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.

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

Horace, ND plant evacuated after fire breaks out. The SunGold Foods plant in the Cass County town of Horace, North Dakota was evacuated as a precaution after a fire broke out in an oven roasting sunflower seeds. The Cass County sheriff's office said the seeds caught on fire about 1:40 p.m. May 12, and flames spread to the oven's exhaust, which fell down and ignited other items. A sheriff's deputy said that about 20 workers gathered outside the plant. He said no one was injured. A damage estimate was not immediately available. Source: http://www.wday.com/event/article/id/33431/

Vandalism suspected in power outages. Two apparent acts of vandalism that cut electricity to most residents in Wahpeton, North Dakota and some in Breckenridge, Minnesota early May 12 could be considered acts of terrorism, said a spokeswoman for Otter Tail Power Co. About 1,800 customers were affected by the power outages, she said. Bolts were removed and switches were opened at two locations to interrupt the flow of electricity, according to the spokeswoman and the Wahpeton police chief. "They obviously, I believe, had to have had tools… and knowledge of how it worked," he said. A police officer noticed the first power outage at 2:27 a.m., affecting the north side of Wahpeton. Otter Tail Power crews restored the switches and reported the outages as vandalism. Electricity was restored to all customers by 3:30 a.m. Police have no suspects. The vandal or vandals interrupted power by opening a distribution-line switch and a larger 41.6-kilovolt transmission-line switch. Source: http://www.dl-online.com/event/article/id/52845/group/News/

Highway reopens after derailment. Law enforcement from Richland and McKenzie counties were called in after a May 8 report of a train derailment where five railroad cars went off the tracks at the Dore, North Dakota Exchange off North Dakota Highway 58, northeast of Fairview. At 5:15 p.m., Yellowstone Valley Rail Road officials reported the cars were filled with liquid propane. The McKenzie County Sheriff's Office, along with Fairview, North Dakota police officers, Fairview firefighters, the North Dakota Highway Patrol and the Department of Transportation, evacuated residents within one mile of the accident as a precautionary measure. Highway 58 remained closed to through traffic from the intersection at N.D. Highway 200 to N.D. Highway 1084 Saturday evening and well into Sunday, May 9, as McKenzie County officials investigated. By 4:15 p.m. May 9, the McKenzie County Sheriff's Office reported all five cars had been successfully placed on the tracks once again. Officials said there were no spills, leaks or injuries, and Highway 58 was reopened. The accident remains under investigation. Source: http://www.sidneyherald.com/articles/2010/05/10/news/breaking_news/doc4be85f9d7e10a049138998.txt

Regional

(Minnesota) **H1N1 flu strain linked to two more deaths in Minnesota.** Two more Minnesota deaths, both in 2009, have been linked to complications of the H1N1 flu strain, bringing the state total to 72 flu deaths in the past year. State health officials announced the confirmation May 12. One death

occurred last September, the other in November. There is often a lag between a death and confirmation that it was flu-related because of the complex investigation and testing required by some cases. In another sign that the flu pandemic is largely spent, the Minnesota Department of Health reported that no outbreaks have been reported in schools or long-term care facilities in the past week. Of the 72 deaths attributed to the flu, all but nine have been linked to the H1N1 strain. Source:
http://www.startribune.com/local/93597214.html?elr=KArks:DCiUHc3E7_V_nDaycUiD3aPc:_Yyc:aUU

(Minnesota) **Most Minnesota fish sampled don't carry Scotchguard chemical.** Fish from 54 Minnesota lakes outside the Twin Cities have low or undetectable levels of PFOS, the chemical formerly in Scotchguard, fire retardants and nonstick cookware that has raised health concerns in recent years. On May 11, the Minnesota Department of Health reported the results from tests conducted by the U.S. Environmental Protection Agency (EPA) and recently published in the scientific journal Environmental Science and Technology. PFOS, perfluorooctane sulfonate, and related chemicals have been traced to immune system and other health issues. Over the past four years they have been found at high levels in some Twin Cities' lakes and rivers, and in groundwater. The EPA study, while not a comprehensive sampling of the state's more than 10,000 lakes, seems to indicate that the chemicals are not widely distributed in the state. "This is the first time we've taken a statewide look at the problem, and the good news is that PFOS weren't found in most fish outside the metro area, or were found in levels so low that they wouldn't trigger an elevated fish consumption advisory," a spokesman for the Minnesota Department of Health, said. Source:
http://www.grandforksherald.com/event/article/id/161091/

(Minnesota) **Lake Zumbro contamination came from Pine Island plating plant.** A major source of perfluorooctane sulfonate (PFOS) that has been contaminating fish in Lake Zumbro has been found in a Pine Island, Minnesota plating plant. DS Manufacturing Inc. used perfluorooctane sulfonates as a way to control pollution because it helped stop chromium from contaminating the air inside or letting it get into the air outside. Use of the chemical was completely legal and the company quit using it many months ago. The company and the Pine Island Wastewater Treatment Plant, which receives wastewater from the DS, have been cooperating with the Minnesota Pollution Control Agency (MPCA). The plating plant is using another chemical to control chromium, one that doesn't contain PFOS. Because the chemical was found in high enough concentrations in the lake, the Minnesota Department of Health tightened its recommendation for people eating fish caught from the lake from unrestricted for the general population to once a week. Also, the MPCA has found lower levels of PFOS coming from the Rochester Wastewater Treatment Plant. Source:
http://www.postbulletin.com/newsmanager/templates/localnews_story.asp?z=2&a=452185

(Minnesota) **State issues new requirements for installing underground gas lines.** New Minnesota guidelines are now in place for any business or crew installing new underground gas lines and documenting the installation process. The new requirements were issued in an Alert Notice from the Minnesota Department of Public Safety Office of Pipeline Safety (MNOPS) that was e-mailed to all 57 gas-distribution operators in Minnesota. The requirements are effective immediately. The new installation and documentation requirements are intended to prevent "cross-boring," where underground gas pipelines intersect and puncture privately owned sewer pipes. Minnesota is the first state to issue such requirements, and operators who fail to follow the new guidelines will be subject to citations and fines. On February 1, 2010, a cleaning contractor damaged a natural gas pipeline that

had been inadvertently installed through a sewer service lateral on Villard Avenue in St. Paul. The gas escaped into a home and ignited, causing an explosion and fire that destroyed the home. Source: http://www.kare11.com/news/news_article.aspx?storyid=850777&catid=14

(Montana) **Medical marijuana stores firebombed in Montana.** The Billings, Montana, City Council planned to take up the issue of regulating medical marijuana May 10, in a meeting expected to be intense in the wake of the firebombings of two of the city's medical marijuana storefronts in the last two days. The southern Montana city's dispensaries legally provide marijuana to medical patients who use it for maladies from glaucoma to nausea to lack of appetite. In the latest incidents, the phrase "Not in our town" was spray-painted on the businesses, police said. The police sergeant said Big Sky Patient Care was hit early May 9 and Montana Therapeutics was the target early May 10. Both had a rock thrown through the front door, followed by a Molotov cocktail. In both cases, he said, the fire was put out swiftly and damage was not extensive. Source: http://www.cnn.com/2010/CRIME/05/10/montana.medical.marijuana/?hpt=Sbin

(South Dakota) **Black Hills National Forest roads to stay closed.** Wet weather is causing road problems in the Black Hills National Forest. Seasonally closed roads were to be reopened for summer use May 14, but the U.S. Forest Service said many roads will remain closed to traffic this weekend. Both rain and recent snowfall have made for difficult, muddy conditions on dirt roads and made them susceptible to damage. Roads will be reopened as soon as they dry out. Source: http://cbs4denver.com/wireapnewswy/Many.Black.Hills.2.1694036.html

National

Secretary Napolitano announces nearly $790 million in Critical Infrastructure and Preparedness Grants. The Homeland Security Secretary on May 13 announced the fiscal year 2010 Preparedness Grants for nine federal programs, totaling nearly $790 million to assist state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies. The FY 2010 grants announced include the following programs: Transit Security Grant Program, Freight Rail Security Grant Program, Intercity Passenger Rail (Amtrak), Intercity Bus Security Grant Program, Port Security Grant Program, Buffer Zone Protection Program, Emergency Operations Centers Grant Program, Interoperable Emergency Communications Grant Program, and Driver's License Security Grant Program. Source: http://www.dhs.gov/ynews/releases/pr_1273760215810.shtm

Authorities arrest first suspect in massive identity-theft ring. Indian police said May 12 that they have detained a Ukranian man charged in the U.S. with stealing some 40 million credit and debit card numbers. The suspect was detained after he landed in New Delhi on a domestic flight from the southwestern holiday state of Goa May 10, a police spokesman said. He is one of 11 people wanted by the U.S. Justice Department in "the largest hacking and identity theft case ever prosecuted," which was filed in August 2008. Besides the suspect, three Americans, two Ukrainians, two Chinese, one Estonian, a Belarussian and an unidentified suspect are on the wanted list, the Justice Department said. The group is accused of obtaining credit and debit card numbers by hacking into the computer networks of major U.S. retailers — including Barnes & Noble, OfficeMax, shoe retailer DSW, and Sports Authority. Once inside the network, "sniffer programs" captured credit card numbers, passwords, and account information, police said. The data was stored in encrypted servers controlled

from Eastern Europe and the United States. Source: http://www.darkreading.com/database_security/security/cybercrime/showArticle.jhtml?articleID=224701874

INTERNATIONAL

2 Russian pilots arrested at Berlin airport. Two Russian men, both pilots, were taken into custody May 12 at Berlin's Tegel Airport after a witness told police she suspected they were planning a hijacking. They were overheard speaking in Russian by a woman at an Air Berlin counter before they boarded the plane. The two men, aged 49 and 26, were booked on an Air Berlin flight to Moscow around midday. Though they were both registered pilots, neither was part of the aircraft's crew. Both have been turned over to Berlin police for questioning.The plane was evacuated and its 135 passengers were all questioned. Most were able to take a later flight to Moscow. Source: http://www.cnbc.com/id/37108945

Egypt detains US passenger with weapons in bags. Egyptian authorities detained a passenger arriving at Cairo airport from New York May 12, after finding guns, bullets and knives in his baggage. A U.S. university professor of Egyptian origin had flown in on an EgyptAir flight from New York's JFK airport. Customs officials noticed the passenger looked nervous and decided to open his luggage. They found two handguns and 250 bullets hidden in metal boxes. In a secret compartment in the bag, authorities also found two swords, five daggers and six knives. An investigation has been launched. Source: http://www.google.com/hostednews/afp/article/ALeqM5i0c_q6pz_vu1ItGWFjwF7UaBASvw

Pirates hijack chemical tanker in Gulf of Aden. Pirates in the Gulf of Aden hijacked a chemical tanker carrying a crew of 15 Bulgarians on Tuesday, the European Union Naval Force Somalia said. The Bulgarian-flagged tanker, the MV Panega, was about 100 nautical miles east of Aden, Yemen, en route from the Red Sea to India, the force said in a news release. "As long as the pirates are on board the ship, we are just monitoring the situation," said a Swedish navy commander for the EU naval force. He said he had no reason to believe that anyone had been hurt. Source: http://edition.cnn.com/2010/WORLD/africa/05/11/pirates.hijacked.ship/

Pakistani with bomb residue on hands arrested in Chile. A 28-year-old Pakistani man with explosive residue on his hands was arrested at the U.S. Embassy in Chile, national police said. The man, who had been in Chile since January, was applying for a visa to the United States, said an official with the Carabineros, Chile's uniformed national police. The suspect was arrested May 10 at the embassy and turned over to Chilean authorities. "The embassy has their security procedures in place and their security measures were activated and that required the support of our personnel," the official said. "Our personnel is on site and, according to agreements and protocols, the individual has been in custody of the interior minister." A senior State Department official confirmed the arrest, telling CNN "we found traces of explosives residue and the man was turned over to the Chilean police." The suspect was doing an internship in tourism at a Chilean hotel, CNN Chile said. He is scheduled to be charged May 11 with violating Chile's law on weapons and explosives, CNN Chile reported. Source: http://news.blogs.cnn.com/2010/05/11/pakistani-with-bomb-residue-on-hands-caught-in-chile/

Man arrested over possible Afghan plane attack. An Afghan man has been arrested after an attempted attack in a civilian passenger plane, but the motives behind the incident were unclear, the

interior ministry said May 10. “One of the passengers had a knife and while the plane was flying mid-flight he wanted to commit a destructive action on the plane,” an interior ministry spokesman told Reuters about the May 9 incident. “But before that could happen, security personnel and passengers inside the plane identified the passenger and arrested this suspect ... we’re questioning the man to find out what was his motive.” The ministry could not immediately confirm which airline was involved nor its route. The Afghan was from a northern province. “We have 72 hours to question him and we will soon let you know for what reason he wanted to do this, whether this (was) a hijack or another destructive plan to bring the plane down,” the official said. While there was no confirmation the incident was linked to any militant attack, the arrest comes as the Taliban announced an offensive against foreign troops, Afghan government officials and diplomats said May 11. Thousands of Western and Afghan troops are gearing up to launch a military campaign against the Taliban in their spiritual stronghold in Kandahar next month. Source:
http://www.reuters.com/article/idUSTRE6493GD20100510

Banking and Finance Industry

Feds close in on network of high-tech ATM thieves. A federal task force continued to close in May 13 on a high-tech network of Romanian thieves who are using electronic spyware to loot the accounts of ATM customers at banks in Connecticut and elsewhere in the Northeast. Federal prosecutors disclosed that they have indicted four more Romanian nationals in the scheme, which has resulted in hundreds of thousands of dollars in losses. The task force of federal, state and local police agencies charged another two suspects one year ago, and it is continuing to hunt for other suspects. All those charged so far in the scheme are accused of installing what are known as skimming devices on ATM machines and on card-activated door locks that banks use to control access to the machines. In addition, the suspects in the scheme are accused of installing pinhole cameras on ATM machines. Banks, which credit customer accounts for fraudulent withdrawals, are the ultimate victims of the scheme, according to federal prosecutors. A U.S. Attorney said May 13 that the four Romanian nationals named in the indictment emptied accounts in Connecticut, New York and Pennsylvania. The four are being held without bail, authorities said. Source:
http://www.courant.com/news/connecticut/hc-hc-atm-skim-0514.artmay14,0,757871.story

(New York) **Wall Street probe widens.** Federal prosecutors, working with securities regulators, are conducting a preliminary criminal probe into whether several major Wall Street banks misled investors about their roles in mortgage-bond deals, according to a person familiar with the matter. The banks under early-stage criminal scrutiny — J.P. Morgan Chase & Co., Citigroup Inc., Deutsche Bank AG and UBS AG — have also received civil subpoenas from the Securities and Exchange Commission (SEC) as part of a sweeping investigation of banks’ selling and trading of mortgage-related deals, the person said. Under similar preliminary criminal scrutiny are Goldman Sachs Group Inc. and Morgan Stanley, as previously reported by The Wall Street Journal. The Manhattan U.S. Attorney’s office and SEC are working hand-in-hand. At issue is whether the Wall Street firms made proper representations to investors in marketing, selling and trading pools of mortgage bonds called collateralized debt obligations, or CDOs. Many major Wall Street banks created CDOs at the behest of players that made bets against the deals — and banks themselves sometimes bet against the deals. Bearish bets paid off when the mortgage market crashed. Federal prosecutors, along with securities regulators, are pursuing a preliminary criminal probe into whether several Wall Street banks misled investors on mortgage-bond deals. Source:

http://online.wsj.com/article/SB10001424052748704247904575240783937399958.html?mod=WSJhpp_MIDDLENexttoWhatsNewsTop

PCI Security Council updates requirements for payment card devices. The council that administers the Payment Card Industry Data Security Standard today released new requirements that vendors of payment card devices will be expected to incorporate into their products going forward. The new requirements are in the latest version of the council's PIN Transaction Security (PTS) requirements and are designed to bolster security on retail point-of-sale card readers and unattended kiosks and payment terminals, such as those found at airports and gas stations. Version 3.0 of the PCI council's PTS includes three new modules to secure sensitive card data for device vendors and their customers. One of the modules contains requirements pertaining to the secure reading and exchange of data on payment-card devices. The requirements would enable the secure reading and encryption of sensitive cardholder data at the point where a credit or debit card is swiped. A second module spells out the security standards that device vendors will be expected to follow while integrating all of the different components that make up an unattended point-of-sale device that accepts PIN-based debit-card transactions. The third module, called Open Protocols, contains a set of new requirements related to wireless-enabled payment-card devices. Source: http://www.computerworld.com/s/article/9176645/PCI_Security_Council_updates_requirements_for_payment_card_devices

(Indiana) **Another bank scam hits Wabash Valley.** Since May 7, both members and non-members of a Normal, Illinois-based credit union, who have service through AT&T, have received text messages saying their ISU Credit Union accounts have been locked. Besides saying the account has been locked, the text message also provides a toll free number to call to fix the problem. "Please do not call the 800 number. They are requesting your debit card number, they want your PIN, they want that security code on the back so that they can run freely with your account information," said the credit union's marketing coordinator. ISU Credit Union said that if anyone receives this text message they should delete it. Also, they should call AT&T and let them know about the scam. Source: http://www.wthitv.com/dpp/news/local/another-bank-scam-hits-the-wabash-valley

FBI promises action against money mules. The FBI's top anti-cyber crime official said May 12 that the agency is planning a law enforcement action against so-called "money mules," individuals willingly or unwittingly roped into helping organized computer crooks launder money stolen through online banking fraud. The acting chief of the FBI's cyber criminal section said mules are an integral component of an international crime wave that is costing U.S. banks and companies hundreds of millions of dollars. He said the agency hopes the enforcement action will help spread awareness that money mules are helping to perpetrate crimes. "We want to make sure the public understands this is illegal activity and one of the best ways we can think of to give that message is to have some prosecutions," the director said at a Federal Deposit Insurance Corporation (FDIC) symposium in Arlington, Virginia, May 11. The conference focused on combating commercial payments fraud. Money mules typically are first contacted by e-mail, usually with a greeting that claims the prospective employer found the recipient's resume on Careerbuilder.com, Monster.com, or some other job-search site. The fraudsters usually represent themselves as international finance or tax companies that are looking to hire "financial agents" to help customers move their money abroad speedily. Candidates often are told the position is a work-at-home job, that no experience is

necessary, and that they need only have access to a computer with an Internet connection. Source: http://krebsonsecurity.com/2010/05/fbi-promises-action-against-money-mules/

Police apprehend Romanian phishing gang. Romanian police investigators have exposed a gang of criminals who fraudulently gained online access to bank accounts and for months, continued to draw money from these accounts. The Romanian Directorate for Investigating Organised Crime and Terrorism (DIICOT) in Bucharest said that after conducting nationwide searches May 9, Romanian police questioned 28 suspects. Since October 2009, the gang is said to have obtained sensitive data, such as online banking and credit card user names and passwords, particularly of Bank of America customers, via phishing attacks. The criminals then transferred money from these accounts via the Western Union financial service and withdrew the money in Vienna, Munich, Prague and Romania. According to the DIICOT, the damages incurred amount to approximately $1 million (Â£665,000). Most of the suspects come from the Romanian city of Constanta on the Black Sea coast. The gang is said to have had 70 members in total. Romanian authorities collaborated with U.S. agencies in investigating the case. Source: http://www.h-online.com/security/news/item/Police-apprehend-Romanian-phishing-gang-997151.html

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Florida) **FBI investigating mosque pipe-bombing as possible domestic terrorism.** FBI agents are reemphasizing the seriousness of a possible hate crime at a Jacksonville, Florida mosque. The FBI is looking at this case as a possible hate crime, and now they are analyzing it as a possible act of domestic terrorism. Surveillance video from the Islamic Center shows the arsonist carrying gasoline and the pipe bomb. When the explosive went off, parts of it were found 100 feet away on 9A. Despite receiving few phone calls from the public, investigators are following up on leads. Source: http://wokv.com/localnews/2010/05/fbi-investigating-mosque-pipeb.html

(New York) **Parts of Times Square evacuated after suspicious package.** Authorities evacuated parts of Times Square in New York City once again due to a suspicious package. The suspicious package was called in at 9:06 p.m., though the package is believed to be garbage, NBC New York reports. Source: http://www.foxnews.com/us/2010/05/11/parts-times-square-evacuated-suspicious-package/

(Washington) **3 accused of failed attempt to firebomb store.** Lacey police have arrested three men in connection with a failed attempt to firebomb a convenience store in Lacey, Washington. Police said the three men were apparently upset about a purchase they had made at the store recently. The men constructed a Molotov cocktail and threw it through the window of Harry's Market on College Street. But damage to the store consisted of a broken window because the men forgot to light the Molotov cocktail on fire before throwing it. Source: http://www.kirotv.com/news/23522042/detail.html

(Florida) **Bogus pipe bomb found in Pompano Beach park.** The Broward Sheriff's Office investigated a report of a pipe bomb at a Pompano Beach, Florida park May 11. The incident occurred shortly before 8 p.m. at Exchange Club Park in the 2800 block of Northeast 24th Street, the sheriff's office

said. The sheriff's bomb squad determined that the object was not an actual explosive device, but instead a bogus bomb about 18 inches long consisting of two PVC pipes with exposed wires, tape, and aluminum foil. Source: http://articles.sun-sentinel.com/2010-05-11/news/fl-pompano-pipe-bomb-report-brf-20100511_1_pipe-bomb-exchange-club-park-actual-explosive-device

(Wisconsin) **Bomb threat forces evacuation of Onalaska business.** A bomb threat forces around 30 employees to evacuate an Onalaska, Wisconsin business May 10. It happened around 4:45 p.m. at IC System in the Center 90 building on Sand Lake Road. An employee got a phone call saying there was a bomb in the building. Onalaska Police called in the La Crosse Police Department's bomb sniffing dog to do a sweep of the building. No bomb was found and IC System employees were allowed back into the building just before 6:30 p.m. Source: http://www.wkbt.com/Global/story.asp?S=12460587

(Pennsylvania) **Prom bomb threat puts an abrupt end to festivities.** State police are investigating a bomb threat made by an unidentified male caller that abruptly ended a high school prom May 8 at Ehrhardt's Waterfront Resort in Palmyra Twp. in Pike County, Pennsylvania. The resort owner said he was told by a male caller that a bomb was on the premises and that all male students had to be evacuated or the bomb would be detonated. The caller also stated that the female students of the Wayne County School District had to remain inside. Resort staff and school officials followed the caller's instructions. All students were eventually evacuated. State police arrived and conducted an extensive search for the bomb but found nothing. Source: http://thetimes-tribune.com/news/prom-bomb-threat-puts-an-abrupt-end-to-festivities-1.779061

Communications Sector

Lawmaker challenges broadband providers on net neutrality. If broadband providers do not want the U.S. Federal Communications Commission (FCC) to reclassify broadband as a regulated service, Congress is willing to pass a network neutrality law and address a major reason for reclassification, a senior lawmaker said May 13. Broadband providers have a second option to the FCC Chairman's proposal to reclassify broadband transmission as a common-carrier service, said a democratic U.S. representative from Virginia, who is also chairman of the communications and Internet subcommittee of the House Energy and Commerce Committee. With enforcement of net neutrality rules a major driver for the chairman's reclassification plan, broadband providers instead could work with the subcommittee to craft a net neutrality law, the representative said. Source: http://www.computerworld.com/s/article/9176721/Lawmaker_challenges_broadband_providers_on_net_neutrality

Telecom DoS hides cyber crime. The recent spike in unsolicited and mysterious telephone calls may be part of a new scheme to use telecommunications distributed denial of service (DDoS) attacks to distract individuals from ongoing cyber crime, the FBI warned recently. According to the FBI, cyber criminals are using telephone calls to mobile and land lines to distract victims from the attempts by criminals to empty their bank and trading accounts. The attacks, known as telephony denial-of–service (TDOS), have surged in recent weeks, according to telecom companies working with the FBI. Using automated systems, cyber crooks place calls to prospective victims, and while the victim is distracted by the call, the criminals transfer funds from the victim's bank or trading accounts. As a result, financial institutions that detect the fraud are unable to get in touch with the victim until it is too late. "Following that first incident in November 2009, we have recently seen an increase in this

activity targeting our customers across the country," said the associate director of global fraud management for AT&T. Source: http://www.thenewnewinternet.com/2010/05/12/telecom-dos-hides-cyber-crime/

Drifting satellite threatens US cable programming. A TV communications satellite is drifting out of control thousands of miles above the Earth, threatening to wander into another satellite's orbit and interfere with cable programming across the United States, the satellites' owners said May 11. The communications company Intelsat said it lost control of the Galaxy 15 satellite April 5, possibly because the satellite's systems were knocked out by a solar storm. Intelsat cannot remotely steer the satellite to remain in its orbit, so Galaxy 15 is creeping toward the adjacent path of another TV communications satellite that serves U.S. cable companies. Galaxy 15 continues to receive and transmit satellite signals, and they will probably overlap and interfere with signals from the second satellite, known as AMC 11, if Galaxy 15 drifts into its orbit as expected around May 23, according to the two satellite companies. AMC 11 receives digital programming from cable television channels and transmits it to all U.S. cable systems from its orbit 22,000 miles (36,000 kilometers) above the equator, SES World Skies said. It operates on the same frequencies as Galaxy 15. Source: http://www.google.com/hostednews/ap/article/ALeqM5jsD1ADq1E1T72pmwbLWgez1asEZgD9FKU1PO0

Bill would require FCC report before reclassifying broadband. A Florida Congressman has introduced legislation to require the U.S. Federal Communications Commission (FCC) to deliver a detailed cost-benefit analysis to Congress before moving forward with a plan to reclassify broadband as a regulated common-carrier service. The bill would also require the FCC to conduct a market study to show "market failure" in the broadband industry before moving forward with the plan to reclassify broadband. The FCC Chairman's plan to reclassify broadband as a regulated service is a mistake the Florida Representative said at a press conference May 11 organized by Americans for Prosperity, an antiregulation advocacy group. The effort will hurt the FCC's goal of making broadband available to all U.S. residents, he said. "I think this is a partisan move by him to regulate the Internet," the Representative said. "This curious step by [the] Chairman would reverse course and ... do an end run around Congress, where this issue should and must be debated first." Source: http://www.computerworld.com/s/article/9176583/Bill_would_require_FCC_report_before_reclassifying_broadband

FCC to establish cyber certification program. The Federal Communications Commission (FCC) wants to establish a cybersecurity certification program for private sector telecommunications networks. In a Federal Register notice released May 11, the agency says the undertaking would be voluntary for broadband and other communication service providers. "The Commission's goals in this proceeding are to increase the security of the nation's broadband infrastructure, promote a culture of more vigilant cyber security among participants in the market for communications services, and offer end users more complete information about their communication service providers' cyber security practices," the FCC writes in the notice. The commission wants vendors to answers numerous questions about how such a program would work, what security criteria should be included, whether they have at the legal authority to even create such a certification program and more. "The security of the core communications infrastructure - the plumbing of cyberspace - is believed to be robust," the FCC states. "Yet recent trends suggest that the networks and the platforms on which Internet users rely are becoming increasingly susceptible to operator error and malicious cyber attack."

PandaLabs reports that in 2009 it detected more new malware than in any of the previous 20 years. It also reports that in 2009, the total number of individual malware samples in its database reached 40 million, and that it received 55,000 daily samples in its laboratory, and this figure has been rising in recent months. The criteria for the voluntary program would address four areas: secure equipment management, updating software, intrusion prevention and detection and intrusion analysis and response. The FCC wants to make the private sector responsible for developing and maintaining the security criteria, accrediting auditors to conduct assessments and maintain a database of service providers who meet the standards. Source: http://www.federalnewsradio.com/?sid=1954347&nid=35

Defense Industrial Base Sector

Strike at Boeing Co. plant, pricey C-17 military-jet production program to suffer. A strike at a Long Beach, California-based Boeing Co. plant has reportedly thrown a thorn in the side of a C-17 military-transport jet program that Congress has fought for years to save from Pentagon cancellation threats. "The real rub is the life of the program," said a Frost & Sullivan aerospace analyst. "While both the union and Boeing talk about the potential for more sales to keep the line open, this may effectively seal its fate ... the defenders of the program in Congress have pretty well spent their chips on past rescues of the program." About 1,700 assembly-line workers from the plant have picketed twice this week, asking for better medical and pension benefits. Employees rejected a 46-month contract offer last week from management. Orders for Boeing-built C-17s, used mainly by the U.S. Air Force at a price tag of about $200 million each, have declined steadily and Boeing officials said that the company will decrease its annual production rate of the jets from 16 to 10 by mid-2011. "The leadership of the Air Force is clear: They do not need and cannot afford more C-17s," the Defense Secretary said in a speech. Source: http://www.mysmartrend.com/news-briefs/news-watch/strike-boeing-co-plant-pricey-c-17-military-jet-production-program-suffer-ba

(California) **Suspect in truck sought after bomb hoax at explosives site.** Authorities are looking for a suspect seen in a black truck outside Pacific Scientific Saturday morning, May 8, shortly before a security guard discovered a suspicious package, which a bomb squad blew up as a precaution before realizing it was a hoax. A security guard at the small-explosives manufacturer located outside Hollister, California along Union Road, noticed the suspicious package shortly after 8 a.m. on a shoulder of the driveway entrance, said a spokesman with the San Benito County Sheriff's Office. It was about the size of a phone book and was wrapped with duct tape, with no other writings or indications of what might have been inside, according to the sheriff's office.The security guard told investigators that a small, black truck had pulled to the side of the road for "some time" before it was left there. When the guard looked up at one point, the truck was gone and the suspicious package was in the road, the spokesman said. Local authorities thought it looked suspicious and called in help from the Santa Clara County Sheriff's Office bomb squad. A three-person bomb-squad team arrived and used a robot to get close to the package. The camera on the robot showed that "something didn't look right," the spokesman said, so a bomb-squad member put on a protection suit, approached the package and used a hand-held X-ray machine to examine it. The X-ray revealed there were a lot of wires within the package. "They couldn't tell if it had any explosives or not," the spokesman said. "It appeared to them it did not." Still, authorities decided to attempt a detonation in case there were explosives inside. They blew up the package at the same spot and determined there

were no explosives, the spokesman said. Source: http://hollisterfreelance.com/news/265535-suspect-in-truck-sought-after-bomb-hoax-at-explosives-site

Critical Manufacturing

Car hackers can kill brakes, engine, and more. University researchers have taken a close look at the computer systems used to run today's cars and discovered new ways to hack into them, sometimes with frightening results. The security researchers said that by connecting to a standard diagnostic computer port included in late-model cars, they were able to do some nasty things, such as turning off the brakes, changing the speedometer reading, blasting hot air or music on the radio, and locking passengers in the car. In a late 2009 demonstration at a decommissioned airfield in Blaine, Washington, they hacked into a test car's electronic braking system and prevented a test driver from braking a moving car — no matter how hard he pressed on the brakes. In other tests, they were able to kill the engine, falsify the speedometer reading, and automatically lock the car's brakes unevenly, a maneuver that could destabilize the car traveling at high speeds. They ran their test by plugging a laptop into the car's diagnostic system and then controlling the car's computer wirelessly, from a laptop in a vehicle riding next to the car. Source: http://www.computerworld.com/s/article/9176778/Car_hackers_can_kill_brakes_engine_and_more

US launches new probe of Toyota over truck recall. The U.S. government launched a new investigation on Monday into whether Toyota Motor Corp promptly notified safety regulators about a pickup truck recall for a steering system problem. The investigation is the latest undertaken by the National Highway Traffic Safety Administration (NHTSA) over disclosure matters that could result in a fine if the company is found to have been tardy in taking action on Hilux trucks. The U.S. safety agency said Toyota conducted a recall of certain Hilux trucks in Japan in 2004 for steering relay rods that were prone to fatigue, cracking, and possible fracture. At the time, Toyota told regulators the problem was limited to vehicles sold in Japan and had not received complaints in the United States, NHTSA said. The automaker then told NHTSA in 2005 the problem had been found in several U.S. models and launched a recall to cover those vehicles. But last week, NHTSA said it was alerted to a number of U.S. consumer complaints filed with Toyota prior to the original 2004 recall in Japan. Source: http://www.reuters.com/article/idUSN1023988320100510

Emergency Services

FBI expanding U.S. Mexican border anti-terrorist corruption task force. The FBI is reporting that they are forming a new border task force to look for and combat possible terrorists entering the U.S. through borders with Mexico and Canada, with a eye on dishonest federal, state and local law enforcement and other officials. FBI-led Border Corruption Task Forces are the cornerstone of efforts to root out corruption. Initially located primarily along the southwest border, the FBI now also has task forces in Detroit, Miami, Florida and San Juan, Texas, and is setting up others in cities like Buffalo, New York, Newark, New Jersey, and Seattle. These task forces generally consist of representatives from the FBI, Department of Homeland Security agencies (including Customs and Border Protection Internal Affairs, Transportation Security Administration, Immigration and Customs Enforcement, and Department of Homeland Security — Office of Inspector General), and state and local law enforcement. Source: http://www.americanchronicle.com/articles/view/155483

Energy

Nothing Significant to Report

Food and Agriculture

Miyazaki plans to slaughter 80,000 pigs, cows on foot-and-mouth outbreak. Japan plans to slaughter more than 80,000 livestock in the southern prefecture of Miyazaki as it seeks to contain an outbreak of foot-and-mouth disease. A total of 73,653 pigs and 6,604 cows have been marked for destruction at 86 farms, the Miyazaki local government said in a statement yesterday. Japan's farm minister said the government plans to compensate farmers, the Nikkei newspaper reported. Source: http://preview.bloomberg.com/news/2010-05-13/miyazaki-plans-to-slaughter-80-000-pigs-cows-on-foot-and-mouth-outbreak.html

(California) **Grape quarantine spreads over half of county's vineyards.** Half of Sonoma County's vineyards soon could come under quarantine due to the European grapevine moth, a pest that infests the Napa Valley and has now been found in six other counties, most recently Merced. California officials are leaning toward a single quarantine area for Sonoma County that extends from north of Healdsburg to the Carneros region south of Sonoma. The exact boundary lines have yet to be spelled out, but "it's pretty much one large quarantine area" rather than a series of smaller ones, a county agricultural commissioner said May 12. The quarantine could take in about 30,000 acres of grapes, about half the county's vineyard land, said the chief deputy agricultural commissioner. The expansion of the quarantine is due to new moths found around Windsor and Healdsburg and to new federal rules. Those rules, proposed by moth experts advising the U.S. Department of Agriculture, now expand the quarantine boundary from three to five miles in all directions from a moth found in an infested area. To date, inspectors have trapped 18 moths in Sonoma County the chief deputy agriculture commissioner said May 12. In contrast, agriculture inspectors have trapped well over 30,000 moths in Napa County, where the pest was first confirmed in the U.S. last September. This year the moth has been found and quarantine areas have been proposed in Sonoma, Mendocino, Solano and Fresno counties. On May 12, a federal spokesman confirmed that three grapevine moths have been found in Merced County, and a quarantine will be established there. The federal government last week announced it has set aside $1 million in emergency funds to fight the moth. Source: http://www.pressdemocrat.com/article/20100512/ARTICLES/100519813/1350?p=all&tc=pgall

Oregon grasshopper plague expected again. Oregon scientists and farmers are predicting a devastating plague of grasshoppers this summer, perhaps worse than western U.S. states experienced last year when Oregon was stormed by 2-inch-long, clear-winged grasshoppers. The grasshoppers ate plants over tens of thousands of acres of in Harney County in 2009 and this summer the ravaged area could double to 140,000 acres in the county. Hungry grasshoppers beginning to hatch in New Mexico and Arizona could make 2010 the worst grasshopper plague since the mid-1980s, said a spokesman for the U.S. Department of Agriculture. Natural population cycles and widespread drought conditions allow the grasshoppers to thrive. Treating the Roaring Springs, Oregon Ranch's grasshopper egg beds with Dimilin, a growth regulator that kills grasshoppers immediately after hatching, probably will cost $4,000 but will save 20,000 acres of grass. Source:

http://www.upi.com/Science_News/2010/05/11/Oregon-grasshopper-plague-expected-again/UPI-78941273611136/

More recalls of Freshway lettuce, second strain of E. coli found. The number of confirmed and probable E. coli O145 infections from Freshway bagged lettuce remained steady at 29 May 11, but additional recalls were announced as evidence of additional contaminated product surfaced. CIDRAP NEWS reported on developing news on a number of fronts. It noted that Freshway has now recalled 72 different types of bagged lettuce in 23 states. The article also pointed out that a second firm, Vaughn Foods of Moore, Oklahoma, has recalled lettuce from the same Yuma, Arizona farm implicated in the original recall. Vaughn is recalling bagged romaine with a sell-by date of either May 9 or May 10, CIDRAP reported. It also indicated that a second, independent strain of pathogenic E. coli was isolated in a Freshway bag of shredded romaine lettuce. CIDRAP said Andrew Smith Co. of California recalled 1,000 cartons or about 23,000 pounds of lettuce sold to Vaughan Foods and to an unidentified third firm in Massachusetts. Source: http://www.foodpoisonjournal.com/2010/05/articles/food-poisoning-information/freshway-lettuce-e-coli-o145-more-recalls-second-strain-of-e-coli/

Poultry industry gets new performance standards. The U.S. Department of Agriculture (USDA) Secretary May 10 announced new performance standards for the poultry industry to use in knocking down Salmonella and Campylobacter contamination levels. He said after two years under the new standards, the USDA's Food Safety and Inspection Service (FSIS) estimates that 39,000 illnesses will be avoided each year under the new Campylobacter standard, and there will be 26,000 fewer illnesses with the revised Salmonella standard. The first-ever Campylobacter standards, and the first revised Salmonella standards since 1996 are targeted at establishments producing young chickens (broilers) and turkeys. The performance standard for Salmonella in young chickens currently is 20 percent or no more tan 12 samples out of 51. After the 60-day comment period when the new standard goes into effect, it will be 7.5 percent or no more than 5 sample tests positive out of 51. USDA will continue to categorize establishments based on their history of test data. The new Campylobacter standard is more complicated, and has existed only since 2005. In the conference call with reporters, the Agriculture Secretary declined to address whether non-O157:H7 strains of E. coli should be banned from meat and poultry. He said he wanted to keep the attention on Salmonella and Campylobacter because they cause so many illnesses. Source: http://www.foodsafetynews.com/2010/05/poultry-industry-gets-new-performance-standards/

U.S. food safety system must integrate human health, animal, and plant pathogen data. The Produce Safety Project May 10, issued a report that examines the steps taken by select European Union (EU) countries to reform their food-safety data collection and analysis systems since the 1990s. Coauthored by the director, and the head of food safety programs at the Emerging Pathogens Institute at the University of Florida, the report, "Building the Science Foundation of a Modern Food Safety System," looks at European countries with strong food-safety systems and makes many recommendations on how to improve those in the United States. A key suggestion is the annual publication of a unified cross-agency report on tracking food-borne pathogens in humans, animals, food and feed. To be produced by the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA) and the U.S. Department of Agriculture (USDA), the annual analyses would summarize surveillance data on human foodborne illnesses – including outbreaks and sporadic cases – and on pathogen contamination in domestic and imported animals, food and feed. "A

national annual report on food safety will actually tell us if we are making progress or not in reducing the burden of food-borne illness," said the director of the Produce Safety Project. "It is a yardstick we don't have now." The analysis would also present trends and provide the evidence basis for measuring food-safety progress and include routinely updated national estimates of the incidence of food-borne illness due to major pathogens. The authors called for these reports to be written in a readable and consumer-friendly manner. Copies of the report are available at www.producesafetyproject.org. Source: http://www.prnewswire.com/news-releases/us-food-safety-system-needs-to-integrate-human-health-animal-and-plant-pathogen-data-93266819.html

Government Sector (including Schools and Universities)

Laptop stolen from VA contractor contains veterans' personal data. A laptop belonging to a contractor working for the Veterans Affairs Department (VA) was stolen earlier this year and the personal data on hundreds of veterans stored on the computer was not encrypted, a violation of a VA information-technology policy, said the top-ranking Republican on the House Veterans Affairs Committee. The VA reported the theft of the laptop from an unidentified contractor to the committee April 28, and informed members that the computer contained personally identifiable information on 644 veterans, including data from some VA medical centers' records, according to a letter to the VA Secretary sent by a Republican Congressman from Indiana. The data was not encrypted, which would have prevented a thief from accessing the information, a requirement Congress and VA issued to all department contractors in 2006 after a laptop containing health data on more than 26 million veterans and their spouses was stolen from a VA employee's home. That laptop later was recovered. The laptop in the recent theft was stolen from a contractor employee's car April 22, and she notified local police within 10 minutes, the chief information officer at VA said. Although the vendor had certified to VA that it had encrypted laptops that stored department data, the chief information officer confirmed the data on the stolen laptop was unencrypted. Source: http://www.nextgov.com/nextgov/ng_20100513_1937.php?oref=topstory
\

(Illinois) **Bomb threats found at two schools.** Two Alton, Illinois district schools were targets of bomb threats May 13, forcing evacuation of students and building searches, with authorities finding no explosives. The disruptions taxed school officials and local law-enforcement agencies. The first bomb threat, in the morning at North Elementary School, 5600 Godfrey Road, in Godfrey, forced students to be bused temporarily to Lewis and Clark Community College. The second threat, in the afternoon at the main building at Alton Middle School, forced relocation of about 750 students — roughly half the student body — and tied up traffic on its Pit parking lot and in the 2200 block of College Avenue. "We took it seriously, but there was not any substance to it," the Alton police chief said about the threat at Alton Middle School. "It's sad that they keep resorting to this horseplay. It disrupts the learning environment, and it is a drain on city resources." The chief said 18 Alton officers responded to the school. Police did not use a canine for the search. "It took nine officers to secure the main building, and nine on the perimeter for traffic control and the evacuation," he said. That left only two officers to respond to any other calls in the city for more than an hour. Source: http://www.thetelegraph.com/news/alton-40075-police-school.html

(Georgia) **Stolen laptop exposes personal data on 207,000 Army reservists.** A laptop stolen from a government contractor last month contained names, addresses and Social Security numbers of more

than 207,000 U.S. Army reservists, Krebsonsecurity.com has learned. The U.S. Army Reserve Command began alerting affected reservists May 7 via e-mail. The public affairs chief for the Army Reserve, said the personal data was contained on a CD-Rom in a laptop that was stolen from the Morrow, Georgia offices of Serco Inc., a government contractor based in Reston, Virginia. The laptop was one of three stolen from Serco offices, but it was the only one that contained sensitive personal information, the public affairs chief said. Serco held the data on reservists as part of its contract with the U.S. Army's Family and Morale, Welfare and Recreation division. As a result, the Army Reserve spokesman said, some of the data on the missing laptop may belong to dependents and spouses of U.S. Army reservists. The e-mail sent to affected service members expresses regret over the incident, but offers little other consolation. Source: http://krebsonsecurity.com/2010/05/stolen-laptop-exposes-personal-data-on-207000-army-reservists/

(Texas) **Man detained with knife at Capitol raises issue of security.** Only a few months after a man opened fire on the south steps of the Capitol in Austin, Texas, another man allegedly brought a knife to a health care meeting May 10 inside the building. The 20-year-old man was detained by Department of Public Safety troopers at a hearing on health-care legislation costs. According to DPS, the man was talking to himself and acting strangely, pointing out lawmakers one by one. A witness reported the man's behavior to authorities, who then took the man out of the room. At some point when the man stood up, a knife fell out from either his pockets or the chair where he was sitting, according to DPS. Someone at the hearing saw the weapon and took it to troopers outside the meeting. The man was then sent to receive a mental health evaluation. Source: http://news8austin.com/content/headlines/270933/man-detained-with-knife-at-capitol-raises-issue-of-security

(Wisconsin) **Dane County bomb squad called to federal courthouse in Madison after abandoned backpack found.** The Dane County bomb squad was called to the federal courthouse in Madison, Wisconsin because of an abandoned backpack. A police spokesman said the bomb squad determined the backpack wasn't a threat about 1 a.m. May 12. Police had cordoned off an area around the courthouse after a guard found the backpack between the building and the building's gas main. The State Journal reports the backpack contained clothing and personal items. Source: http://www.fox11online.com/dpp/news/wisconsin/dane-county-bomb-squad-called-to-federal-courthouse-in-madison-for-abandoned-backpack

(Florida) **Police: Student intended to blow up school.** Students from a Sharpes, Florida high school are back in class May 12 after a fellow student is accused of wanting to blow up their school. Authorities said a 16-year-old Eau Gallie High School student was caught with bomb-making materials May 11 in Brevard County. Police said the student had written instructions defining the best locations to place bombs to cause the most destruction at the school. At school in the student's backpack and locker, police found bomb-making instructions, wire cutters, knives, and unspecified ingredients for bombs. Police did not describe the ingredients or say if they were explosive. The student was arrested before school started. According to the school's principal, "Teachers and the school resource officer were tracking the teenager's Internet use while at school for weeks." The student is charged with attempting to make a destructive device and is being held at the Juvenile Detention Center in Sharpes. Source: http://www.wesh.com/news/23526217/detail.html

(North Carolina) **School locked down briefly after explosive device found on playground.** An elementary school in Winston-Salem, North Carolina was placed on lockdown after a suspicious device was found on a playground May 10. The device made of soda bottles was discovered on a playground at Whitaker Elementary School in Winston-Salem. An official with the Winston-Salem Police Department said some kids were playing near the school this weekend and were trying to build an explosive using soda bottles and antifreeze. The school was placed on lockdown while officials investigated the device. Emergency officials were called to the scene to detonate some of the bottles. No one was injured and the lockdown was lifted shortly after 9 a.m. Source: http://www.myfox8.com/news/wghp-story-school-lockdown-100510,0,3870154.story

Information Technology and Telecommunications

E-mail attack targets HR departments. A targeted attack aimed at human resources departments and hiring managers in the U.S. and Europe that was spotted this week sent 250,000 e-mails during a four-hour period May 12. Researchers at Websense Security Labs discovered the attack, which included the subject line "New resume" and came with a ZIP file attachment and what appeared to be a picture file. When opened, the files spreads bot malware and, ultimately, fake antivirus software. "From what the Websense Security Labs has ascertained, the e-mail campaign would be most relevant to HR departments and managers considering hiring. Employees in these types of roles would most likely be encouraged to view the attachments," said a senior manager of security research for Websense Security Labs. An executable inside the ZIP file contains the Oficla bot, according to the researchers; the bot connects to a command and control server in the davidopolku.ru domain, and also communicates with topcarmitsubishi.com.br, get-money-now.net, mamapapalol.com, and li1i16b0.com. The malware issues a warning message that the victim's PC is "infected," and then it downloads the Security Essentials 2010 fake AV program. The researcher said the attackers appear to be trying to make money both by selling fake AV, and by building out a botnet. "This attack installed a downloader onto the infected user's computer. This means that any payload could be delivered with different directives," he said. Source: http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=224800010

Facebook makes security changes as privacy controversy swirls. Amid a controversy about privacy, Facebook unveiled new security features designed to protect user accounts. "Over the last few weeks, we've been testing a new feature that allows you to approve the devices you commonly use to log in and then to be notified whenever your account is accessed from a device you haven't approved," a software engineer on Facebook's site integrity team, wrote in Facebook's blog. To try out the feature, users can go to the Account Settings page and select the option to receive notifications for log-ins from new devices. "When you log in, you'll be asked to name and save the various devices you use to access Facebook. For example, you can save your home computer, your school or work computer, and your mobile phone. Once you've done this, whenever someone logs in to your account from a device not on this list, we'll ask the person to name the device," he wrote. Facebook is still dealing with controversy over its privacy policies. A European group of data-protection authorities sent a letter to Facebook May 13, about changes the site made late in 2009 that "fundamentally changed the default settings on its social networking platform to the detriment of a user," the group charged. Earlier May 13, Facebook had a meeting where employees asked executives questions about privacy. Facebook officials would not comment on exactly what was said

in the meeting. Source: http://www.eweek.com/c/a/Security/Facebook-Makes-Security-Changes-as-Privacy-Controversy-Swirls-870436/

Twitter phishing scam uses iPhone 4G bait. Security experts are warning of a Twitter phishing scam designed to harvest personal data with the offer of a new iPhone 4G as a lure. A Sophos senior technology consultant wrote in a blog post that the scam employs a "gaggle of profiles, using avatars of sexy young women, pumping out messages to users" saying they could win the device. "A quick look at one of the Twitter accounts spamming out the messages underlines that she is by no means a regular user, but set up specifically to advertise a data-collecting form on behalf of the shady guys behind this scheme, " he said. "Clicking on any of these links takes you to a Web page (currently offering an iPod Shuffle as a prize, rather than an iPhone 4G - that's a letdown, isn't it?) that asks you to fill in a form with your personal data." The form asks users to fill in information such as date of birth, marital status, telephone number and address. Source: http://www.v3.co.uk/v3/news/2263048/phishing-spam-spotted-iphone-4g

'Tamper evident' CPU warns of malicious backdoors. Scientists have devised a chip design to ensure microprocessors have not been surreptitiously equipped with malicious backdoors that could be used to siphon sensitive information or receive instructions from adversaries. The on-chip engines at the heart of these "tamper evident microprocessors" are the computer equivalent of cellophane shrink wrap or aluminum seals that flag food or drug packages that have been opened by someone other than the consumer. They are designed to monitor operations flowing through a CPU for signs its microcode has been altered by malicious insiders during the design cycle. The design, made public this week at the 31st IEEE Symposium on Security & Privacy, comes as an investigation by Engineering & Technology magazine reported that at least 5 percent of the global electronics supply chain includes counterfeit elements that could "cause critical failure or can put an individual's data at risk," according to The Inquirer. While most of that appears to be coming from grey-market profiteers, analysts have long fretted that bogus routers and microprocessors could pose a threat to national security. Source: http://www.theregister.co.uk/2010/05/12/tamper_evident_microprocessor/

European officials chastise Facebook privacy settings. Facebook made "unacceptable" changes to its privacy settings at the end of last year that are detrimental to users, a coalition of European data protection officials warned the social-networking sites May 12. The warning, contained in a letter to Facebook from the Article 29 Data Protection Working Party, could spell more difficulties for Facebook, which was hit with a complaint by U.S. regulators over similar concerns earlier this month. The working party told Facebook of the need for default settings that would only allow access to profile information and friends to self-selected contacts, and that access by search engines should be the explicit choice of users. Facebook has moved to make even more of its users' information publicly available. The defaults settings are typically the most permissive, and users must manually change to more restrictive settings. Privacy groups have said the settings are confusing, frequently change and some users aren't aware of the options, putting their personal data at risk. Source: http://www.computerworld.com/s/article/9176698/European_officials_chastise_Facebook_privacy_settings

Only two patches released by Microsoft for May, as main talking point surrounds SharePoint vulnerability. Microsoft released two bulletins for critical vulnerabilities on the May 11 patch Tuesday. Security bulletin MS10-030 is a Windows-based update resolving a vulnerability affecting

Outlook Express, Windows Mail and Windows Live Mail. Microsoft claimed that to successfully take advantage of this vulnerability, an attacker would either have to host a malicious mail server or compromise a mail server, or they could perform a man-in-the-middle attack and attempt to alter responses to the client. The data and security team manager for Shavlik Technologies, claimed that this bulletin affects every supported Microsoft operating system, however the Microsoft e-mail clients - Windows Live Mail and Windows Mail - are not installed by default on some of the affected operating systems and will require a user to install the client. The other bulletin, MS10-031 addresses one vulnerability in Microsoft Visual Basic for Applications (VBA). The update addresses the vulnerability by modifying the way VBA searches for ActiveX controls embedded in documents. Source: http://www.scmagazineuk.com/only-two-patches-released-by-microsoft-for-may-as-main-talking-point-surrounds-sharepoint-vulnerability/article/169998/

Phishing scheme targets Apple gift cards. Hackers have constructed a bogus Web site designed to steal the account numbers and PINs of gift card holders. This latest consumer phishing scam uses a typosquatted Web site disguised as an official Apple site to trick users into entering their card numbers and PINs in order check the available balance on gift cards for Apple products. The scam is just the latest in a line of sophisticate phishing attacks that has security software companies and law-enforcement agencies urging consumers to take their time and pay close attention to where they are actually conducting transactions to avoid being ripped off. Source: http://www.internetnews.com/security/article.php/3881251/Phishing+Scheme+Targets+Apple+Gift+Cards.htm

New attack tactic sidesteps Windows security software. A just-published attack tactic that bypasses the security protections of most current anti-virus software is a “very serious” problem, an executive at one unaffected company said May 11. On May 5, researchers at Matousec.com outlined how attackers could exploit the kernel driver hooks that most security software uses to reroute Windows system calls through their software to check for potential malicious code before it is able to execute. Calling the technique an “argument-switch attack,” a Matousec-written paper spelled out in relatively specific terms how an attacker could swap out benign code for malicious code between the moments when the security software issues a green light and the code actually executes. “This is definitely very serious,” said vice president of engineering at Immunet, a Palo Alto, Calif.-based anti-virus company. “Probably any security product running on Windows XP can be exploited this way.” According to Matousec, nearly three-dozen Windows desktop security titles, including ones from Symantec, McAfee, Trend Micro, BitDefender, Sophos, and others, can be exploited using the argument-switch tactic. Source: http://www.infoworld.com/d/security-central/new-attack-tactic-sidesteps-windows-security-software-339

Windows 7 ‘compatibility checker’ is a Trojan. Scammers are infecting computers with a Trojan horse program disguised as software that determines whether PCs are compatible with Windows 7. The attack was first spotted by BitDefender May 9 and is not yet widespread; the antivirus vendor is receiving reports of about three installs per hour from its users in the U.S. But because the scam is novel, it could end up infecting a lot of people due to the interest in Windows 7. The scammers steal marketing text directly from Microsoft, which offers a legitimate Windows 7 Upgrade Advisor on its Web site. “Find out if your PC can run Windows 7,” the e-mails read, echoing Microsoft’s Web page. Users who try to install the attached, zipped file end up with a back-door Trojan horse program on their computer. BitDefender identifies the program as Trojan.Generic.3783603, the same one that is

being used in a fake Facebook password reset campaign. Once a victim has installed the software, criminals can pretty much do whatever they want on the PC. Source: http://www.networkworld.com/news/2010/051010-windows-7-compatibility-checker-is.html?hpg1=bn

National Monuments and Icons

(District of Columbia) **Planters averted worse damage at museum.** The UPS truck that smashed into a lobby window of the Smithsonian Institution's Hirshhorn Museum in Washington D.C. plowed through five of the building's 1,200-pound cement security planters, but the planters slowed the runaway vehicle and prevented more damage. The May 10 incident, in which the delivery truck inexplicably careened off Independence Avenue SW, flattened a decorative street light, and smacked into the museum, remains under investigation. The unidentified driver was treated and released from a hospital the same night. Although apparently an accident, the crash seems likely to prompt concern over the hierarchy of security around the city's monument and government core and the evolution of security levels at Washington's icons. Although the truck seemed to push the security planters aside easily, the planters did what they were designed to do: slowed the truck and prevented the damage from being worse. Additional permanent security measures are planned for a future fiscal year. The truck has been recovered and would be part of a company examination of the incident. The cause of the accident is unknown. Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/05/11/AR2010051104778.html

(Texas) **Wildfire danger growing in East Texas.** Due to extremely dry conditions, the Texas Forest Service has shifted some fire crews to southeast Texas because of increasing wildfire occurrence and the presence of hurricane debris. The agency also has mobilized a helicopter to the region to assist with wildfire suppression and structure protection. A recent fuel-dryness map produced by the state forestry and rural firefighting agency shows most vegetation in southeast Texas is either critically or extremely dry. An accompanying fire-danger graphic shows fire danger within this region as either high or very high. Southeast Texas residents especially must use increased caution with all outdoor fire and equipment use. Source: http://www.kfdm.com/news/texas-37769-fire-southeast.html

Postal and Shipping

Nothing Significant to Report

Public Health

CDC issues update on E. coli O145 outbreak. On May 13, the Centers for Disease Control and Prevention (CDC) issued an update on the E. coli O145 outbreak linked to Freshway Foods romaine lettuce. As of May 11, there are 23 confirmed and 7 probable cases related to this outbreak from Michigan, New York, Ohio, and Tennessee. The number of ill persons identified in each state with this strain is: Michigan (10 confirmed and 3 probable), New York (4 confirmed and 3 probable), Ohio (8 confirmed and 1 probable), and Tennessee (1 confirmed). To diagram the outbreak trend, the CDC has created an epidemic curve, or a chart that describes the number of persons that became ill each day. Among the confirmed and probable cases with reported dates available, illnesses began

between April 10 and April 26. Infected individuals range in age from 13 years old to 31 years old and the median age is 19 years. Sixty-six percent of patients are male. Health investigators in New York recently obtained an E. coli O145 isolate from an unopened bag of romaine lettuce that matches the outbreak strain. A separate case-control study in Michigan supported this, finding a significant association between illness and consumption of romaine lettuce from the same processing facility, which is believed to be located in Yuma, Arizona. The CDC said that investigators are using pulsed-field gel electrophoresis, a type of DNA fingerprint analysis of E. coli bacteria obtained through diagnostic testing to identify cases of illness that might be part of this outbreak. This testing is done in public health laboratories as part of the PulseNet network. Investigators have established a common definition of confirmed and probable cases related to this outbreak. An Ohio resident filed an E. coli lawsuit against Freshway Foods May 11. Source: http://www.foodsafetynews.com/2010/05/update-in-e-coli-o145-outbreak/

New enforcement tools help fight health-care fraud. The government says it recovered $2.5 billion in overpayments for the Medicare trust fund last year as the current administration focused attention on fraud-enforcement efforts in the health care industry. Investigators have new tools this year to help crack down on health-care fraud, with the Justice Department and the Health and Human Services Department (HHS) working cooperatively to police companies. The newly enacted Affordable Care Act is designed to lengthen prison sentences in criminal cases, and the new law provides an additional $300 million over the next 10 years for stronger enforcement. It also gives the government new authority to step up oversight of companies participating in Medicare and Medicaid. Under the Affordable Care Act, providers could be subject to fingerprinting, site visits and criminal background checks before they begin billing Medicare and Medicaid. To combat fraud, the act allows the HHS Secretary to bar providers from joining the programs, and allows her to withhold payment to Medicare or Medicaid providers if an investigation is pending. In a report slated for release May 13, the Justice Department and HHS said they are putting investigative resources into areas where health-care fraud is especially widespread, including south Florida; Los Angeles; Houston; Detroit; New York City's Brooklyn borough; Baton Rouge, Louisiana; and Tampa, Florida. Source: http://www.google.com/hostednews/ap/article/ALeqM5gVyFvPO6tDLsg228D_xK6c123SvAD9FLT46O0

Obama strategy treats illegal drugs as public health issue. The White House is putting more resources into drug prevention and treatment, part of the President's pledge to treat illegal drug use more as a public health issue than a criminal-justice problem. The new drug-control strategy to be released May 11 boosts community-based anti-drug programs, encourages health care providers to screen for drug problems before addiction sets in, and expands treatment beyond specialty centers to mainstream health-care facilities. "It changes the whole discussion about ending the war on drugs and recognizes that we have a responsibility to reduce our own drug use in this country," said a White House official in a statement. The plan calls for reducing the rate of youth drug use by 15 percent over the next five years and for similar reductions in chronic drug use, drug abuse deaths and drugged driving. Source: http://www.foxnews.com/politics/2010/05/11/obama-strategy-treats-illegal-drugs-public-health-issue/?test=latestnews

TRANSPORTATION

(Massachusetts) **U.S. airport security officers targeted in ID theft.** A Massachusetts couple has been charged with stealing the identities of dozens of Transportation Security Administration (TSA) officers, who screen passengers and baggage at U.S. airports. On May 12, a federal grand jury accused the pair of conspiracy and aggravated identity theft, alleging they stole personal information including the Social Security numbers of dozens of TSA workers at Boston's Logan International Airport. While there was no indication the information was passed to any militant group that might be planning an attack, the case suggests federal officers are vulnerable to identity theft. Prosecutors said that, between July 2008 and December 2009, the couple obtained information on TSA workers from a relative of one defendant who worked as a contractor for TSA's human resources department at the airport. The grand jury alleged both defendants used the identities to obtain electricity, cable television, telephone, and other services for themselves, relatives, friends, and customers. Source: http://www.reuters.com/article/idUSTRE64B63X20100512

(New York) **Bomb threat puts a scare into Staten Island Ferry operations.** A homeless man was busted for phoning in false bomb threats to the Staten Island Ferry May 10, police said. Both the Whitehall terminal in Manhattan and the St. George terminal were briefly shut down and sweeps were conducted by New York Police Department personnel, said a police spokesman. The scare at Whitehall forced the brief evacuation of the terminal about 8:50 p.m. The upper-level waiting area was cordoned off with yellow caution tape and commuters were directed to temporarily board ferries from the lower level, according to a Department of Transportation spokesman. The threats were deemed unfounded and no boats were delayed by the threats, officials said. The calls apparently were made about 8:15 p.m. from a pay phone in the vicinity of Orchard and Rivington streets in Manhattan, according to a police source. About 8:30 p.m., police canvassing the area spotted a 47-year-old man wheeling a cart, the source continued. He was stopped and, during interviews, the source continued, he made statements to police implicating himself as the source of the bomb threats. "He appeared slightly intoxicated and not all there," said the source. The suspect was taken to the 7th Precinct stationhouse and, through a comparison with 911 tapes, his voice was positively identified as that of the caller, the source said. He is expected to be charged with making terroristic threats and aggravated harassment. Source: http://www.silive.com/news/index.ssf/2010/05/bomb_threat_puts_a_scare_into.html

CBP may screen passengers on cruises. The Department of Homeland Security (DHS) currently checks passenger manifests for commercial airplanes to determine if any potential terrorists have booked a flight and it could start doing the same for cruise ships. The Government Accountability Office (GAO) recommended May 10 that U.S. Customs and Border Protection (CBP) examine the possibility of checking passenger reservations for cruise ships in much the same way that the Transportation Security Administration (TSA) does for airlines. "Cruise ships are the single largest passenger conveyances in the world, with one ship currently in service that can carry more than 8,500 passengers and crew," GAO said in its report, Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain. "The Coast Guard considers cruise ships to be highly attractive targets to terrorists, and according to a 2008 RAND Corporation report, cruise ships can represent high-prestige symbolic targets for terrorists. Moreover, terrorists have either targeted

cruise ships or been able to board cruise ships in the past." In 2008 (the last year examined by GAO), more than 9 million passengers sailed from U.S. ports onboard cruise ships. The Coast Guard is the lead agency charged with assessing risk onboard cruise ships as it holds responsibility for maritime security functions at DHS. But CBP has expertise in vetting passenger reservation data, and has performed analysis of cruise-ship passenger manifests in the past as a means to analyze the level of risk various cruises might face from terrorism, the GAO report noted. As such, CBP is well positioned to conduct a study to see if reports on passenger data from cruise lines would prove beneficial to protecting them from terrorist attack as well as to determine the best means of vetting such passenger data, GAO suggested. A terrorist attack that closed ports could cause a ripple effect, slowing down the demand for cruise travel for some time, crippling an industry that contributed roughly $19 billion to the U.S. economy in 2008, the report said. Source: http://www.hstoday.us/content/view/13223/128/

Water and Dams

(Rhode Island) **Vandal(s) release water from Watson Reservoir.** Someone broke into the control area at Watson Reservoir, turned the spigots and released as much as 40-million gallons of water last week. Authorities have no suspects but continue to investigate this crime, the Little Compton, Rhode Island police chief said May 11. Police were alerted to the incident Wednesday, May 5, by a worker from the Newport Water Department who had discovered it during a routine check. Locks had been cut as had the chains that secure the large reservoir valve handles. The chief said that one or two of the valves had been opened, allowing large amounts of water to escape. The water loss is a rough estimate, he said, based on the fact that the Newport Water employee said the water level of the 688-acre reservoir had dropped by about a foot. The water ran into Pachet Brook and from there toward Nonquit Pond and on into the Sakonnet River. Police do not know if this was a random act of vandalism or whether someone had purposely targeted the reservoir for some reason, the chief said. They also do not know how long the water had been flowing before the release was discovered. Several years ago, someone released a large volume of water from that same reservoir during the dry season by removing a control board from the dam. Newport Water owns and manages the reservoir's water, which it usually uses as a supplemental source in the dry, summer months. Source: http://www.eastbayri.com/detail/135827.html

(Texas) **Vandals blamed for wastewater spill.** Officials are blaming vandals for a 250,000-gallon waste-water spill in southwestern Austin, Texas. Austin Water Utility officials said the spill happened May 9 just off Loop 1 near Slaughter Creek Park. The utility said vandals blocked the sewer line with construction fencing and rocks, causing a spill into Slaughter Creek, a stream that feeds into the Barton Springs segment of the Edwards Aquifer. The utility is asking well users in the area to boil their water, and Austin parks officials have closed Barton Springs Poll for water testing. Source: http://www.chron.com/disp/story.mpl/ap/tx/6998901.html

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**