

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANIT-TERRORISM SUMMARY



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

UNCLASSIFIED

UNCLASSIFIED

NDSLIC DISCLAIMER

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

QUICK LINKS

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

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

[Information Technology and
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security
Contacts](#)

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA

Device made from fireworks prompts evacuation of law enforcement center in North Dakota.

A resident caused a stir when he found a homemade explosive device near the Heart River and brought it into the law enforcement center in Mandan, North Dakota. The Bismarck Tribune reported the Mandan Law Enforcement Center was evacuated for about an hour and a half July 5 while the police bomb squad from neighboring Bismarck was called in. The bomb squad dismantled the device and no one was hurt. Police said it appears someone made the device out of "a large amount" of fireworks, and that it had the potential to cause serious injuries.

Source: <http://www.therepublic.com/view/story/9e89f3fdb684c37a24ea3c0064ff73a/ND--Explosive-Evacuation/>

5,000 gallons of oil spill in ND tanker accident. A semitrailer hauling oil from Canada rolled off a highway in far northeastern North Dakota, injuring the driver and spilling thousands of gallons of oil. The North Dakota Highway Patrol reported that a 24-year-old was driving the rig with two tanker trailers when it drifted into the shoulder of Highway 18 in the evening July 4, just north of Cavalier. The accident report said the truck and trailers rolled onto their sides into the roadside ditch. About 5,000 gallons of oil spilled from the first tank, but the second tank remained intact. The driver was injured and taken by ambulance to Pembina County Memorial Hospital in Cavalier. The extent of his injuries were not immediately known. The accident report said he was traveling from Winnipeg, Manitoba, with a load of road oil. Source:

<http://www.ctpost.com/news/article/5-000-gallons-of-oil-spill-in-ND-tanker-accident-1452281.php>

Missouri rises as releases fall. The Missouri River continued to defy expectations as it rose June 30 in spite of falling releases from the Garrison Dam in North Dakota. The cause, experts said, is likely sediment deposited in the riverbed. The Missouri River in Bismarck-Mandan was at 19.22 feet at 9 p.m. June 30, higher than a few days earlier, before the U.S. Army Corps of Engineers lowered outflows from the dam peak of 150,000 cubic feet per second (cfs) to 145,000 cfs. The river was at 19.19 feet at 9 p.m. June 29. The condition is due to the high velocity of the water carrying away the riverbed, creating a deeper channel that could conduct more water at a higher rate. The river is beginning to slow down and replacing the riverbed it lost with sediment from upstream. Because the river has less power to blast sediment downstream, it is depositing it. Experts did not think back-up from Oahe was creating a higher river at Bismarck-Mandan. The Corps plans to lower releases to 110,000 cfs by July 29, and it is working to lower Lake Sakakawea by 3.9 feet over the month of July. Oahe is forecast to fall by 1.9 feet over the next month, according to the Corps' forecast. Source:

http://www.bismarcktribune.com/news/local/article_7c6c0be2-a362-11e0-bcef-001cc4c002e0.html

Garrison Dam releases being lowered earlier than planned; Oahe to go up but not as quickly.

The U.S. Army Corps of Engineers began lowering water releases from Garrison Dam in North Dakota June 26 to reduce pressure on Missouri River reservoirs downstream. Releases were lowered from 150,000 cubic feet per second (cfs) to 145,000 cfs. After July 9, releases will be

UNCLASSIFIED

UNCLASSIFIED

slowly lowered to 120,000 cfs by July 18. The Corps said inflows into Lake Sakakawea behind the dam are lower than previously forecast. At Oahe Dam in South Dakota, releases will be rising slightly, though slower than planned because of the reduced flows from Garrison. Source: <http://www.therepublic.com/view/story/b192ff8a1e4e4fea9c08f2e0179f79a9/ND--Missouri-River-Flooding-Dakotas-Dams/>

REGIONAL

(Minnesota) Tick-spread virus claims life of northern Minnesota woman. A northern Minnesota woman is dead from a virus caused by the bite of a deer tick, the Minnesota Department of Health reported June 29. The woman, who was in her 60s, was the first person in Minnesota to die from the Powassan virus, the health department said in a news release. The virus, caused by the bite of an infected deer tick (aka blacklegged tick), caused a brain infection. The woman was one of two people to contract Powassan in northern Minnesota this year, the news release said. The other involved an Anoka County man, also in his 60s, who was hospitalized with a brain infection after visiting his cabin in northern Minnesota. He was released from the hospital and is recovering at home. Powassan cases are rarely identified, said the state epidemiologist with the health department in the news release. But they are fatal in 10 percent of cases, and survivors may experience long-term neurological problems. Since the disease is caused by a virus, it cannot be treated by an antibiotic. Symptoms occur within 1 to 5 weeks after an infectious tick bite. Source: <http://www.duluthnewstribune.com/event/article/id/203147/>

(Minnesota) Prairie Island nuclear plant licenses renewed. Federal regulators have renewed the operating licenses for the Prairie Island nuclear power plant near Red Wing, Minnesota, which will allow it to run for 20 more years, Xcel Energy Inc. announced June 28. The utility also said it plans to invest at least \$500 million in the plant through 2015, and even more if the Nuclear Regulatory Commission approves an increase in generating capacity at the plant. The renewal was opposed by the Prairie Island Indian Community, whose reservation is next to the plant. Tribal officials said they have longstanding health and environmental concerns they do not believe were adequately addressed in the review process. Concerns include long-term exposure to low-level radiation, and radioactive contamination of groundwater at the site, as well as plans for increasing the power output of the plant, which will require additional storage of spent nuclear fuel. Source: http://www.forbes.com/feeds/ap/2011/06/28/general-multiutilities-mn-xcel-energy-prairie-island_8539326.html

(Montana) Government orders Exxon to craft pipeline safety plan. U.S. pipeline safety regulators July 5 said Exxon Mobil must make fixes to its ruptured Montana oil pipeline and submit a restart plan before oil can flow again. The U.S. Transportation Department's Pipeline and Hazardous Materials Safety Administration also ordered the company to re-bury the pipeline segment, and do a risk study where it crosses any waterway. The Transportation Secretary said in a statement that those found responsible for the leak would be held accountable. Exxon Mobil does not have a definite repair plan yet for the ruptured Montana

UNCLASSIFIED

UNCLASSIFIED

crude oil pipeline that it shut over the weekend of July 2 and 3, and company and government officials are still trying to determine the cause of the spill, a top executive said earlier July 5. Oil deposits from the rupture may have traveled as far as 240 miles downstream, the government said in its order. Exxon estimated that up to 1,000 barrels (42,000 gallons) of oil spilled into the rain-swollen Yellowstone River when its Silvertip crude oil pipeline ruptured late July 1. Exxon said it shut the 40,000 barrels per day pipeline early July 2 within minutes of discovering a pressure loss that indicated a rupture. Source: <http://www.reuters.com/article/2011/07/06/us-montana-spill-exxon-idUSTRE7646W420110706>

(Montana) EPA to test air in homes near Montana oil spill. The Environmental Protection Agency (EPA) said July 7 it will collect indoor air samples from homes downstream of a Yellowstone River oil spill after residents raised concerns about health risks from the tens of thousands of gallons of crude that poured into the watercourse. About 150 people showed up at an EPA meeting July 6 with questions about health risks, the duration of the cleanup, and whether the oil will permanently damage their livestock or property. Health officials said symptoms residents have reported, such as nausea, dizziness, and shortness of breath, are likely to ease as the chemicals in the oil evaporate or break down. Laboratory results from the air testing are expected to take about a week. A spokesman said Exxon Mobil's contractors will collect duplicate samples so their results can be verified by government scientists. The cause of the July 1 pipeline rupture beneath the riverbed in Montana remains under investigation, but the prevailing theory among officials and the company is that the raging Yellowstone caused erosion and exposed the line to damaging rocks or debris. There is still no definitive word on how far downriver the spill could spread. Source: <http://www.cbsnews.com/stories/2011/07/07/ap/business/main20077661.shtml>

(Montana) Rising river complicates Exxon oil spill cleanup. The initial cleanup along the oil-fouled Yellowstone River could be tested July 5 as rising waters make it harder for Exxon Mobil Corp. to get to areas damaged by the crude spilled from a company pipeline. The National Weather Service predicts the Yellowstone River, swelling with mountain snowmelt amid hot summer temperatures, will peak at Billings, Montana in the afternoon July 5 — a day after the Exxon Mobil Pipeline Co. President promised to do — whatever is necessary to mop up oil spilled from the duct at the river bottom. That pledge included sending crews to walk the river banks in search of pooled oil once the flooding river recedes. The 12-inch pipeline burst July 1 upstream from a refinery in Billings, where it delivered 40,000 barrels of oil a day. Up to 1,000 barrels, or 42,000 gallons, of crude oil oozed into the legendary Yellowstone before the leak was stopped, according to Exxon Mobil estimates. After downplaying assertions from state and federal officials that damage from the spill was spread over dozens of miles, Exxon Mobil acknowledged July 4 that the scope of the leak could extend far beyond a 10-mile stretch of the river. The 20-year-old Silvertip pipeline followed a route that passes beneath the river. It was temporarily shut down in May after Laurel officials raised concerns that it could be at risk as the Yellowstone started to rise. Also twice in the last year, regulators warned Exxon Mobil of several safety violations along the line. The company decided to restart the line after examining its safety record and deciding it was safe, the Exxon Mobil Pipeline Co. President said. Source: <http://abcnews.go.com/US/wireStory?id=13997242>

UNCLASSIFIED

UNCLASSIFIED

(Wisconsin) Suspect in SD homicide planned to kill president. The man arrested in Madison, Wisconsin after allegedly killing a 75-year-old woman in her Sioux Falls, South Dakota home is telling a television station he planned to travel to Washington, D.C., to kill the U.S. President. The suspect told WKOW-TV, he planned to kill the President while he was golfing. He cited the President's economic policies, but also said the President is controlled by aliens. Authorities said that hours before the suspect's interview July 6 with WKOW at the Dane County jail, a Secret Service agent interrogated him. The man faces first-degree murder and burglary charges in South Dakota for allegedly entering the home of a woman, killing her, and then fleeing in her vehicle. Source: <http://www.timesunion.com/news/article/Suspect-in-SD-homicide-planned-to-kill-president-1454424.php>

(South Dakota) Fort Randall Dam reservoir in SD hits record level. The Yankton Press & Dakotan newspaper reported that the U.S. Army Corps of Engineers said the Fort Randall reservoir in South Dakota hit a record 1,372.5 feet above sea level June 27 as a result of the Missouri River flooding. The previous record was 1,372.2 feet in 1997. The Mitchell Daily Republic newspaper reported that the communities of Chamberlain and Oacoma were threatened by flooding because of the rapid rise of the reservoir downstream, and the loss of water storage capacity there. Source: http://www.rapidcityjournal.com/news/state-and-regional/article_125be198-e020-55f2-bca7-8fc949fe295d.html

NATIONAL

Napolitano sets plan to curb Mexico border drug smuggling. The DHS Secretary July 7 rolled out the U.S. President's administration's 2011 strategy to curb drug smuggling on the Mexico border, pledging to boost intelligence sharing and technology to tighten security. The U.S. President has been under intense pressure to beef up security on the porous southwest border to curb immigrant and drug smuggling north from Mexico, and halt the flow of guns and cash proceeds south. Among goals going forward was boosting intelligence and information sharing with state, local, and tribal law enforcement agencies along the nearly 2,000-mile border, and enhanced liaison with Mexican authorities. The plan also sought to increase the use of technologies such as X-Ray machines at land border crossings to detect drugs headed north to U.S. markets, and bulk cash proceeds and guns headed south to Mexico to arm the Mexican cartels. Part of the emphasis also focuses on reducing U.S. demand for drugs through education, community development, and providing rehabilitation for drug users. Source: <http://www.reuters.com/article/2011/07/07/us-usa-mexico-drugs-idUSTRE7667M020110707>

(Washington) Grand jury indicts two in South Seattle terror attack plot. A Seattle, Washington grand jury July 7 indicted two men arrested June 22 on allegations that they planned to attack a South Seattle military processing center. Following on charges filed the day after their arrests, the grand jury indicted a 33-year-old and a Los Angeles, California man on nine counts related to the purported plot against the Military Entrance Processing Station. Charged June 23 with planning a suicidal attack against a East Marginal Way South recruit processing center, the men

UNCLASSIFIED

UNCLASSIFIED

have been jailed since. They are charged with planning to storm the center with automatic rifles and grenades to kill recruits and Department of Defense employees working there. Prosecutors claim the plot was thwarted in the 11th hour after another Muslim man approached by one of the suspects in late May went to Seattle police, then acted as an informant. The men were indicted on charges of conspiracy to murder officers and agents of the United States, and conspiracy to use weapons of mass destruction. Source:

<http://www.seattlepi.com/local/article/Grand-jury-indicts-two-in-South-Seattle-terror-1456771.php>

(Kansas; Missouri) Flood becomes second-highest on record. Flood waters from the Missouri River forced the closure of a bridge in Atchinson, Kansas, and a popular flood-viewing spot in Leavenworth June 28. The U.S. Army Corps of Engineers upped the long-range forecast for the scope of the expected crest in Leavenworth to between 28 and 34 feet as the northern communities of St. Joseph, Missouri, and Atchison, Kansas, moved from moderate to major flood stage. Recent observations made this flooding event the second-worst on record, behind the 1993 crest of 35.34 feet, according to the National Weather Service. The flood waters are not expected to recede until August. The city of Leavenworth closed Landing Park at 9 p.m. June 28, and the Kansas Department of Transportation closed Kansas Highway 7 from the Nebraska border to the city of Sparks, Kansas, late June 27. In addition, U.S. Highway 59 at the Amelia Earhart Bridge over the river in Atchison has also been closed. Source:

<http://www.leavenworthtimes.com/topstories/x2069930187/Flood-becomes-second-highest-on-record>

INTERNATIONAL

Vietnam culls 45,000 animals due to FMD. According to reports over the weekend of July 2 and 3, nearly 38,000 pigs had already been culled in Vietnam in attempts to control a foot-and-mouth disease (FMD) outbreak. The disease is reported to have infected 39 provinces. According to the head of Vietnam's Ministry of Agriculture and Rural Development's animal health department (AHD), local producers and officials failed to manage areas with the greatest virus exposure, and did not destroy infected cattle as instructed, allowing the virus to spread quickly and broadly, vetsweb.com reported. According to the U.S. Department of Agriculture's Foreign Agricultural Service, Vietnam ranks about 6th in world pork production at 1.85 million metric tons. It stands at No. 12 in terms of U.S. pork exports (10,108 metric tons) and at No. 10 for U.S. pork variety meats (6,636 metric tons). The country comes in at No. 9 for global pork consumption. As for other animals impacted by the FMD outbreak, AHD officials report 5,000 buffaloes, 938 cows, and 329 goats have also been culled. AHD officials urged officials and producers within the affected provinces to implement disease-prevention programs, and organize vaccinations for the rest of 2011. It also has pushed for appropriate vaccine use, as FMD virus strains evolve continuously. Source: <http://www.dairyherd.com/bovine-vet/industry-news/Vietnam-culls-45000-animals-due-to-FMD-125040479.html?ref=479>

UNCLASSIFIED

UNCLASSIFIED

Arrests in Moldova over possible uranium smuggling. Police in Moldova said June 29 they had arrested six people involved with a criminal group that said it was dealing in smuggled nuclear materials, and was active in the former Soviet Union and in Arab countries. The group had been negotiating the sale of uranium, police officials said in a statement, and authorities suggested the material had come from Russia. Some of the suspects were arrested while they were carrying a lead canister. In a video released to news media, police officers wearing gloves showed how a Geiger counter clicked rapidly when brought near the dull gray metal tube. Police said the contents of the tube would be sent for analysis. The Moldovan authorities said that the suspects, who included four Moldovans, one Russian, and one resident of the Russian-backed separatist region of Transnistria in eastern Moldova, had sought a buyer for what the suspects said was bomb-grade uranium. Source:

http://www.nytimes.com/2011/06/30/world/europe/30moldova.html?_r=1

9 militants, 9 others dead after attack on Kabul hotel. At least nine people were killed in a brazen, carefully-orchestrated attack on a Kabul, Afghanistan hotel that began the night of June 28, officials said. The Taliban has claimed responsibility for the siege, and authorities said nine militants died as well. Two police officers are among the dead in the attack that raged into the early hours of June 29 at the Hotel Inter-Continental, according to the Afghan interior ministry. Twelve people were wounded in the attack, the chief of criminal investigations for Kabul police said June 29. Critical information that helped end the siege came from an unmanned U.S. Predator drone that flew over the hotel during the attack, providing video of the militants as the situation unfolded, two coalition military officials said. The attack came on the eve of a news conference that was scheduled to take place at the hotel June 29 to discuss the planned transition of security from international to Afghan forces that the U.S. President announced the week of June 20. A spokesman for the Taliban said suicide attackers entered the hotel after killing security guards at the entrance. The top of the hotel was on fire June 29, but the flames went out within a few hours. The Taliban penetrated the hotel's typically heavy security in the attack, and one of the militants detonated an explosive on the second floor, said a journalist for The Daily in Kabul. Rocket-propelled grenades were launched from the roof of the hotel toward the first vice president's house. A few moments later, the hotel was rocked by three explosions. At about 2 a.m., 4 hours after the attack began, North Atlantic Treaty Organization International Security Assistance Force (ISAF) helicopters fired at insurgents on the roof, killing at least three of the gunmen, an ISAF spokesman told CNN. A U.S. Blackhawk helicopter carried the ISAF snipers, who fired on as many as six insurgents on the hotel roof, the officials said. At about 3 a.m., ISAF said, Afghan security forces had cleared the roof and were clearing the rest of the hotel. "The last suicide attacker was killed at around 7 a.m. during the search operation," an Afghan interior ministry spokesman said. There were no indications that U.S. military or diplomatic personnel were staying at the hotel, U.S. officials told CNN. Source:

<http://edition.cnn.com/2011/WORLD/asiapcf/06/29/afghanistan.kabul.attack/>

(Texas) Mexican troops replace police in Tamaulipas, a state that borders Texas. Mexican troops have replaced policemen in half of a large state that borders Texas, in the deep south, because there were fears the officers were corrupt and helping drug cartels. Some 2,800 heavily armed soldiers were deployed in 22 of Tamaulipas's 43 cities over the weekend of June

UNCLASSIFIED

UNCLASSIFIED

25 and 26 — this was done, in part, as the Mexican president moved to defend his drug war strategy. Mexico's ministry of defense insisted "the support is of temporary and extraordinary character", but an official in Nuevo Laredo, who wished to remain anonymous, told CNN that local police have been replaced while they are investigated for corruption. Troops were moved in to San Fernando, too, where authorities discovered mass graves containing more than 200 corpses earlier this year, while investigating the kidnapping of passengers from a bus. Source: <http://www.dailymail.co.uk/news/article-2008556/Mexican-troops-replace-police-Tamaulipas-state-borders-Texas.html>

E. coli in France linked to deadly German outbreak. The outbreak of E. coli affecting more than a dozen victims in Bordeaux, France, is now almost conclusively linked to the ongoing epidemic of E. coli O104:H4 in Germany that has claimed the lives of 48 Europeans so far. Doctors said they are 99 percent sure that the French outbreak, which appears to have plateaued at 13 victims, is related to the massive outbreak attributed to German-grown sprouts, the French health minister said June 27. This latest outbreak is thought to have come from sprouts served at a community event in Begles as a garnish for many dishes. Eight of the victims reported attending the event. The sprouts were grown in France, but the seeds were purchased from an English company, Thompson & Morgan, which said the seeds came from an Italian supplier. So far it is unclear whether the bacteria may have originated on the seeds themselves, or could have contaminated the sprouts during the growing process from irrigation water or human contact. In Germany, the number of outbreak victims has risen to 4,800, but the rate of new cases is declining significantly, according to the Robert Koch Institute. Source: <http://www.foodsafetynews.com/2011/06/e-coli-in-france-linked-to-deadly-german-outbreak/>

BANKING AND FINANCE INDUSTRY

F.D.I.C. rule to allow seizure of executives' pay if firms fail. Federal regulators will be able to take back up to 2 years of Wall Street executives' pay if they are found responsible for the collapse of a major financial firm, under a plan approved July 6. The provision is part of a broader Federal Deposit Insurance Corporation (FDIC) rule laying out the order in which creditors will be paid during a government liquidation of a large, failing financial firm. The Dodd-Frank financial oversight law gives financial agencies the power to recoup executives' pay, but bankers complained regulators were taking it too far. The FDIC's final rule provided some relief by clarifying "negligence" as the standard. The agency noted it was not using the more narrow standard of "gross negligence." The liquidation authority is a major part of the Dodd-Frank law. The idea is to preserve economic stability by unwinding troubled firms, but in a way that is less politically explosive than taxpayer-financed bailouts and less traumatic to the markets than bankruptcies like the Lehman Brothers collapse of 2008. At the top of the list of what will be paid off first under the new resolution system are any debts the FDIC or receiver took on as part of the cost of seizing a firm, administrative expenses, money owed to the U.S. Treasury, and money owed to employees for things such as retirement benefits. Source: <http://www.nytimes.com/2011/07/07/business/07fdic.html>

UNCLASSIFIED

UNCLASSIFIED

(Florida) Four charged in reverse mortgage scheme. Three loan officers and a title agent were charged in Florida July 6 with defrauding seniors and financial institutions in a \$2.6 million reverse mortgage scheme. The U.S. Attorney for the Southern District of Florida filed conspiracy to commit wire fraud charges against the four suspects. The charges carry up to 30 years in prison plus a \$1 million fine. Federal agents allege that while the three loan officers worked at 1st Continental Mortgage in Fort Lauderdale and Boca Raton in 2009 and 2010, they engaged in a scheme that stole from borrowers, reverse mortgage lender Genworth Financial Home Equity, and the Federal Housing Authority, which insures loans. It is alleged the three fraudulently inflated property appraisal values so borrowers would get reverse mortgages without having real equity. Authorities also claim that when the title agent closed the loans, she wired the proceeds to herself instead of paying off the borrowers' existing mortgages. She allegedly filed fraudulent documents showing the existing mortgages had been paid off. Officials also claimed she sent the other three defendants \$988,086 in loan proceeds for their personal benefit. It is alleged the four then tried to cover up their actions by creating fictitious offers to buy the properties in short sales. Source:

<http://www.bizjournals.com/southflorida/news/2011/07/06/four-charged-in-reverse-mortgage-scheme.html?page=all>

Morgan Stanley data breach hits investors. Personal information belonging to 34,000 investment clients of Morgan Stanley Smith Barney has been lost, and possibly stolen, in a data breach. According to two letters sent to clients, and obtained by Credit.com, the information includes clients' names, addresses, account, and tax identification numbers, the income earned on the investments in 2010, and — for some clients — Social Security numbers. The data was saved on two CD-ROMs that were protected by passwords, according to the letters, but the CDs were not encrypted. The company mailed the CDs containing information about investors in tax-exempt funds and bonds to the New York State Department of Taxation and Finance. It appears the package was intact when it reached the department, but by the time it arrived on the desk of its intended recipient the CDs were missing, a spokesman for Morgan Stanley Smith Barney said. The state notified Morgan Stanley Smith Barney about the lost data June 8. The company took 2 weeks to conduct an "exhaustive search" of all the facilities the package passed through, the spokesman said, and then mailed the letters to clients June 24. Source:

<http://www.credit.com/blog/2011/07/morgan-stanley-data-breach-hits-investors/>

Federal agency issues new security rules for financial institutions. The federal agency that regulates banks June 28 issued new rules for online security for financial institutions, instructing them to use minimal types of "layered security" and fraud monitoring to better protect against cybercrime. It is the first time the Federal Financial Institutions Examination Council (FFIEC) has updated its rules since 2005, and the instructions to regulated financial services today focus on protecting high-dollar Automated Clearinghouse (ACH) transactions that have been targeted by sophisticated cybercrime groups that hijack business PCs in order to initiate fraudulent transactions. The FFIEC also instructs banks and financial institutions to focus their network defense on layered security protections that involve fraud monitoring; use of dual customer authorization through different access devices; the use of out-of-band verification; and the use of "positive pay," debit blocks and other technologies to appropriately limit the transactional

UNCLASSIFIED

UNCLASSIFIED

use of the account. The FFIEC guidelines also tell financial institutions they must use "two elements at a minimum" as "process designed to detect anomalies and effectively respond to suspicious and anomalous activity." The fraud-detection processes must include: initial login and authentication to customers requesting access to the institution's electronic banking system, and initiation of electronic transactions involving the transfer of funds to other parties.

Source:

http://www.computerworld.com/s/article/9217999/Federal_agency_issues_new_security_rules_for_financial_institutions

Fake IRS spam campaign pushing Zeus bot. There is a large scale spam campaign underway in which attackers use fairly well-crafted e-mails that appear to come from the IRS to infect victims with the Zeus bot. The attack has been ongoing for a couple of weeks and researchers said that although the attackers have taken some precautions to prevent analysis of the sites and malware being used, they also made some key mistakes. The Zeus-laden fake IRS e-mails have been making the rounds since mid-June. The subject line typically says, "Federal Tax payment rejected" or "Your IRS payment rejected", and the sender's address is spoofed to include the irs.gov domain. The body of the e-mails often have some spelling and grammatical errors and include a link to a PDF file. That file directs the victim to a download that will drop the Zeus binary on his or her machine. Source: http://threatpost.com/en_us/blogs/fake-irs-spam-campaign-pushing-zeus-bot-062911?utm_source=Recent+Articles&utm_medium=Left+Sidebar+Blogs&utm_campaign=Den nis+Fisher

Bank of America in \$8.5B mortgage settlement. Bank of America and its Countrywide unit will pay \$8.5 billion to settle claims that the lenders sold poor-quality mortgage-backed securities that went sour when the housing market collapsed. The Charlotte, North Carolina, bank said the settlement with 22 investors is subject to court approval and covers 530 trusts with original principal balance of \$424 billion. As a result of the settlement, Bank of America put its second-quarter loss at \$8.6 billion to \$9.1 billion. Excluding the settlement and other charges, the bank expects to post a quarterly loss of \$3.2 billion to \$3.7 billion. Source:

<http://www.cbsnews.com/stories/2011/06/29/business/main20075317.shtml>

Citi: Millions stolen in May hack attack. Citigroup acknowledged June 27 that a hacking incident last month stole millions of dollars from customers' credit card accounts. Citigroup told CNN that about \$2.7 million was stolen from about 3,400 accounts on May 10. The hackers actually accessed a much larger number of accounts: 360,083. Fewer than 1 percent of the hacked accounts had money removed from them, according to Citigroup. The bank reiterated that customers will not be responsible for financial losses from the attacks. Citigroup announced June 16 that more than 200,000 new credit cards had been issued to hacked customers. In some cases, customers had already closed their account or had received a new credit card, so they didn't need the Citi-initiated replacement. Citigroup waited until June 3, more than 3 weeks after its discovery of the hack, to start sending out notification letters. However, the company insisted that it acted quickly to deal with the security problem. Source:

http://money.cnn.com/2011/06/27/technology/citi_credit_card/

UNCLASSIFIED

UNCLASSIFIED

Mastercard.com slammed again as punishment over WikiLeaks. MasterCard's main Web site was unavailable June 28 as it appeared hackers were again targeting the company for its refusal to process donations for the whistle-blowing site WikiLeaks. MasterCard along with companies such as Visa, PayPal and the Swiss Bank PostFinance stopped processing payments for WikiLeaks shortly after the site began releasing portions of 250,000 secret U.S. diplomatic cables in November 2010. The hacking collective known as Anonymous spearheaded a drive to conduct distributed denial-of-service attacks against those sites. WikiLeaks wrote on Twitter June 28 that "hacktivists" had taken down MasterCard "over the continuing WikiLeaks fiscal embargo." In another Twitter posting, it said the "unlawful banking blockade" was in its sixth month and named Visa, MasterCard, PayPal, Bank of America, and Western Union as targets. Source:

http://www.computerworld.com/s/article/9217980/Mastercard.com_slammed_again_as_punishment_over_WikiLeaks

U.S. mortgage-fraud reports up 31% in 1Q -report. Reports of mortgage fraud in the United States rose 31 percent in the first 3 months of this year as banks scoured their files for shady loans made during the housing boom, according to a government report released June 28. The Financial Crimes Enforcement Network, a Treasury Department agency, reported 25,485 "suspicious activity reports" related to suspected mortgage fraud in the January-March 2011 period. That was up from 19,420 in the same quarter a year earlier. The increase was attributed to large mortgage servicers performing thorough reviews of loan files after receiving demands from mortgage investors to repurchase mortgages that have fallen into default. In the January-March period, 86 percent of mortgage-fraud reports involved activities that occurred more than 2 years ago. Source: <http://www.nasdaq.com/aspx/stock-market-news-story.aspx?storyid=201106280014dowjonesdjonline000007&title=us-mortgage-fraud-reports-up-31in-1qreport>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Database of toxic chemicals opened for public access. The Environmental Protection Agency (EPA) released two databases scientists and the public can use to access chemical toxicity and exposure data. The Toxicity Forecaster database (ToxCastDB) and a database of chemical exposure studies (ExpoCastDB), link exposure and toxicity data, which are connected through EPA's Aggregated Computational Toxicology Resource (ACToR), an online data warehouse that collects data on more than 500,000 chemicals from more than 500 public sources. ToxCast uses advanced tools to predict toxicity of chemicals, and to provide a cost-effective approach to prioritize what chemicals require further testing. ToxCast is screening 700 more chemicals, and the data will be available in 2012. ExpoCastDB consolidates human exposure data from studies that have collected chemical measurements from homes and child care centers. Data include the amounts of chemicals found in food, drinking water, air, dust, indoor surfaces, and urine. Additionally the EPA has made public the identities of more than 150 chemicals contained in 104 health and safety studies that had been claimed confidential by industry. Among the newly

UNCLASSIFIED

UNCLASSIFIED

declassified toxic chemicals were some that were used in the Gulf oil spill cleanup and consumer products in 2010. Source: <http://www.hstoday.us/briefings/today-s-news-analysis/single-article/database-of-toxic-chemicals-opened-for-public-access/6391a3c8180d63c40f266ee70acee07e.html>

(New York) Device with radioactive materials missing in NY. A portable moisture density gauge that uses radioactive materials was reported stolen June 27 from a truck in a suburb north of New York City, New York. Stony Point police reported to the media July 2 that they are searching for the over \$4,000 device, which is regulated by the U.S. Nuclear Regulatory Commission (NRC). The gauge is licensed to a company that inspects construction material. The gauge was reported stolen June 27 from a truck parked outside the home of an employee who works for the testing company. The device's radioactive sources are categorized by the NRC as —very unlikely to cause permanent injury to individuals. A State Department of Health spokesman said the radioactive sources are —doubly encapsulated and secured. Exposure would occur if the device broke. Source: <http://www.seattlepi.com/news/article/Device-with-radioactive-materials-missing-in-NY-1450738.php>

Mock attackers 'strike' 24 nuclear plants, 'breach' two. Mock commandos who staged attacks on 24 nuclear power plants in pre-announced drills in 2010 were able to "damage" or "destroy" critical targets at two of the plants, according to the Nuclear Regulatory Commission (NRC.) The NRC did not identify the nuclear plants that failed the security tests, citing security concerns and other sensitivities. But it said inspectors remained at those plants until security shortcomings were addressed. According to an unclassified version of an NRC report released June 29, the NRC conducted force-on-force inspections at 24 nuclear power plants and one nuclear fuel facility during 2010. It identified 23 deficiencies, but none was in the upper range of severity. At two unidentified sites, the utilities failed to "effectively protect" the target during mock attacks, the report said. Source: <http://www.cnn.com/2011/US/06/29/nuclear.plants.security/>

Court orders Louisiana to take action on radiation threat from oil and gas production. The Louisiana State Court of Appeals has ordered state regulators to begin monitoring pollution in wastewater discharged from oil and gas production activities into the Gulf of Mexico. Since 2002, oil and gas rigs operating in Louisiana waters within 3 miles of the coast have been discharging wastewater directly into the Gulf under an expired general permit from the Louisiana Department of Environmental Quality (LDEQ). The discharges contain toxic heavy metals, cancer-causing benzene and other petroleum compounds, and naturally occurring radioactive materials including radium, thorium, and uranium. The appeals court agreed there was a preponderance of evidence that the oil-production wastewater is dangerous, and that LDEQ failed to protect the public interest. It ordered the agency to take immediate action. Source: <http://www.southernstudies.org/2011/06/court-orders-louisiana-to-take-action-on-radiation-threat-from-oil-and-gas-production.html>

UNCLASSIFIED

UNCLASSIFIED

COMMERCIAL FACILITIES

(Missouri) Man indicted for Clayton parking garage bombing. A former Democratic political operative has been indicted by federal authorities for allegedly planting a bomb in a Clayton, Missouri parking garage in 2008, KTVI 2 St. Louis reported July 7. The bomb went off, seriously injuring a Clayton attorney. Police believe he was not the bomber's intended target, but instead he was trying to kill a different lawyer. The suspect is well known to law enforcement. He is also well known in Democratic political circles. The feds now say he is the one who planted a bomb in a garage at 190 Carondelet plaza in Clayton October 15, 2008. The suspect has a history of felony drug and gun charges. He is now in federal custody. Source:

<http://www.kplr11.com/news/ktvi-st-louis-man-indicted-2008-bombing-clayton-parking-garage-20110707-story,0,2429925.story>

(Texas) Texas Rangers fan dies trying to catch ball. Almost a year after a similar incident, tragedy struck again at a Texas Rangers Major League Baseball (MLB) game July 7 when a fan fell over a railing while trying to catch a ball. The fan flipped over the railing of the outfield seats at Rangers Ballpark in Arlington, Texas. He fell about 20 feet — crashing head-first into an area near a scoreboard as his son watched. The man was rushed to a hospital where he died, the Arlington Fire Department said. MLB officials said the incident occurred in the second inning of the game after an outfielder threw a ball in the stands for fans. Another fan who was sitting near the victim saw him leaning over the rail. The second man tried to grab on to the victim's shirt but could not hold on. The incident occurred almost a year after another fall at a Texas Rangers game. On July 9, 2010, a fan fell from the second deck of the ballpark while trying to catch a foul ball. The man survived the 30-foot fall but fractured his skull, and injured his foot and ankle. Source:

http://www.cnn.com/2011/SPORT/07/07/texas.rangers.game.death/index.html?hpt=hp_t2

(Alabama) 15 now ill with E. coli after visiting Opelika Splash Park. The Alabama Department of Public Health (ADPH) said the E. coli outbreak in Lee County has climbed to 15 illnesses with 13 children and 2 adults now ill. Each of the victims either played in the Splash Park or swam in the pool at the Opelika SportsPlex and Aquatic Center in Opelika between June 4 and June 22, according to the ADPH, and all have had severe gastrointestinal illness. The health department said it contacted parents of children connected to seven day care centers who had children at the Splash Park during the period of concern. The Splash Park was closed June 20, and testing was done on the facility several times, but negative results came back for any contamination each time. Following U.S. Centers for Disease Control guidelines, the City of Opelika has treated all facilities at the Splash Park and Aquatic Center, and the facilities reopened June 26. Source:

<http://www.wsfa.com/Global/story.asp?S=14993058>

COMMUNICATIONS SECTOR

Nothing Significant to Report

UNCLASSIFIED

CRITICAL MANUFACTURING

Changzhou Globe Tool Group recalls electric log splitters due to laceration or amputation hazard. The U.S. Consumer Product Safety Commission, in cooperation with Changzhou Globe Tool Group Co. Ltd. of China, July 7 announced a voluntary recall of about 20,000 Task Force 5-ton electric log splitters. They were imported into the United States by LG Sourcing, Inc. of North Wilkesboro, North Carolina. The electric log splitters have a hydraulic arm that, during use, slides under the handle used to move the machine. The moving hydraulic arm poses a laceration or amputation injury hazard to individuals who place their hands on that handle while the splitter is in operation. The log splitters are silver and black, electric 5-ton models. The log splitter brand name, model and item number is Task Force 26083 241483, and were sold Lowe's stores nationwide from January 2008 through March 2011. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11273.html>

Hamilton Beach recalls toasters due to fire hazard. The U.S. Consumer Product Safety Commission, in cooperation with Hamilton Beach, June 30 announced a voluntary recall of 300,000 Hamilton Beach classic chrome 2-slice toasters. Consumers should stop using this product immediately. The heating element in these toasters can remain energized indefinitely when an item is placed in the toaster which may ignite the contents, posing a fire hazard if the toaster is near flammable items. The toasters are the model 22600 with series codes beginning with C or D and have the format of CXXXXBI or DXXXXBI where XXXX is a four digit number between 0190 and 5290. The toasters were sold at mass merchandisers and department, grocery, and home center stores nationwide, as well as various online retailers, from February 2008 through June 2011. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11265.html>

Toyota to recall 82,200 vehicles in the U.S. Toyota Motor Corp. said June 29 it will recall about 82,200 hybrid SUVs in the United States due to computer boards with possible faulty wiring. The recall involves about 45,500 Highlander Hybrid and 36,700 Lexus Rx 400h vehicles, the company's U.S. subsidiary said in a press release. Toyota said the affected vehicles' hybrid system has a computer board with inadequate soldering that could be damaged during high-load driving. If damage were to occur, the company said the vehicles would either continue to operate under reduced power for a short distance, or coast to a stop. Source: <http://www.foxnews.com/us/2011/06/29/toyota-to-recall-82200-vehicles-in-us/?test=latestnews>

DEFENSE/ INDUSTRY BASE SECTOR

Geek swap: DOD, private sector IT workers switch. The Department of Defense (DOD) launched a program that exchanges IT workers with the private sector in an effort to share technology expertise, InformationWeek reported July 6. The Information Technology Exchange Program, currently in pilot, allows the department to trade civilian employees with private-

UNCLASSIFIED

sector organizations to share best practices and collaboration in particular IT areas, including service-oriented architectures, cloud computing, enterprise architecture, mobile devices, and cybersecurity, according to the DOD. Source:

<http://www.informationweek.com/news/government/leadership/231001065>

(California) FBI assesses terrorist threat against Monrovia-based AeroVironment. FBI officials June 30 warned AeroVironment Inc. employees of al-Qaida threats against 11 senior executives of the Monrovia, California-based company, according to sources with knowledge of the warning. Monrovia city officials said security at the West Huntington Drive facility of the defense contractor would be beefed up over the July 4 weekend after threats surfaced on a jihadist Web site. An FBI spokeswoman said she had not heard of a specific threat to AV, but said the FBI takes such threats seriously. An AV employee said company officials led by the senior vice president and general manager conducted a meeting June 30 with employees regarding the threat. Monrovia's mayor said the city is coordinating with several agencies to help ensure public safety. A June 23 online blog post on Homeland Security Today said top U.S. military leaders, and AeroVironment's CEO and other AV executives have been identified as targets on several jihadist Web sites. AV makes a variety of unmanned surveillance aircraft systems, including the Dragon Eye, Raven, Wasp, and Puma AE, that are used extensively by U.S. military forces in the global war on terrorism. Source:

http://www.whittierdailynews.com/news/ci_18385448

Army's faulty computer system hurts operations. POLITICO reported June 29 the U.S. Army's \$2.7 billion computing system designed to share real-time intelligence with troops fighting in Afghanistan and Iraq has hurt, rather than helped, efforts to fight insurgents because it does not work properly, according to several analysts who used the system. The analysts' comments mirror concerns raised by the top military intelligence officer in Afghanistan and members of Congress over the past 2 years in an unsuccessful bid to get the Army to consider alternatives to its portion of the military's Distributed Common Ground System (DCGS-A), according to documents obtained by POLITICO. The system is a cloud-based computing network designed to collect information from multiple sources for real-time analysis that quickly puts usable intelligence in the hands of battlefield commanders. The analysts said DCGS-A was unable to perform simple analytical tasks. The system's search tool made finding the reports difficult, and the software used to map the information was not compatible with the search software. There were also problems with the hardware, with the system being prone to crashes and frequently going off-line, he and another former Army intelligence officer said. Source:

<http://www.politico.com/news/stories/0611/58051.html>

(Maryland) U.S. Navy JSFs resume flight ops after glitch. Flying operations for the U.S. Navy's Lockheed Martin F-35C Joint Strike Fighter test program resumed June 23 after a 6-day suspension to fix a software problem. The aircraft were grounded June 17 when engineers at Patuxent River Naval Air Station in Maryland discovered a "logic fault" that could have prevented the proper action of aircraft control surfaces — the flaps, rudders, and other movable elements that maneuver the plane through the air. The Navy stressed no actual fault took place on any aircraft. The software problem affected the "safety mechanism that ensures

UNCLASSIFIED

UNCLASSIFIED

the wings are folded properly," a Navy spokeswoman said. "It's the mechanism that prevents the flaps from moving in flight." The safety monitoring function for the mechanism should be turned off during flight, she said, but the software was not properly turning off the function. The problem has yet to be fully corrected, but the aircraft have resumed flying with restrictions, a statement from Naval Air Systems Command said. Source:

<http://www.defensenews.com/story.php?i=6915380&c=AME&s=SEA>

EMERGENCY SERVICES

(New York) NY troopers warn of e-mail hoax ticket and computer virus. A hoax e-mail circulating nationally appears to carry an attached traffic ticket by New York State troopers, but it is believed to really carry an unknown computer virus, according to state police. E-mails sent primarily to Yahoo accounts direct recipients to open an attached zip file to access a copy of a traffic ticket that they are supposed to fill out and return to a town court. An unknown type of virus is believed to be attached to the file, which is currently being analyzed by the state police computer forensics lab, according to a news release from the New York State Police. Police warn the e-mail's subject line may contain the line, "UNIFORM TRAFFIC TICKET," with the message accusing the recipient of a violation of "speed over 55 zone" July 2. Police ask that recipients of the hoax e-mail delete the e-mail and not forward it. They advise computer users to activate anti-virus software, firewalls, and take other security measures, only opening e-mails from familiar sources. Source:

http://www.cnn.com/2011/US/07/07/new.york.hoax.ticket/index.html?hpt=us_c2

Mexico gangs threaten to behead DEA agents. A spray-painted sign threatening death for U.S. Drug Enforcement Administration (DEA) agents was found July 1 next to a school in a northern Mexico state capital, officials said. Addressed with profanity to "Gringos (D.E.A.)," the unsigned graffiti warned: "We know where you are and we know who you are and where you go. We are going to chop off your (expletive) heads." Also July 1, five copies of a message addressed to the Chihuahua governor were found painted in Ciudad Juarez, a city across the border from El Paso, Texas. Those messages, apparently posted by rivals of the Sinaloa drug cartel, accused officials of protecting the Sinaloa organization. It was not clear if the messages in Chihuahua and Ciudad Juarez were related. The threatening message against the governor comes amid threats to the governor of Nuevo Leon, another northern state bordering Texas. Two of the governor's bodyguards were mutilated, killed, and dismembered in June. Source:

<http://www.cbsnews.com/stories/2011/07/01/ap/latinamerica/main20076278.shtml>

(New York) DHS demonstrates next-gen radiation detection systems at race track. While crowds filled the stands to watch the Belmont Stakes races in New York in mid-June, the U.S. Department of Homeland Security Domestic Nuclear Detection Office (DNDO) worked with police from Nassau and Suffolk counties to explore concepts of operation for three experimental next-generation radiation detection systems. The prototype systems are designed to identify and precisely locate sources of radiation. Two of the prototypes were stand-off radiation detection systems (SORDS), and the other was a roadside tracker. SORDS consist of

UNCLASSIFIED

UNCLASSIFIED

detection equipment placed in a truck and on a trailer that were driven around the facility to search for stationary sources. The roadside tracker consists of two trailers placed opposite each other that scan for sources of radiation as vehicles moved between them. SORDS are designed to detect a millicurie of radiation — which is equivalent to one millionth the radiation used to treat cancer — from 100 meters, and determine its location within 10 meters both horizontally and vertically. The roadside tracker can detect a millicurie of radiation across five lanes of traffic in a vehicle traveling up to 70 mph. Since SORDS allow an operator to precisely identify and locate sources of radiation, the commanding officer of the Suffolk County Police Department's Special Patrol Bureau said they could help reduce the time needed to identify potentially dangerous sources of radiation. The county's current system requires an officer to investigate the source on foot and identify it, something that would be difficult if the location was not open to the public. Source: <http://www.emergencymgmt.com/safety/DHS-Radiation-Detection-Systems-Race-Track.html>

(Oklahoma) Five Tulsa police cars broken into over weekend. Police in Tulsa, Oklahoma, said five police cars were broken into over the weekend of July 1 at the department's main garage. Police made the discovery July 3 in the 1400 block of Charles Page, where they park a fleet of cars not currently assigned to officers. Police said all of the vehicles had their rear windows busted out. It is believed police property was stolen from the trunk of one of the cars. Police are investigating. Source: <http://www.newson6.com/story/15020082/five-tulsa-police-cars-broken-intoit>

(Georgia) Federal Agent's home burglarized, guns taken. A federal agent said someone broke into his DeKalb County, Georgia home and stole several guns. He had at least five guns stolen from his home in Ellenwood, including his service weapon. He was on vacation in Arkansas when burglars busted through a basement window early July 2 and ransacked his house. He showed WSBTV 2 Atlanta how the bandits broke down the double-locked door to his bedroom where he kept his guns. He said the burglars got away with at least five guns, including his service weapon, plus electronics, thousands of dollars in savings bonds, two safes full of personal paperwork, and the truck in his driveway. Source: <http://www.wsbtv.com/news/28442690/detail.html>

ENERGY

(Arkansas) Arkansas man indicted for damaging Marcellus gas pipeline. An Arkansas man, unhappy he was fired from a job in the Marcellus Shale fields in Lycoming County, Pennsylvania, used a mechanical excavator to dig up and destroy a gas pipeline he had just helped build, federal prosecutors said. The U.S. attorney's office quickly indicted the 44-year-old on charges of destroying an energy facility, and damaging an intrastate gas pipeline. If convicted of both charges, he faces a maximum sentence of 40 years in prison, supervised release, and a \$500,000 fine. According to the indictment, the suspect worked for about 5 weeks for Houston-based Holloman Corp., which was working to build a natural gas pipeline in Cogan House

UNCLASSIFIED

UNCLASSIFIED

Township. Source: http://articles.mcall.com/2011-06-30/news/mc-marcellus-gas-pipeline-sabotage-in20110630_1_gas-pipeline-arkansas-man-marcellus-shale-fields

FOOD AND AGRICULTURE

(Hawaii) Bento recall bacteria could lead to serious illness. The U.S. Department of Agriculture (USDA) July 6 said the Hawaiian company Warabeya USA was pulling about 1,550 pounds of packaged meals because they may be contaminated with listeria. The recall includes meals called the Big Bento, Breakfast Scramble Bowl, and the Little Smokies Snack Pack, sold exclusively at Hawaii's 64 7-Eleven stores. The bentos were made at a processing plant in Mapunapuna, Hawaii. Warabeya made the bentos June 28 with a best-eaten-by date of June 30. The USDA said they could have gotten contaminated when they came into contact with the pan of a food scale that tested positive for the bacteria. The USDA classifies the health risk as "high." Pregnant women and the elderly are especially vulnerable. New bentos at 7-Eleven were deemed safe to eat. Source: <http://www.hawaiinewsnow.com/story/15045272/bento-recall-bacteria-could-lead-to-serious-illness>

(Colorado) Equine herpes under control/restrictions lifted. The Colorado Department of Agriculture's State Veterinarian's office has released all hold and quarantine orders associated with the recent spread of Equine Herpes virus (EHV-1). Animal Health officials said in a statement released July 5 the disease is considered contained within Colorado, and there have been no new confirmed cases since May 20. Horses traveling into the state on or after July 9 will no longer need an import permit. Import requirements for horses entering Colorado will revert to those used before the outbreak. Those requirements are a health certificate issued within 30 days of an animal's arrival, and a negative Coggins test within the last 12 months. Colorado had nine confirmed cases of horses with EHV-1, sending ripples through the state's equine industry. Two horses that tested positive for EHV-1 were euthanized after showing severe neurological problems. Source: <http://www.krdo.com/news/28457237/detail.html>

Banned chemicals found in tons of imported fish. Fish from overseas contaminated with chemicals not allowed in the U.S. food supply are showing up for sale in the United States. Three American fish importers pleaded guilty earlier in 2011 in Mobile, Alabama, to federal felony charges of mislabeling fish and seafood. Their illegal haul included more than 120,000 pounds of imported fish, brought in to Mobile and Seattle, Washington, that tested positive for the suspected human carcinogen malachite green, an antifungal agent, and for an antibiotic that U.S. authorities also prohibit for use on fish that people consume. "I can tell you right off the bat that 40 percent of the imported fish we test is positive for banned drugs that are not safe for human health," said the deputy commissioner for the Alabama Department of Agriculture and Industries. Over the past year, Georgia and Arkansas found evidence of fluoroquinolones, a banned family of antibiotics, in imported fish. Arkansas detected crystal violet, a carcinogen. The United States today imports almost 85 percent of its seafood, and about half of it is from aquaculture, which frequently uses antibiotics to control disease. Most of the seafood comes from China, Thailand, Canada, Indonesia, Vietnam, and Ecuador. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.tennessean.com/article/20110706/NEWS07/307060098/Banned-chemicals-found-tons-imported-fish?odyssey=tab|topnews|text|FRONTPAGE>

(South Carolina) Ham with Listeria risk recalled. Carolina Pride Foods of Greenwood, South Carolina, recalled 18,416 pounds of boneless, fully cooked diced ham products that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service said July 5. The problem was discovered through third-party microbiological sampling contracted by the company. All the products were produced May 13, and distributed throughout the southeastern United States to retail outlets or for institutional use. Source: <http://www.foodsafetynews.com/2011/07/18416-pounds-of-ham-with-listeria-risk-recalled/>

Europe's E. coli outbreaks linked to Egyptian seeds. Imported fenugreek seeds from Egypt may be the source of highly toxic *E. coli* outbreaks in Germany and France that have killed at least 48 people, according to initial investigations by European scientists. More than 4,000 people across Europe and in North America were infected in the deadliest outbreak of *E. coli* so far recorded, which started in early May. Almost all of those sickened lived in Germany or had recently traveled there. The German outbreak, and a smaller cluster of *E. coli* centred around the French city of Bordeaux have both been linked to sprouted seeds. Experts from the Sweden-based European Center for Disease Prevention and Control (ECDC) and the Italy-based European Food Safety Authority (EFSA) said initial investigations suggested that "the consumption of sprouts is the suspected vehicle of infection in both the French cluster and the German outbreak. "The tracing back is progressing and has thus far shown that fenugreek seeds imported from Egypt either in 2009 and/or 2010 are implicated in both outbreaks," they said in a joint statement posted on the ECDC's Web site late June 29. Source:

<http://www.reuters.com/article/2011/06/30/ecoli-europe-egypt-idUSL6E7HU0EZ20110630>

Sprouts linked to salmonella outbreak in U.S. The U.S. Food and Drug Administration (FDA) is warning people not to eat alfalfa sprouts or spicy sprouts produced by Evergreen Produce because of a danger of salmonella contamination. The FDA said the sprouts have been linked to 20 reported cases of *Salmonella* Enteritidis infection in Idaho, Montana, New Jersey, North Dakota, and Washington State, one of which resulted in hospitalization. Officials said this particular strain of salmonella is rarely seen in such frequency. The tainted alfalfa and spicy sprouts are packaged in plastic bags labeled "Evergreen Produce" or "Evergreen Produce Inc." The alfalfa sprouts associated with the outbreak are packaged in 4-ounce and 16-ounce plastic bags with pre-printed "Evergreen Produce" or "Evergreen Produce Inc." labels. They are also packaged in 1-pound and 5-pound plastic bags with stick-on labels. The spicy sprouts are packaged in 4-ounce plastic bags with pre-printed labels, and 1-pound plastic bags with stick-on labels. Source: <http://www.webmd.com/food-recipes/food-poisoning/news/20110628/sprouts-linked-to-salmonella-outbreak-in-us>

(Arizona) Cantaloupes sold at Sam's Club recalled. Eagle Produce of Scottsdale, Arizona, recalled 1,760 cartons of cantaloupes because the melons may be contaminated with *Salmonella*, Food Safety News reported June 25. The recall is the result of a routine and random

UNCLASSIFIED

UNCLASSIFIED

test directed by the U.S. Department of Agriculture and carried out by the New York Department of Agriculture. The company has ceased the production and distribution of the cantaloupes. The recalled cantaloupes were sold at Sam's Club between June 2 and June 17. Sam's Club has withdrawn all cantaloupes and notified members who purchased them. The brown cardboard cartons, which contain nine melons, have the Kandy logo in white with the word "Cantaloupes" in white lettering on a red background. The lot code 147 count 9 is printed on the side of the carton. Each melon bears a Kandy sticker with the words "Cantaloupe USA." Source: <http://www.foodsafetynews.com/2011/06/cantaloupe-sold-at-sams-club-recalled/>

(New Jersey) Listeria concerns prompt recall of Serrano ham. Specialities Agro Alimentation of Millington, New Jersey, recalled about 5,700 pounds of imported boneless Serrano ham that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) said June 24. The problem was discovered when FSIS microbiological testing resulted in a positive sample for *Listeria monocytogenes*. The production lots that tested positive were refused entry into the United States. FSIS then notified Spanish authorities, who conducted their own assessment of the facility in Spain where the ham was produced, and they discovered that associated products had entered the country separately. There have been no reports of illness associated with the ham. The recall is for 11-pound cases of "Noel Jamon Serrano Boneless Spanish Dry-Cured Ham" and "Bloc Noel Serrano Ham," with production codes "11000481" or "11000119" on the shipping container and the label. In addition, each package subject to this recall states "Product of Spain" and includes the establishment number "Est. 26" (Spain) on the label. The products were produced on various dates and were shipped to retailers nationwide. Source: <http://www.foodsafetynews.com/2011/06/listeria-concern-prompts-recall-of-serrano-ham/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Florida) FBI investigates 'Anonymous' hackers. The hackers who have been bombarding the city of Orlando, Florida with cyberattacks, are now threatening the city's mayor and police officers. Police said members of the group Anonymous released a set of disturbing photos in their latest attack. The group posted two photos to their Twitter account. One shows the mayor's home in the background. The second photo depicts two headless Orlando police officers, and a mask in the bottom right corner. The FBI was called to investigate who posted the images. Anonymous said its actions are in response to the city ordinance that restricts the number of times a group can feed the homeless at Lake Eola. The group said they are siding with Food Not Bombs, a homeless feeding organization. Orlando police are treating the photos as a threat. The department bolstered patrols around the mayor's home. Source: <http://www.wftv.com/countybycounty/28468987/detail.html>

(Oregon; Florida; Washington) Man arrested for threats to kill Obama, family. An Portland, Oregon man was detained for a mental health evaluation after appearing in federal court July 5

UNCLASSIFIED

UNCLASSIFIED

to face charges he threatened to kill the U.S. President and the his family. The Secret Service arrested the man July 1. Prosecutors said he made threats in numerous phone calls to federal prosecutors' offices in Oregon and Washington, a county government office in Florida, and the Associated Press. An assistant U.S. attorney told a federal judge in Portland the man was considered a flight risk, and a safety risk. The man's arraignment was set for August, when he will enter a plea. According to the criminal complaint, the suspect made threatening calls to a series of government offices, including three to the county commissioner's office in Palm Beach County, Florida, 44 voicemail messages left June 19 with the U.S. attorney's office in Portland, and three calls to the U.S. attorney's office in Seattle, Washington June 30. He was arrested the following day. He also had called the AP bureau in Seattle May 2, leaving a message that said he would seek weapons for al Qa'ida to shoot the president and his family. "I may have to get in touch with al Qa'ida and get a hold of at least one, possibly two good working machine guns and blast my way into the White House," the voicemail said. Source:

<http://www.cbsnews.com/stories/2011/07/06/politics/main20077118.shtml>

(Washington) Cyberattack prompts PNNL to shut computer. Pacific Northwest National Laboratory (PNNL) shut down its Web site and blocked incoming e-mail July 1 after it discovered it was targeted in a highly sophisticated cyberattack, according to a lab spokesman. As a precaution, employees of the Department of Energy national lab in Richland, Washington, also were stopped from sending e-mails to addresses outside the lab or using the Internet. PNNL evidently was not the primary target of the attack, but it was passed on to the lab, the spokesman said. The corporate offices of Battelle, which operates the Richland lab, and at least one other national lab also were under cyberattack. No classified information at PNNL was compromised or was in danger of being compromised, he said. The lab's Web site, pnnl.gov, was back up by the evening of July 1, but its external e-mail service was not scheduled to be restored until PNNL staff fully diagnosed what happened and added any needed security patch. It was unknown July 1 how long that would take. Cyberattacks are common at the lab, with 4 million attacks on its external computer network every day, the spokesman said. Source: <http://www.thenewstribune.com/2011/07/02/1733293/cyberattack-prompts-pnnl-to-shut.html>

Hackers steal info on military, defense personnel. E-mail addresses and names of subscribers to DefenseNews, a highly-regarded Web site that covers national and international military and defense news, were accessed by hackers and presumed stolen, Gannett announced June 27. DefenseNews' subscribers include active and retired military personnel, defense contractors, and others in the United States' and other countries' defense establishments. "We discovered the attacker gained unauthorized access to files containing information of some of our users," said Gannett Government Media, an arm of the media chain that publishes DefenseNews, and the Military Times and Federal Times Web sites, as well as a number of military-specific magazines and journals, ranging from the Army Times to the Intelligence, Surveillance and Reconnaissance Journal. In a message posted to its site June 27, Gannett acknowledged the accessed information included first and last names, e-mail addresses, account passwords, and duty status branch of service for military personnel. Gannett urged registered users to reset their site passwords, "as well as your other online accounts, particularly those that use the

UNCLASSIFIED

UNCLASSIFIED

same email address used for your Gannett Government Media Corporation account." The attack was first detected June 7. Source:

http://www.computerworld.com/s/article/9217995/Hackers_steal_info_on_military_defense_personnel?taxonomyId=17

(West Virginia) Copper thieves knock out phone, Internet at W.Va. Dept. of Agriculture.

Copper thieves struck again June 28, knocking out phone and Internet service at the West Virginia Department of Agriculture. Employees were able to make calls to one another within the building about 10 miles from Charleston. Department workers could not dial out, nor could anyone on the outside try to reach them, and the department's Web site could not be accessed. Department officials asked the public to limit calls to emergency situations. The department remained on its regular work schedule. Frontier officials said they hoped to restore services by the evening of June 28. An agriculture commissioner said the same thing happened two months ago. The department has fences around the property and guards, but the phone and fiber optic lines were cut off site. Officials managed to forward some calls to cell phones, but they were not able to perform some emergency functions. Frontier managers said similar thefts are happening almost daily. They have put some safeguards in place such as cameras and alarms. About 200 customers were affected by this outage. State police are investigating.

Source:

http://www.wsaz.com/charleston/headlines/Copper_Thieves_Knock_Out_Phone_Internet_at_WV_Dept_of_Agriculture_124677714.html

(Florida) FBI investigating powders sent to senators in Fla. Authorities are trying to determine whether there was a link between powdery substances sent to the Jacksonville offices of Florida's U.S. Senators. A Jacksonville Sheriff's Office bomb squad was called to a Republican Senator's office June 28 after two of his staff members discovered a powdery substance in a letter. The building was evacuated and two people were evaluated before the substance was deemed safe. The Senator was in Washington D.C.. A Democratic Senator's office was evacuated June 27 after staff found a powdery substance inside a threatening letter. The Senator was in Jacksonville for a fundraiser, but had already left his office when the substance was discovered. The powder turned out to be corn starch. An FBI spokesman told the Florida Times-Union that the agency's Jacksonville office is investigating the mailings. Source:

<http://www.miamiherald.com/2011/06/29/2290496/fbi-investigating-powders-sent.html>

(Florida) Anonymous declares war on the City of Orlando. The hacktivist group Anonymous may be setting its sights on the city of Orlando, Florida. The group is threatening to take down a different city-related Web site every day, starting with Orlando Florida Guide, which does not appear to be owned by the city of Orlando. So any random Web site extolling the virtues of Orlando could be targeted. The Distributed Denial of Service (DDoS) attacks are justified in the press release as retaliation for the repeated arrests of members of a non-profit group called Food Not Bombs, which feeds homeless people in a park without a permit. The leader of the group was recently arrested. "This is a declaration of war," wrote Anonymous in its press release describing "Operation Orlando." It warned the entire city that "Anonymous will now begin a massive campaign against you and your city web assets. Everyday we will launch a new

UNCLASSIFIED

UNCLASSIFIED

DDoS attack on a different Target.” Its first target will be Orlando Florida Guide, which it threatened to take down between 10 a.m. and 6 p.m. June 29. Source:

http://www.washingtonpost.com/business/technology/anonymous-declares-war-on-the-city-of-orlando/2011/06/28/AGqGpcoH_story.html

(Florida) White powder in letter prompts evacuation of Bill Nelson’s Jacksonville office. A U.S. Senator’s office in Jacksonville, Florida, had to be evacuated June 27 after a white, powdery substance was found inside a threatening letter. The powder discovered was determined to be corn starch. Six people in the Democratic Senator’s office were evacuated while firefighters evaluated the powder. The Senator was in Jacksonville for a fundraiser, and to discuss the future of the Mayport Naval Station. He had already left his office when a staff member opened the letter. Source:

<http://www.floridatoday.com/article/20110628/BREAKINGNEWS/110628001/White-powder-letter-prompts-evacuation-Bill-Nelson-s-Jacksonville-office>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

New rootkit infects NTFS loader. Security researchers from Kaspersky Lab identified a new piece of malware that writes malicious code to the NTFS boot loader. The threat which Kaspersky detects as Cidox, features two rootkit drivers, one for 32-bit versions of Windows, and one for 64-bit ones. As part of its infection routine, Cidox determines the version of the operating system and copies the relevant driver to empty sectors at the beginning of the drive. It only infects NTFS partitions, and determines the active one by looking at MBR code. It then proceeds to replace the Extended NTFS initial program loader (IPL) code. The original one is encrypted and saved at the end. This is part of a special technique that leverages Windows kernel features to load the malicious driver into the system. The driver has the purpose of hooking into several processes including svchost.exe, iexplore.exe, firefox.exe, opera.exe, and chrome.exe via a special Dynamic-link library. Source: <http://news.softpedia.com/news/New-Rootkit-Infects-NTFS-Loader-210135.shtml>

Even more Siemens industry control systems vulnerable. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued a warning explaining the recently reported replay attacks on control systems (Programmable Logic Controllers or PLCs) sold by Siemens affect more models than previously believed, H Security reported July 7. In such attacks, attackers can get access to the automation network and send unauthorized commands to a PLC, allowing them to shut it down. PLCs are used for automated or electromechanical processes in chemical, energy, nuclear, and manufacturing plants. In mid-June, Siemens said it believed its SIMATIC S7-1200, a relatively rarely used system, was the only one vulnerable. Now, it appears the very popular SIMATIC S7-200, S7-300, and S7-400 are also vulnerable. Attackers are able to sniff the traffic between PLCs and other systems and replay packets (with commands) later. According to the report, the attack partly works because the International Organization for Standardization Transport Service Access Point (ISO-TSAP) protocol used for communication does not support authentication or encryption. ICS-CERT said such

UNCLASSIFIED

UNCLASSIFIED

communication protocols for industry were designed to be open. The lack of security functions was not a problem in the past because of the closed environments such systems are used in, but such systems are increasingly networked, which increases the risk. In its warning, ICS-CERT did not say whether the devices are also vulnerable to the DoS hole reported for the S7-1200. Siemens and ICS-CERT said they are working to solve the problem. Siemens recommended blocking external access to PROFIBUS, MPI, and PROFINET. Source: <http://www.h-online.com/security/news/item/Even-more-Siemens-industry-control-systems-vulnerable-1275226.html>

Popular FTP package download tarball poisoned. A backdoor was discovered in the source code of a widely used FTP package. Version 2.3.4 of the source code for vsftpd – billed as probably the most secure and fastest FTP server for Unix-like systems – was replaced with a compromised version with an invalid signature. The dodgy tarball version of the code was uploaded onto the main download site and available for around 3 days before the hack was detected by the author of vsftpd July 3. He moved the main download to a new site, <https://security.appspot.com/vsftpd.html>, which is hosted by Google App Engine. The counterfeit code was poorly disguised and it is unlikely too many of the tech-savvy users of vsftpd fell victim to the hack. The incident illustrates code repositories can be poisoned and the importance of checking digital signatures as a safeguard against falling victim to such schemes. Source: http://www.theregister.co.uk/2011/07/05/ftp_backdoor_shenanigans/

Critical vulnerabilities patched in phpMyAdmin. The phpMyAdmin development team released critical updates for the popular Web-based database management tool in order to patch several vulnerabilities that can be exploited to execute arbitrary code. The new 3.3.10.2 and 3.4.3.1 versions address a total of four security issues rated as highly critical by vulnerability research company Secunia. One of the flaws (CVE-2011-2505) stems from an error in the Swekey authentication function and can be exploited to manipulate the PHP session superglobal. This can be leveraged in other attacks, including the injection and execution of arbitrary PHP code. Another vulnerability (CVE-2011-2507) stems from the improper sanitizing of input passed to the PMA_createTargetTables() function in libraries/server_synchronize.lib.php. This allows attackers to truncate the pattern string and pass the /e modifier to preg_replace() which causes the second argument to be executed as PHP code. The third vulnerability (CVE-2011-2508) is also related to improperly sanitized input, but in the —PMA_displayTableBody() function. The vulnerability can be leveraged to include files from local resources via directory traversal techniques. Finally, a weakness in setup scripts (CVE-2011-2506) was addressed. Attackers can exploit it to overwrite session variables and this can lead to arbitrary code injection. A researcher from Xxor AB is credited with discovering all of these vulnerabilities. None of them affect the older 2.11.x phpMyadmin branch. Source: <http://news.softpedia.com/news/Critical-Vulnerabilities-Patched-in-phpMyAdmin-209862.shtml>

Massive botnet 'indestructible,' say researchers. A new and improved botnet that has infected more than 4 million PCs is "practically indestructible," security researchers said. "TDL-4," the

UNCLASSIFIED

UNCLASSIFIED

name for both the bot trojan that infects machines and the ensuing collection of compromised computers, is "the most sophisticated threat today," said a Kaspersky Labs researcher in a detailed analysis June 27. The director of malware research at Dell SecureWorks and an internationally-known botnet expert agreed during an interview June 29. The researchers based their judgments on a variety of TDL-4's traits, all which make it an extremely tough character to detect, delete, suppress, or eradicate. The Kaspersky Lab researcher said TDL-4 infects the master boot record (MBR) of the PC with a rootkit — malware that hides by subverting the operating system. The master boot record is the first sector — sector 0 — of the hard drive, where code is stored to bootstrap the operating system after the computer's BIOS does its start-up checks. Because TDL-4 installs its rootkit on the MBR, it is invisible to both the operating system, and more importantly, security software designed to sniff out malicious code. What makes the botnet indestructible is the combination of its advanced encryption and the use of a public peer-to-peer (P2P) network for the instructions issued to the malware by command-and-control (C&C) servers. Source:

http://www.computerworld.com/s/article/9218034/Massive_botnet_indestructible_say_researchers

DHS releases software security scoring system. The DHS, along with the SANS Institute and Mitre, released a scoring system June 26 designed to help enterprises verify whether the software they are using meets reasonable standards for secure coding. The organizations released an updated list of the Top 25 most dangerous programming errors found in software, and a measuring system that lets enterprises score the security of their software based on the presence or absence of those flaws. The goal is to give enterprises information that will let them make more informed decisions regarding the security of their software, said the director of research at SANS. The hope is that organizations within the private sector and government will use the Top 25 list and scoring system during the software procurement process, he said. Source:

http://www.computerworld.com/s/article/9217968/DHS_releases_software_security_scoring_system

Thousands of Tumblr accounts compromised. Tumblr users have been targeted with an aggressive phishing campaign within the last week, and are still being lured into entering log-in credentials for access to adult content, Help Net Security reported June 28. The scheme appears to be successful, as GFI researchers accessed a dropzone for the stolen credentials and discovered a massive amount of data. The scammers used the compromised Tumblr accounts to set up more and more phishing pages. Various domains were also used to perpetuate the scam, including tumblriq(dot)com, tumblrlogin(dot)com, and tumblrsecurity(dot)com — all registered in the last few weeks to bogus clients. "The problem has become so pervasive that regular Tumblr users are setting up dedicated anti phishing sites to advise users of the problem," the researchers said. Also, Tumblr created an automated reply for people reporting the scheme, in which it advises affected users to reset the password for their account, to remove the fake log-in template by choosing a new theme, and to "unfollow" all the blogs their account is following thanks to the scammers. Source: <http://www.net-security.org/secworld.php?id=11234>

UNCLASSIFIED

NATIONAL MONUMENTS AND ICONS

(New Mexico) 'One thing after another': Floods threaten blaze-ravaged New Mexico. As firefighters made progress saving Indian pueblo lands on the north end of New Mexico's largest wildfire, officials worried July 4 about flash floods. The fast-burning Las Conchas fire, which triggered the temporary evacuation of the Los Alamos nuclear laboratory, has since charred more than 123,500 acres, the biggest torching of the state's lands in history. Forecasters said seasonal rains were showing up across the tinder-dry Southwest, moving toward New Mexico. The superintendent of the Bandelier National Monument, a revered ancestral home of New Mexico's pueblo Indian natives, said more than 50 percent of the park, which consists of a total of 33,750 acres, has been scorched by the Las Conchas fire. The visitors center, historic lodge, and the ancient Tyounyi Pueblo ruins have been spared. But those structures may be threatened by flash floods expected with the state's monsoon season. Crews at Bandelier began working July 4 to clear stream beds, removing logs and other debris creating a clearer path so waters cannot back up and flood historic sites and buildings. Forestry and police investigators said they have determined the origin of the mammoth Las Conchas fire. It was ignited June 26 when strong winds tipped an aspen tree onto nearby power lines in the Santa Fe National Forest about 12 miles southwest of Los Alamos. Source:

<http://today.msnbc.msn.com/id/43636442/ns/weather/>

(New Mexico) Los Alamos fire to become state's biggest ever. The Las Conchas fire threatening the Los Alamos nuclear weapons laboratory was expected to become the biggest in New Mexico's recorded history July 1, the Christian Science Monitor reported. The fire has chewed up tens of thousands of acres a day since it started June 26, charring nearly 145 square miles, or 92,735 acres, by the morning of June 30. The previous record-holder, the Dry Lakes fire, burned 94,000 acres in 2003. According to data published jointly by the National Oceanic and Atmospheric Administration, the U.S. Department of Agriculture, and the University of Nebraska, New Mexico, much of Texas — which has had a record fire season — and the southeastern U.S., are in the throes of extreme to exceptional drought conditions. United Press International reported the wildfire near Los Alamos brought new challenges to fire crews. "We're seeing fire behavior we've never seen down here, and it's really aggressive," the Los Alamos County Fire Chief said June 30. While firefighters are confident they can keep both the lab and town safe from the fire, other areas were less fortunate with the fire's northern front burning sacred Native American sites, and threatening the town of Santa Clara Pueblo. The governor of Santa Clara Pueblo said his people were devastated by the news coming in from the front lines of the firefighting efforts — cultural sites destroyed, forest resources lost, and plants and animals that the pueblo's 2,800 residents depend on gone. Source:

<http://today.msnbc.msn.com/id/43604230/ns/weather/>

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

(Arizona) Health experts watching for valley fever after huge dust storm hits Valley. Health experts in Phoenix, Arizona, were warning about potential valley fever cases from a fungal spore that lives in soil after a monstrous dust storm swept through Phoenix July 12. "... When you add a dust storm that brings [fungal spore] up and people breathe it in ... it settles in your lungs and it can make you sick," said an infectious prevention nurse with Banner Desert Medical Center in Mesa. The disease can hit anywhere between a week to six weeks after inhaling the spores. It affects everyone differently. Some valley fever patients may feel mild cold and flu-like symptoms, while others, where the disease disseminates past the lungs, can be more extreme causing severe debilitation and even death. The nurse said the best way to avoid valley fever is to stay indoors. She recommended that people who feel ill see a doctor to get tested for valley fever. Source:

http://www.abc15.com/dpp/news/region_phoenix_metro/central_phoenix/health-experts-watching-for-valley-fever-after-huge-haboob-hits-the-valley

(New York) Suffolk whooping cough cases increase to 40. Suffolk County health officials in New York said the number of cases of Pertussis, or whooping cough, have increased from 13 to 40. The first cases involved students at St. James Elementary School, Tacken Elementary School, and Nesaquake Middle School in Smithtown, Huntington, and Babylon. Health officials advised parents to make sure their children's immunizations are up to date, but officials said the pertussis immunization may be only 80 percent effective. Its effectiveness often diminishes by the pre-pubescent years, they said. Pertussis is a highly contagious bacterial respiratory illness that causes uncontrollable, violent coughing that can last for weeks or months. Once a susceptible individual is exposed to the illness, it can take up to 21 days for symptoms to develop. Officials have mailed camp directors letters for parents and staff advising them how to help prevent the outbreak from spreading. Source:

<http://www.longislandpress.com/2011/06/30/suffolk-whooping-cough-cases-increase-to-40/>

(Wisconsin) Hepatitis C cases in region on the rise. Federal, state, and local health officials are trying to understand why the number of hepatitis C cases in six central and northern Wisconsin counties has increased. The Centers for Disease Control and Prevention and state Department of Health Services are working with health departments in Wood, Portage, Marathon, Langlade, Lincoln, and Oneida counties to figure out the reason the number of new cases among people younger than 30 more than doubled in 2009 and 2010, a Wood County public health nurse said. From 2004 through 2008, the six-county area had a combined average of 12.2 cases a year. In 2009 and 2010, they averaged 27 cases annually. One of the potential causes for the trend is an increase in intravenous drug use as one new case of hepatitis C seen in Portage County in 2010

UNCLASSIFIED

involved intravenous Heroin use. Nationally, health department officials think 35 to 70 percent of drug users who inject are infected with hepatitis C. Unlike with hepatitis A and B, there is no prevention vaccine. Source:

<http://www.wausaudailyherald.com/article/20110705/WDH0101/107050433/Hepatitis-C-cases-region-rise>

Copper kills 97 pct of hospital ICU bacteria-study. Antimicrobial copper surfaces in intensive care units (ICU) kill 97 percent of bacteria that can cause hospital-acquired infections, according to preliminary results of a multisite clinical trial in the United States. The results also showed a 40 percent reduction in the risk of acquiring an infection. The study, presented at the World Health Organization's 1st International Conference on Prevention and Infection Control (ICPIC) in Geneva, Switzerland, July 1, backed what research teams at three U.S. hospitals suggested 4 years ago: replacing the most heavily contaminated touch surfaces in ICUs with antimicrobial copper will control bacteria growth and cut down on infection rates. Source:

<http://www.reuters.com/article/2011/07/01/copper-antimicrobial-idUSN1E7600JD20110701>

Musty odor again causes Johnson & Johnson to recall Tylenol Extra Strength Caplets. Johnson & Johnson has announced yet another Tylenol recall due to a musty moldy odor linked to a trace chemical. The company's McNeil Consumer Healthcare unit is recalling more than 60,000 bottles of Tylenol Extra Strength Caplets made in February 2009 and distributed in the United States. The chemical, known as TBA, is a byproduct of a chemical preservative sometimes used on shipping pallets. Besides causing an unpleasant odor, TBA has been associated with temporary and non-serious gastrointestinal symptoms. Since September 2009, New Brunswick, New Jersey-based Johnson & Johnson has had about two dozen recalls of prescription and nonprescription medicines, replacement hips, contact lenses, and diabetes test strips, including tens of millions of bottles of children's and adult Tylenol and Motrin. Source:

http://www.washingtonpost.com/business/musty-odor-again-causes-johnson-and-johnson-to-recall-tylenol-extra-strength-caplets/2011/06/28/AGxAAqpH_story.html

(Indiana) Indiana Measles outbreak prompts vaccine message. Measles cases in the United States have hit a 15-year high according to the U.S. Centers for Disease Control, and on June 23, the Indiana State Department of Health has confirmed five cases in Noble County. Nearly all the cases can be traced to outbreaks overseas in countries such as India and France, including those in Indiana. Measles symptoms start 3 to 5 days after exposure, and the disease can be deadly. Even though just two doses of the MMR (Measles, Mumps, and Rubella) vaccine during childhood can prevent measles for life, many parents in Europe fueled recent outbreaks after opting their children out of the vaccines because of concern about potential side effects.

Source: <http://www.fox59.com/news/wxin-measles-outbreak-indiana-measles-outbreak-prompts-vaccine-message-20110623,0,7543855.story>

UNCLASSIFIED

TRANSPORTATION

(Arizona) Phoenix man arrested after laser pointed at police helicopter. Phoenix, Arizona police July 7 were spreading the word that people who shoot laser beams at aircraft are liable to go to jail. That is exactly what happened July 6 when a suspect, age 24, admitted to officers that he had aimed a green-laser pointer at a police helicopter flying above the 2300 block of West Portal Lane, south of Greenway Road, at about 10:30 p.m., a police spokesman said. Two officers with the police air unit were piloting the helicopter at the time. Authorities said lasers can temporarily blind or distract pilots or crew members on board an aircraft, making it difficult to safely land. The spokesman said that, several times a month, people on the ground direct laser pointers at police aircraft. Source:

<http://www.azcentral.com/arizonarepublic/local/articles/2011/07/07/20110707phoenix-laser-pointer-helicopter-abrk.html>

Amtrak opted out of safety improvements. KCRA 3 has obtained reports that indicate Amtrak opted out of safety improvements that would have aided emergency responders in the deadly Amtrak crash June 17, outside of Reno, Nevada that killed at least six people. Three days after the accident that saw a semi truck drive into the train at a railroad crossing, investigators still can't find two passengers, and Amtrak can't say whether those passengers were definitely on board because of deficiencies in their passenger accounting system. KCRA 3 found a 2002 National Transportation Safety Board report that recommended Amtrak improve its passenger accountability procedures. The 2002 report was in response to a similar deadly Amtrak accident in Crescent City, Florida. KCRA 3 obtained a U.S. Department of Transportation report responding to that recommendation. An Amtrak spokesman admitted recent technology improvements have made a better accounting system feasible. He said Amtrak is currently testing a new electronic ticketing system on the East Coast that could lead to an accurate count of passengers on board trains. Source: <http://www.kcra.com/news/28377964/detail.html>

(Nevada) Investigators piece together Nevada Amtrak crash. Investigators struggled June 27 to piece together how a truck driver who plowed into an Amtrak train in the Nevada desert failed to notice the crossing gates and blinking lights that should have been visible a half-mile away. At least six people were killed and five people are unaccounted for after the fiery June 24 crash that gutted two rail cars, and left the semi-truck buried inside one. A Nevada Highway Patrol trooper said authorities would consider all factors as they investigated the cause of the accident, including fatigue, driver inattention, and drugs or alcohol, with toxicology and autopsy results due within days. It could take up to a year to pinpoint the cause of the crash that killed the truck driver, a conductor and four others on the train. The semi-trailer truck hit the California Zephyr at a highway crossing about 70 miles east of Reno. A National Transportation Safety Board (NTSB) member said flashing lights at the crossing were set to blink 25 seconds before a train approaches. Three days after the accident, a variety of factors remained unknown, including how fast the driver was going. Two other truck drivers in the convoy and the train's engineer watched the semitrailer skid the length of a football field before crashing into the train. The other drivers stopped when they saw the gates come down and the warning lights go off as the California Zephyr approached, the NTSB member said. The driver of the big

UNCLASSIFIED

rig in the lead did not. The train's engineer slammed on the emergency brakes, but the train, which was going about 78 mph in an 80-mph zone, traveled a half-mile more before it finally stopped. The driver was working for John Davis Trucking Co. in Battle Mountain, Nevada. Its Web site said it was family owned and specialized in hauling ore from local mines, as well as moving gravel and sand. Source: <http://www.kptv.com/story/14982983/investigators-piece-together-nevada-amtrak-crash>

WATER AND DAMS

(Iowa) Des Moines River flood danger rising, corps says. Residents downstream of Lake Red Rock near Pella, Iowa, were warned of potential flooding from the Des Moines River June 29. The U.S. Army Corps of Engineers increased the release to 30,000 cubic feet per second (cfs), 8,000 more than the normal 22,000 cfs. The Corps said that when the pool reaches 776 feet above sea level, the outflow gradually will be raised to 35,000 cfs. Source: <http://www.kttc.com/story/14995684/des-moines-river-flood-danger-rising-corps-says>

(Washington) Wash. official says water a serious concern. An official from the Washington State Department of Ecology said June 28 that water shortages are acute in the Yakima region, where "the river and reservoir system does not have enough water to meet everyone's needs." Decline in groundwater levels threaten the quality of life in communities in the West Plains area west of Spokane, in the Odessa area east of Moses Lake and around Pullman, he said. "We're just pumping more out than (the aquifer) is recharging," said the official, who retires this week after 33 years at the agency. "We issued more water rights than we have water." Most water in river basins was allocated for municipal, agricultural, or industrial use decades ago, and the backlog for water rights applications is 7,000 long. Meanwhile, climate change, population growth, and the need to protect fish and wildlife habitat put new pressures on water supplies statewide. Under a 1945 law, the state allows some wells to be drilled without a permit as long as water usage is held to 5,000 gallons a day. Source: http://seattletimes.nwsources.com/html/localnews/2015452898_apwawashingtonwater1stldwr itethru.html

(Washington) PacifiCorp to remove 14.7 MW hydropower dam in Washington. The utility PacifiCorp said it would decommission its 14.7 MW Condit Dam in Washington State, starting October 2011. The company considers the removal of the dam cheaper than the renewal of its license, which would require the establishment of a fish passage under the federal dam licensing process. The decommissioning is expected to cost \$32 million, including spending during the planning process. Decommissioning of the is dam expected to be complete by August 31, 2012. Source: http://www.hydroworld.com/index/display/news_display.1445466213.html

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA HOMELAND SECURITY CONTACTS

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

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

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

UNCLASSIFIED