

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

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

REGIONAL

NATIONAL

INTERNATIONAL

**BANKING AND FINANCE
INDUSTRY**

**CHEMICAL AND HAZARDOUS
MATERIALS SECTOR**

COMMERCIAL FACILITIES

COMMUNICATIONS SECTOR

CRITICAL MANUFACTURING

**DEFENSE INDUSTRIAL BASE
SECTOR**

EMERGENCY SERVICES

ENERGY

FOOD AND AGRICULTURE

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

**INFORMATION TECHNOLOGY
AND TELECOMMUNICATIONS**

**NATIONAL MONUMENTS AND
ICONS**

POSTAL AND SHIPPING

PUBLIC HEALTH

TRANSPORTATION

WATER AND DAMS

**NORTH DAKOTA HOMELAND
SECURITY CONTACTS**

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(Minnesota) Another Minn. water park linked to cryptosporidium. Another water park in Minnesota was linked to the intestinal disease cryptosporidiosis, the Associated Press reported March 29. Minnesota Department of Health officials said a case of the water-borne disease was connected to the Lodge at Brainerd Lakes. A state epidemiologist said the lodge worked with the department's environmental health officials and highly chlorinated the water park. The pool was closed March 26 and reopened March 29. The Brainerd Dispatch said the health department confirmed one case of the disease linked to the lodge's water park and at least two other suspected cases. The health department recently linked the parasitic disease to the Edgewater Resort and Water Park in Duluth. Source:

<http://www.kare11.com/news/article/970160/396/Another-Minn-water-park-linked-to-cryptosporidium>

(Minnesota) Outbreak of mail thefts reported. March 23, the Hasting Star-Gazette reported mail was being stolen from mailboxes in Hastings, Minnesota, and the surrounding area, according to the city's postmaster. She said rural areas have been targeted in recent months, with Denmark Township being hit especially hard. The week of March 19, at least two homes near the Hastings Country Club had mail stolen from them. A witness observed a black Honda Accord or similar vehicle stop by the mailbox, and observed a white male driver and white female passenger. Hastings police are investigating the cases. "We definitely want people to report any type of suspicious activity," the chief of police said. "Right now we don't have a great deal of information indicating that the proceeds of these thefts have been used in other types of fraudulent activities." Source:

<http://www.hastingsstargazette.com/event/article/id/27037/group/News/>

(Minnesota; Wisconsin) Waterborne disease outbreak is traced to Duluth water park. An outbreak of a waterborne diarrheal disease has been linked with Duluth's Edgewater Resort and Water Park, a Minnesota health official said March 27. Three cases of cryptosporidiosis have been confirmed, and six more are suspected in Minnesota and Wisconsin, said an epidemiologist for the Minnesota Department of Health who specializes in the disease. The cases involved adults and children, and all of those who came down with the illness spent time at the water park during March 2012. The epidemiologist said many other cases may have gone unreported. The water park voluntarily closed March 26, and all of the water facilities were treated with super-chlorination to kill the parasite. The water park reopened March 27. The parasite is spread through the feces of infected humans, according to the Wisconsin Division of Public Health. Cryptosporidiosis is one of the most frequent causes of waterborne illness in the United States, according to the Centers for Disease Control and Prevention. Source:

<http://www.duluthnewstribune.com/event/article/id/226895/group/homepage/>

UNCLASSIFIED

UNCLASSIFIED

(Montana) Copper thieves targeting rail lines. Thieves made at least seven raids in four weeks on copper wire strung along railroad tracks from Huntley to Laurel, Montana, the Billings Gazette reported March 26. “We see thievery whenever metal prices go up,” said a Yellowstone County Sheriff’s Department captain. “But this has been quite an increase this past month.” March 19, someone stole wire between Billings and Laurel along Montana Rail Link’s (MRL) right-of-way running parallel to Interstate 90. March 21, someone ran off with wire in the same area. These two thefts will cost MRL at least \$7,500, including the labor and wire to make the repairs. Burlington Northern Santa Fe was investigating copper theft across its system and is cracking down on trespassers because of the theft problem and accidents when people get too close to trains. Source: http://billingsgazette.com/news/local/copper-thieves-targeting-rail-lines/article_be7a83ea-527b-51cb-9cf5-4fb97bec5e7b.html

(Montana) EPA orders oil firms to pay for moving Poplar-area drinking wells. The U.S. Environmental Protection Agency (EPA) announced an agreement with Murphy Exploration & Production, Pioneer Natural Resources USA Inc., and Samson Hydrocarbons March 26, which requires the three oil companies to pay the city of Poplar, Montana, \$320,000 for costs the city incurred moving water wells out of the path of a pollution plume that began in the East Poplar oil field. The plume is moving toward the eastern Montana city and threatening its water supply. A second provision in the agreement requires that the companies continue to monitor Poplar’s water supply monthly and provide treatment, or an alternate drinking water source, if certain “trigger levels” indicating a decline in water quality are reached. The EPA estimates that more than 40 million gallons of brine entered the drinking water aquifer over 5 decades. Water treated by the city’s treatment system is safe to drink, but monthly samples collected by the oil companies indicate an upward trend in total dissolved solids, chloride, and sodium, according to the EPA. The saline wastewater also has trace metals, inorganic salt concentrations, and volatile organic compounds. Source: <http://www.greatfallstribune.com/article/20120327/NEWS01/203270301/EPA-orders-oil-firms-pay-moving-Poplar-area-drinking-wells>

(South Dakota) Corps to inspect spillway area. To survey possible damage caused by high releases during 2011’s summer flooding, the U.S. Army Corps of Engineers will begin an underwater inspection March 30 of the spillway apron at Gavins Point Dam near Yankton, South Dakota. The Corps has been inspecting parts of the spillway not under water, and contracted divers will move forward with an extensive inspection of the spillway apron. The project operations manager said the main focus of the inspection will be on the condition of about 250 drains that help release hydraulic pressure in the spillway. The inspection will also include ground penetrating radar to determine the condition of the concrete slab and the gravel frost blanket underneath the concrete. The inspection is expected to be complete April 6. Boating and fishing will be prohibited in the spillway area during the inspection. Source: <http://www.yankton.net/articles/2012/03/30/community/doc4f752e6c489e4004411453.txt>

UNCLASSIFIED

NATIONAL

(Michigan) Michigan militia members acquitted of conspiracy; leader faces lesser charges. The trial against members of the so-called Hutaree militia resumed March 29 for the Michigan-based group's leader and his son, who face weapons charges. The stakes, however, are considerably lower after a federal judge in Detroit March 27 dropped the more serious charges of sedition and conspiracy to use weapons of mass destruction against the government. The directed verdict cleared several of the original nine defendants of all charges. Federal authorities accused the nine members of the "Christian warrior" militia of homegrown terrorism. The FBI planted a secret informant and FBI agent in the militia in 2008 to record the activities of the group. The video and audio recordings became the crux of the federal case, including clips of the man's son making anti-government statements and remarks about killing police officers. The defendants all faced a maximum sentence of life in prison. However, in a trial that began in February, the federal district judge said she did not find the government's evidence sufficiently proved that the Hutaree militia had planned a conspiracy against the government. The remaining charges of weapons possession rest on the leader and his son, both of whom have already spent 2 years in prison. The government claims the two were in possession of unregistered automatic weapons. If convicted, the pair could face a maximum penalty of 10 years in prison. Source: http://www.cnn.com/2012/03/28/justice/michigan-militia-trial/index.html?hpt=us_c2

INTERNATIONAL

Very high radiation, little water in Japan reactor. One of the crippled nuclear reactors at Japan's Fukushima nuclear power plant still has fatally high radiation levels and much less water to cool it than officials had estimated, according to an internal examination conducted March 27. An industrial endoscope equipped with a tiny video camera, a thermometer, a dosimeter, and a water gauge was used to assess damage inside the No. 2 reactor's containment chamber. The No. 2 reactor is the only one that officials have been able to closely examine so far. Radiation levels of up to 70 sieverts per hour inside the container were found, according to a spokesman for Tokyo Electric Power Co. The probe also found that the containment vessel had cooling water up to only 60 centimeters (2 feet) from the bottom, far below the 10 meters estimated when the government declared the plant stable in December. Source: http://santamariatimes.com/news/world/very-high-radiation-little-water-in-japan-reactor/article_62088f25-1aeb-5167-8664-2760ffe9104f.html

North Sea exclusion zone set as gas surges from leak. A cloud of explosive natural gas boiling out of a leaking drilling platform off the coast of Scotland led to the evacuation of hundreds of workers and the creation of a 2-mile exclusion zone, MSNBC reported March 27. Coast guard officials ordered shipping to come no closer than 2 miles from the abandoned Elgin platform, located 150 miles off Aberdeen, and said there was a 3-mile exclusion zone for low-flying aircraft such as helicopters, the BBC reported. Energy firm Total UK, which operates the platform, said it did not know the source of the leak and was considering all options including drilling a relief well — a solution that could take 6 months. It evacuated 238 workers from the

UNCLASSIFIED

platform after the leak was spotted March 25, according to a report in the Scotsman. The report said Shell reduced its workforce on two nearby offshore installations because of the drifting gas. Reuters reported the company enlisted the services of Wild Well Control, which was heavily involved in the BP's Deepwater Horizon oil spill in the Gulf of Mexico in 2010.

Source: <http://worldnews.msnbc.msn.com/news/2012/03/27/10884614-north-sea-exclusion-zone-set-as-gas-surges-from-leak>

Villages evacuated, two trapped after dam explosion in Turkey. Two workers were left trapped under rubble after an explosion tore through a water pumping station at HancagÄ±z Dam in the southeastern province of Gaziantep, Turkey, March 26. There were no initial reports of damage to the dam itself, but officials evacuated surrounding villages in case of a possible collapse. The workers entered a 400-meter tunnel to open a main valve at a pumping station when an explosion shook the tunnel. A 1-ton generator at the pumping station was torn apart and the workers were trapped under the wreckage. Officials said the explosion happened 200 meters from the dam, and that cracks formed on pipes carrying waters to agricultural fields. There is a risk the cracks could become wide tears along the pipes, they added. The explosion was thought to have been caused by methane gas trapped in the tunnel. Source:

<http://www.hurriyetdailynews.com/villages-evacuated-two-trapped-after-dam-explosion-in-turkey.aspx?pageID=238&nid=16893&NewsCatID=341>

BANKING AND FINANCE INDUSTRY

Hackers breach credit card processor; 50K cards compromised. Global Payments Inc, an Atlanta-based payments processor, was broken into by hackers, leaving more than 50,000 card accounts potentially compromised, according to news reports March 30. The breach occurred sometime between January 21 and February 25 according to notices that Visa and MasterCard sent to banks recently. The extent of the breach and damages are still unknown, but it appears to be rather small based on initial reports from the Wall Street Journal and elsewhere. A notice sent by credit union service organization PSCU to its customers indicated Visa alerted it March 23 that 46,194 Visa accounts might have been compromised. However, that number was downgraded to just 26,000 after eliminating duplicate account numbers and cards with invalid expiration dates, according to the Journal. Only about 800 accounts are known to have had fraudulent activity on them so far, according to a security blogger who broke the story and reported that Track 1 and Track 2 data had been taken, making it easy for criminals to clone the cards and use them for fraudulent activity. The number of accounts showing fraudulent activity could rise, however, as the investigation continues. Source:

http://www.wired.com/threatlevel/2012/03/global-payments-breached/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+%28Wired:+Index+3+%28Top+Stories+2%29%29&utm_content=Google+Reader%20%3Chttp%3A%2F%2Fwww.wired.com

Justice Department sues national tax preparation firm and franchisees to stop alleged pervasive tax fraud. The United States has filed civil injunction lawsuits in five cities seeking to shut down both the company that operates Instant Tax Service (ITS) as well as five owners of

UNCLASSIFIED

UNCLASSIFIED

ITS franchises, the Justice Department (DOJ) announced March 28. The government's complaint accuses ITS Financial and its owner of deliberately ignoring systemic and pervasive fraud by ITS franchisees. The complaints allege franchisees across the country intentionally prepare and file fraudulent tax returns to maximize refunds. They do this so ITS Financial and its franchisees can extract large tax preparation fees and charges. The government claims the fees are outrageously high and are often not disclosed. The franchisees named in the complaints allegedly invent phony businesses, fabricate deductions, falsify filing statuses, claim bogus dependents, and disregard rules for claiming the earned income tax credit. The DOJ alleges ITS employees at these franchises have little tax preparation experience, and that the franchise owners encourage them to prepare fraudulent tax returns. The complaint against ITS Financial states that the estimated tax losses from allegedly fraudulent return preparation in 2011 at ITS locations in St. Louis, the Kansas City area, Chicago, Indianapolis, and Las Vegas exceed \$16 million. Source: <http://www.justice.gov/tax/2012/txdv12393.htm>

Hackers turn credit report websites against consumers. The most important tool consumers have to fight against identity theft has been turned against them by hackers, MSNBC reported March 26. Web sites that offer consumers a chance to see credit reports are being brazenly used by hackers to steal information. The prices of the reports rise and fall depending on the credit score of the victim. For consumers with credit scores in the 750s, report data might fetch \$80; reports from victims with scores in the low 600s sell for about half that, according to "for sale" pages viewed by MSNBC. The most troubling part of these markets however — many hosted in the .su domain, which stands for the now-defunct Soviet Union — is the ready availability of credit reports and the hackers' bragging about how easy it is to infiltrate Web sites such as AnnualCreditReport.com or CreditReport.com. Criminals with stolen credit cards can obtain background reports, credit reports, and ultimately open new accounts using the data, a researcher with Internet security firm CloudEyez.com said. In one how-to posted on a bulletin board, a hacker describes one brute-force attack used to gain access to credit report Web sites. Most sites are protected by "challenge" questions such as, "Which bank holds the mortgage on your home?" But there us a critical flaw, the hacker said: "Normally all ... of them will ask you the same question," the hacker wrote. Because the sites use the multiple choice format, it is easy to use the process of elimination and determine the correct answers, he claims. Source: <http://redtape.msnbc.msn.com/news/2012/03/26/10875023-exclusive-hackers-turn-credit-report-websites-against-consumers>

Treasury targets Iranian arms shipments. The U.S. Department of the Treasury March 27 announced the designation of an Iranian cargo airline, Yas Air; Behineh Trading; three Iranian Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF) officials; and one Nigerian shipping agent — all pursuant to Executive Order 13224 for acting for, on behalf of, or providing support to, the IRGC-QF, a designated terrorist entity. The airline, the trading company, and the IRGC-QF officials were involved, respectively, in shipments of weapons to the Levant and Africa, further demonstrating Iran's determination to evade international sanctions. Based in Tehran, Yas Air is an Iranian cargo airline that acts for or on behalf of the IRGC-QF to transport illicit cargo — including weapons — to Iran's clients in the Levant. Yas Air has moved IRGC-QF personnel and weapons under the cover of humanitarian aid. Behineh Trading and the Nigerian

UNCLASSIFIED

UNCLASSIFIED

agent were involved in a weapons shipment seized in Nigeria in late October 2010. This weapons shipment – orchestrated by the IRGC-QF and intended for The Gambia – is part of a larger pattern of Iranian lethal aid shipments to clients in Africa and around the world. Source: <http://www.treasury.gov/press-center/press-releases/Pages/tg1506.aspx>

Traders drop price of silver by exploiting NASDAQ vulnerability. Experts have long argued the flaws present in trading systems can be leveraged to manipulate prices and basically perform fraudulent operations, but a recent incident demonstrated these vulnerabilities. “On March 20, 2012 at 13:22:33, the quote rate in the ETF symbol SLV sustained a rate exceeding 75,000/sec (75/ms) for 25 milliseconds. Nasdaq quotes lagged other exchanges by about 50 milliseconds. Nasdaq quotes even lagged their own trades — a condition we have jokingly referred to as fantaseconds,” Nanex reported. This means that some traders flooded the system which, due to the security holes that exist, caused silver prices to drop considerably. High frequency traders took advantage of the flaws and exploited the NASDAQ silver ETF, a researcher explained. The fantaseconds Nanex refers to is a term that defines a unit of time measurement unveiled back in September 2011 when a “time warp” was recorded in the trading of Yahoo! stock. At the time, exchange timestamps revealed the Yahoo! trades were executed on quotes that came into existence only 190 milliseconds later. By taking advantage of this flaw, traders can execute quotes before they even exist in the system. Zero Hedge believes someone wanted the price of silver to drop at precisely 13:22:33, March 20, so they “bent the laws of relativity” and executed quotes in the future. Source: <http://news.softpedia.com/news/Traders-Drop-Price-of-Silver-by-Exploiting-NASDAQ-Vulnerability-260499.shtml>

Microsoft leads seizure of Zeus-related cybercrime servers. March 26, Microsoft said it and several partners disrupted several cybercrime rings that used a piece of malicious software called Zeus to steal \$100 million over the last 5 years. The company said a consolidated legal case was filed against those allegedly responsible that for the first time applies the Racketeer Influenced and Corrupt Organizations Act. Zeus is difficult for financial institutions to address because of its stealthy nature and advanced spying capabilities that center around stealing online banking and e-commerce credentials. According to a complaint filed under seal March 19 in New York, Microsoft accused the defendants of infecting more than 13 million computers and stealing more than \$100 million. The civil complaint lists 39 “John Doe” defendants, many of whom are identified only by online nicknames. The senior manager of investigations for Microsoft’s Digital Crimes Unit said the creators of Zeus sold “builder kits” to other would-be cybercriminals. Simple versions sold for as little as \$700, while more advanced versions could cost \$15,000 or more, the affidavit said. Microsoft also said this is the first time other parties joined it as a plaintiff in a botnet case. The other plaintiffs are the Financial Services Information Sharing and Analysis Center, and the National Automated Clearing House Association. The court granted Microsoft and its partners permission to seize servers located in Scranton, Pennsylvania, and Lombard, Illinois, March 23. Microsoft took control of 800 domains that are part of Zeus’ infrastructure in an attempt to completely wrest control of the networks from their operators. Source: http://www.computerworld.com/s/article/9225529/Microsoft_leads_seizure_of_Zeus_related_cybercrime_servers

UNCLASSIFIED

UNCLASSIFIED

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

Nothing Significant to Report

COMMUNICATIONS SECTOR

Operation Global Blackout: Real danger or irrelevant? Will the hacker group Anonymous make good on its threat to take down the Internet March 31? Probably not. But it could slow it down, according to many security experts. It may depend in part on how unified Anonymous is about the attack. Anonymous threatened retaliation for the arrests of about 25 of its members in February, and is also focused on what its members believe is a continuing threat by Congress to censor the Internet through anti-piracy legislation. Anonymous is daring anyone to stop Operation Global Blackout — the group announced March 31 as the date of the attack, along with the method they intend to use — disabling the Domain Name Service (DNS) through distributed denial of service attacks on the root servers of the DNS with a tool called “ramp,” or “reflective amplification.” Even with the advance warning, a professor in the department of computing at the University of Surrey believes Anonymous could do some damage. In a piece for BBC, he said the top-level DNS systems are in different countries, are monitored by different organizations, and run on different technologies. He said Anonymous could bring a server down with ramp, in which an army of bots spoof the IP address of a target system and, “cause the DNS to flood the very network it is supposed to be serving.” Source:

[http://www.computerworld.com/s/article/9225635/Operation_Global_Blackout_Real_danger_or_irrelevant?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm_content=Google](http://www.computerworld.com/s/article/9225635/Operation_Global_Blackout_Real_danger_or_irrelevant?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google)

iPhone passcodes can be cracked as quickly as XRY. The four-digit password on Apple’s iPhone is no match for Micro Systemation’s XRY application, according to experts. The password on the popular smartphone can probably keep a regular person who finds the device from breaking into it. However, the software from the Swedish company, which it sells to law enforcement agencies, can crack the code on an iPhone or a smartphone running Google’s Android mobile operating system within minutes. XRY essentially jailbreaks the device in the same manner that regular jailbreakers do. It then runs every combination of four-digit passcodes until it hits the right one. Once that happens, all the data on the phone can be accessed, according to the company. Source: <http://www.eweek.com/c/a/Security/iPhone-Passcodes-Can-Be-Cracked-as-Quickly-as-XRY-708506/>

UNCLASSIFIED

CRITICAL MANUFACTURING

Honda recalls 554,000 SUVs over headlights. Honda Motor Co Ltd, March 30, announced the recall of about 554,000 sport utility vehicles in the United States to inspect for faulty wiring in headlights. Honda said in a statement that the recall affects CR-V SUVs from model years 2002 to 2004 and Pilot SUVs from model year 2003. The automaker will inspect and replace parts of the headlight wiring system that could fail, causing the low-beam headlights not to work and increase the risk of crash. Source: <http://news.yahoo.com/honda-recalls-554-000-suvs-over-headlights-111306046.html>

BMW recalls 367,000 cars in the U.S. BMW announced March 26 that it was recalling 367,000 5-series and 6-series cars manufactured between 2003 and 2010 because a battery cable cover in the trunk may have been incorrectly installed. The problem could lead to chafing of the battery cable which could, in turn, lead to electrical problems, trouble starting, and in some cases fire, the automaker said. In all, BMW recalled 1.3 million cars worldwide for this problem. Owners of affected vehicles will be notified by mail and will be asked to bring their vehicle to a BMW dealer for a 30-minute repair. Source: http://money.cnn.com/2012/03/26/autos/bmw_recall/index.htm?hpt=hp_t2

Arena Lamp recalled by Great American Opportunities due to electrical shock hazard. The U.S. Consumer Product Safety Commission, in cooperation with Great American Opportunities Arena Lamp, March 27 announced a voluntary recall of about 14,500 Great American Opportunity Arena Lamps. The electrical design and construction of the lamps poses the risk of an electric shock to consumers. No injuries have been reported. The recall involves Arena Lamps, also called Disco Lights, Disco Light Projectors, and Arena Light Kaleidoscopes. The lamps were sold at warehouse sales (in temporarily rented space) in Chattanooga and Nashville, Tennessee; Conyers, Georgia; and Bloomington, Illinois from April 2008 through December 2011. The lamps were also given to schools and civic organizations in conjunction with fundraising activities during the same period. Source: <http://www.cpsc.gov/cpsc/pub/prere/12/12139.html>

DEFENSE/ INDUSTRY BASE SECTOR

Oxygen problem in F-22 Raptor remains a mystery. A U.S. Air Force advisory panel said it still cannot explain what caused blackouts and dizziness among pilots flying its supersonic F-22 Raptor. Officials told a Pentagon press conference March 29 that the stealth fighter is safe and continues to fly in the continental United States, with pilots using special sensors, filters, and other safety steps to mitigate problems with the plane's on-board oxygen system. The Air Force said it is putting into place a number of safety recommendations made in the 7-month study. The head of the study panel said officials will continue to investigate the problem until they find its cause. The Air Force's entire fleet of those fighters, which are made by Lockheed Martin Corp., was grounded for 4 months in 2011 until mid-September after pilots complained of lack of oxygen. Source: <http://www.sacbee.com/2012/03/29/4376857/oxygen-problem-in-f-22-raptor.html>

UNCLASSIFIED

China nabbing ‘great deal’ of U.S. military secrets. Testifying before the U.S. Senate Armed Services Committee March 27, the head of the National Security Agency (NSA) and Cyber Command said China is stealing a “great deal” of the U.S. military’s intellectual property, adding that the NSA sees “thefts from defense industrial base companies.” He confirmed speculation that China was behind 2011’s attacks on RSA. Those attacks proved extremely troublesome for U.S. defense contractors. In 2011, Chinese hackers allegedly stole data related to RSA’s SecurID two-factor authentication devices. Soon after, that information was used to break through security safeguards at defense contractors Lockheed Martin, L-3 Communications, and Northrop Grumman. Source: http://news.cnet.com/8301-13506_3-57405684-17/china-nabbing-great-deal-of-u.s-military-secrets/

Internet search yields bogus arms parts from China. U.S. government investigators, using a fictitious company, were able to easily find electronic parts for weapons from China on the Internet and every single item they bought was counterfeit, despite China’s pledge to crack down on fake products, Reuters reported March 26. A new report by the Congressional Government Accountability Office showed that 334 of 396 vendors who offered to sell parts to the fictitious company were from China. It said all 16 parts eventually purchased by the fake company came from 13 China-based vendors, and all were determined by an independent testing laboratory to be counterfeit. Source: <http://www.reuters.com/article/2012/03/26/usa-china-weapons-idUSL2E8EQBM020120326>

EMERGENCY SERVICES

(California) Safety expert praises 2010 burning of bomb house. A safety expert said the burning of a house packed with bomb-making chemicals in San Diego County went so well that safety professionals nationwide use it as a model, the Associated Press reported March 27. The North County Times said a spokesman praised the operation March 26 at an American Chemical Society convention in San Diego. Authorities burned the Escondido-area home in 2010 after deciding it was too dangerous to remove bomb components, thousands of rounds of ammunition, and stockpiles of unstable chemicals that could go off with a tap. Sixty agencies were involved and the unprecedented operation went off without injury or contamination. Source: http://www.mercurynews.com/news/ci_20264500/safety-expert-praises-2010-burning-bomb-house

ENERGY

EPA proposes rules for carbon dioxide emissions from new power plants. New coal-fired power plants will have a harder time getting built if they do not include technology that limits carbon emissions under proposed rules released March 27 by the U.S. Environmental Protection Agency (EPA). The rules would put national limits on the amount of carbon released by power plants run by natural gas, coal, or other fossil fuels. However, they would apply only to new plants or plants set to begin construction within the next year. The EPA Administrator said the rules reflect industry moves toward natural gas as the fuel of choice for new electric

UNCLASSIFIED

UNCLASSIFIED

power plants. The rules will limit future greenhouse gas emissions, she said. Source: <http://newsok.com/epa-proposes-rules-for-carbon-dioxide-emissions-from-new-power-plants/article/3661345>

(Indiana; Illinois) Magellan shuts oil products pipeline after diesel leak. Magellan Midstream said it shut down a refined products pipeline in Illinois March 21 after reporting a potential 250 barrels leak of diesel fuel 30 miles west of Chicago. The 12-inch diameter pipeline, which runs between Iowa City, Indiana, and Franklin Park, Illinois, was shut down. "This incident will not impact supply to our terminals in Iowa, Illinois, or other terminals connected to the Magellan Pipeline system," a Magellan spokesman said. March 22, he said Magellan had not determined when it would restart the pipeline. Source:

<http://www.reuters.com/article/2012/03/22/pipeline-operations-magellan-idUSL1E8EM64720120322?feedType=RSS&feedName=marketsNews&rpc=43>

FOOD AND AGRICULTURE

FSIS issues new trim sampling requirements. The USDA's Food Safety & Inspection Service (FSIS) issued a notice the week of March 19 that gives its inspection personnel specific instructions on how to randomly select the beef trimmings to be tested under the MT50 project code, which includes E. coli testing in trim. The notice instructs inspectors to collect samples from all types of trim if a plant is producing multiple types. Previously, inspectors were only required to collect samples for one type of trim. The notice also has instructions for sampling ammoniated beef. Inspectors "are not to combine samples from two piece chucks with source materials designated for anhydrous ammonia treatment. The intent is that, through random selection, all products that fall under the beef manufacturing trim sampling program will likely be selected over time." FSIS samples beef manufacturing trimmings at the slaughter establishment. Inspectors then submit information on the type of trim collected through the Public Health Information System. Source: <http://www.foodsafetynews.com/2012/03/fsis-issues-new-trim-sampling-requirements/>

(Illinois; Michigan) Listeria tests prompt recall of halal 'Kubba' beef. Mosul Kubba of Chicago is recalling approximately 1,100 pounds of stuffed, layered beef products due to possible contamination with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced March 29. The problem was discovered during routine FSIS testing. The fully cooked, ready-to-eat, halal beef products were produced March 20 and then shipped to a single distributor in Detroit. Source:

<http://www.foodsafetynews.com/2012/03/listeria-tests-prompt-recall-of-halal-kubba-beef/>

UN: Egypt's foot-and-mouth outbreak could spread. A U.N. agency is warning that an outbreak of foot-and-mouth disease in Egypt could spread and threaten livestock in North Africa and the Middle East, leading to possible food shortages, the Associated Press reported March 29. The disease is not a direct threat to humans, but meat and milk from sick animals are unsafe for consumption. The Italy-based Food and Agriculture Organization said 40,222 cases of the disease are suspected in Egypt and 4,658 animals, mostly calves, have already died. The agency

UNCLASSIFIED

UNCLASSIFIED

said 6.3 million buffalo and cattle and 7.5 million sheep and goats are at risk in Egypt. The agency said Egypt needs regional help in obtaining vaccines. Source:

<http://www.9news.com/news/article/259578/188/UN-Egypt's-foot-and-mouth-outbreak-could-spread>

BPI suspends 70 percent of ammoniated beef production. Responding to a dramatic drop in consumer demand, Beef Products Inc, the nation's leading maker of ammoniated beef now widely known as "pink slime," announced it is suspending production at three plants, Food Safety News reported March 27. The suspended plants account for about 70 percent of the company's capacity to produce Lean Finely Textured Beef (LFTB) treated with ammonium hydroxide. LFTB is essentially low-cost filler made from leftover trimmings once relegated to pet food and other byproducts. Because all beef trimmings are at risk for E. coli or Salmonella contamination, the company adds a mixture of ammonia and water (ammonium hydroxide) to kill bacteria. The product, which is 90 percent lean, is then mixed in with other, higher fat content ground beef. The company said it would temporarily suspend the operations at production facilities in Garden City, Kansas; Amarillo, Texas; and Waterloo, Iowa, which employ around 650 people. The Dakota Dune, South Dakota headquarters plant will continue operating but not at capacity, according to a company spokesman. Source:

<http://www.foodsafetynews.com/2012/03/bpi-suspends-70-percent-of-ammoniated-beef-production/>

(Texas) Drought cost Texas nearly \$8 billion in agriculture losses. Agriculture officials said losses from Texas' historic drought are more than \$2 billion more than previously thought, USA Today reported March 22. The Texas AgriLife Extension Service now estimates crop and livestock losses at \$7.62 billion for 2011. The extension service's preliminary estimate of \$5.2 billion in August 2011 already topped the previous record of \$4.1 billion in 2006. Texas has a long history of drought. Since 1998, it has cost the state's agriculture industry more than \$14 billion. 2011 was the driest year in state history. Source:

<http://www.usatoday.com/weather/drought/story/2012-03-22/texas-drought-losses/53703926/1>

Allergen alert: Mini chocolate chip cookies with walnuts. Whole Foods Market said people who have an allergy or sensitivity to walnuts should not eat certain Mini Chocolate Chip Cookies, which are being recalled due to a labeling error in which walnuts were left off the ingredient list, Food Safety News reported March 23. The recalled cookies were sold at Whole Foods Market stores in Arkansas, Louisiana, Oklahoma, and Texas. Source:

<http://www.foodsafetynews.com/2012/03/allergen-alert-mini-chocolate-chip-cookies-with-walnuts/>

Beef patties recalled due to possible E. coli threat. A Seattle food products distributor is recalling about 16,800 pounds of ground beef patties due to a risk of contamination by E. coli bacteria, the U.S. Department of Agriculture (USDA) reported, according to seattlepi.com March 25. Sysco Seattle Inc. is recalling meat imported from Canada that may have been tainted by potentially deadly E. coli O157:H7. The patties were produced by New Food Classics

UNCLASSIFIED

UNCLASSIFIED

of Burlington, Ontario, and were intended for distribution to restaurants in Washington, Arizona, Colorado, and Texas, the USDA's Food Safety and Inspection Service reported. New Food Classics has been at the center of several recalls in Canada first announced by the Canadian Food Inspection Agency. At least one illness was reported from consumption of meat products affected by the Canadian recall. Source: <http://www.seattlepi.com/local/article/Beef-patties-recalled-due-to-possible-E-coli-3434061.php>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Michigan) Mich. militia head, son plead guilty to gun charge. A Michigan militia leader and his son pleaded guilty March 29 to possessing a machine gun, giving prosecutors their only gain in a domestic terror trial that was upended when the judge dismissed charges of plotting war against the government. The leader and six militia members were cleared March 27 of conspiracy charges. Gun charges were all that remained for the leader and his son after the federal judge said prosecutors in 6 weeks had failed to present evidence of a specific plan to go to war against law enforcement and federal authorities. Source: http://www.google.com/hostednews/ap/article/ALeqM5ieVw2p_yjO8H2uO6fGkMIHhTOhQ?dclid=cd331cd03992481d9027876b33a8cdda

Malicious code in the IT supply chain threatens federal operations. Agencies that deal with national security data and programs must do more to secure their information technology supply chains, said a report released by the Government Accountability Office (GAO) March 23. Federal agencies are not required to track "the extent to which their telecommunications networks contain foreign-developed equipment, software or services," the report said, and they typically are aware only of the IT vendors nearest to them on the chain, not the numerous vendors downstream. That has left IT systems at the Energy, Homeland Security, and Justice departments more vulnerable to malicious or counterfeit software installed by other nations' intelligence agencies or by non-state actors and hackers. U.S. enemies could use the software to secretly pull data from government systems, erase or alter information on those systems, or even take control of them remotely. The Justice Department has identified measures to protect its supply chain, but has not developed procedures to implement those measures, the report said. Energy and Homeland Security have not identified measures to protect their supply chains at all, according to the GAO. It also examined the Defense Department, which it said had designed and effectively implemented a supply chain risk management program. Defense has reduced its supply chain risk through a series of pilot programs and expects to have "full operational capability for supply chain risk management" by 2016, the report said. The U.S. Computer Emergency Readiness Team inside the DHS found about one-fourth of roughly 43,000 agency-reported security incidents during fiscal 2011 involved malicious code that could have been installed somewhere along the supply chain, the GAO said. The report recommended that Energy and Homeland Security officials develop and implement firm procedures to protect against supply chain threats. The departments largely agreed with the

UNCLASSIFIED

UNCLASSIFIED

GAO's assessments, the report said. Source:

http://www.nextgov.com/nextgov/ng_20120323_1655.php

(Virginia) Virginia Tech approves new firearms ban. A new regulation at Virginia Tech in Blacksburg, Virginia, bans concealed firearms and other weapons from university buildings and major events such as football games. The school's board of governors approved the measure March 26. The new rule replaces an existing policy, and it concerns firearms carried both by concealed permit holders and non-permit-holders. The state attorney general said in July 2011, universities did not have the authority to ban people from bringing guns into school facilities, as long as they have concealed carry permits. Those permitted under Virginia state law to own a firearm must be allowed to carry it openly, or concealed with a permit on the open grounds of public institutions, he said. But in January, the Virginia Supreme Court ruled public universities could ban open carrying of firearms in buildings and at events. Virginia Tech officials said March 26 that legal opinion had changed, and the regulation was approved without comment. Source: http://www.msnbc.msn.com/id/46869819/ns/local_news-washington_dc/#.T3H6tdl26U8

Warning: New Homeland Security phishing scheme. A new e-mail spoofing the DHS has been spotted making the rounds, WPXI Pittsburgh reported March 23. The message indicates the government agency intercepted a cashier's check with the recipient's name on it and they need additional information. At first glance, the e-mail looks authentic, with a colorful letterhead and a government address. Further examination, however, reveals red flags. These include the fact the sender's address is from a Gmail account. "Many times the red flags that we see in these phishing emails are misspelling of words or language that normally we wouldn't use," said the president and CEO of the Pittsburgh Better Business Bureau. The e-mail asks for a user's name, address, and phone number, along with financial data such as a bank account number or an ATM card. Source: <http://www.wpxi.com/news/news/local/warning-new-homeland-security-phishing-scheme/nLbjp/>

(Mississippi) Mississippi State president: Student's shooting believed 'isolated incident'. The shooting death of a Mississippi State University student in a campus dorm room in Starkville, Mississippi, is thought to be an "isolated incident," and there is no indication others are endangered, the school's president said March 25. Campus police were notified March 24 of an incident in Evans Hall, a dorm for male students. The student was found with "what appeared to be serious injuries". He was transported to a nearby hospital, but "could not be saved," the president said. The vice president for student affairs said the victim was shot more than once. Three men who did not appear to be university students were seen fleeing in a blue sedan, he said. The shooting prompted the school to send out a campus-wide alert through a series of text messages. Police were talking to witnesses and reviewing surveillance tapes. Campus police stepped up patrols, the president said, assisted by officers from Starkville and the Oktibbeha County Sheriff's Office. Source: http://articles.cnn.com/2012-03-25/justice/justice_mississippi-college-shooting_1_campus-police-campus-safety-dorm?_s=PM:JUSTICE

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Challenges remain in switch to governmentwide ID security system. Federal agencies still are struggling to implement a government wide strategy for securing employee log-in credentials and smart card IDs, General Services Administration (GSA) representatives said March 28. Under a February 2011 directive from the Office of Management and Budget, all executive branches were supposed to have aligned themselves with Federal Identity, Credential, and Access Management (FICAM) by October 2011. FICAM standards are based on a former U.S. President-era Homeland Security Presidential Directive for streamlined and more secure verification procedures within the government. The director of GSA's identity assurance and trusted access division, noted March 28 at a conference at the International Spy Museum in Washington, D.C. that federal security has become so fragmented that some agencies are "almost issuing their own cards just for access to the cafeteria." The FICAM roadmap mandates that agencies switching to OpenID systems for easier Web site logins must "connect authoritative data sources and share data with the shared infrastructure." However, defining "authoritative" raises its own challenges, explained a GSA expert on digital security and service orientation. Though the federal government is not specifically required to use the OpenID blanket identification method for anything besides allowing citizens to logon to dot-gov Web sites, he said the system as it applies to mobile devices is a promising avenue for the government to explore. Source: http://www.nextgov.com/nextgov/ng_20120328_8907.php

FTC charges that security flaws in RockYou game site exposed 32 million email addresses and passwords. The operator of a social game site agreed to settle charges that, while touting its security features, it failed to protect the privacy of its users, allowing hackers to access the personal information of 32 million users. The Federal Trade Commission (FTC) also alleged in its complaint against RockYou that the company violated the Children's Online Privacy Protection Act Rule (COPPA Rule) in collecting information from about 179,000 children. The proposed FTC settlement order with the company bars future deceptive claims by the company regarding privacy and data security, requires it to implement and maintain a data security program, bars future violations of the COPPA Rule, and requires it to pay a \$250,000 civil penalty to settle the COPPA charges. Source: <http://ftc.gov/opa/2012/03/rockyou.shtm>

Malware to increasingly abuse DNS. Security researchers have looked at ways to abuse the domain-name service (DNS) for years. Now, some researchers are warning the protocol may increasingly be used to help criminals communicate with compromised systems. At the RSA Conference in February, a senior security consultant with InGuardians predicted more malware would hide its commands and exfiltrated data in DNS packets. The advantage for malware writers is that, even if a company bars a potentially infected computer from contacting the Internet, malware could send DNS requests to a local server, which would then act as a proxy, bypassing defenses. To date, the tactic has been relatively rare: Perhaps a dozen malware variants have used the domain-name system to send commands and updates to botnets. Source: <http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/232700369/malware-to-increasingly-abuse-dns.html>

UNCLASSIFIED

Kaspersky knocks down Kelihos botnet again, but expects return. For the second time in 6 months, researchers from Kaspersky Lab carried out an operation to take down the newest iteration of the Kelihos botnet, also known as “Hlux.” Microsoft and Kaspersky worked together in September, 2011, on the first Kelihos take-down. The bot then resurfaced in January only to be shut-down again in March by a combination of private firms including Kaspersky, Dell Secure Works, and Crowd Strike Inc. Kelihos is used to send spam, carry out distributed denial-of-service attacks, and steal online currency such as bitcoin wallets. It operates as a “peer-to-peer” bot network, which are more difficult to take down than those with centralized command and control (C&C) servers, according to a senior researcher at CrowdStrike. Peer-to-peer botnets are distributed, self-organizing, and may have multiple command and control servers that disguise themselves as peers. In Kelihos’s case, there were three C&C servers and each had two unique IP addresses, he said. Source: http://threatpost.com/en_us/blogs/kaspersky-sinkholes-kelihos-botnet-again-expects-resurrection-032812

Study: More than 50% of Global 500 use vulnerable open source components. According to a joint research report issued March 25 by Sonatype and Aspect Security, more than 50 percent of the world’s largest corporations have open source applications with security vulnerabilities. That is because more than 80 percent of software applications built in-house by enterprise developers incorporate open source components and frameworks that may be vulnerable. The report — based on a survey of 2,550 developers, architects and analysts — maintains that the widely held view that open source software is consistently high quality “overlooks ecosystem flaws,” chiefly the lack of a notification system alerting developers about vulnerabilities and new versions with fixes. Source: <http://www.zdnet.com/blog/open-source/study-more-than-50-of-global-500-use-vulnerable-open-source-components/10660>

LulzSec hackers return to target CSS Corp and military dating sites. Hacker group LulzSecReborn targeted CSS Corp and Military Singles’ sites, publishing data reportedly taken in the cyber raid online. The hackers claim to have obtained the e-mail details for all staff at IT services firm CSS Corp, and published some details online. Prior to the attack March 25, LulzSecReborn published what it claims are the names, usernames, passwords, and e-mails of 170,937 accounts on MilitarySingles.com. The group has since suggested it still has access to the two sites’ networks and could delete CSS’s information at will. LulzSecReborn said it is not affiliated with the original LulzSec group and has no knowledge regarding the authenticity of LulzSec’s rumored April 1 return. Source: <http://www.v3.co.uk/v3-uk/news/2163902/lulzsec-hackers-return-target-css-corp-military-dating-sites>

Survey scammers fling spam at Pinterest punters. Cyber criminals have latched on the success of social networking site Pinterest by launching a variety of money-making scams. Just like Facebook before it, Pinterest has become a haven for survey scams. Would-be targets are invited to complete surveys under the pretext that they might win an iPad or obtain a discount voucher. In reality, they end up revealing personal information to unscrupulous marketing firms or signing up for mobile phone subscription services of dubious utility. In some cases, these

UNCLASSIFIED

UNCLASSIFIED

scams are even used to distribute malware. Source:

http://www.theregister.co.uk/2012/03/23/pinterest_attracts_scammers/

New TGLoader Android malware found in alternative markets. The TGLoader malware appeared in some alternative Android app markets recently, and researchers at North Carolina State University discovered and analyzed it, finding it has a wide range of capabilities. The malware uses the “exploit” root exploit to get root privileges on compromised phones, and from there it starts installing a variety of apps and Android code that are designed to perform myriad malicious actions. “After that, it further installed several payloads (including both native binary programs and Android apps) unbeknownst to users. The malware also listens to remote C&C servers for further instructions. Specifically, one particular “phone-home” function supported in TGLoader is to retrieve a destination number and related message body from the C&C servers. Once received, it composes the message and sends it out in the background. This is a typical strategy that has been widely used in recent Android malware to send out SMS messages to premium-rate numbers,” an assistant professor at North Carolina State wrote in an analysis of the new malware. Source: http://threatpost.com/en_us/blogs/new-tgloader-android-malware-found-alternative-markets-032612

Facebook scammers host Trojan horse extensions on Chrome Web Store. Cybercriminals are uploading malicious Chrome browser extensions to the official Chrome Web Store and using them to hijack Facebook accounts, according to security researchers from Kaspersky Lab. The rogue extensions are advertised on Facebook by scammers and claim to allow changing the color of profile pages, tracking profile visitors, or even removing social media viruses, a Kaspersky Lab expert said March 23. He recently observed an increase in Facebook scams that use malicious Chrome extensions and originate in Brazil. Once installed in the browser, these extensions give attackers complete control over the victim’s Facebook account and can be used to spam their friends or to Like pages without authorization. In one case, a rogue extension masqueraded as Adobe Flash Player and was hosted on the official Chrome Web Store, the expert said. By the time it was identified, it was already installed by 923 users. Uploading multiple rogue extensions on the Chrome store and running many Facebook spam campaigns to advertise them allows attackers to quickly compromise thousands of accounts. The accounts are then used to earn scammers money by Liking particular pages. The people behind these campaigns sell packages of 1, 10, 50, or 100 thousand Likes to companies who wish to gain visibility on Facebook. Source:

[http://www.computerworld.com/s/article/9225536/Facebook_scammers_host_Trojan_horse_extensions_on_Chrome_Web_Store?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm](http://www.computerworld.com/s/article/9225536/Facebook_scammers_host_Trojan_horse_extensions_on_Chrome_Web_Store?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm)

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

UNCLASSIFIED

POSTAL AND SHIPPING

(California) San Jose post office reopens after powder found. Authorities reopened a post office in downtown San Jose, California, about two and a half hours after an evacuation March 27 prompted by concerns about a white powder discovered in a package. A U.S. Postal Service spokeswoman told the San Jose Mercury News the powder turned out to be a harmless herbal remedy from Vietnam that a man had ordered for his child. Fire officials said two employees had complained of sore throats and headaches after being exposed to the package. They said the pair, as well as a third employee in the area, were decontaminated by a HAZMAT unit. Source: http://abclocal.go.com/kgo/story?section=news/local/south_bay&id=8597216

PUBLIC HEALTH

(Washington) Washington state hit hard by whooping cough. Whooping cough is hitting the State of Washington particularly hard, ABC News reported March 28. Numbers released March 27 showed that whooping cough cases have risen to 549 in 2012. At this time in 2011, there were 88 pertussis cases in the state, said the communications director of Washington's health department. The annual number of cases will likely exceed the 950 yearly total the state saw in 2011. Source: <http://abcnews.go.com/blogs/health/2012/03/28/washington-state-hit-hard-by-whooping-cough/>

Dot Pharmacy: New web weapon in war on duff drug peddlers. An American trade group wants to create top-level domain name .pharmacy to stem the sale of bogus medicines online. The National Association of Boards of Pharmacy (NABP) will file the application with Internet policymaker ICANN, according to FairWinds Partners, a domain-name consulting firm. "The goal of .pharmacy is to provide pharmacists, doctors, nurses, caregivers, patients and others a secure space in which to search for information about or purchase prescription drugs online without having to worry about cybercrime or receiving counterfeit drugs," FairWinds said. Before getting a .pharmacy Web address, companies would be vetted to ensure they are in fact legitimate and licensed, according to FairWinds. FairWinds said the .pharmacy gTLD would be subject to ongoing monitoring for compliance via LegitScript, a U.S.-based pharmacy certification program provider. The news comes as the NABP wages war against a small number of domain name registrars it says are not doing enough to fight the sale of counterfeit treatments online. Source: http://www.theregister.co.uk/2012/03/26/dot_pharmacy_bid/

TRANSPORTATION

Feds probe bus defect that may have caused crashes. Federal safety regulators have begun investigating buses made by Motor Coach Industries Inc. over the past 20 years because the drive shafts can fall out and cause drivers to lose control. The problem has led to two crashes that killed 2 people and injured 50 others, said documents filed March 26 on the National Highway Traffic Safety Administration's (NHTSA) Web site. The probe covers about 4,000 MCI D-Series buses with a steerable rear axle made from 1992 until 2012. Schaumburg, Illinois-based MCI said on its Web site it is the leading maker of intercity buses in the United States and

UNCLASSIFIED

Canada. The probe stems from a complaint filed with the NHTSA by transportation company FirstGroup America, parent of Greyhound bus lines. The company said several drive shafts failed on MCI buses starting March 2010, and the shafts were not held up by safety loops that are supposed to keep them in place. In two cases, drivers lost control, causing multiple injuries and fatalities, the complaint said. Source: <http://www.businessweek.com/ap/2012-03/D9TOCOHO1.htm>

FAA finds Philippine aviation standards lacking. The U.S. Federal Aviation Administration (FAA) found lingering deficiencies in Philippine air safety standards despite the country's efforts to fix the problems, the Associated Press reported March 20. Unqualified personnel inspect aircraft and airport facilities, inspectors accept free rides on the same airlines they are checking, and airlines receive certification despite failing to meet requirements, according to a report summary made available to the Associated Press. Safety and management concerns led the U.S. aviation watchdog to downgrade the Civil Aviation Authority of the Philippines in 2007 and limit U.S.-bound flights from the Philippines. In 2010, the European Union also blacklisted Philippine carriers. The country's transportation and communications secretary said March 20 the government would take measures to address the deficiencies. He acknowledged the FAA findings will adversely affect the Philippine airline industry and may discourage tourists. A team from the Philippine aviation authority is set to visit Washington, D.C. in mid-April to present an action plan to address the more than 20 issues mentioned in the FAA report following the technical review in January. Source: <http://www.businessweek.com/ap/2012-03/D9TK6OT00.htm>

(California) Man arrested at Sacramento airport security with 4 guns. A Montana man was arrested after he tried to bring four loaded guns through a security checkpoint at Sacramento International Airport in Sacramento, California, and is being held without bail, the sheriff's office said March 24. The suspect was arrested March 22 after Transportation Security Administration officers at a checkpoint found a firearm inside a carry-on bag, the Sacramento County Sheriff's Department said in a statement. Further checks showed he was carrying a loaded handgun and had three loaded firearms in his carry-on bags, it said. Sheriff's deputies searched his car at an off-site parking lot and turned up eight more firearms, several of them loaded. The man faces charges including unlawful possession of a loaded firearm, unlawful possession of a concealed firearm, possession of an unauthorized weapon in a public building, and possession of a firearm within a sterile area of an airport, the sheriff's department statement said. Source: <http://www.chicagotribune.com/news/sns-rt-us-airport-gunsbre82n0b3-20120324,0,7550388.story>

WATER AND DAMS

(Florida) Keys man charged in computer hacking. A Key West, Florida man was arrested and charged with illegally accessing computers that belong to the Key Largo Water Treatment Facility, WPLG 10 Miami reported March 25. The man used to work at the facility, but his contract was not renewed. He used usernames and passwords of other current employees to access the system from home. He bragged to police detectives who interviewed him March 14,

UNCLASSIFIED

UNCLASSIFIED

saying he was able to prove the computer system was not secure. The man downloaded e-mails and documents from the system pertaining to him. The facility's computer manager called police in February 2012 after doing a routine check of the e-mail system and finding a number of e-mails addressed to what he recognized as the man's personal e-mail address. The former employee faces 9 misdemeanor and 21 felony counts. Source:

<http://www.local10.com/news/Keys-man-charged-in-computer-hacking/-/1717324/9696274/-/ln6ek/-/>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY);** Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota 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