gas, and other hazardous liquids. There have been an average of 40 pipeline accidents per year since 2006 that have killed or injured people. Many of the safety improvements in the legislation were sought by the Transportation Department's Pipeline and Hazardous Materials Safety Administration (PHMSA). The bill specifically reauthorizes the agency through 2014 and strengthens its authority. Source: <http://www.reuters.com/article/2011/02/03/us-usa-pipeline-legislation-idUSTRE7129JF20110203>

FOOD AND AGRICULTURE

Smoked salmon recalled in 20 states for Listeria. St. James Smokehouse Inc., of Miami, Florida, recalled 600 pounds of smoked salmon that was shipped to 20 states after routine sampling by the Florida Department of Agriculture and Consumers Services found the product may be contaminated with *Listeria monocytogenes*. The company recalled its Scotch Reserve Whiskey & Honey Smoked Scottish Salmon. The 4-ounce retail packs have the lot code 5797 and batch code 4759 with the UPC number 853729001151. No illnesses have been linked to the product. The recall was announced in a news release dated February 4 but published February 10, by the U.S. Food and Drug Administration. The recalled salmon was distributed and sold at Fresh Market stores in Florida, North Carolina, South Carolina, Tennessee, Georgia, Virginia, Kentucky, Alabama, Indiana, Illinois, Ohio, Louisiana, Maryland, Arkansas, Wisconsin, Mississippi, Pennsylvania, Massachusetts, Connecticut, and New York. Source: <http://www.foodsafetynews.com/2011/02/smoked-salmon-recalled-over-listeria-fears-1/>

(Iowa) Corn supply shrinks to 16-year low. Demand for corn for ethanol and other uses has shrunk surplus stocks in elevators and farmers' bins to the lowest levels since 1995, the U.S. Department of Agriculture (USDA) said February 9. That surplus amounts to an 18-day supply of corn ready for immediate use, compared with more than 40 days a year ago. As a result, corn prices have doubled from \$3.50 last June. Food makers, meatpackers, and restaurants have already warned consumers will pay higher prices as a result. The USDA's monthly supply and demand report issued February 9 increased its demand forecast for corn for ethanol by 50 million bushels, to 4.95 billion bushels this year. The use of corn for ethanol has risen about 33 percent since 2008, and will consume almost 40 percent of the 12.4 billion bushels of corn produced in the United States in 2010. Source: <http://www.desmoinesregister.com/article/20110210/BUSINESS01/102100329/Corn-supply-shrinks-to-16-year-low?SPORTS12>

ADT to expand food defense strategy. ADT announced February 8 it is expanding its efforts in the food defense sector to help food manufacturers and suppliers meet new regulations outlined in the Food Safety Modernization Act. Signed into law in January by the U.S. President, the legislation requires food suppliers to identify potential problems that could affect the safety of their products, and outline steps they can take to prevent these issues from occurring. To help food suppliers keep up with the new mandates, ADT said it will provide them with security expertise to help them develop food defense strategies. ADT has been active in continuing education within the food processing and manufacturing industry, hosting a 2-day food defense event last year. The company has also teamed up with remote video auditing and software firm Arrowsight, at the Food Defense Demo Lab in Huntsville, Alabama, to show food processors new technologies and solutions in a real world setting. Source: <http://www.securityinfowatch.com/adt-expand-food-defense-strategy>

(Maine) Maine oysters suffer MSX outbreak. A deadly pathogen spurred an outbreak of disease in Maine oyster farms for the first time in 2009. The spore-forming protozoan *Haplosporidium nelsoni* (MSX) is jeopardizing the \$3 million industry in the northeast states. MSX is harmless to humans and can exist in small numbers without damaging oysters. The protozoan impairs oysters' feeding and reproduction, weakening and eventually killing the mollusk. "In July, we started to notice a troubling sign," said a spokesman of Pemaquid Oyster Company and director of the Maine Aquaculture

UNCLASSIFIED

Innovation Center. "Two or three oysters in each basket were dead when we returned to collect them, their shells cracked." By mid-August, they sent 60 oysters to a laboratory for testing, and found MSX was the culprit. Oyster growers on the river tested each growing area for the pathogen and worked with the Maine Department of Marine Resources to impose quarantine on transferring oysters from the Damariscotta River to other waters to contain the outbreak. MSX nearly wiped out the oyster population in the Chesapeake Bay several years ago. How MSX spreads remains unknown, but researchers surmise that it uses a third-party host to infect the mollusks, making eradication from the local environment impossible. Source:

<http://fis.com/fis/worldnews/worldnews.asp?monthyear=2-2011&day=4&id=40395&l=e&country=&special=&ndb=1&df=0>

(California) California firm recalls 3,000 lbs. of beef. About 3,170 pounds of fresh ground beef patties and other beef products distributed to Southern California restaurants has been recalled, federal officials said. The U.S. Agriculture Department (USDA) said in a release February 5 that the beef from American Food Service in Pico Rivera may be contaminated with E. coli O157:H7. The USDA said the products were produced January 31 and bear the establishment number "EST. 1913" inside the USDA mark of inspection. The departments said there is a concern some product may be frozen and in restaurant freezers. Source: http://www.upi.com/Health_News/2011/02/06/California-firm-recalls-3000-lbs-of-beef/UPI-12411296971022/

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

White House attack e-mails were faked, says UK official. A cyberattack targeting British officials, which at first appeared to be carried in White House e-mails, actually originated in China, with the perpetrator using a hoax e-mail address that resembled a White House account, officials in the United Kingdom said. Nevertheless, U.K. officials are using the opportunity to call for more cooperation among governments to jointly agree on policies for state-based covert cyber activity. The initial reports February 4 from the British foreign secretary indicated e-mail messages alleged to be from the White House were sent to several British officials in late December. The e-mails contained links that, if opened, would download a virus onto the user's computer. It was first unclear if the attack came from authentic White House e-mail accounts that had been hacked and infected with a virus or from fake e-mail accounts made to resemble White House e-mail messages. In recent days, the latter scenario appears the more likely. Although the foreign secretary did not name the country behind the attacks, intelligence sources familiar with the incidents made it clear the originating country was China, the Guardian said in an article February 4. Source:

<http://gcn.com/articles/2011/02/07/alleged-white-house-email-cyberincident-now-called-spoof-attack-from-china.aspx>

White House gets tough on ID card reader requirements. Beginning October 1, the White House will penalize agencies that fail to outfit facilities and information technology systems with electronic identity card readers by withholding funds for other programs, according to a new White House memo. Federal employees and contractors are required to carry ID badges embedded with digital fingerprints and photos to access federal buildings and networks, under the 2004 Homeland Security Presidential Directive 12. But agencies have long struggled to employ the electronic features of the

UNCLASSIFIED

UNCLASSIFIED

badges. The February 3 Office of Management and Budget guidance directs agency heads to submit implementation policies by March 31 on required uses of the smart cards, and stipulates that funds be frozen at offices that do not follow the rules. The memo stops short of restricting bonuses and awards at agencies that have not fully complied with HSPD-12, a penalty that the nonprofit Center for Strategic and International Studies recommended during the Presidential/Vice Presidential transition. The IDs — mentioned in the U.S. President's 2009 comprehensive cyber policy review, are to be issued following standard security checks on individuals. Source:

http://www.nextgov.com/nextgov/ng_20110207_9583.php?oref=topnews

(Nevada) Deputies arrest Wells man on school bomb threat charge. A Wells, Nevada, man was arrested February 4 by a sheriff's deputy after he reportedly made a bomb threat at Wells High School. According to a sheriff's lieutenant, the 18-year-old suspect is a student. He was overheard by a fellow student allegedly threatening to blow up the school. The principal suspended the suspect from classes for 3 days. Later that day, the suspect returned to the school, and he was arrested by a sheriff's deputy for allegedly making a bomb threat and for trespassing. Source:

http://elkodaily.com/news/local/article_adaeb688-33a9-11e0-bbaf-001cc4c002e0.html

(District of Columbia) Teen arrested for Molotov cocktail at D.C. school. A 13-year-old is under arrest and the school system wants him expelled for bringing a Molotov cocktail to Jefferson Middle School in Washington D.C. The assistant press secretary at D.C. Public Schools said school security found a small bottle of liquid wrapped in duct tape in the boy's bookbag. The discovery was made during x-ray weapons screenings before the boy entered the building. The student has been charged with possession of a destructive device, D.C. police said. D.C. Public Schools said the student will not be allowed to return to school until the expulsion procedure is completed. Source:

<http://www.wtopnews.com/?sid=2263950&nid=596>

U.S. TRANSCOM operates despite enemy attacks. U.S. Transportation Command (TRANSCOM) suffers more cyber attacks than any other combatant command, according to its Air Force General commander. This is partly because, unlike other commands, TRANSCOM relies on unclassified and commercial networks to deliver supplies and passengers all over the world, the commander said February 7 at the Center for Strategic and International Studies in Washington. In 2010, there were 33,326 "computer network events against TRANSCOM," according to the four-star's briefing. In addition to cyber attacks, TRANSCOM is the target of piracy and other supply-route attacks, a particular vulnerability for operations in Afghanistan, a landlocked country. TRANSCOM conducts 90 percent of its operations by surface transportation, leaving 10 percent carried out by airlift. However, in Afghanistan, 30 percent is delivered by air, the commander said. Air transport is 10 times more expensive than surface delivery, he said. Sensitive, high-value products travel by air, according to the commander, who said he is confident about the transit options available. In case something unforeseen happens, such as the floods in Pakistan, the coup in Kyrgyzstan or the volcano in Iceland, TRANSCOM has enough options to fall back on, he said. Source:

<http://www.defensenews.com/story.php?i=5644269&c=AME&s=AIR>

(Wisconsin) Police make arrest in Lake Geneva bomb threat. Police in Lake Geneva, Wisconsin, have arrested a 15-year-old Badger High School boy they believe is responsible for e-mailing a bomb threat to administrators the week of January 31. Lake Geneva School District closed five schools January 31 after receiving an e-mail saying a bomb was located in Badger High School and others, according to a

UNCLASSIFIED

UNCLASSIFIED

Lake Geneva Police Department press release. All the buildings were searched and nothing was found. The FBI assisted in the investigation. Police said the student admitted to sending the message and told them he acted alone. He said he “never thought this incident would cause such a commotion,” the release said. Lake Geneva police referred charges to the district attorney’s office. There was no indication as to when the student was arrested or why he sent the e-mail. Source: <http://gazettextra.com/weblogs/latest-news/2011/feb/07/police-make-arrest-lake-geneva-bomb-threat/>

(Michigan) College student charged with making false threat. A Wayne State University student is charged with making false threats of violence against the school in Detroit, Michigan, via the Internet. The FBI said the suspect of Dearborn wrote in November he was planning to take an AK-47 to the General Lectures building and kill more than the 32 people who died at Virginia Tech University in 2007. The FBI said the suspect pledged to set up a Web cam to record it December 1 and wrote, “Be sure to tune in.” Nothing happened, and the suspect told an agent he did not intend to attack anybody. The suspect appeared in federal court February 4 and was released. He is also charged with possessing child pornography. Source: <http://www.victoriaadvocate.com/news/2011/feb/07/bc-mi-university-threat/?news&nation-world>

(Arizona) US legislators targeted by identity thieves and account hijackers. Facebook accounts of four Missouri state representatives and one staffer have been compromised and are sporting mortifying messages. The affected politicians agree on one thing: they have been using the free Wi-Fi network instead of the protected account for legislators. Even though the legislators have been made aware that they should be using the dedicated protected Internet access when doing official work or performing other sensitive assignments and that there is an inherent risk in using the public wireless Internet, many still fail to do so because they ignore the warning, forget to use it, or simply do not know how. And while the founder of the company that provides wireless Internet to the Arizona Capitol speculates the account compromises may be the result of the use of the Firesheep extension, a representative from the Center for Strategic and International Studies in Washington D.C. thinks that it is possible that the malicious individual behind the attack has simply guessed the passwords. Source: <http://www.net-security.org/secworld.php?id=10552>

(Florida) Man held after bomb threat to local IRS. A man threatened local IRS workers when he walked into an office in Sarasota, Florida, February 7 and said he would detonate a bomb, authorities said. The man is in police custody and is being interviewed by Sarasota County sheriff’s detectives. The building was evacuated; no one was hurt and a bomb squad later found the man was not carrying any explosives in a package he brought in. The man threatened the office shortly after 11 a.m. and told workers that he would blow them up. Deputies were able to arrest the man without incident. Source: <http://www.heraldtribune.com/article/20110208/ARTICLE/102081027/2055/NEWS?Title=Man-held-after-bomb-threat-to-local-IRS&tc=ar>

(Ohio) Party ejection led to Ohio frat house shooting, police say. Two men were accused of shooting into a Youngstown State University (YSU) fraternity house in Youngstown, Ohio, February 6, killing 1 and wounding 11, including six YSU students. According to a police statement February 7, the two men were apparently angry because they were thrown out of a party there. Police identified the suspects as a 22-year-old man and 19-year-old man. Both are residents of Youngstown. A 25-year-old

UNCLASSIFIED

UNCLASSIFIED

man died in the shooting. He was shot once in the back of the head and several times in the lower body, said a forensic pathologist at the Mahoning County Coroner's Office. All but three people hurt in the shooting had been treated and released by the afternoon of February 6, a spokeswoman for St. Elizabeth Health Center in Youngstown said. The shooting happened early in the morning during an impromptu party at the off-campus fraternity house of Omega Psi Phi, police said. Of the people who remained hospitalized, one was in critical condition with a head wound. Those injured in the shooting ranged in age from 17 to 31. Source: <http://www.cnn.com/2011/CRIME/02/07/ohio.students.shot/>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Low security awareness found across IT. A broad spectrum of IT people, including those close to security functions, appear to have little awareness of key security issues impacting their organizations, a new survey showed. The survey, which polled 430 members of the Oracle Application Users Group conducted by Unisphere Research and sponsored by Application Security Inc. included directors and managers of information technology, developers and programmers, database and systems administrators, systems architects and analysts, and professionals from the HR and financial functions. About 22 percent of respondents claimed to be extensively involved in security functions, 60 percent claimed a limited or supporting role, and the rest said they were not involved with security at all. About 100 respondents belonged to companies with more than 10,000 employees. What the survey showed was a surprising lack of awareness of security issues among the respondents. For instance, just 4 percent admitted to being fully informed about security breaches within their organizations. About 80 percent of those who said their organizations had suffered a data breach in the past year were unable to tell which IT components might have been impacted by the breach. Source:

http://www.computerworld.com/s/article/9208890/Low_security_awareness_found_across_IT

Flash Player security update fixes critical vulnerabilities. Adobe has released a major Flash Player update, which, in addition to several new features, patches critical security vulnerabilities that could allow attackers to compromise computers. The new Flash Player 10.2.152.26 version fixes a total of 13 flaws, all of which could be exploited to crash the application and execute arbitrary code. Ten of the security issues fixed are described as memory corruption vulnerabilities, one as an integer overflow, another as a font-parsing bug and the last as a library-loading weakness. Source:

<http://news.softpedia.com/news/Flash-Player-Security-Update-Fixes-Critical-Vulnerabilities-183286.shtml>

Critical security update released for Adobe Reader and Acrobat. Adobe has released its scheduled quarterly security updates for Adobe Reader and Acrobat, addressing a large number of critical vulnerabilities. In total, the updates provide fixes for 29 vulnerabilities in Adobe Reader and Acrobat X (10.0), 9.4.1 and 8.2.5 on Windows and Mac. Updates for the UNIX platform are expected around February 28. A number of 23 security issues could be exploited to execute arbitrary code, while an additional 3 might have the same impact, but it has not been demonstrated yet. Two of the remaining vulnerabilities stem from input validation weaknesses that could trigger cross-site scripting conditions, while the last one is a file permissions issue that could be exploited to elevate privileges. Two remote code execution flaws affect only Mac flavor of the products, while the file privilege

UNCLASSIFIED

UNCLASSIFIED

escalation one is a Windows-only problem. Source: <http://news.softpedia.com/news/Critical-Security-Update-Released-for-Adobe-Reader-and-Acrobat-183239.shtml>

More than half of iPhone apps track users. A recent study found that more than half of all iPhone apps could track users and collect data without an individual's knowledge. Researchers analyzed more than 1,400 iPhone apps to determine how they handle sensitive data, and found that more than half collect an individual's unique device ID or track a user's location. When combined with links to a Facebook account, the app could gain a lot of sensitive data. Researchers found that 36 apps blatantly violated privacy rights by accessing an individual's location without informing the user, while another 5 went so far as to take data from the user's address book without first seeking permission. Source: <http://homelandsecuritynewswire.com/more-half-iphone-apps-track-users>

Malware increases by 46% in only one year. There is a steady growth of threats to mobile platforms, according to a new McAfee report. The number of pieces of new mobile malware in 2010 increased by 46 percent compared with 2009. The report also uncovered 20 million new pieces of malware in 2010, equating to nearly 55,000 new malware threats every day. Of the almost 55 million total pieces of malware McAfee Labs has identified, 36 percent was created in 2010. Concurrently, spam accounted for 80 percent of total e-mail traffic in Q4 2010, the lowest point since the first quarter of 2007. Source: http://www.net-security.org/malware_news.php?id=1622

Number of malicious PDFs on the rise. Security vendor GFI Software warned that the number of malicious PDF files detected in the wild significantly increased in January with two detections making it into the top 10. According to data gathered by the company's ThreatNet system, two PDF exploits detected as Exploit.AdobeReader.Gen and Exploit.PDF-JS.Gen, finished in eighth and ninth place as far as malware detections go. No Java exploit made its presence in the GFI's list. Seven of the top 10 threats detected by GFI in January were trojans, including all malware that finished in the first five positions. These seven threats accounted for four of all detection registered by the security company's products. The other threat in the top 10 is a variant of the Conficker worm, which still remains strong even if abandoned by its creators a year ago. GFI researchers are also concerned about a spike in the number of scareware applications detected in January. Source: <http://news.softpedia.com/news/Number-of-Malicious-PDFs-on-the-Rise-182722.shtml>

US hosts the highest percentage of ZeuS command and control servers. According to statistics gathered by Trusteer, the highest number of ZeuS command and control servers are hosted in the United States. The United States is usually at the top of malware charts, either as top hoster, the country with largest number of infected computers, or the primary source for spam. Given the major crackdown on ZeuS-related fraud in the United States in 2010 and the amount of damage suffered by companies in the country as a result of this banking trojan, expectations were to see a decrease in the number of ZeuS C&Cs hosted there. However, Trusteer reports that almost 40 percent of the global ZeuS infrastructure is still based in the United States. Source: <http://news.softpedia.com/news/US-Hosts-the-Highest-Percentage-of-ZeuS-Command-and-Control-Servers-182723.shtml>

UNCLASSIFIED

NATIONAL MONUMENTS AND ICONS

(Georgia) Ocmulgee National Monument fire ruled arson. A 154-year-old house that survived a Civil War raid was nearly destroyed in an arson fire February 9 at the Ocmulgee National Monument in Georgia. Macon police arrested a man with cuts on his hands who was watching the commotion as crews battled the blaze. Just before 3:40 a.m., a fire alarm alerted firefighters, who arrived to find the back side of the superintendent's house on fire near the entrance to the park. The man who used to live there moved his family off the property more than 4 years ago. The house had been vacant since the fall when a law enforcement ranger left. A 57-year-old Macon man was charged with arson, burglary, and criminal trespass, according to the Bibb County Sheriff's Office. He is being held at the Bibb County jail without bond. The sheriff's office, federal law enforcement rangers, and the Macon-Bibb County Fire Department are investigating. Source:

<http://www.macon.com/2011/02/10/1445829/ocmulgee-national-monument-fire.html>

(District of Columbia) Fire breaks out at Smithsonian building. A fire broke out February 7 in Washington D.C. at a building next to the Smithsonian's Museum of Natural History that houses the facility's cooling tower, D.C. fire officials said. Around 7:30 a.m., D.C. firefighters were dispatched to the museum, and heavy smoke pouring from a detached building at Ninth Street and Constitution Avenue NW. Maintenance workers had been in the area when a fire started in the interior of the cooling tower, a D.C. Fire spokesman said. A hazardous materials unit was called in because the interior components of the unit contained plastic and various chemicals. Museum officials said no smoke entered the green-domed building that houses millions of artifacts and collections. Officials planned to open the museum later in the day after completion of the fire investigation. Source:

<http://washingtonexaminer.com/blogs/capital-land/2011/02/fire-breaks-out-smithsonian-building>

POSTAL AND SHIPPING

(Alabama) Albertville woman charged with mailing 2 fake anthrax letters. A federal grand jury has charged an Albertville, Alabama, woman with sending two fake anthrax letters to the local Social Security Administration (SSA) office. The 43 year-old woman faces two counts of mailing a letter containing a powdery substance and a note to someone at the Albertville SSA. The powder did not test positive for any biological hazards. The U.S. Postal Inspection Service, the SSA Office of the Inspector General, and the Department of Homeland Security Federal Protective Service jointly investigated the case, which is being prosecuted by an assistant U.S. attorney. Source:

http://blog.al.com/breaking/2011/02/albertville_woman_charged_with_1.html

(Texas) MacArthur HS clear after suspicious package investigation. Authorities evacuated MacArthur High School in the Irving Independent School District in Irving, Texas around 1:15 p.m., February 8 after a suspicious package was discovered on the campus. Students and faculty were evacuated to a safe area south of the school while emergency crews worked on the package with a water cannon. Irving Police said the package was wrapped in birthday wrapping paper and addressed generically to the high school from another address out of the state. Police mentioned some misspellings on the address label that made them suspicious. Students were let back inside the building around 2:30

UNCLASSIFIED

p.m., when the situation was cleared by officials. There was no explosive material in the package. The police investigation is ongoing. Source: <http://www.nbcdfw.com/news/local-beat/MacArthur-HS-Evacuated-Due-to-Suspicious-Package-115585704.html>

PUBLIC HEALTH

Tool developed to monitor pandemic threats. Created with a grant from the U.S. Agency for International Development (USAID), an Emerging Pandemic Threats (EPT) tool, known as “Predict,” will enable scientists and the public to track outbreaks of communicable animal diseases. The goal of the program is to preempt or combat, at their source, newly emerging diseases of animal origin that could threaten human health. The tool is being produced by experts on human and animal diseases from a consortium that first came together in 2009 during the pandemic of H1N1 swine flu. The experts have focused their attention on animal diseases that infect humans, such as the virus that caused the outbreak of SARS and the viruses (Ebola included) that are believed to have originated in bats. Predict will monitor data from 50,000 Web sites with information from World Health Organization alerts, online discussions by experts, wildlife trade reports, and local news. The EPT program is being managed by USAID with technical support from the U.S. Centers for Disease Control and Prevention and the U.S. Department of Agriculture Source: <http://homelandsecuritynewswire.com/tool-developed-monitor-pandemic-threats>

Synthetic biology industry poses security challenges, experts say. The rate of technological change produced by the rapid growth of the synthetic biology field could outpace government restrictions intended to ensure extremists cannot acquire or produce biological warfare materials, experts said at a conference February 3. Synthetic pathogens are man-made infectious agents created either from the manufacture or adaptation of DNA, cells, and other biological structures. While scientists have been tweaking genetic sequences for decades, recent breakthroughs such as the production from scratch of cells that do not exist in nature have some security experts worried the technology could be exploited by terrorists to create or redesign biological weapons. Source: http://www.globalsecuritynewswire.org/gsn/nw_20110209_8875.php

Protected health information breach analysis. Redspin released an analysis of all protected health information breaches publicly recorded between August 2009 and the end of 2010, as per the interim final breach notification of the HITECH Act. A total of 225 breaches of protected health information affecting 6,067,751 individuals have been recorded since the interim final breach notification regulation was issued in August 2009 as part of the HITECH Act. These numbers only include breaches that affected more than 500 individuals. According to the report, 43 states, Washington D.C., and Puerto Rico have suffered at least 1 breach affecting over 500 individuals. Also according to the report, 78 percent of all records breached are the result of 10 incidents, 5 of which are the result of theft of common storage media; 61 percent of breaches are a result of malicious intent; 66,000 individuals, on average, are affected by a single breach of portable media; and 40 percent of records breached involved business associates. Source: <http://www.net-security.org/secworld.php?id=10560>

Setbacks seen in bioshield procurements. The U.S. Health and Human Services Department said it faced many setbacks in 2009 to a program aimed at developing countermeasures to biological agents and other weapons of mass destruction (WMD) materials, Homeland Security Newswire reported the

UNCLASSIFIED

UNCLASSIFIED

week of January 30. “Significant events transpired in 2009 for Project Bioshield products that have further sharpened our understanding of the challenges we continue to face in the complex undertaking of medical product approval,” said the annual report to Congress covering program developments over the 2009 calendar year. The Food and Drug Administration ruled out approval in 2009 of the anthrax countermeasure ABthrax until additional analyses could be completed. In a bid to produce a more refined next-generation anthrax vaccine, officials in December 2009 scrapped an application process for biotechnology firms to propose projects aimed at creating the treatment. Project Bioshield provided \$5.6 billion for the purchase of medical treatments for the U.S. Strategic National Stockpile. Roughly \$2.4 billion was left at the end of 2009. Source: http://www.globalsecuritynewswire.org/gsn/nw_20110208_5731.php

(Indiana) Flu now widespread in Indiana. Indiana has joined 29 other states reporting widespread cases of influenza as the apparent peak of the flu season sweeps through the state. In its latest report issued February 8, the Centers for Disease Control and Prevention (CDC) said Indiana joined four other new states reporting a widespread outbreak of influenza. “Most key flu indicators increased this week, including the number of people visiting doctors for influenza-like illness, the number of states reporting widespread influenza activity and the proportion of deaths attributed to pneumonia and influenza,” the CDC said in a news release. It is likely that Indiana is in or near the peak of flu activity this season. The CDC said the typical seasonal flu peak is in late January or February. Doctors offices and health clinics, such as CVS’ MinuteClinic and Walgreens’ Take Care Clinic, have been overflowing with patients for the last week. Source: <http://www.theindychannel.com/health/26787660/detail.html>

HHS now has its own most-wanted list — for health-care fraud. The U.S. Department of Health and Human Services’ Office of Inspector General (IG) has a first-ever list of the most-wanted health-care fugitives, featuring 10 of the 170 people wanted on health fraud and abuse charges. Only 8 of the 10 are still at large. Two were captured while the new Web site was being developed, a spokeswoman for the IG’s office said. Their replacements will be selected soon, she said. The people on the list are not necessarily the worst offenders in terms of dollars or harm, though; she said they represent a cross-section of the types of fraud and offenders. Still on the list are three brothers who allegedly defrauded Medicare of \$110 million with an HIV infusion scam, and another man accused of collecting \$525,000 in fraudulent claims for motorized wheelchairs, scooters, and other durable medical equipment. In total, the 10 allegedly cost taxpayers \$124 million, with the full list representing “hundreds of millions of dollars,” the spokeswoman said. Some estimates put the amount lost to Medicare fraud each year as high as \$60 billion. Source: <http://blogs.wsj.com/health/2011/02/04/hhs-now-has-its-own-most-wanted-list-for-health-care-fraud/>

TRANSPORTATION

Air traffic control error numbers double. Safety experts are puzzled about why reports of mistakes by air traffic controllers have nearly doubled in a time of unparalleled aviation safety in the United States. The Federal Aviation Administration said in the 12 months ending September 30, 2010, there were 1,889 operation errors — usually aircraft coming too close together. During the same period 1 year earlier, there were 947 errors. And the year before that — 1,008 errors. One air traffic controller

UNCLASSIFIED

UNCLASSIFIED

at the facility in Ronkonkoma, New York, said there's a lax atmosphere in the control room. He said he's complained to the Transportation Department's Inspector General and to the Office of Special Counsel about controllers sometimes watching movies and playing with electronic devices during nighttime shifts when traffic is slower. The facility where the air traffic controller works handled the latest near midair collision of an American Airlines jet with 259 people aboard and two Air Force transport planes southeast of New York City. Source:

http://www.weartv.com/template/inews_wire/wires.national/2cde2cd8-weartv.com.shtml

U.S. officials eye ways to increase airport security. U.S. authorities are considering ways to tighten security in public areas at U.S. airports after a deadly attack in Moscow, Russia, last month, the head of the Transportation Security Administration (TSA), said February 10. A suicide bomber last month killed 36 people and injured more than 100 after detonating the device in the international arrivals hall of Moscow's busy Domodedovo airport, sending U.S. airport officials scrambling to address the security gap. The ideas included checkpoints before vehicles are allowed to pull up to the airport terminals, small security teams patrolling the grounds and using officers who are trained to detect unusual behavior, the TSA head told a House of Representatives' subcommittee on transportation security. U.S. authorities have ramped up security for air travelers, luggage and cargo in the wake of several attempts by al Qaeda militants to attack the United States, adding full-body scanners and requiring more screening for cargo. Source: <http://www.reuters.com/article/2011/02/10/us-usa-security-airports-idUSTRE7196WC20110210?feedType=RSS&feedName=domesticNews>

(Florida) Officials: No bomb found on cruise ship. Officials said no bomb was found on a Norwegian Sun cruise ship after several hours of security sweeps and searches in Port Canaveral, Florida. Law enforcement from the U.S. Coast Guard, Port Canaveral police, and the Brevard County Sheriff's Office spent most of the day February 5 investigating a bomb threat. About 1,800 passengers were on board the cruise ship when the call came in before 9 a.m. An anonymous person called an employee on the ship and said there was a bomb on the 11th deck. The Brevard County Sheriff's Office bomb squad, the FBI, and Coast Guard crews evacuated passengers. Travelers trying to start their vacation got caught in the chaos. The bomb squad searched the ship for 2 hours but never found a bomb. Passengers were eventually allowed to board the ship around 2 p.m. Coast Guard officials said they were working with the FBI to determine who made the call and why. Source:

<http://www.wftv.com/news/26759762/detail.html>

WATER AND DAMS

(Pennsylvania) U.S. city of Buffalo bans hydraulic fracturing. Buffalo, New York banned the natural gas drilling technique of hydraulic fracturing February 8 in a largely symbolic vote that fuels debate over the potential harm to groundwater from mining an abundant energy source. The city council voted 9-0 to prohibit natural gas extraction including the process known as "fracking" where chemicals, sand and water are blasted deep into the earth to fracture shale formations and allow gas to escape. The ordinance also bans storing, transferring, treating or disposing of fracking waste within the city. No such drilling projects had been planned in Buffalo, though city officials were concerned fracking wastewater from nearby operations was reaching the city sewer system. Backers of the measure hope it will help build pressure against fracking, which environmentalists say endangers groundwater as a result of leaking chemicals. Pittsburgh, Pennsylvania, has enacted a similar ban.

UNCLASSIFIED

UNCLASSIFIED

Industry supporters said fracking is proven to be safe and can provide a much-needed domestic energy source. The U.S. Environmental Protection Agency is studying the impact of fracking and February 8 submitted a draft of its study to the agency's science advisory board for review. Initial findings from the study are expected to be made public by the end of 2012. Source:

<http://www.reuters.com/article/2011/02/08/energy-natgas-usa-buffalo-idUSN0818750720110208>

(Connecticut) Counterterror laws hobble monitoring of water supplies. In an effort to secure U.S. critical infrastructure after the terrorist attacks of September 11, 2001, sensitive data regarding community water plans such as where wells are drilled have been tightly guarded. According to the executive director of the Connecticut Water Works Association, DHS has evidence that al Qaeda was exploring methods to destroy water infrastructure or introduce chemicals into the water supply. Environmentalists do not dispute that terrorists could be targeting the U.S. water supply, but are instead pushing for greater transparency to ensure adequate water supplies for their communities. "Enemies poisoning each other's water are a threat in times of conflict, but we may do serious harm by abandoning our watershed stewardship," said the executive director of the Rivers Alliance of Connecticut, an organization dedicated to responsibly managing the state's waterways. She and her organization want to make it easier to obtain basic data from water companies to foster debate and hold companies responsible for maintaining local water supplies. The Wallingford Water Company claimed it does not have the ability to comply with state department of environmental protection regulations, citing an internal study that found that it would cost \$10 million to comply. Source: <http://homelandsecuritynewswire.com/counterterror-laws-hobble-monitoring-water-supplies>

(Idaho) Palisades Dam security upgrades up for review. The U.S. Bureau of Reclamation has taken the next step toward bomb-proofing the Palisades Dam in Bonneville County, Idaho. As part of the federal government's post-9/11 protocol for securing infrastructure throughout the nation, the bureau has published a series of options for protecting Palisades from terrorist attacks. They are listed in a draft version of an environmental assessment published last month. According to the draft assessment, the dam's greatest vulnerability is to vehicles carrying explosives traveling across the crest. Explosives delivered by divers, boats or airplanes are less of a concern because of the dam's gently sloping sides. Here is a quick look at the alternatives the bureau has proposed: Widen the dam's crest and move traffic flow 21 feet upstream. This would protect the dam's most vulnerable area from a potential blast. Projected cost: \$4.7 million. Raise the crest — and the surface that vehicles drive on — by 5 feet. This action would provide a buffer for any explosion occurring on the top of the dam. Projected cost: \$5.8 million. Build a 10-foot-wide barrier in the middle of the dam's crest, leaving 12-foot lanes for each direction of travel. Bureau officials have suggested this would work only temporarily because it does not fully address the dam's vulnerabilities. Projected cost: \$2.8 million. Close the dam's crest to public traffic and build a bridge a half-mile downstream of the dam that accesses popular recreation areas on the west side of the Palisades Reservoir and South Fork of the Snake River. This option would completely remove potential threats from the dam's vicinity, but it could disrupt a park downstream of the dam and lead to traffic problems on the other side of the river. Projected cost: \$3.7 million. The bureau has yet to settle on a preferred alternative. Source: <http://www.securityinfowatch.com/node/1319544>

UNCLASSIFIED

UNCLASSIFIED

(Colorado) **Overseers face threats to dams.** Colorado dam safety overseers said they face about a dozen security incidents each month at water storage facilities around the state. These range from reports of suspicious activity, such as a person spotted on a downstream face of a dam taking photos, to people threatening to blow up dams with explosives, said the chief of dam safety in the Colorado Department of Natural Resources. “On a weekly basis, I get about three or four suspicious-activity reports,” he said. He represents Colorado on a U.S. Department of Homeland Security dam safety coordinating council meeting the week of February 7 in Washington, D.C. Most recently, a bomb threat was reported at a dam near South Fork in southwestern Colorado. The threat was made “by a disgruntled resident of South Fork who wanted to get back at the sheriff’s department for giving him a DUI,” he said. Source: http://www.denverpost.com/news/ci_17314477

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