



UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



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

UNCLASSIFIED

NDSLIC DISCLAIMER

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

QUICK LINKS

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

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

[International](#)

[Information Technology and Telecommunications](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials Sector](#)

[National Monuments and Icons](#)

[Commercial Facilities](#)

[Postal and Shipping](#)

[Communications Sector](#)

[Public Health](#)

[Critical Manufacturing](#)

[Transportation](#)

[Defense Industrial Base Sector](#)

[Water and Dams](#)

[Emergency Services](#)

[North Dakota Homeland Security Contacts](#)

NORTH DAKOTA

Propane Fire at Hankinson casino sends flames 30 feet in air. A large fire forced the Dakota Magic Casino and Hotel in Hankinson, North Dakota to evacuate for about 1 hour October 18. The Richland County emergency manager said the fire broke out at about 3:20 am on a vaporizer that's connected to a 30,000 gallon propane tank. The fire was contained to the vaporizer, which was destroyed. Ten area fire departments responded to the blaze, that shot flames 30 feet into the air and was 20 feet wide. There was no damage to the casino or hotel, and guests were allowed back in after 1 hour. The emergency manager said the vaporizer is the heat source for the facility, and he is working with the casino to look at other options for heating alternatives. Source:

<http://www.wday.com/event/article/id/39564/>

Suspicious-passenger report causes flight to be diverted to Fargo. A commuter jet on its way from Minneapolis, Minnesota to Grand Forks, North Dakota, October 17 was diverted to Fargo, North Dakota after a flight attendant thought a passenger tampered with a fire extinguisher in the jet's lavatory, and left some suspicious putty-like material in the lavatory's waste container. After noticing a male passenger behaving in a suspicious manner, a flight attendant on Pinnacle Airlines Flight 4375 decided to check the lavatory after he emerged. She found the fire extinguisher was not in its proper place, according to a Pinnacle spokesman. The flight attendant also spotted some putty-like material that she feared might be explosive, but it was later found to be harmless. The attendant notified the pilot, who diverted the flight to Fargo, where it landed without incident at 10 a.m. October 17, authorities said. The suspicious passenger was interviewed by the FBI and local law enforcement officials before being released. No charges resulted from the incident. Source:

<http://www.startribune.com/business/105141734.html?elr=KArksLckD8EQDUoaEyqyP4O:DW3ckUiD3aPc: Yyc:aUvckD8EQDUJ>

REGIONAL

(Minnesota) Sinkhole near levee kept dry, stable with pumps. A sinkhole at the foot of an earthen levee in LeHillier near Mankato, Minnesota, is dry and no longer sucking in dirt, and should stay that way thanks to some new pumps to keep rainwater out of ruptured pipes. Hours after the hole was discovered September 26, officials assumed it was caused by a broken pipe sucking dirt away along with rainwater. That diagnosis was later confirmed by a camera that was snaked through drainage pipes. Still, "we don't exactly know the total extent of any damage," said a geologist with the U.S. Army Corps of Engineers. The broken pipes could cost \$2 million to fix. At least one broken pipe is located 16 feet underground. This particular pipe is under the ground on the dry side of the levee — not in the middle of the earthen mound itself. Some of the large pipes under the earth, one nearly 5 feet in diameter, carry rainwater that falls on the highway. The township and the Minnesota Department of Transportation (MnDOT) have installed pumps in the area that will take the place of the drainage pipes, keeping them dry. The pipes were running with water for a few weeks after the rain stopped because the water table was still high, said an MnDOT maintenance operations

UNCLASSIFIED

engineer. More than 100 dump truck loads of clay were dumped on the site after the hole was discovered. The Corps has a backup plan to build a secondary levee in the unlikely event this one fails. Both MnDOT and the Corps have emergency work orders pending for the sinkhole so the work gets done before spring rains. Source: <http://mankatofreepress.com/local/x356196694/Sinkhole-near-levee-kept-dry-stable-with-pumps>

(Minnesota) National Guard digs into levee cleanup. In Mankato, Minnesota, the Minnesota National Guard was cleaning up debris from levees October 16. The infrastructure superintendent for the public works department said removing the vegetation is important to maintaining the integrity of the levees. It might seem counterintuitive — that the root systems of plants would help hold the earthen levees together, but the roaring water of a flood can pull entire trees out of the levee — roots and all. When that happens, the earth comes with the roots and a cavity is left behind that the floodwaters will slowly enlarge, he said. And that is not an easy thing to fix during a major flood. The guard soldiers, working with about 10 public works employees, broke into five teams that tackled brush from near the Highway 14 bridge to Sibley Park. Source: <http://mankatofreepress.com/local/x1744206097/National-Guard-digs-into-levee-cleanup>

(South Dakota) Truck explodes near Brandon. A large truck left the road and exploded in flames near Highway 42 and 481st Street near Brandon, South Dakota, about 3 a.m. October 21. Deputies think there were chemicals in the truck that caused the explosion but they were not sure. The driver of the Matco vehicle was transported to a hospital with non-life-threatening injuries. The man driving the truck was not a Matco employee, but a mechanic who had serviced the vehicle and was taking it for a test drive. An accident reconstruction specialist began to investigate the explosion that night. Source: <http://www.argusleader.com/article/20101022/NEWS/10220340/1001/news>

NATIONAL

Gunbattles stir panic in Mexican border cities. Mexican soldiers battled gunmen in two cities across the border from Texas October 20, leaving two people dead, and prompting panicked parents to pull children from school, and factories to warn workers to stay inside. Authorities said one of the two people killed in the city of Ciudad Juarez was a Texas National Guard soldier, according to local reports. The U.S. Consulate in the city of Nuevo Laredo warned American citizens to stay indoors. A statement by the Consulate said there were reports of drug gangs blocking at least one intersection near the consulate in the city across from Laredo, Texas. Assaults in a third city, Matamoros, across the border from Brownsville, Texas threw a grenade at an army barracks. The local government and witnesses in Nuevo Laredo reported several blockades in addition to the one mentioned in the U.S. Consulate's statement. Shootouts also erupted in Reynosa, across from McAllen, Texas causing a huge traffic jam in the highway connecting the city with Monterrey and Matamoros. Source: http://www.msnbc.msn.com/id/39772666/ns/world_news-americas/

Deaths, injuries raise questions for popular Remington 700 rifle. The manufacturer of the world's most popular hunting rifle has been wrestling for decades with a critical safety issue, and at least twice considered a nationwide recall of the gun, according to corporate insiders and internal documents revealed in a 10-month CNBC investigation. But the Remington Arms Company has never alerted the public to the internal concerns, and insists the gun is free of defects, despite thousands of customer complaints. The controversy over the 700 is explored in a CNBC Original documentary,

UNCLASSIFIED

UNCLASSIFIED

"Remington Under Fire: A CNBC Investigation," that was slated to premier October 20 at 9 p.m. ET/PT. The Remington Model 700-series rifle — with more than 5 million sold — is famous for its accuracy and smooth trigger. In addition to being popular with hunters and target shooters, a version of the 700 is also widely used by law enforcement and military snipers. "The Model 700 is the most popular, reliable, accurate, and trusted bolt-action rifle in the world, with over five million rifles produced and billions of rounds fired over nearly five decades," Remington said in a statement to CNBC. But the customer complaints, and more than 75 lawsuits, have alleged the 700 is susceptible to firing without the trigger being pulled. At least two dozen deaths and more than 100 injuries have been linked to accidental discharges involving the 700's trigger mechanism. Source: http://www.usatoday.com/money/industries/manufacturing/2010-10-20-remington-700-trigger-cnbc_N.htm

Coast Guard outreach needed in the Arctic. Although the U.S. Coast Guard has made efforts to coordinate with an array of stakeholders on Arctic policy and operational issues, some stakeholders, especially local officials and Alaska native groups, want more information on the agency's Arctic planning efforts, according to a report from the Government Accountability Office (GAO). Entitled "COAST GUARD: Efforts to Identify Arctic Requirements Are Ongoing, but More Communication about Agency Planning Efforts Would Be Beneficial," the report was based on interviews with 15 representatives of foreign, federal, state, and local governments; Alaska Native interest groups; and private and nonprofit entities. Interviewers found that 9 of the 15 state and local officials GAO met with wanted more information on the status and results of the Coast Guard's efforts to develop its future Arctic requirements. While the Coast Guard remains singularly focused on communication with Congressional and federal stakeholders, the report notes, the agency "could be missing an opportunity to create shared expectations and report on its progress with stakeholders central to future Arctic operations." Based on these findings, GAO recommended that the Coast Guard better communicate with key stakeholders on the process and progress of its Arctic planning efforts, a recommendation the Coast Guard concurred with. Source: <http://www.hstoday.us/content/view/15121/128/>

INTERNATIONAL

150,000 evacuated, shipping routes closed as Typhoon Megi approaches China. Hundreds of thousands of people have been evacuated from coastal areas in southeast China in the path of Typhoon Megi, disaster relief authorities said October 21. Typhoon Megi was expected to make landfall in southern Fujian either October 22 or October 23, the chief commander of the headquarters said. Local authorities have ordered fishermen to stay ashore, and managers of dams in populated areas to prepare to discharge water in case of torrential rain. Authorities have issued a red warning, the highest of four warnings, that the typhoon could cause huge waves that could devastate coastal sea areas, including Guangdong, Fujian, and the Taiwan Strait. The red warning gives local authorities 6 hours to evacuate residents at risk and implement storm precautions, and order schools, shops and airports to close, and all vessels to return to port. Megi is the 13th typhoon and possibly the strongest to hit China this year. Southern provinces, including Hainan, Guangdong, Jiangxi, and Fujian, are bracing for heavy rains and strong winds. Source: http://news.xinhuanet.com/english2010/china/2010-10/21/c_13568748.htm

UNCLASSIFIED

UNCLASSIFIED

Grenade attack in Nuevo Laredo. Across the Mexican border October 19, Nuevo Laredo police and Mexican soldiers are on high alert after a grenade was launched into a municipal police substation. It happened less than 1 block from city hall around 8 p.m. October 19. No one was killed or hurt in the incident. A police cruiser was blown up but other than that there was only minor damage. It comes as Nuevo Laredo has seen several weeks of rest from the bloodshed and violence. Authorities said it is unclear if drug traffickers carried out the attack. Officers and soldiers are stepping up patrol on the streets until further notice. Source: <http://www.pro8news.com/news/local/Grenade-Attack-in-Nuevo-Laredo-105316018.html>

Bomb threat halts trading at Philippine stock market. A bomb threat forced a halt to trading at the Philippine Stock Exchange October 21, but trading resumed after police cleared the building, officials said. Bomb disposal teams and sniffer dogs searched an office tower housing the exchange's trading floor in the financial district of Makati while hundreds of office workers filed out of the building. "We halted trading for security reasons. We implemented evacuation measures immediately for the safety of the employees and trading participants," the exchange president said in a statement. The official did not say where the threat came from nor how it was sent. Spokesmen for the exchange said they were checking who received the threat. After police called the alert off, the exchange sent an advisory saying that trading hours would be extended by about 1 hour to make up for the time that was lost due to the bomb threat. A spokesman for the president said the incident was a "concern" but that the government was happy that no bomb was found. Source: http://www.google.com/hostednews/afp/article/ALeqM5iFY3PEHIKQNSQWn1zfQeCNHOP_xw?docId=CNG.a748b69f22077ddd5d23e00c220bc69a.331

Man holding Uranium busted in Czech Republic. Czech authorities earlier this month detained a 45-year-old German citizen in possession of a quantity of uranium as well as a range of firearms and explosives, the Prague Post reported October 20. Police arrested the man October 7 over transactions involving chemicals. "We searched his house October 8 and found a large amount of highly explosive substances, machine guns, various military arms and ammunition, along with nuclear material, uranium 238 and 235," a regional police spokeswoman said. "Because of the nature of the chemicals, we had to call in firefighters as well as the State Office for Nuclear Safety to help with the confiscation." The material seized did not include weapon-grade uranium, the Post reported. An October 9-10 search of a separate apartment the suspect owns in Germany turned up machine gun components, ammunition, an explosives trigger, and "obscure chemicals," the deputy state prosecutor in the city of Koblenz said in a statement. The German, who has studied pyrotechnics, told Czech authorities of his longtime interest in chemistry. The Czech Republic has charged the man with unauthorized production and possession of nuclear materials, and with unauthorized possession of arms and ammunition. In Germany, he has been formally accused of violating the War Weapons Control Act and the Explosives Act. Source: http://www.globalsecuritynewswire.org/gsn/nw_20101021_7353.php

Mexican drug cartels diversify. Mexico's drug cartels have diversified their operations in recent years, branching out into piracy, prostitution, theft of oil and minerals, the sale of adulterated liquor, and other illegal activities. The oil industry has been affected by the encroachment of organized crime, which has stolen \$300 million worth of natural gas liquids from state energy monopoly Petroleos Mexicanos' facilities over the past 4 years, according to official figures. Since 2007, the police have guarded Pemex's installations to prevent employees from aiding and abetting the theft of

UNCLASSIFIED

fuel by drug traffickers. Five members of the Los Zetas cartel involved in this crime were arrested in July 2010, while 1 month earlier, five Pemex workers and two employees of a Pemex contractor were kidnapped and are still missing. Source:

<http://www.laht.com/article.asp?ArticleId=372998&CategoryId=14091>

BANKING AND FINANCE INDUSTRY

FBI warns of ‘Corporate Account Takeover’ scams. Cybercriminals are targeting the financial accounts of small and midsize businesses (SMBs), fraudulently transferring money directly from their accounts, the FBI warned October 20. In a fraud alert issued October 20, the FBI said “corporate account takeover” attacks use malware to steal passwords and other credentials from senior executives at SMBs and then use those credentials to empty the companies’ coffers. “To obtain access to financial accounts, cyber criminals target employees—often senior executives or accounting, HR personnel, and business partners—and cause the targeted individual to spread [malware], which in turn steals their personal information and log-in credentials,” the FBI says in its full report. “Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts,” the report explains. “Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account.” In addition to targeting account information, attackers also seek to gain customer lists and other proprietary information, often using the same malware-spreading techniques, the report says. The FBI first began warning enterprises about corporate account takeovers in 2006, but they are rising in numbers because cybercriminals have found them rather easy to perpetrate—especially when it comes to SMBs that do not have a dedicated IT security staff, the report says. The rewards are great—often surpassing hundreds of thousands of dollars—and the risk is low. Source: <http://www.darkreading.com/smb-security/security/perimeter/showArticle.jhtml?articleID=227900529>

Avalanche gang switches from traditional phishing to ZeuS. Security researchers warn that one of the world’s largest phishing gangs, known in the security industry as Avalanche, is now relying on the infamous ZeuS trojan to steal sensitive data from users. The announcement came from the Anti-Phishing Working Group (APWG), an international association of security vendors, financial organizations and law enforcement agencies, that aims to prevent identity theft and fraud resulting from phishing attacks. The Avalanche gang is a large cybercriminal syndicate believed to operate out of Eastern Europe. According to APWG’s statistics, it was responsible for as much as two thirds of the phishing attacks recorded during the second half of 2009. Since then the group seems to have scaled back their traditional phishing operations significantly in favor of the more efficient ZeuS information stealing trojan. APWG reports that only four Avalanche-related phishing attacks were observed during July 2010, which is significantly lower than 2009. Source: <http://news.softpedia.com/news/Avalanche-Gang-Switches-from-Traditional-Phishing-to-ZeuS-162138.shtml>

FBI warning targets work-from-home schemes. The FBI has issued a consumer warning October 13 as thousands of consumers continue to lose money from work-from-home scams. Officials claim scam victims are often recruited by organized cybercriminals through a variety of outlets, ranging

UNCLASSIFIED

from newspaper ads to online employment services, and unsolicited e-mails. Once a person is recruited for the job, officials said often times the consumer becomes a “mule” for cyber criminals to steal and launder money. Now, federal officials are warning consumers to be on the lookout for these types of scams and to take precautions to avoid becoming a victim. Those looking for work are asked to be wary of work-from-home opportunities and to research a company before signing on for work. Source: <http://www.wmbfnews.com/story/13355810/fbi-warning-targets-work-from-home-schemes>

Number of fake electronic tax payment emails has spiked. Security researchers warn that a Zeus distribution campaign producing e-mails about failed electronic tax payments, has significantly increased its aggressiveness the weekend of October 16-17. The rogue e-mails started hitting in-boxes from October 11-15 and come with a subject of “Your Tax Payment ID ##### is failed. Update information.” The from field is spoofed to appear as if the e-mail is originating from “EFTPS Tax Payment,” and it tells users their tax payments submitted through the Electronic Federal Tax Payment System (EFTPS) has failed. Also, the messages claim the payment failed with an R21 error code and provide a link to obtain additional information. Clicking on the link takes recipients through a series of redirects until they land on a drive-by download page, where their computers are targeted with exploits for outdated versions of many popular applications. Successful exploitation results in a variant of the Zeus banking Trojan being installed. This malware is commonly used by fraudsters to steal online banking credentials, credit card details and other sensitive data. According to researchers from e-mail security provider AppRiver, the number of these Zeus distribution e-mails spiked October 16, with over 100 new domains being used in the attack. Source: <http://news.softpedia.com/news/Number-of-Fake-Electronic-Tax-Payment-Emails-Has-Spiked-161368.shtml>

Phishers use mobile credit bait. Security researchers from Symantec warn of a phishing campaign, which promises free mobile credits in order to trick online banking users into exposing their credentials and phone numbers. This particular attack targeted customers of an Italian bank, but it’s a good indication of the various methods used by phishers to lure victims. The phishing page was hosted on a domain that was a typo of the bank’s real Web address, a technique known as typosquatting. The site claimed that if the users recharged their mobile credit through the bank system with 10 euros, they would receive an additional 40 euros as a bonus. This attack is a double phishing attempt, because the users are first asked to log in to their accounts, which exposes online banking credentials, and then they must input mobile phone numbers. Source: <http://news.softpedia.com/news/Phishers-Use-Mobile-Credit-Bait-161597.shtml>

(Ohio) Suspicious package found outside bank. The Dayton Bomb Squad was called to downtown Xenia, Ohio October 18 after a suspicious package was found outside a bank. A witness told police he saw someone leaving a container with foil and rubber bands on it outside the Huntington Bank on North Detroit Street. The bomb squad was called out to investigate and the intersection was shutdown for several hours. The contents were later determined to be pedialyte for cats, a substance to help keep cats hydrated. Source: http://www.wdtn.com/dpp/on_air/sunrise/suspicious-package-found-outside-bank

UNCLASSIFIED

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

No US reactors to shut over GE/Hitachi crack report. None of the more than two dozen U.S. boiling-water reactors named in a report from General Electric Co (GE.N)/Hitachi Ltd's (6501.T) nuclear venture will have to shut in the near future, the U.S. Nuclear Regulatory Commission said on October 21. GE/Hitachi told the NRC in a report that it had found "crack indications" on control rod blades at a non-U.S. nuclear power plant. The U.S. reactors were named because they have a similar control rod blade design to the reactor with crack indications. The GE/Hitachi notification is a standard Part 21 report used to tell the industry about something that does not meet NRC standards. So far in 2010, nuclear equipment manufacturers and operating companies have filed over 40 Part 21 reports with the NRC, several of which list many affected reactors. The operators of the U.S. reactors with the blades in question will likely check whether they found any indication of cracks in previous inspections, an NRC spokesman said. Source:

<http://www.reuters.com/article/idUSN219367520101021>

NNSA office of emergency operations develops cutting-edge nuclear terrorism software. The National Nuclear Security Administration (NNSA) October 19 announced its office of emergency operations has developed and delivered a new X-ray image processing capability to U.S. emergency responders. X-Ray Toolkit (XTK) is an application used by field responders and NNSA Laboratory experts to acquire, process and analyze X-ray images obtained during a potential nuclear terrorism incident. XTK development was sponsored by NNSA's emergency operations technology integration program, and implemented by its stabilization program. "We have received overwhelmingly positive feedback about XTK software from our operational partners," said NNSA's Associate Administrator for Emergency Operations. XTK was designed for joint use by Explosive Ordnance Disposal (EOD) and NNSA Laboratory personnel during nuclear render safe operations, where specialized procedures, methods and tools prevent the detonation of a nuclear device. Previous software was converted for use from the medical diagnostic industry, not specifically designed for use by EOD experts. Source:

<http://www.yournuclearnews.com/nnsa+office+of+emergency+operations+develops+cutting-edge+nuclear+terrorism+software+55411.html>

COMMERCIAL FACILITIES

(California) Major northern Calif. mall burns after standoff. Part of a high-end regional mall in Northern California was destroyed October 21 after police say a man barricaded himself inside and started a fire. Police said the man holed up in a video game store at the Roseville Galleria and started a small blaze that later blew up, damaging an entire arm of the mall. The 1.3 million-square-foot Galleria was evacuated by the time the fire erupted and spread to the roof, and no injuries were reported. City officials said part of the roof on the mall's south end collapsed. A Roseville fire department spokesman said the fire burned a wing of the mall that appeared to extend several hundred yards between two anchor tenants, Macy's and J.C. Penney. He said water and smoke damage was extensive beyond that wing. Police descended on the mall when a man claiming to have a gun entered a GameStop store and told employees to get out. The employees said the man then barricaded himself in a back room and started a fire. He was hiding outside the store when a SWAT

UNCLASSIFIED

team entered the mall, and he was arrested without further incident. Authorities had thought the mall's sprinkler system doused the blaze. But police later said the fire began spreading as members of the bomb squad were checking the man's backpack to see if it contained explosives, forcing them to flee the building. Source: <http://abcnews.go.com/US/wirestory?id=11939532&page=1>

(New York) NY's Times Square reopened after threat. Police temporarily closed streets around New York City's Times Square at lunchtime October 20, but soon reopened the streets when a suspicious vehicle turned out to be harmless, police said. An unattended Chevy minivan was parked with its lights on outside the Westin Hotel and near a Port Authority bus terminal, a police spokesman said. After shutting several blocks and examining the vehicle, police reopened traffic and gave the "all clear" signal, witnesses said. Investigations of suspicious packages are common in the Times Square area. Police typically close streets when unattended baggage is found at the busy section of Manhattan known as the Crossroads of the World. Source: <http://www.reuters.com/article/idUSTRE69J4LB20101020>

(Louisiana) 'Suspicious device' found next to Gulf Highway neutralized. Authorities with Louisiana State Police dispatched their hazardous materials unit to Gulf Highway and East Lincoln in Lake Charles October 20 in response to a suspicious device found on the side of the road. The device was found on the side of Gulf Highway near Lincoln Road south of the Lake Charles Regional Airport. The device, which was found near a natural gas pipeline, was neutralized by the haz-mat unit. A perimeter remained in place for much of October 20 as crews searched for possible secondary devices as well as evidence. Traffic was diverted for a while, but all roads were re-opened. Source: <http://www.kplctv.com/Global/story.asp?S=13356698>

'All of Mexico' travel warning could affect Texas tourism. A strong warning from the Texas Department of Homeland Security is advising people not to visit Mexico right now and that includes all cities. Concerns over travel to Mexico have been growing for years as violence in border cities claims more and more lives. After an American man turned up missing in September 2010 in a fatal shooting that some claim involved Mexican pirates on Lake Falcon, fears may have reached a fever pitch. On October 14, the Texas Homeland Security director said Americans should avoid Mexico altogether. He made the statement in testimony before a Senate committee, saying nobody should be going into Mexico, including tourist cities like Cancun and Cozumel. Wide scale travel warnings can affect tourism in the United States as well, according to the Marfa Chamber of Commerce. "It does have an effect. A person from California who hears that has no idea that we're an hour away from the border. It may impact our tourism," said a chamber spokesperson. A U.S. Department of State travel warning singles out various "no-visit zones" in Mexico, but also points out that millions of Americans travel to the country safely and without incident every year. Source: <http://www.cbs7kosa.com/news/details.asp?ID=22054>

COMMUNICATIONS SECTOR

Broadcasters file for more time for updating EAS. A number of broadcast groups has filed a request to extend the timeframe for broadcasters to re-equip their stations for the Emergency Alert System (EAS). As it stands, broadcasters have until late March of 2011 to install equipment that is capable of receiving messages using the Common Alerting Protocol (CAP). But, the broadcasters say they need more time. The National Association of Broadcasters and other broadcast groups told the Federal

UNCLASSIFIED

UNCLASSIFIED

Communications Commission (FCC) the March 2011 deadline is simply too soon, since it was only late September 2010 when the clock started ticking on the mandatory upgrades. That is when FEMA announced it had approved the most recent version of CAP, a message standard. The broadcasters say they need more than the 180-day window they have been given to see which vendors will be declared CAP compliant, get operational and regulatory issues resolved, buy equipment, and install it. They would like the timetable pushed back to September 30, 2011, giving them a year to comply. Source: <http://www.emergencymgmt.com/emergency-blogs/alerts/Broadcasters-File-for-More-102210.html>

The Android IM app that brought T-Mobile's network to its knees. According to T-Mobile's filings with the Federal Communications Commission (FCC), close to 1 year ago an Android-based instant messaging application "caused an overload of T-Mobile's facilities for an entire city." the director of T-Mobile's national planning and performance engineering, described in a statement filed with the FCC in January 2010. "T-Mobile network service was temporarily degraded recently when an independent application developer released an Android-based instant messaging application that was designed to refresh its network connection with substantial frequency," the director wrote in the filing. "One study showed that network utilization of one device increased by 1,200 percent from this one application alone. These signaling problems not only caused network overload problems that affected all T-Mobile broadband users in the area; it also ended up forcing T-Mobile's UMTS radio vendors to re-evaluate the architecture of their Radio Network Controllers to address this never-before-seen signaling issue. Ultimately, this was solved in the short term by reaching out to the developer directly to work out a means of better coding the application." Source: <http://www.fiercewireless.com/story/android-im-app-brought-t-mobiles-network-its-knees/2010-10-14>

FCC workshop will address critical cybersecurity threats. The Federal Communications Commission (FCC) will hold a workshop November 5 to discuss the most critical cyber threats to the communications grid. The National Broadband Plan tasked the FCC with developing a Cybersecurity Roadmap that identifies and addresses the five most critical cyber threats to the communications infrastructure and its users. Participants in the workshop will provide input on what should be included in the roadmap and how those threats can be mitigated. The commission's workshop is open to the public, but seating is limited and the deadline to register is November 3. The event will also be broadcast live over the Web. Source: <http://thehill.com/blogs/hillicon-valley/technology/124867-fcc-workshop-will-address-critical-cybersecurity-threats>

Privacy Commissioner wants Google to delete data. Google may have picked up personal information through Wi-Fi while it created Street View. Now, Canada's Privacy Commissioner is demanding that data be deleted. A UBC Internet and Privacy expert said if one's Wi-Fi is unsecured, Google's Street View camera cars may have picked up things a person would not want the company to see. Blame a glitch in the imaging software. The data included complete e-mails, the addresses, user names, passwords, names and residential phone numbers, et cetera. The privacy commissioner called it a careless error that likely affected thousands of Canadians and the company should have addressed privacy concerns before developing Street View. She added if the data cannot be deleted right away, it should be secured with restricted access. Source: <http://www.news1130.com/news/local/article/117075--privacy-commissioner-wants-google-to-delete-data>

UNCLASSIFIED

UNCLASSIFIED

Collaborators sought for emergency communications network demo. The U.S. National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA) are seeking partners in the telecommunications industry to help create a demonstration broadband communications network for the U.S. emergency services agencies. The demonstration network, currently being developed by the joint NIST-NTIA Public Safety Communications Research (PSCR) program, will provide a common site for manufacturers, carriers, and public safety agencies to test and evaluate advanced broadband communications equipment and software tailored specifically to the needs of emergency first responders. Alcatel-Lucent is the first vendor of public safety broadband equipment to formally join the PSCR demonstration network project, signing a Cooperative Research and Development Agreement (CRADA) with NIST and NTIA in September 2010. The two agencies hope that other companies will follow suit, creating a multivendor environment for testing and evaluating the demonstration network, as well as the eventual building of the system. Partners may participate in many ways, such as donating equipment, providing access to infrastructure, or supporting tests. PSCR provides objective technical support — research, development, testing, and evaluation — in order to foster nationwide public safety communications interoperability. Source: <http://homelandsecuritynewswire.com/collaborators-sought-emergency-communications-network-demo>

CRITICAL MANUFACTURING

Chrysler recalls vehicles for possible fire hazard. Chrysler Group LLC is recalling 26,397 vehicles, stating a malfunction with the power steering pressure hose may cause steering fluid to leak over a hot engine and cause a fire. The affected vehicles include the 2011 Dodge Ram, the 2010 Chrysler Sebring, Chrysler 300, Dodge Charger, Dodge Avenger, Dodge Challenger, and Dodge Journey, according to an October 18 letter posted on the National Highway Traffic Safety Administration Web site. A spokesman for Chrysler, the U.S. automaker controlled by Fiat SpA, did not immediately comment. The company said in the letter that it was not aware of any injuries or accidents related to this issue. Chrysler notified U.S. safety regulators of the problem earlier in October. The supplier of the hose is YH America South Carolina LLC. Source: <http://www.reuters.com/article/idUSTRE69J31P20101020>

Toyota to recall over a million cars in US and Japan. Toyota has announced a recall of more than 1.5 million cars worldwide over brake and fuel pump defects. The carmaker said the decision affected certain Avalon, Highlander, and several Lexus cars, including 740,000 cars in the United States, 600,000 in Japan, and 17,000 in the United Kingdom. It wants to ensure that fluid does not leak from the brake master cylinder, causing the warning light to turn on. The fault could cause the brake pedal to feel spongy, and braking performance to "gradually decline." Toyota said that if the brake warning light is triggered, drivers still have another 200 miles to drive to find help before the brake performance deteriorates. Toyota is not aware of any accidents because of the issue. The models affected in the U.K. are some Lexus IS, GS and RX models built between 2003-2005. The U.S. recall affects 2005-06 Avalon cars, 2004-06 Highlander (non Hybrid) and Lexus RX330 cars, and 2006 Lexus GS300, IS250, and IS350 cars, according to the company's press release. The recall also affects 33,000 cars in continental Europe, 60,000 in China, 30,000 in Australia, and 50,000 in the rest of Asia. Car owners will be notified early in November, and the manufacturer will arrange for the brake master

UNCLASSIFIED

cylinder cup to be replaced with a newly designed version. Source:

<http://www.bbc.co.uk/news/business-11593952>

DEFENSE / INDUSTRY BASE SECTOR

Army field tests curvy uniform for women soldiers. The U.S. Army will field-test the first combat uniform shaped to fit women's curves. Some 160,000 women currently serve in the Army, and they have long had to make do with unisex uniforms that were made with men in mind. As a result, complaints poured in that the uniforms hampered movement and were not comfortable. According to Paris-based news agency AFP, the new camo outfits cinch at the waist and feature smaller shoulders and vents for their bustlines, and the pants have elastic waistbands instead of drawstrings. About 600 women soldiers will field test their new uniforms starting in January. If all goes well, they will be standard issue sometime in 2012. Source: http://mystateline.com/fulltext-news/?nxd_id=204656

Navy to test alt-fuel powered vessel. The Navy will conduct a full power demonstration of an alternative fuel powered Riverine Command Boat October 22 at Naval Station Norfolk. The 49-foot vessel will run on a blend of 50 percent algae-based and 50 percent NATO F-76 fuel. The Riverine has been used in the Iraq War to patrol rivers. It has a shallow draft and travels at speeds of 40 knots. "From a strategic perspective, we are reducing reliance on fossil fuels from unstable locations. Tactically, efficient use of energy resources extends our combat range and use of non-petroleum fuels assures multiple supplies are available," said the director of the Chief of Naval Operations Energy and Environmental Readiness Division. The testing and demonstration of alternative fuels for ships is led by Naval Sea Systems Command's advanced fuels program office. The office, in coordination with the Task Force Energy Maritime Working Group, is working to achieve the Secretary of the Navy's energy target of a Green Strike Group in local operations by 2012 and deploy a Strike Group, the Great Green Fleet, by 2016 composed completely of alternatively powered ships. Source: <http://www.wavy.com/dpp/military/Navy-to-test-alt-fuel-powered-vessel>

As UAV use grows, bandwidth limits become a concern. The U.S. Air Force is facing a dilemma: The need and utility of unmanned aircraft continues to grow, but the technology could also limit the service's operational responsiveness. However, while current technologies may be reaching their limits, the Defense Department is also investing in future systems that will vastly increase the capabilities of robot aircraft through increased autonomy. Ongoing operations in Southwest Asia continue to drive the voracious demand for pilots, support personnel and bandwidth above all, said an Air Force Colonel, speaking at the recent C4ISR Journal Conference in Washington D.C. He said the military needs additional 24-hour surveillance and close air support orbits by unmanned aerial vehicles (UAVs). The Air Force Times reported the service already provides 44 such orbits; that number is scheduled to expand to 65 by 2013. This increased autonomy comes with a price. The Colonel said the bandwidth required to support these capabilities may actually limit commanders' operational flexibility because they may have to choose between large numbers of relatively static surveillance missions or a few very flexible multi-mission operations. Source: <http://defensesystems.com/articles/2010/10/19/air-force-ponders-uav-technologies.aspx?admgarea=DS>

UNCLASSIFIED

Army set to test new 'airburst gun'. The Army is set to test out a new weapon that could change how troops battle enemies in Afghanistan. The XM-25 Counter Defilade Target Engagement System, better known as the "Airburst Gun," is a shoulder-fired gun that shoots a fist-sized round packed with an explosive warhead that detonates in the air at pre-determined ranges. Officials are calling it a cross between a grenade launcher and a mortar. The XM-25 weighs about 12 pounds, and uses laser targeting to determine a target's range. Soldiers then dial in exactly where the round is going to land or explode. Army officials said the weapon is perfect for long-distance battles with Afghan enemies who fight from behind cover. A spokesman added that the accuracy of the XM-25 is going to change battles and "open up whole new ideas on how to use it." The Army plans to buy thousands of the XM-25 in the future, placing one airburst weapon in each infantry squad. Source:

<http://www.nbcwashington.com/news/local-beat/Army-Set-to-Test-New-Airburst-Gun-105025899.html>

EMERGENCY SERVICES

FBI releases 2009 statistics on law enforcement officers killed and assaulted. According to information released October 18 by the FBI, 48 law enforcement officers were feloniously killed in the line of duty last year; 47 officers died in accidents while performing their duties; and 57,268 officers were assaulted in the line of duty. The 2009 edition of Law Enforcement Officers Killed and Assaulted provides comprehensive tabular data about these incidents and brief narratives describing the fatal attacks. The number of officers feloniously killed in 2009 increased by seven compared with the 2008 figure (41 officers). Source: http://www.fbi.gov/news/pressrel/press-releases/leoka_101810

(California) Explosive material found in container. Explosives and hazardous-materials technicians were called to the Stockton, California Police Department October 15 to handle a dangerous substance a man had turned in after finding it near the airport. The police department said the substance was in a container a man had found on a Highway 99 frontage road. On the exterior of the container was a warning that its contents would explode if exposed to water. Police said the man opened the container and saw that it was full, then he noticed it was warming. The man took the container to the police department, where members of the fire department's hazardous-materials team and the police department's bomb squad inspected and removed the container. It was to be destroyed at a remote location. A firefighter confirmed the substance was calcium carbide, which is potentially explosive and dangerous. Source:

http://www.recordnet.com/apps/pbcs.dll/article?AID=/20101016/A_NEWS02/101019870/-1/a_news

Uniform bomb suits standard being developed. Federal agencies are looking to protect the first responders and soldiers who check out and defuse potentially explosive devices with improved bomb suits. Bomb suit manufacturers run tests on their protective suits to ensure they can withstand an explosion, but there currently is no single set of requirements that the suits must meet before they can be sold. TechNewsDaily reported that several federal agencies are now working with first responders to create the first nationwide standard for minimum bomb suit performance requirements. To develop the standard, federal agencies first researched the most common types of explosives bomb squads encounter, according to the deputy director of the Office of Standards at DHS's Science and Technology Directorate (S&T) Test & Evaluation and Standards Division. Personnel at the U.S. Army Natick Soldier Research Development and Engineering Center blew up, burned, and projected fragments at suits to determine what kinds of tests the suits would need to pass to ensure

UNCLASSIFIED

UNCLASSIFIED

they protect bomb technicians adequately. Having a standard will give some assurance of quality to DHS and other agencies that award grants to bomb squads for equipment purchases. If the standard is adopted, DHS will change its grants process to ensure awards are spent on bomb suits that meet the requirements. Source: <http://homelandsecuritynewswire.com/uniform-bomb-suits-standard-being-developed>

ENERGY

(South Carolina) Copper thieves knock out power to thousands in Chesnee October 21. Thousands of Duke Energy customers in Spartanburg County, South Carolina, lost power overnight October 20 after a substation was vandalized apparently to steal copper. The Spartanburg County Sheriff's Office said a deputy was called to the substation early October 21 at West Manning Street and Hanna Height Drive in Chesnee. Parts of a transformer had been cut to steal the metal. The incident report said about \$500 worth of copper wire was stolen. Duke Energy reported more than 2,800 customers lost service because of the theft. Most service was restored by 5 a.m. The deputy said a suitcase and a pair of bolt cutters were found at the facility. Damage, labor to repair it, and the loss of revenue would bring the estimated loss to the power company to about \$20,000. Source: <http://www2.wspa.com/news/2010/oct/21/2/vandals-knock-out-power-thousands-chesnee-thursday-ar-991416/>

(Oklahoma) Copper thieves cause power outage. In Norman, Oklahoma, thousands of people were without power October 17 after copper thieves broke into a power substation. It happened at a station near 149th and Choctaw. According to the Oklahoma Electric Cooperative (OEC), thieves stripped out the copper wiring, which then sparked a fire. Officials estimate there is close to \$1 million in damage. However, OEC said the thieves only got away with a few hundred dollars worth of copper. "It takes somebody very brazen to do this, and it has happened all around the country," said the OEC operations manager. He said a lot of the equipment at the station now must be replaced, and copper was also taken at two other nearby substations. Officials estimated close to 3,300 homes were without electricity. Crews were able to restore power within a few hours. Source: <http://www.kfor.com/news/local/kfor-copper-thieves-cause-power-outage-story,0,4073008.story>

DOD plans project to thwart cyber attacks, tap renewable energy. The Department of Defense (DOD) wants to make sure that when disaster strikes, renewable energy sources can still help keep the lights on at military bases. Starting this fall, the Pentagon expects to join with a coalition of other agencies and national labs to create the first installation-level "microgrid" technology. The end result will be cyber secure, it said. The \$42 million project — assuming Congress approves the money — will integrate energy from existing diesel-powered generators alongside alternative and renewable energy sources. It will help power an installation's day-to-day operations when the base is hooked up to the commercial grid and will also allow it to function independently of that utility grid, should the need arise. "You could think of this as a buffet of options that are all being synchronized through a demand-side cyber secure system," said the national labs liaison to the U.S. Northern Command and one of the project leaders. While the final microgrid is slated for Marine Corps' Camp H.M. Smith in Hawaii, the DOD is completing different stages of the work at bases including Joint Base Pearl Harbor-Hickam, also in Hawaii, and Fort Carson in Colorado. One major selling point of the microgrid is better protection for a base's power sources against cyber attack, the liaison said. Another is improving energy efficiency and energy storage, which in turn allows the department to better meet

UNCLASSIFIED

UNCLASSIFIED

government mandates to reduce energy use. This project — the Smart Power Infrastructure Demonstration for Energy Reliability and Security, or SPIDERS, for short — aims to change that.

Source: <http://www.nytimes.com/cwire/2010/10/18/18climatewire-dod-plans-project-to-thwart-cyber-attacks-ta-12633.html>

FOOD AND AGRICULTURE

Pesticides taint one-fifth of kids' food. More than one-quarter of the food eaten by a small number of U.S. children contained pesticides, confirming again that food is a source of chemical exposures for youngsters. Researchers measured 14 varieties of pesticides in the fruits, vegetables, and juices tested. While many studies have measured levels of pesticides in various foodstuffs on grocery shelves and a few have looked at levels excreted from the body, little has been known about the level of pesticides found in the food that children actually consume. The study attempted to capture the pesticide levels of foods just as they were prepared and in the amounts eaten by the children. High levels of pesticide exposure among fetuses and children have been linked to negative health effects ranging from increased rates of attention deficit hyperactivity disorder (ADHD) to increased blood pressure. In addition, recent research finds evidence of pesticide by-products in nearly 94 percent of children studied. Source: <http://www.environmentalhealthnews.org/ehs/newscience/pesticides-found-in-one-fifth-of-produce-kids-eat>

(Michigan; Arizona) Del Monte recalls cantaloupes for Salmonella. Del Monte Fresh Produce N.A. Inc. on October 21 recalled certain cantaloupes grown and shipped from Arizona for distribution in the Detroit, Michigan area. In a statement, Del Monte Fresh said the recalled cantaloupes “have the potential to be contaminated with Salmonella.” The bad cantaloupes were discovered through random testing by the Michigan Department of Agriculture. No illnesses have yet been associated with the recall. An estimated 81 cartons of cantaloupes, each containing 15 cantaloupes per carton, were distributed beginning October 11 to wholesalers in Detroit who in turn sold them to other wholesalers and/or to retail and foodservice outlets. Source:

<http://www.foodsafetynews.com/2010/10/del-monte-recalls-cantaloupes-for-salmonella-contamination/>

(North Carolina) Barbecue pork products recalled due to Salmonella contamination. The Murphy House, a Louisburg, North Carolina establishment, recalled approximately 4,920 pounds of ready-to-eat (RTE) pork barbeque products that may be contaminated with Salmonella, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced October 20. The problem was discovered through FSIS' microbiological sampling program. FSIS has received no reports of adverse reactions due to consumption of these products. These products were cooked October 6 and October 7, 2010, packed between October 6 and October 12, 2010, then distributed to wholesale and retail establishments throughout North Carolina. Source:

<http://www.foodpoisonjournal.com/2010/10/articles/foodborne-illness-outbreaks/barbecue-pork-products-recalled-due-to-salmonella-contamination>

(Tennessee) Fungicide resistance found in soybean field. Research conducted by the University of Illinois (U of I) and the University of Tennessee confirms that the fungus that causes frogeye leaf spot of soybean, *Cercospora sojina*, has shown resistance to strobilurin fungicides in a Tennessee soybean field. “Strobilurin fungicides belong to the chemistry class known as the quinone outside inhibitors

UNCLASSIFIED

UNCLASSIFIED

(QoIs), which are the most widely used group of foliar fungicides applied to field crops to manage plant diseases,” a U of I Extension plant pathologist said. These fungicides can be sold as one-active ingredient products such as Headline (BASF Corp.) or Quadris (Syngenta Crop Protection) or in products that combine them with a fungicide in a different chemistry class known as the demethylation inhibitors, sometimes referred to as triazoles, he said. Products that include a strobilurin-triazole combination of active ingredients include Quilt (Syngenta Crop Protection) and Stratego (Bayer CropScience). Strobilurin fungicides have been deemed high risk for fungal pathogens developing resistance to them. In the major soybean production areas in the United States, soybean fields are generally treated once during the season with a fungicide (if treated at all), the plant pathologist said. “However, we were somewhat surprised to find resistance so soon,” he added. “Every time you apply a fungicide, you increase the selection pressure and the opportunity to select out individuals in the pathogen population that have resistance or reduced sensitivity to the fungicide.” Source: <http://www.croplife.com/news/?storyid=2935>

(Texas) Texas closes produce plant linked to five deaths. Deadly chopped celery contaminated with *Listeria monocytogenes* was traced back October 20 to Sangar Fresh Cut Produce in San Antonio, Texas, and the company was ordered to stop processing food and recall all products shipped since January. The order came from the Texas Department of State Health Services (DSHS). Five deaths in Texas appear to be associated with chopped celery contaminated with *Listeria*. The order to shutdown Sanger was issued after laboratory tests of chopped celery from the plant indicated the presence of *Listeria monocytogenes*. The recalled products — primarily cut fresh produce in sealed packages — were distributed to restaurants and institutional entities, such as hospitals and schools. The products were not sold in grocery stores. The testing was done as part of a DSHS investigation into 10 listeriosis cases, including five deaths, reported to the department over an 8-month period. Six of the 10 cases have been linked to chopped celery from the Sangar plant. The illnesses occurred in Bexar, Travis and Hidalgo counties. Source: <http://www.foodsafetynews.com/2010/10/texas-closes-produce-plant-associated-with-five-deaths/>

Deadly pneumonia traced to domestic sheep. New research claims to settle the controversial and long-running debate over whether domestic sheep can infect bighorn sheep with the bacteria that cause fatal respiratory pneumonia. A research team at the Washington State University College of Veterinary Medicine tagged *Mannheimia haemolytica* isolated from domestic sheep to show that domestic sheep could transmit the deadly bacteria to bighorn sheep when they were in contact with each other. The four bighorn sheep in the study all died from pneumonia traced back to bacteria originating in the domestic sheep. The bighorns showed no signs of illness while they were kept 32.8 feet away from the domestics during the first phase of the study. It was only after the animals were allowed to commingle that the bighorns became visibly ill and eventually died. The research, which appeared in the July 2010 issue of the *Journal of Wildlife Diseases*, follows on the heels of an unprecedented high number of pneumonia outbreaks among bighorn sheep in several Western states. Source: <http://www.avma.org/onlnews/javma/nov10/101101n.asp>

(California) First U.S. infestation of worst known palm tree pest found by landscaper in Orange County. Agricultural officials confirmed October 18 the detection of a red palm weevil in the Laguna Beach area of Orange County, California — the first-ever detection of the pest in the United States. The weevil is considered to be the world’s worst pest of palm trees. An infestation typically results in the death of the tree. “This invasive pest is a threat not only to our nursery growers and date palm

UNCLASSIFIED

UNCLASSIFIED

farmers,” said the California Department of Food and Agriculture (CDFA) secretary. “It also endangers all of the decorative palms that are so common in our landscape and so much a part of the classic California backdrop.” In response to the original contact by the landscaper, state and local agricultural officials, working in partnership with the U.S. Department of Agriculture, began extensive, door-to-door survey in the neighborhood, and are setting about 250 traps to determine if an infestation exists. Protocols for this pest call for an initial survey covering a 1.5 square mile radius around the detection property, resulting in a trapping array covering 9 square miles. Source: http://www.oc180news.com/article/West_Orange_County_Features/Current_Interest/First_US_Infestation_Of_WORST_Known_PALM_Tree_Pest_Found_By_Landscaper_In_Orange_County/19257

(North Carolina) Asian fruit fly may plague state next year. An Asian fruit fly recently discovered in North Carolina could create problems in 2011 for gardeners and commercial farmers who grow small fruits such as blueberries and apples. A county extension agent in Asheboro the summer of 2010 captured the state’s first confirmed spotted wing drosophila in a trap in her backyard. The fruit fly, native to cooler parts of east Asia, was discovered in the mainland United States in California in fall 2008. By 2009, it had appeared in Florida, said an extension specialist and assistant professor of entomology at N.C. State University. The Asian pest is capable of destroying 20 percent of a fruit crop. After its appearance in Florida, the extension specialist organized a trapping project in North Carolina, South Carolina, and Virginia to gauge the fly’s migration. Adult flies were trapped during the summer, and the first significant North Carolina larval infestation was discovered in September 2010 at the Upper Mountain Research Station in Ashe County, in the northwest corner of the state. The flies found in 2010 were discovered after most of the state’s small fruit had been harvested, so their true effect will not begin to be felt until 2011. Source: <http://www.newsobserver.com/2010/10/20/750341/asian-fruit-fly-may-plague-state.html#ixzz12uXwChlt>

(Oregon) ALF incident in Molalla does not concern ranchers here. Fallow deer ranchers in Jackson County, Oregon, said it would remain business as usual for them despite an act of sabotage against a Molalla deer ranch October 9 claimed by the Animal Liberation Front (ALF). The incident, in which a section of fencing was removed in an unsuccessful attempt to allow the deer to escape, joins a July firebombing at a former Astoria mink farm as two recent crimes claimed on behalf of the ALF, which had strong roots in southern Oregon more than a decade ago. “It never entered into my mind that someone would be interested in that,” said a woman, who has a state license to raise up to 63 fallow deer on her White City farm. The family has been raising and selling fallow deer and butchered deer meat for 10 years. They have suffered no vandalism nor worry about being targeted by animal-rights extremists, despite knowing deer-ranching licenses are public record, she said. In an anonymous e-mail posted by the North American Animal Liberation Press Office Web site labeled a “communique,” the ALF removed the fencing in Molalla so the captive deer could escape into the surrounding forest. An FBI spokeswoman in Portland said agents are investigating. Source: <http://www.mailtribune.com/apps/pbcs.dll/article?AID=/20101017/NEWS/10170338>

(Wisconsin) Otto’s Meats in Luxemburg recalls products. Otto’s Meats in Luxemburg, Wisconsin, voluntarily recalled all processed, cooked meats produced in 2010 because of possible underprocessing, according to food safety officials with the Wisconsin Department of Agriculture, Trade and Consumer Protection. There have been no reports of illness associated with the products. All products carry Otto’s Meats on the label and were made in 2010. All items were sold at Otto’s

UNCLASSIFIED

UNCLASSIFIED

Meats retail store in Luxemburg. The problem was discovered during a routine inspection October 8. Source: <http://www.greenbaypressgazette.com/article/20101016/GPG1008/10160423/Otto-s-Meats-in-Luxemburg-recalls-products>

(New York) New York beverage company recalls juices. A beverage company in Bronx, New York, has recalled carrot, carrot beet, carrot lime and cucumber juices because the products were inadequately processed and may contain foodborne pathogens, the New York State Agriculture Commissioner reported October 15. The products from Pats Exotic Beverages Inc, 2919 Tiemann Ave., were sold at retail outlets in the New York City metro area. The potential for contamination was discovered after a New York State Department of Agriculture and Markets Food inspection. Sales of the products have been suspended. All packages and codes of these products are subject to the recall. Source: <http://www.foodsafetynews.com/2010/10/new-york-beverage-company-recalls-juices/>

Lead found in salted plum candy from China. Consumers are being warned not to eat “Candy El Pecas Saladitos con Chile” and “Candy El Pecas Saladitos con Limon,” salted plum candy imported from China, after the California Department of Public Health (CDPH), discovered elevated levels of lead in the product. The CDPH analysis found “Candy El Pecas Saladitos con Chile” contained lead levels as high as 0.70 parts per million (ppm) and “Candy El Pecas Saladitos con Limon” contained lead levels as high as 0.42 ppm. Consumption could result in a lead exposure exceeding the maximum legal limit by as much as seven times. Pregnant women and parents of children who may have consumed the candy should consult their physician or health care provider to determine if medical testing is needed. Candy El Pecas in Chula Vista, which distributed the candy, has initiated a voluntary recall and is working with businesses to ensure the contaminated products are removed from the market. Source: <http://www.foodsafetynews.com/2010/10/salted-plum-candy-recalled-in-california/>

(Tennessee) Supplier recalls frozen vegetables because of glass fragments. Packages containing frozen vegetables sold by Wal-Mart nationwide and Kroger stores in the Southeast may contain glass fragments, the supplier said October 15 in announcing a voluntary recall. The Pictsweet Co. of Bells, Tennessee, is advising the public not to eat the recalled store-brand vegetables because of the potential for harm. Consumers should return them to the place of purchase for a full refund, Pictsweet said. The voluntary recall covers the following items: Kroger 12-ounce Peas and Carrots, and Green Peas; Great Value 12-ounce Steamable Sweet Peas, and Mixed Vegetables. Source: <http://www.cnn.com/2010/HEALTH/10/16/veggie.recall/index.html?hpt=Sbin>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Massachusetts) Bomb scare empties Fall River courthouse for two hours. The Fall River Justice Center in Massachusetts was shut down for two hours October 21 as police officers, court officials, and trained dogs swept through the five-story structure, looking for a suspicious package. Safety officials typically do not discuss the specifics of false alarms or bomb scares, but fire and police officials confirmed nothing was found. Everyone returned to business late in the day. Until officials decided it was safe to go back inside, police officers and firefighters shut down South Main Street and Second Street from Borden to Spring Streets, blocking the center of downtown from 9:30 to 11:30

UNCLASSIFIED

UNCLASSIFIED

a.m. Source: <http://www.wickedlocal.com/westport/highlight/x2030534885/Bomb-scare-empties-Fall-River-courthouse-for-two-hours>

(Alabama) Birmingham City Hall reopens after bomb scare. Birmingham City Hall in Alabama was locked down October 21 due to a bomb threat. Birmingham Police said at least three suspicious packages were discovered at two entrances to City Hall. One of the packages, a piece of luggage, was found at the 19th Street entrance to City Hall, and the other two were found on the opposite side of the building. The bomb squad checked all of the suspicious pieces and found them to be empty. City Hall officials said no one was allowed in nor out of the building during the incident. No one was hurt. Source: <http://www.myfoxa.com/Global/story.asp?S=13364454>

(Connecticut) 2nd bomb threat at UConn in a week. A bomb threat October 21 at the University of Connecticut's Greater Hartford campus in West Hartford forced an evacuation for the second time the week of October 18. Classes were canceled for the rest of the day, the university said. The threat, received about 8 a.m., indicated a bomb would be detonated on campus, but no specific target was mentioned. Police are doing a sweep of the buildings. A bomb threat was also received October 19 via e-mail. The university is not sure if the threats are related. Source: <http://www.wtnh.com/dpp/news/crime/west-hartford-uconn-bomb-threat>

(Pennsylvania) Bomb threat forces closure of Blair County courthouse. A bomb threat October 20 forced the evacuation of the Blair County Courthouse in Hollidaysburg, Pennsylvania. A commissioner said the incident began around 11:15 a.m. with a short phone call to the county's main telephone number. A bomb-sniffing dog was brought in from Penn State University to search the building. Employees were sent home after lunch, but county department heads and managers stayed and manned the emergency operations center. An all-clear was given around 4 p.m. The commissioner said one criminal and two civil trials were recessed until October 22. The county was unable to trace the call back to the perpetrator. Hollidaysburg Borough Police and state police at Hollidaysburg are investigating the threat. Source: http://wrtta.com/page.php?page_id=59453

(Florida) Deputies: Charlotte man threatened to blow up school. The Charlotte County Sheriff's Office in Florida arrested a parent after they say the man threatened to blow up an elementary school in Punta Gorda. The 28-year-old suspect was arrested by a Charlotte County Sheriff's School Resource Officer (SRO) October 19 after allegedly threatening to blow up Deep Creek Elementary School. Charlotte deputies took a call just before 12:30 p.m. The caller told deputies that the man made the threat to blow up the school when students were off campus. The arrest report stated the man made the threat after he found out a school staff member told the Florida Department of Children and Families about the burn mark on his child's arm. The school principal said she had legitimate concern about the threat because she knew the man to be a hostile and aggressive parent from previous encounters. The SRO and two deputies went to the man's home and talked to him about the threat, which he said was just a joke. Deputies said there was probable cause to charge the man with Threat to Discharge a Destructive Device. He was taken to the Charlotte County Jail. Source: <http://www.nbc-2.com/Global/story.asp?S=13352235>

(Wisconsin) Capitol evacuated due to bomb threat. The Wisconsin State Capitol in Madison was evacuated October 19 because of a bomb threat, according to the department of administration. The threat was sent first to an unidentified media outlet, which then informed the Capitol. Capitol Police

UNCLASSIFIED

UNCLASSIFIED

and the Dane County Sheriff's K-9 unit searched the area and ultimately allowed people back in the building in the early afternoon. According to a state representative, Capitol workers were evacuated for a few hours starting at 10 a.m., and they were calm and orderly as they were evacuated. Although the Capitol is open to the public, police continue to survey the area. The investigation is ongoing.

Source: <http://www.dailycardinal.com/news/capitol-evacuated-due-to-bomb-threat-1.1716772>

(Ohio) Medina Middle students back in class after bomb squad checks out box. Medina Middle School students in Columbus, Ohio, returned to their building after the school got a call reporting a bomb and a box found on the grounds was determined safe October 20. Columbus police and fire were called to Medina Middle School on reports of suspicious packages at about 8 a.m. The school received a phone call about a bomb being on the property. School security checked the area and found a suspicious box on school grounds near a clothing donation box. The students were evacuated to nearby Huy Elementary School, 1545 Huy Rd. Columbus fire's bomb squad was called to the scene and arrived at about 8:20 a.m. The squad's bomb robot determined the box was ordinary and safe shortly after 9 a.m. The students returned to their building and classes resumed. Source:

<http://www2.nbc4i.com/news/2010/oct/20/5/ccs-middle-school-evacuated-suspicious-packages-ar-265961/>

(Virginia) Shots fired at the Pentagon, police say. Shots were fired at the Pentagon in Arlington, Virginia October 19, authorities said, striking a window of the building. A Pentagon police spokesman said it is not known who fired the shots. Pentagon police officers heard at least five shots around 4:50 a.m. According to another Pentagon Force Protection Agency spokesman, two bullets hit the Pentagon on the south side of the building — one striking a window and the other hitting the building itself. This is an unoccupied part of the building that is being renovated. The spokesman said a fragment of one of the bullets is lodged in the window. The windows, which are bullet-proof, did not shatter. There was a partial lockdown of the Pentagon's south parking lot and south entrance for about 1 hour after the shooting, and authorities briefly shut down a portion of Interstate 395 going out of the capital — which runs along the south side of the Pentagon — to conduct a search in the investigation. Source:

<http://www.cnn.com/2010/CRIME/10/19/dc.pentagon.shots.fired/index.html?hpt=T1>

(North Carolina) Streets closed again as Charlotte bomb probe continues. Authorities have closed a portion of Mount Holly Road and several nearby streets October 19, while they continue their search of a northwest Charlotte, North Carolina, house linked to an explosion October 18 of a pen at a school. One student was injured at the school, and three firefighters were hurt in the explosion of materials at the Mount Holly Road home later in the day. Police, firefighters and the haz-mat team returned to the house about 8 a.m. October 19. Two teens who live at the house have been charged in the case. "Hazmat and other agencies continue to remove hazardous materials from the house," a Charlotte-Mecklenburg Police Department spokeswoman said. Meanwhile, classes at Turning Point Academy resumed at 8 a.m. October 19. Source:

<http://www.charlotteobserver.com/2010/10/19/1770635/pen-explodes-cms-student-hurt.html>

(Virginia) Bullet holes found in Marine Corps museum windows. Police in Prince William County, Virginia, said bullet holes have been found in windows at the National Museum of the Marine Corps. A cleaning crew at the museum in Triangle called police when they noticed the bullet holes in windows high up in a part of the building that faces Interstate 95. Police believe the shots were fired

UNCLASSIFIED

UNCLASSIFIED

late October 16 or early October 17, when no one was inside. Investigators used a crane to inspect the damage October 18. Because of the height of the holes, police suspect the bullets were likely fired from a rifle, but they are still working to determine what caliber of bullet was used. Several glass panels were hit, causing about \$20,000 in damage. None of the museum's artifacts — including a harrier jet hanging near the damaged windows — were hit. Source:

<http://wtop.com/?sid=2084662&nid=730>

(Florida; Pennsylvania) Bomb threat leads to courthouse evacuation. A Pennsylvania prison inmate with a penchant for writing threatening letters prompted Volusia County sheriff's deputies to evacuate the DeLand, Florida courthouse mailroom October 18 because of one of his letters, a sheriff's spokesman said. The inmate is serving a long prison sentence in Pennsylvania, said a sheriff's spokesman. "The letter alleged that bombs had been placed in several courthouses around the state, and DeLand was one of them," the spokesman said. "I don't know that he has any particular connection to DeLand." Deputies with bomb detection dogs were sent to the courthouse at noon. A dog hit on a package but it turned out to be a delivery to the courthouse's information technology office, which had a substance in it detected by the dog, the spokesman said. He said the mailroom and offices around it were evacuated in an "abundance of caution." Source: <http://www.news-journalonline.com/news/local/west-volusia/2010/10/19/bomb-threat-leads-to-courthouse-evacuation.html>

(North Carolina) Authorities search Charlotte school after explosion. Multiple emergency agencies were on the scene of a home in Charlotte, North Carolina October 18, where an explosion sent three firefighters to the hospital. The home is being searched in connection with an explosion that occurred in a local school, injuring a student there. The first explosion happened inside a classroom at Turning Point Academy in Charlotte around 9 a.m. A student opened up a desk, took out a pen, and it exploded. The 15-year-old suffered some scrapes and bruises, but was not burned. The student was taken to the hospital as a precaution. "They're in the process of investigating to try to figure out who put the device there," a Charlotte-Mecklenburg Police Department captain said. Authorities searched the area three times and didn't find any other devices. Students were evacuated to a gym across the street from the school and classes were canceled. Later October 18, police began searching a home off of Mt. Holly Road in connection to the school incident. During the search, another explosion happened, injuring three firefighters. Investigators said sample product that was being field tested at the home caused the explosion. Police confirmed they have a set of teenage brothers in custody in connection to both explosions. Source: <http://www.wcnc.com/home/Possible-explosion-at-Charlotte-school-105172054.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Global e-crime gang transitions to crimeware. The world's most prolific phishing gang has completed a transition from using conventional phishing to massively propagating stealthy password-stealing crimeware that does not require user cooperation to surrender financial account credentials, according to a report by APWG. While the Avalanche botnet infrastructure had been used to launch conventional spam-based phishing attacks over the past two years, the phishing has been replaced with a scheme that infects users' PCs with the potent Zeus Trojan, a powerful banking credential-stealing malware. The phishing syndicate had been successfully using the Avalanche botnet for conventional spam-based phishing attacks that provoke a user to visit a counterfeit website and enter

UNCLASSIFIED

UNCLASSIFIED

or his or her credentials. This Avalanche phishing accounted for two-thirds of all phishing attacks observed worldwide in the second in late 2009. But the Avalanche infrastructure was involved in just four conventional phishing attacks in the month of July 2010. Instead, the Avalanche-based syndicate ramped up a concerted campaign of crimeware propagation to fool victims into receiving the Zeus crimeware and infecting their PCs with it. Avalanche has been sending billions of faked messages from tax authorities such as the IRS, false alerts/updates purporting to be from popular social networking sites, and other lures. These lures take victims to drive-by download sites, where the criminals infect vulnerable machines. Source: <http://www.net-security.org/secworld.php?id=10026>

Halloween-themed spam already in circulation. Security companies warn that affiliate marketing spammers have already begun exploiting Halloween to trick people with fake prizes, contests, and offers. "Halloween is drawing near, so the spammers are busy laying out bait in the form of Halloween jackpots, sweepstakes, gift cards, e-cards, personalized gifts, online contests, and even print products and costumes," a security researcher at Symantec warned. Searching for holiday-themed screensavers or wallpapers on the Internet during this period has a great chance of leading to malware. Some examples of Halloween spam e-mail subjects seen by Symantec so far include the following: "Halloween Series Campaign Vol1", "Halloween Treat Bags, Home Decorations, and More", "Open this! \$1 Million Prize", "Halloween Special! Up to 85% off ink and toner", "Halloween E-card - no cost." Meanwhile, cloud-security provider Zscaler warned that spammers compromised legit Web sites, including some that belong to educational institutions, and used them in black hat SEO campaigns to drive traffic to the Web site of a Halloween costumes retailer. Source: <http://news.softpedia.com/news/Halloween-Themed-Spam-Already-in-Circulation-162074.shtml>

Mac users warned of growing virus threat. Attacks on the Mac are now significant enough to warrant Apple users investing in an anti-virus product, security company Panda Security said. There are now 5,000 "strains" of malware that target the Mac, and the company said it is seeing 500 new Mac-specific samples appearing every month. In 2009, 34 vulnerabilities were detected in Apple's OS X, which had risen to 175 so far for 2010, with a 20-year total of 170,000 macros "viruses" affecting the platform. Such security threats relate only to Apple desktop and laptop computers. Security companies eying Apple users is nothing new, and every notable antivirus company now has a Mac product. Questions remain about the scale of the threat, however. Source: <http://www.networkworld.com/news/2010/102110-mac-users-warned-of-growing.html>

Zynga sued for leaking Facebook user IDs to advertisers. Only days have passed since news broke out that top Facebook applications shared users IDs (UIDs) with advertisers, and Zynga has already been sued over the practice. Zynga is the largest Facebook developer and is responsible for six of the top ten most used applications on the platform. ComputerAndVideoGames (CVG) reported that a lawsuit seeking class action status was filed in U.S. District Court in San Francisco. The lawsuit alleges that Zynga broke federal law, as well as Facebook's terms of service, by sharing personal data of 218 million users with its advertising partners. It asks for unspecified monetary relief and an injunction that would ban Zynga from engaging in similar actions in the future. According to The Register, Zynga representatives called the lawsuit without merit and stressed that they are preparing a strong defense. Source: <http://news.softpedia.com/news/Zynga-Sued-for-Leaking-Facebook-User-IDs-to-Advertisers-162090.shtml>

UNCLASSIFIED

UNCLASSIFIED

Phishers target Xbox players via fake Gamertag changer. Security researchers from Sunbelt warn that phishers are trying to steal Live IDs from Xbox users, through a fake program which promises a free Gamertag change. According to a senior threat researcher at Sunbelt (now part of GFI Software), there is a program called “Gamertag Changer” going around that does nothing more than steal Windows Live credentials from Xbox gamers. The application claims that it will file numerous complaints regarding the user’s Gamertag in order to trigger an automatic change from the system. Users who fall for the trick and input their credentials will see a message asking them to leave the application open for at least 2 minutes and then try to re-login on Xbox LIVE. Meanwhile in the background, the program sends the captured Gamertag, Live ID, and password to an e-mail address controlled by the phisher. Source: <http://news.softpedia.com/news/Phishers-Target-Xbox-Players-via-Fake-Gamertag-Changer-161812.shtml>

Fake Firefox and Chrome warning pages distribute malware. Security researchers warn a new malware distribution campaign uses fake versions of the malicious site warnings commonly displayed by Firefox and Google Chrome. Both Chrome and Firefox tap into Google’s Safe Browsing service to check if the accessed URLs are known attack sites. Security researchers from F-Secure now warn malware pushers are increasingly abusing the trust users associate with these warnings to infect them. Malicious Web sites that mimic both Firefox’s “Reported Attack Page” alert, as well as Chrome’s “this site may harm your computer” warning, have been spotted. The pages look exactly the same as the real thing, except for a button that reads “Download Updates,” suggesting that security patches are available for the browsers. The executable files served when these buttons are pressed install rogue antivirus programs, which try to scare users into paying a license fee. However, the users who land on these latest sites discovered by F-Secure are also exposed to drive-by downloads via a hidden IFrame, which loads the Phoenix exploit kit. Source: <http://news.softpedia.com/news/Fake-Firefox-and-Chrome-Warning-Pages-Distribute-Malware-162022.shtml>

Report: Malware delivery technique focus on HTML attachments. Use of malicious HTML e-mail attachments increased significantly in the third quarter, Commtouch reported October 18 in its third quarter Internet Threats Trend Report. The HTML attachments displayed phishing pages on the user’s local computer or redirected users to sites hosting malware or spam products. The Q3 report examines the methodology within blended attacks, such as the “Here You Have” worm, which spread widely in September using Outlook contact lists from infected PCs. Both Here You Have and numerous fake LinkedIn invitations relied on a combination of social engineering and masked hyperlinks to lead users to Web sites with malware scripts. During Q3, the PayPal, LinkedIn, Craigslist, Bell Canada, NewEgg, and Amazon brands were used by spammers to inspire action by consumers. The report also features the unusual bedfellows of a pharmacy spam campaign based on solidarity with several European politicians and celebrities. The increased use of HTML attachments shows how prominent the multi-stage attack vector has become, said a Commtouch vice president. Source: http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.jhtml?articleID=227900192&subSection=Application+Security

Drive-by kit generates fake Twitter home pages. Security researchers warn of the increasing popularity of a drive-by kit, which allows attackers to create fake copies of the Twitter home page and use them to distribute malware. The real Twitter main page currently promotes a video about the site’s new design. The malware toolkit, which was discovered by researchers from Sunbelt

UNCLASSIFIED

UNCLASSIFIED

Software (now part of GFI), allows attackers to edit the part of the page where the video is located and change it with whatever their wish. In some live examples, the malware pushers used a video thumbnail depicting a scantily-dressed woman. Clicking the image prompted the execution of a malicious Java applet. The applet tried to exploit a vulnerability in older versions of Java to install malware on the victim's computer. The attackers upload these pages to free Web hosting accounts and then target users on Twitter via shortened URLs included in spam messages. They hope that when users open them, they will click on the intriguing picture without verifying the URL in the address bar. Source: <http://news.softpedia.com/news/Drive-By-Kit-Creates-Fake-Twitter-Home-Pages-161536.shtml>

RealPlayer receives critical security update. Real Networks has issued a security update for RealPlayer, addressing flaws in versions 1.1.4 and earlier of the application. The company said RealPlayer 1.1.5 and later for Windows is not believed to be vulnerable to attack, neither is the Mac RealPlayer 12.0.0.144 and later release, or the latest RealPlayer Enterprise and RealPlayer for 11.0.2.1744 for Linux release. The update patches seven vulnerabilities ranging from buffer overflow and injection flaws to issues that could allow an attacker to remotely execute code on a targeted system. Real Networks advised administrators to upgrade RealPlayer installations to the most current stable version. No active exploitations of the flaw have been reported in the wild. Source: <http://www.v3.co.uk/v3/news/2271764/realplayer-receives-critical>

Tests show consumer antivirus programs falling behind. The latest tests of consumer of antivirus software released October 19 show the products are declining in performance as the number of malicious software programs increases. NSS Labs tested 11 consumer security suites and found that the products are less effective than 1 year ago as far as blocking the download and execution of malicious software programs. The company also tested if those programs detected and blocked malicious Web sites. The download and execution blocking rate for the top performing product, Trend Micro's Titanium Maximum Security, fell from 96.4 percent to 90.1 percent from the third quarter of 2009 to the same period this year. All of the rates were lower except for two products: McAfee's Internet Security and F-Secure's Internet Security 2010, which upped their detection and blocking rates by 3.6 percent and .4 percent respectively. The biggest drop occurred for AVG's Internet Security 9, which fell 18.5 percent, and Kaspersky's Internet Security 2011, which fell 16.5 percent. The tested security products have not necessarily fallen in quality, but rather the threats are evolving at a rapid pace, said the president of NSS Labs. Source: http://www.computerworld.com/s/article/9191718/Tests_show_consumer_antivirus_programs_falling_behind?taxonomyId=17&pageNumber=1

F-Secure blocks spying app for Windows and Android. F-Secure is blocking a sophisticated mobile phone spying application, despite being ambivalent about the creator's motives. Phone Creeper is a Windows Mobile application that lets an outside user access a mobile phone's calls, SMS logs, contacts, calendar information, and GPS data that tracks location. The developer has said an Android version will be released shortly. "This is a phone espionage suite. It can be silently installed by just inserting an SD card with the files below on it," said the Phone Creeper creator from XDA-Developers in the latest update. However, in an ethical statement, he said he created the code to show what was possible with the handset, and because it was fun to develop something unique. He said he will work with other XDA developers to find a solution to blocking the flaws and will release it as open source code. F-Secure said it is blocking the application with its mobile security software because of its

UNCLASSIFIED

UNCLASSIFIED

functionality, but does not believe the creator's motives are in question. Source:

<http://www.v3.co.uk/v3/news/2271661/f-secure-blocks-mobile-spying>

Newly discovered evasion method for targeted attacks silently bypasses network, application security. CERT-Finland has reported a newly discovered technique that evades network and security devices — namely IDS/IPS systems, could also work against network firewalls and Web application firewalls — and lets attackers sneak in and conduct targeted attacks against an enterprise network. The threat, which was discovered by researchers at Stonesoft's Helsinki labs, is based on vulnerabilities inherent in several vendors' IDS/IPS products, according to CERT-Finland, which has alerted the affected IDS/IPS vendors. The names of the vendors and their products have not been released publicly. The head of vulnerability coordination at CERT-FI, which first issued an alert on the threat October 4, will update its vulnerability alert on the threat October 18. “[The attack method] takes advantage of the fact that the TCP protocol allows conservative creation of packets, but liberal receiving of packets,” said the director of U.S. product management at Stonesoft. He said it lets the attacker work his way inside the network without being noticed. Source:

<http://www.darkreading.com/security/perimeter/showArticle.ihtml?articleID=227900122>

Facebook in privacy breach. Many of the most popular applications, or “apps,” on the social-networking site Facebook Inc. have been transmitting identifying information — in effect, providing access to people's names and, in some cases, their friends' names — to dozens of advertising and Internet tracking companies, a Wall Street Journal investigation has found. The issue affects tens of millions of Facebook app users, including people who set their profiles to Facebook's strictest privacy settings. The practice breaks Facebook's rules, and renews questions about its ability to keep identifiable information about its users' activities secure. The problem has ties to the growing field of companies that build detailed databases on people in order to track them online. It is unclear how long the breach was in place. On October 17, a Facebook spokesman said it is taking steps to “dramatically limit” the exposure of users' personal information. Source:

<http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>

NATIONAL MONUMENTS AND ICONS

(New Jersey) Vandals hit veterans monuments in Paterson again. Veterans in Paterson, New Jersey discovered another wrecked monument October 17 at Hayden Heights Park. “Enough is enough,” said a Vietnam veteran and president of the Paterson Veterans Council who, for the second time in a week, surveyed the damage at the park, where monuments and military vehicles are on display. This time, a 4-foot tall Disabled American Veterans “Argonne Chapter 18” monument was knocked over, he said. The Argonne monument is next to an American Legion granite monument that was pulverized into four pieces October 11. Source:

http://www.northjersey.com/news/101710_Vandals_hit_veterans_monuments_in_Paterson_again.html

POSTAL AND SHIPPING

(Tennessee) Reward in Tennessee postal killings increased to \$50,000. The U.S. Postal Inspection Service October 19 doubled to \$50,000 the reward it is offering for information leading to the arrest and conviction of whoever fatally shot two female postal employees October 18 at the post office in

UNCLASSIFIED

UNCLASSIFIED

western Tennessee, about 50 miles northeast of Memphis. The service identified the victims as a retail clerk, and a rural carrier associate. The shootings occurred at the post office in Henning between 8:30 a.m. and 9 a.m. The case is being jointly investigated by the U.S. Postal Inspection Service; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; the FBI; the 25th Judicial District Attorney General's Office; the Tennessee Bureau of Investigation; the Tennessee Highway Patrol; the Lauderdale County Sheriff's Office; the Tipton County Sheriff's Office; and the Henning Police Department. More than 60 law enforcement officers nationwide have been assigned to the case, the service said. Source: <http://edition.cnn.com/2010/CRIME/10/19/tennessee.postal.shootings/>

(Texas) HISD's mystery envelopes may be linked to Dallas case. The discovery of envelopes containing suspicious white powder at 17 campuses in the Houston Independent School District (HISD) in Texas may be linked to an investigation originating in the Dallas area. Since early August, more than a dozen envelopes also containing white powder were sent to churches, mosques, businesses and at least two schools in North Texas, authorities said. FBI officials in Dallas confirmed October 19 that similarities exist between their cases and those in Houston. "But we're not in a position to say they are or are not from the same person," said an FBI Special Agent. The Dallas-area envelopes contained a short message that made a cryptic reference to al-Qaida. Similar letters — all postmarked from North Texas — were sent to Austin, Lubbock, Chicago, Illinois and the Boston suburb of Waltham, Massachusetts. A pair of schools in Washington, D.C. also received envelopes from North Texas containing white powder. HISD officials initially said the envelopes contained powder, but would not confirm they contained messages. FBI officials now say they did. Source: <http://www.chron.com/disp/story.mpl/metropolitan/7254944.html>

(Pennsylvania) Tanker cars vandalized. Vandals ruptured several railroad tanker cars, dumping about 240,000 gallons of used cooking oil and 1,500 gallons of diesel into a rail yard in Falls, Pennsylvania October 14. The fire marshal said employees of Tyburn Railroad Co. discovered pools of oil and fuel when they arrived at work. The company notified the state department of environmental protection, police, fire officials and the U.S. Coast Guard, due to the proximity to the Delaware River. The rail yard is designed to pool spills in designated areas. Tanker trucks used vacuum hoses to suck up the oil and diesel, then deposited the fluids back in the repaired tanker cars. The company hired to help clean the spill received assistance from Waste Management, which created sand berms between the oil and river in the event rainwater would cause oil to flow into the river or the river to flood to the oil. Source:

<http://webcache.googleusercontent.com/search?q=cache:IU6fclQEVMJ:www.phillyburbs.com/news/local/courier+times/courier+times+news+details/article/28/2010/october/17/tanker-cars-vandalized.html-###>

(Tennessee) Two people killed in shooting at Henning post office. Two people were killed October 18 in a shooting at the post office in Henning, Tennessee. Sources with the Lauderdale County Sheriff's Department said two female employees were killed in an incident that was reported around 9 a.m. The circumstances that led to the shooting are unclear, and information about a possible suspect is not yet available. Henning is located about 50 miles northeast of Memphis. Source: <http://www.wmctv.com/Global/story.asp?S=13341548&hpt=T2>

(New Mexico) Mailbox blown up by homemade bomb. Albuquerque, New Mexico police are searching for the person responsible for blowing up a mailbox with a homemade bomb. Authorities

UNCLASSIFIED

UNCLASSIFIED

tell KOB-TV that someone put a chemical bomb inside a mailbox at a northeast Albuquerque business, near Washington Street and Paseo del Norte Boulevard. The bomb went off early October 14. Police suspect the explosion was a careless teenage prank, and do not believe the business was targeted for any particular reason. Source: http://www.alamogordonews.com/ci_16343876

PUBLIC HEALTH

(Kansas) Explosive device causes alarm at SE Kan. hospital. A southeast Kansas sheriff said two men meant no harm when they showed up at a hospital in Girard with an explosive device. They just wanted to help doctors determine caused one of them to be burned. The October 20 incident at Girard Medical Center brought out police, the Kansas Highway Patrol and personnel from McConnell Air Force Base in Wichita. KOAM-TV reported the injured man came to the hospital with burns apparently caused by an explosion. A search of his vehicle turned up the suspicious device. The Crawford County Sheriff said the item was an M22 Launch Simulator the men had bought earlier that day. The injury happened when the men tried to dismantle it. The device simulates anti-tank guided missile and rocket launchings. It contains magnesium, which causes smoke and a flash. Source: <http://www.kansas.com/2010/10/20/1551212/explosive-device-causes-alarm.html>

(California) Whooping cough claims life of 10th baby in Calif. Health officials said whooping cough caused the death of a 6-week-old baby in San Diego County last week, bringing the number of babies who have died in California during this year's epidemic to 10. The baby who died was treated at Rady Children's Hospital in San Diego. The highly contagious illness has symptoms similar to the common cold, but a persistent cough that lasts weeks may indicate the illness, which is also known as pertussis. More than 5,270 people have been infected in California. All the babies who have died this year were too young to be fully immunized, so health officials are urging parents and caretakers to get booster shots to create a cocoon of immunity around vulnerable children. Source: <http://www.sacbee.com/2010/10/19/3116605/whooping-cough-claims-life-of.html#ixzz12uXccSNB>

West Nile virus often overlooked. Only an estimated 26 percent of those with West Nile virus infection may develop symptoms of the disease, recent study data suggest. To examine the frequency and characteristics of West Nile virus-related symptoms, researchers from the American Red Cross and the Center for Disease Control and Prevention analyzed a population of blood donors whose donations reacted with West Nile virus RNA during initial screening between 2003 and 2008. They confirmed diagnoses with laboratory tests and collected information on symptoms from patients via questionnaire before notifying them of their diagnoses. Of 1,997 blood donors with West Nile virus RNA-reactive samples, 55 percent had confirmed infection, according to the researchers, and represented approximately half of the more than 2,000 donors with West Nile virus reported to blood centers in the United States during the study period. "Our data indicate that many [West Nile virus]-related illnesses are clinically significant but are nonspecific and remain undiagnosed," the researchers wrote. Source: <http://www.infectiousdiseaseneews.com/article/76784.aspx>

Tylenol product recalled after complaints of moldy odor. The maker of Benadryl and Tylenol has added another popular over-the-counter drug to its growing list of recalled products. The October 18 recall affects Tylenol 8-hour caplets 50 count, sold in the United States and Puerto Rico. The lot number is BCM155. Complaints of a musty or moldy odor led to the recall, McNeil Consumer Healthcare said. The company believes the odor is caused by the presence of trace amounts of a

UNCLASSIFIED

UNCLASSIFIED

chemical called 2,4,6-tribromoanisole. McNeil, a subsidiary of Johnson and Johnson said the “risk of adverse medical events is remote.” Adverse event reports are consumer complaints of a serious side effect associated with the use of a medical product, according to the Food and Drug Administration. The company has issued several recalls this year of non-prescription cold and pain drugs such as Tylenol, Benadryl and Motrin — prompting a Congressional inquiry. Source: <http://www.cnn.com/2010/HEALTH/10/19/tylenol.recall/index.html?hpt=T2>

Cellphones reveal emerging disease outbreaks. A person’s cellphone could be a key tool in the fight against disease by relaying a telltale signature of illness to doctors and agencies monitoring new outbreaks. “This technology is an early warning system,” said a researcher at the Massachusetts Institute of Technology, whose team concluded that one could spot cases of flu by looking for changes in the movement and communication patterns of infected people. Epidemiologists know disease outbreaks change mobility patterns, but until now have been unable to track patterns in any detail. After researchers gave cellphones to 70 students in an undergraduate dormitory, a characteristic illness signature emerged from the data, which was gathered over a 10-week period in early 2009. However, researchers will need to think hard about the causes of the changes they saw in the cellphone data. An MIT colleague looked at cellular data from a series of cholera outbreaks in Rwanda between 2006 and 2009. He saw a clear reduction in people’s movement, which may have been due to the disease. But the outbreak was caused by floods, which also limited mobility. Source: <http://www.newscientist.com/article/mg20827824.800-cellphones-reveal-emerging-disease-outbreaks.html>

TRANSPORTATION

(Rhode Island) Rhode Island port adds chemical threat detectors. Rhode Island homeland security officials have beefed up security at the Port of Providence by placing three chemical detectors to sample the air for potential chemical threats. The detectors can tell security officials if an accidental or intentional release of dangerous chemicals has occurred, the Providence Journal reports. The devices can detect 15 industrial chemical compounds, including ammonia, and can identify seven bioterrorist chemical agents, including sarin and mustard gas. Providence Homeland Security officials staged a simulated emergency this week to demonstrate the capability of the chemical detectors. The simulated emergency involved an accident that involved a truck hitting a moving railroad train which, in turn, caused a chlorine release, the Providence Journal reports. The chemical detectors will mainly be monitored by the Enforcement Division of the state Department of Environmental Management. Source: <http://www.bioprepwatch.com/news/218251-rhode-island-port-adds-chemical-threat-detectors>

Pilot’s licenses still short on security measures. In an attempt to improve security, Congress told the Federal Aviation Administration (FAA) in 2004 to come up with a pilot’s license that included the pilot’s photo and could contain biometric information like fingerprints or iris scans. Today licenses lack photos or biometric data. In an October 19 letter, a Florida Congressman asked the heads of the FAA, the Transportation Security Administration and DHS to explain why they haven’t complied with the law he helped write. FAA officials have told the congressman one reason the licenses don’t contain biometric information is they’ve been waiting for TSA and DHS to decide on criteria and the equipment necessary to read the data. He said the three agencies have been pointing fingers at each other. The law doesn’t say the licenses must contain biometric data, just that they are capable of

UNCLASSIFIED

UNCLASSIFIED

doing so. That would require they be embedded with microchips capable of storing fingerprints, iris scans or personal data that can be used to verify someone's identification. Lawmakers left it up to FAA administrator to decide what biometric information should be included. FAA officials said that unlike state motor vehicles departments, the agency doesn't have conveniently located offices where pilots can present themselves to have their photos taken. However, Congress also gave the FAA permission to designate a local authority, such as a police department or an airport, to take the photos. Source: <http://www.wtol.com/Global/story.asp?S=13352308>

Airline may let fliers use cellphones. Early next year, Singapore Airlines will begin to install technology in dozens of planes to let passengers surf the Internet and send e-mail from 35,000 feet in the air, the airline has announced. The circuitry it plans to install in at least 40 long-haul jets by 2013 would also allow passengers to make airborne cellphone calls. But Singapore Airlines remains undecided whether to allow cellphone calls. "As we get closer to the launch date, we will decide whether voice calling in the cabin will be activated," said a Singapore Airlines spokesman. One consideration, he said, is whether passengers want to make calls in flight. The hesitation is not surprising. Although a handful of airlines in the Middle East and Europe allow cellphone calls, U.S. regulators prohibit the practice, saying the calls may interfere with navigation systems. But the problem may not be the technology. After all, Emirates airline has allowed cellphone calls since 2008. Cathay Pacific announced plans in July to let passengers use their cellphones in the plane by 2012. A bigger issue may be that passengers and airline crews hate the idea of turning a crowded, airborne cabin into a flying phone booth. The Federal Communications Commission considered lifting the ban in 2004, but it stopped looking into the idea after being inundated with letters, e-mails and calls in opposition. The pending reauthorization bill for the Federal Aviation Administration includes a proposal to ban all cellphone calls on U.S. commercial planes — except by airline crews and law enforcement. In a 2005 survey by the National Consumers League and the Association of Flight Attendants, 63 percent of airline passengers said they opposed cellphone use on planes. Source: http://voices.washingtonpost.com/dr-gridlock/2010/10/early_next_year_singapore_airl.html

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

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

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

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED