

UNCLASSIFIED



North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners. If you have any comments to improve this summary or local information you would like to see in the summary please send the information to; kihagel@nd.gov

UNCLASSIFIED

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**

NORTH DAKOTA

Fargo-Moorhead diversion-impact analysis only half finished. The impact of a proposed Fargo-Moorhead flood diversion on downstream river levels may be greater than previously estimated, but a U.S. Army Corps of Engineers official cautioned Wednesday that the analysis is only half-completed and the numbers will likely change. The Corps project manager would not say how much larger the downstream impact could be than the 10.4 inches estimated by the Corps in February. But he did say the impact isn't as large as the 14.5 inches reported by one media outlet that cited a leaked report. "We had some discussions about it during our internal team meeting," he said. "The number we discussed was not 14.5." Estimates of the diversion's impact will change in the near future, and for now the figures released in February are the best available, he said. He said the Corps should have new numbers to release at its next round of public meetings June 9 and 10. Source:

<http://www.grandforksherald.com/event/article/id/158703/>

UNCLASSIFIED

Bismarck-area boaters hitting objects in river. North Dakota's Transportation Department is urging Missouri River boaters to use caution in the area of the new Liberty Memorial Bridge between Bismarck and Mandan because of objects in the water. There have been numerous reports of boaters hitting obstructions, and the department said the bridge contractor would determine if debris from the project is to blame. The new bridge opened in July 2008, and the old one was blown up that fall. The head of Moritz Marine said he has had seven boats in for repairs to damaged propellers, and he has heard of other damage reports including one boat with a torn-up hull. The transportation department said markers are being placed in the river to alert boaters that they should not travel on the east side of the channel near the bridge. Source:

<http://www.grandforksherald.com/event/apArticle/id/D9F8OT600/>

REGIONAL

(Minnesota) Campfires restricted in northeastern Minnesota beginning Friday. The Minnesota Department of Natural Resources (MDNR) and U.S. Forest Service have announced more burning restrictions due to very high fire danger. Put into effect Friday, April 23, the new restrictions cover campfires, fireworks, outdoor welding, and prescribed burning. The restrictions cover 37 Minnesota counties, including all of northeastern Minnesota. Campfires will be restricted to the hours between 6 p.m. and 8 a.m. Campfires must be in a fire receptacle associated with a residence, resort, or developed public and private campgrounds. People who light campfires must have adequate water on hand. Campfires will be banned completely within the Chippewa and Superior National Forests, including the Boundary Waters Canoe Area Wilderness. Gas and propane camp stoves are still allowed. The MDNR is also restricting fireworks and outdoor welding across northeastern Minnesota. Fireworks will not be allowed outside municipalities and devices with open flames, such as welders and acetylene torches, will be prohibited in forest and grass areas, except under special permits. The MDNR is no longer allowing prescribed burning and running fires until conditions improve. Source:

<http://www.fox21online.com/news/all-fires-banned-bwcaw-superior-and-chippewa-national-forests>

(Montana) Great Falls airport shut down after package scare. Great Falls International Airport officials said a suspicious package caused them to close their passenger terminal for about two hours. The package turned out to be a battery charger with protruding wires that was in luggage being loaded onto a flight. The airport public safety manager said a Transportation Security Administration employee flagged the package after it was X-rayed Tuesday about 7:30 a.m. Officials evacuated the terminal and contacted police and the Explosive Ordnance Disposal teams with the Montana Air National Guard and Malmstrom Air Force Base. Using a robot, the military teams determined that the luggage was safe to be opened, revealing the battery charger. It was unclear how many other flights were affected by the delay. Source: <http://www.kulr8.com/news/state/92267019.html>

(Montana) New scammer phishing for card numbers. Officials with Rocky Mountain Credit Union are cautioning members not to be taken in by a scam that is attempting to lure people to give out their account numbers over the phone. According to the credit union's marketing and business development specialist, several members — and non-members — have contacted the credit union about text messages and telephone messages they've received that are purportedly from Rocky Mountain Credit Union. The text message read, "Rocky Mountain CU Alert: Your CARD has been DEACTIVATED. Please contact us at 406-545-4719 to REACTIVATE your CARD." The specialist said a call earlier this week to the number led to an automated message asking people to enter their 16-

UNCLASSIFIED

UNCLASSIFIED

digit account numbers. A call to the number, which has a Billings prefix code, at midday April 23 resulted in a message that the mailbox at the number was full. The specialist said on April that the credit union is not aware of any members falling for the scam. The specialist said the credit union would not contact members via text or automated message. Source:

http://helenair.com/news/article_3eedea7c-4f69-11df-b0cc-001cc4c002e0.html

(Montana) No chemicals found in Malta's water. Malta's water storage tanks were not contaminated with any chemicals when a fence was cut, but the Montana State Department of Environmental Quality (DEQ) said Thursday that it still is waiting for the results of radiological tests. "We haven't found anything out of the ordinary in the water," said the manager of the DEQ's Public Water Supply Program. The state received the results of chemical tests Thursday. He said those tests all came back clean. It is highly unlikely the water has radioactive products in it, but the test was recommended by the Agency for Toxic Substances and Disease Registry, which is part of the national Centers for Disease Control, the manager said. The radiological test results were due back Friday. A cut in the fence protecting the town's water storage tanks was discovered April 18, prompting a warning to not drink the water, in case the tanks had been contaminated. On April 20, after tests for bacteria turned out OK, the water was pronounced safe. At that time, chemical and radioactive tests still had to be conducted. The DEQ manager said the storage tanks were shut off pending the test results, but the town still has water because wells are operating. He added that even if the people who cut the fence were just partying — an open-beer container and an energy drink were found — it could be deemed tampering with a public-water supply, which is a federal felony offense. The case is being investigated by the criminal investigation division of the Environmental Protection Agency, he said. Source: <http://www.greatfallstribune.com/article/20100423/NEWS01/4230342>

(South Dakota) Preservation work continues at Rushmore. Crews at Mount Rushmore National Monument will begin two weeks of preservation work on the granite carving April 26 to protect the sculpture from erosion damage. Some of the work involves workers being suspended on ropes to inspect the four presidential faces and to remove vegetation and hazardous rocks. Officials said the annual preservation work also would prepare the mountain for a detailed 3D digital laser scanning project in May. Source: <http://www.ktiv.com/Global/story.asp?S=12373512>

(South Dakota) Grasshopper outbreak potential high. The United States Department of Agriculture's Animal and Plant Health Inspection Service Plant Protection and Quarantine office based in Pierre, South Dakota has predicted a high potential for crop devastation from a grasshopper outbreak this year based on grasshopper counts last year, said a South Dakota State University Extension entomologist. The adults from last year presumably laid eggs in the soil. Their eggs may have successfully overwintered and may hatch successfully and result in an outbreak this year. Last fall, the USDA warned that the grasshopper species that it saw in large numbers last year was the two-striped grasshopper, which is particularly destructive. In the 1920s and 1930s, it destroyed many of the crops and shelterbelts in eastern South Dakota. It was only the severity of the drought in the 1930s that devastated crops that also stopped the destruction of the grasshopper. Source:

<http://mobile.dakotafarmer.com/main.aspx?ascxid=cmsNewsStory&rmid=0&rascid=&args=&rargs=9&dt=634078697998320000&cmsSid=37620&cmsScid=9>

UNCLASSIFIED

NATIONAL

Scientist: Money to fight beetles as fire mitigation not productive. In an effort to mitigate the risk of wildfires, a Colorado U.S. Senator introduced forest legislation last November that specifically targets the mountain pine beetle and spruce beetle. The bill, in part, seeks to provide increased federal assistance to 12 "affected" Western states, including Colorado, which have large numbers of forest lands containing disease-ridden trees caused by beetle outbreaks and other insect infestations. The Senate Energy and Natural Resources Subcommittee on Public Lands and Forests this month held a hearing and received testimony on the National Forest Insect and Disease Emergency Act of 2009, and three other public-lands bills. However, one scientist that has studied the connection between beetle infestation and forest fires and disease for more than 10 years told the panel that insect infestations are not the major cause of forest fires in Colorado. He said allocating federal assistance to combat the critters would be unproductive. "The best available science indicates that outbreaks of mountain pine beetle and spruce beetle do not increase the risk of fire in most types of forests," said the scientist, in his April 16 testimony. Furthermore, the scientist stated that scientific evidence indicates that fires do not burn more quickly or more severely in dead, disease-ridden forests than in dense, live forests under current climate conditions. He argued that the presence of flammable materials and the failure to use fire-resistant materials in home construction also enhance fire risk in forests and surrounding communities. A former research scientist at the University of Colorado at Boulder and current professor at Clark University in Massachusetts also discounted the notion of beetles causing forest fires during his testimony. He said climate, not insects, plays the most important role in forest fires, as wildfires are more likely to occur during droughts. Source: [http://durangoherald.com/sections/News/2010/04/23/Scientist Money to fight beetles as fire mitigation not productive/](http://durangoherald.com/sections/News/2010/04/23/Scientist_Money_to_fight_beetles_as_fire_mitigation_not_productive/)

INTERNATIONAL

Four wounded in grenade attack on dam. A series of grenade blasts hit a hydropower project in Burma Tuesday, wounding four workers in the latest unrest in the military-ruled country, officials said. The attacks occurred at the Thaukyegat hydropower plant under construction in Bago division, about 220 kilometres (137 miles) northeast of the country's main city Rangoon, a local official told AFP. "Four workers were injured during three grenade attacks at the Thaukyegat hydropower project site," the official said, asking not to be named because he was not authorized to speak to the media. The Burmese company behind the project, Asia World Construction, was also involved in a controversial dam project in Kachin state where there was a series of bombs blasts earlier this month, injuring one engineer. Three other bombs April 15, hit a water festival in Rangoon, in the city's worst attack in five years. The death toll from that attack has now risen to 10 people, with at least 170 people wounded. Burmese authorities have arrested some suspects in their search for the perpetrators of those blasts, officials said, but they did not give any further detail as the investigation is still underway. Burma has been hit by several bomb blasts in recent years, which the junta has blamed on armed exile groups or ethnic rebels. The latest attacks come as the country prepares for elections planned for this year. Source: <http://www.dvb.no/news/four-wounded-in-grenade-attack-on-dam/8780>

UNCLASSIFIED

Swiss police foil bomb attack against IBM. Police have arrested two men and a woman suspected of planning to bomb an IBM Corp. research facility near Zurich, Swiss media reported Monday. Prosecutors said two Italians and a Swiss national suspected of planning a bomb attack against an international company had been arrested, but declined to confirm the target. They said the arrests occurred April 15 near Rueschlikon about 6 miles (10 kilometers) south of Zurich. Police discovered "explosive and further items in their car" as well as a note "indicating a planned attack on the branch of an international company," said a spokeswoman for the federal prosecutors office. All of those arrested remain in detention, she said. The SonntagsBlick newspaper reported the suspects intended to attack a nanotechnology research facility that IBM Corp. is building in Rueschlikon. Source: http://hosted.ap.org/dynamic/stories/E/EU_SWITZERLAND_IBM_BOMB?SITE=NHPOR&SECTION=HOME&TEMPLATE=DEFAULT

TAU professor tips off US over security flaw in e-passports. A Tel Aviv University (TAU) researcher has enabled the US State Department to fix security holes in its electronic passports, and now has set his sights on at-risk credit, debit and "smart" cards used by hundreds of millions of people around the world. E-passports contain biometric data, electronic fingerprints and pictures of the holder, as well as a wireless radio frequency identification (RFID) transmitter. Although the original system was designed to operate at close range, the TAU computer science professor realized hackers were able to access data from afar. Noticing this security problem, the professor helped ensure that the computer chip in American e-passports could be read only when the passports were opened. In 2007, the U.S. State Department outfitted every new passport with both a security chip and conductive fibers on the back. A U.S. Embassy spokesman told The Jerusalem Post Thursday that there had "been a problem" in the past with his country's e-passports, but added that it had been dealt with. Now, a new study by the TAU professor has found serious security drawbacks in similar chips that are being embedded in credit, debit and smart cards. The vulnerabilities of this electronic approach – and of the private information contained in the chips – are becoming more acute, he said. Using simple devices constructed from \$20 disposable cameras and copper cooking-gas pipes, the professor and his team of students have demonstrated how easily the cards' radio frequency (RF) signals can be disrupted. The professor has suggested some small steps that can be taken to make smart cards smarter, the easiest one being to shield the card with something as simple as aluminium foil to insulate the e-transmission. Source: <http://www.jpost.com/LandedPages/PrintArticle.aspx?id=173841#>

Somali pirates indicted for attacks on Navy ships. Federal grand juries in the Eastern District of Virginia have returned two, separate indictments charging 11 men from Somalia with piracy and related offenses pertaining to attacks on two Navy ships. The indictments charge separate attacks by separate groups on the U.S.S. Nicholas and the U.S.S. Ashland. "Since the earliest days of this country, piracy has been a serious crime," said the U.S. Attorney for the Eastern District of Virginia. "Piracy threatens human lives and disrupts international commerce. When pirates attack U.S. vessels by force, they must face severe consequences." "The Naval Criminal Investigative Service provides unique forward-deployed, law-enforcement capabilities to the U.S. Navy's Maritime Strategy," said a NCIS Special Agent in Charge. "This case demonstrates the working relationship between uniformed military forces and NCIS — which is a civilian agency — and our federal partners to ensure cooperative security and stability across the maritime domain." Source: <http://norfolk.fbi.gov/doipressrel/pressrel10/nf042310.htm>

UNCLASSIFIED

BANKING AND FINANCE INDUSTRY

Barclays security chief: assume all networks are compromised. IT security professionals should operate under the assumption that their networks are compromised, and look at ways to ensure that the system works regardless, according to the head of information risk management at Barclays. He argued during a panel debate at Infosecurity Europe April 28 that it is wrong for security chiefs to try to create a “bubble of safety” in their systems because it is a false hope given the numerous threats and flaws. He clashed with his fellow panelists, both heads of information security at large multinationals, arguing that users do not benefit from feeling that they are being “watched” and should not be treated like children. It is the information security professional’s responsibility to educate users so that they can make the right decisions, according to the Barclay’s executive. “I believe that it is not all the user’s fault. Users generally make informed and sensible decisions, and our goal is to educate and inform them,” he said. Source:

<http://www.v3.co.uk/v3/news/2262198/barclays-security-chief>

Better communication could enhance the support FinCEN provides to law enforcement. Better communication could enhance the support the Financial Crimes Enforcement Network (FinCEN) provides to law enforcement, the Government Accountability Office (GAO) has found. It detailed steps that could be taken to improve anti-money-laundering efforts in a study issued April 28. The GAO noted that in December 2009, it found that the majority of 25 Law Enforcement Agencies (LEA) surveyed found FinCEN support useful in their efforts to investigate and prosecute financial crimes. But the GAO also found that FinCEN could enhance its support by better informing LEAs about its services and products and actively soliciting their input. GAO recommended that FinCEN establish a process for soliciting input regarding the development of its analytic products. FinCEN agreed with the recommendation and in April 2010 outlined a number of steps it plans to take to better assess law-enforcement needs, including ongoing efforts to solicit input from LEAs. GAO recommended that FinCEN develop a mechanism to collect sensitive information regarding regulatory changes from LEAs. In April 2010, FinCEN reported that it developed an approach for collecting sensitive information without making the comments publicly available. Source:

<http://www.gao.gov/products/GAO-10-622T>

Inside the brains of a professional, bank-hacking team. Following the cyberspying breaches at Google, Adobe, Yahoo!, Intel, Juniper and others, there has been much discussion and dissection of targeted attacks. But rarely is an individual operation laid out in step by step detail. And rarer still is an account told from the hacker's perspective. But just such an account has been provided by the individual who runs Netragard, a cybersecurity consultancy that, among other services, performs penetration tests on clients to expose their security vulnerabilities. In a blog post April 26, the consultant laid out a recent hacking operation that his SNOsoft research team was hired to perform on a bank client. Though he does not name the target, he describes step by step the social engineering involved in sussing out the bank's defenses, including staging a fake job interview with unwitting employees of the company. The technical strategy for breaching the bank's defenses — a targeted, booby-trapped, PDF attachment — is not a surprise. But the detailed description of the preparation for that exploit is a rare window into the hacking process. Source:

<http://blogs.forbes.com/firewall/2010/04/27/inside-the-brains-of-a-professional-bank-hacking-team/>

UNCLASSIFIED

U.S. businesses face skimming-fraud increase. U.S. banks are grappling with a recent increase in skimming attacks, which are being carried out by Eastern European gangs aiming to steal consumer bank account numbers and Personal Identification Numbers, according to a Gartner analyst. These types of attacks are not new, but the scale and the organization behind them is, the Gartner vice president told SCMagazineUS.com April 27. Over the past six months, fraudsters increasingly have been mounting well-organized and systematic attacks that involve placing skimming devices on not just ATM machines — the most commonly targeted device — but also point-of-sale systems and gas-pump card readers. The analyst said she heard about the increase in skimming at a recent fraud conference attended by officials from numerous financial-services firms. Source: <http://www.scmagazineus.com/us-businesses-face-skimming-fraud-increase/article/168793/>

(Florida) Police looking for high tech ATM scammers. Police are looking for some high-tech ATM scammers in Palm Beach Gardens, Florida. In a new scam, suspects are placing high-tech devices on ATM's to swipe both card and personal identification numbers at the same time. Transactions process normally, but the card data and pin numbers are captured and saved. Often the devices are indiscernible from real ATM parts. Once the information is captured, the scammers can make fake, ATM cards with the information and access the victims' bank accounts. Incidents like this have been happening nationally, and Palm Beach Gardens police have recorded three incidents. The most recent took place at the Bank of America at 5560 PGA Blvd where a customer discovered a skimming device had been installed over the ATM's card slot. The customer tugged at the device and it came off, then took the device and contacted police. Immediately after the customer left with the device, two men were captured on the ATM's security camera removing a video camera from the ATM's overhang. They were gone by the time police arrived. Authorities said that it is unusual to actually recover a skimming device. The one recovered in this incident has been sent for forensic analysis. Source: <http://www.cbs12.com/news/atm-4725783-device-police.html>

FTC warns against credit-card, interest-rate reduction scams. U.S. consumers are being inundated with prerecorded “robocalls” from companies claiming they can negotiate lower credit-card interest rates – for a fee. The Federal Trade Commission urges extreme skepticism about these offers, because many of them are fraudulent. In a new consumer alert, Credit Card Interest Rate Reduction Scams, the FTC said consumers have just as much clout with their credit card issuers as these companies do. It urges consumers to avoid paying middlemen, and negotiate directly with the credit-card companies. Source: http://www.foodconsumer.org/newsite/Non-food/Miscellaneous/credit_card_interest_rate_reduction_scams_2404100850.html

Pair of fines levied on breached companies show real costs of database hacks. Two different companies in the past two weeks were fined by regulatory agencies for separate database breaches, totaling well over \$1 million. The first incident was an insider breach initiated by a former database administrator (DBA) at Certegy, a wholly owned subsidiary of Jacksonville, Florida-based Fidelity National Information Services (FIS), which cost the company \$975,000 in fines to the Florida Attorney General. The second event was an external attack precipitated by a SQL injection exploit against a customer database owned by brokerage firm Davidson & Co., for which the Financial Industry Regulatory Authority (FINRA) fined the firm \$375,000. “In one case it was hackers, and in another case it was an internal employee — a DBA — but in both incidents, the issue was that they didn’t have any real-time monitoring in place. That’s how these two stories are related,” said the vice president of security strategy of Guardium, an IBM company. “What a SQL injection attack [does] is

UNCLASSIFIED

UNCLASSIFIED

give the attacker privileged user credentials. So if you're monitoring your privileged users like your DBAs, you're also getting the bonus of monitoring for external threats at the same time." The more extreme case among the two fined companies was Certegy's breach, which showed how database breach costs can really rack up for a company. In this incident, a malicious insider at the company exposed about 5.9 million customer records. The \$850,000 fine levied by Florida to pay its investigative costs and attorney fees, and the additional \$125,000 demanded to help fund a state-wide, crime-prevention program, are just a tip of the breach cost iceberg for Certegy. Source: http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=224600140

Debt-settlement firms misled consumers, GAO report says. A government investigation into the burgeoning, debt-settlement industry has found that many firms misled consumers by claiming to be affiliated with federal stimulus programs, and exaggerating their ability to reduce consumers' loans. Presented on April 22 at a Senate Commerce Committee hearing, the Government Accountability Office report included audio recordings of salesmen describing their companies as "government approved" and linking settlements to the federal bailout of troubled banks. Another sales recording stated that all customers eliminated their debt in three years, while others encouraged customers to stop paying their creditors — a practice that violates the industry's own standards. "It is appalling beyond words," the senator who heads the committee said at the hearing. "These debt-settlement companies are kicking people when they are down." The number of debt-settlement companies has ballooned to more than 1,000 during the past five years, after changes to the federal bankruptcy law made it more difficult for consumers to qualify for bankruptcy and as the recession ravaged household budgets. The companies promise to negotiate with a customer's creditors to reduce the principal, rather than just interest and fees, as many credit-counseling firms do. But consumer advocacy groups have attacked the industry for charging hefty, up-front fees before calls to creditors are made. In addition, the consumer advocates have accused debt-settlement firms of misleading consumers in sales pitches and instructing them not to pay bills. Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/22/AR2010042205523.html>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Helium-3 shortage could mean nuke detection 'disaster'. Stopping nuclear smuggling is already tough. But it's about to get a lot harder. Helium-3, a crucial ingredient in neutron-particle-detection technology, is in extremely short supply. A Democratic congressman from North Carolina, who serves as chairman of the House Subcommittee on Investigations and Oversight, chided the Departments of Energy and Homeland Security at a hearing on the issue late last week, suggesting that they created a preventable "disaster." The Energy Department is the sole American supplier of helium-3, and DHS is supposed to take the lead in spotting and stopping illicit nuclear material. The helium-3 isotope represents less than 0.0002 percent of all helium. Of that, about 80 percent of helium-3 usage is devoted to security purposes, because the gas is extremely sensitive to neutrons, like those emitted spontaneously by plutonium. Helium-3 is a decay product of tritium, a heavy isotope of hydrogen used to enhance the yield of nuclear weapons, but whose production stopped in 1988. The half-life decay of tritium is about 12 years, and the U.S. supply for helium-3 is fed by harvesting the gas from dismantled or refurbished nuclear weapons. However, production of helium-3 hasn't kept pace with the exponential demand sparked by the September 11 attacks. Projected demand for the nonradioactive gas in 2010 is said to be more than 76,000 liters per year, while U.S. production is a

UNCLASSIFIED

UNCLASSIFIED

mere 8,000 liters annually, and U.S. total supply rests at less than 48,000 liters. This shortage wasn't identified until a workshop put on by the Department of Energy's Office of Nuclear Physics in August 2008. Source: [http://www.wired.com/dangerroom/2010/04/helium-3-shortage-could-mean-nuke-detection-disaster/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+WiredDangerRoom+\(Blog+-+Danger+Room\)](http://www.wired.com/dangerroom/2010/04/helium-3-shortage-could-mean-nuke-detection-disaster/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+WiredDangerRoom+(Blog+-+Danger+Room))

EPA opens access to chemical-information searchable database. The U.S. Environmental Protection Agency had made it easier to find chemical information online. On April 29, it announced the releasing of a database called ToxRefDB that allows scientists and the general public to search and download thousands of toxicity testing results on hundreds of chemicals. ToxRefDB captures 30 years and \$2 billion of testing results. The database provides detailed chemical toxicity data in an accessible format. It is a part of ACToR, an online data warehouse that collects data from about 500 public sources on tens of thousands of environmentally relevant chemicals, including several hundred in ToxRefDB. People interested in chemical toxicity can query a specific chemical and find all available public hazard, exposure, and risk-assessment data, as well as previously unpublished studies related to cancer, reproductive, and developmental toxicity. ToxRefDB contains toxicity information that forms the basis for pesticide risk assessments when combined with other sources of information, such as those on exposure and metabolism. Source: <http://yosemite.epa.gov/opa/admpress.nsf/0/43216C4F52D46B0B85257713007C197B>

Hot-work explosions cause deaths. Performing hot work around combustible gases is as clear-cut a recipe for disaster as can be found in industrial environments. Yet this highly dangerous activity is one of the most common causes of worker deaths, said the U.S. Chemical Safety Board (CSB). Following investigations of several hot-work accidents that killed workers in the past two years, CSB recently issued a safety bulletin identifying seven key lessons aimed at preventing worker deaths during hot work in and around storage tanks containing flammable materials. Hot work is any activity that involves burning, welding, cutting, brazing, grinding, soldering, or similar spark-producing operations that can ignite a flammable atmosphere. CSB investigated explosions ignited by hot work at an oil refinery, a food manufacturer, a produce company, and a waste-oil facility, among others. Each incident resulted in worker deaths or severe injuries. CSB said it has identified more than 60 fatalities that have occurred since 1990 as the result of explosions and fires caused by hot work. "A common feature of virtually all these accidents is the failure to recognize all the locations where a flammable atmosphere could be present," said the CSB investigations supervisor. "The absence of flammables needs to be verified before and during any hot work." CSB notes that combustible-gas monitors are relatively inexpensive, hand-held electronic instruments that measure the amount of flammable material in the atmosphere. Proper training and calibration are essential for using gas monitors effectively, said CSB. The Occupational Safety and Health Administration does not require combustible-gas monitoring for hot work on or near flammable storage tanks. Source: <http://safety.blr.com/news.aspx?id=115988>

Debate over chemical plant security heats up — again. Some lawmakers want to toughen up federal chemical-plant safety legislation, due for renewal before it expires this fall. But chemical-industry company executives prefer the continuation of the current measure, which was passed in 2007. The key debate is over whether or not DHS should be in a position to impose the use of safer and less-volatile chemicals on plants closest to large urban centers. Industry leaders argue that many plants

UNCLASSIFIED

UNCLASSIFIED

have already made the switch voluntarily. Source: <http://homelandsecuritynewswire.com/debate-over-chemical-plant-security-heats-again-ii>

(Louisiana) It may take months to close BP oil well leak. BP Plc said it may take months to drill a well to stop an oil spill under the Gulf of Mexico that threatens to become an environmental disaster. BP and Swiss drilling contractor Transocean Ltd. began using remote-controlled vehicles Sunday to try to halt the 1,000 barrel-a-day leak. If that doesn't work, BP may need to pump heavy fluid into a relief well to stop the flow of crude from the seabed. The clean-up following an explosion that sank Transocean's Deepwater Horizon rig last week about 50 miles off the coast of Louisiana is the biggest in at least 20 years, according to the Marine Spill Response Corp., one of the companies involved in the operation. The disaster, which left 11 missing, has caused a 600-square-mile oil slick, which is about the same size as Houston. Source: <http://www.businessweek.com/news/2010-04-26/bp-oil-well-leak-may-take-months-to-close-after-gulf-rig-sinks.html>

U.S. oil, chemical plants underreporting pollution. The nation's oil and chemical plants are spewing a lot more pollution than they report to the Environmental Protection Agency (EPA) — and the EPA knows it. But the federal agency has yet to adopt more accurate, higher-tech measuring methods that have been available for years, according to experts. Significant changes will not be seen for at least two more years, even though an internal EPA watchdog called for improvements in 2006, and some of the more sophisticated measuring devices have been used in Europe since the 1990s. Records, scientific studies and interviews by the Associated Press suggest pollution from petrochemical plants is at least 10 times greater than what is reported to the government and the public. Some European countries employ lasers, solar technology, and remote sensors to measure air pollution, while the U.S. relies to a large degree on estimates derived from readings taken by plant employees using hand-held "sniffer" devices that check for leaks in pumps and valves. The failure to get a true assessment of industrial emissions hinders attempts to monitor and regulate public health and air quality. Although U.S. oil and chemical companies have criticized some of the high-tech measuring devices, complaining they do not yield a full and accurate picture, the industry said it would embrace technologies that work and are affordable. Under the federal Clean Air Act, plants must bear the cost of pollution-monitoring equipment. And the newer, high-tech devices could easily cost a plant hundreds of thousands of dollars. Also, more accurate measuring devices could lead to bigger fines against industrial polluters and force them to pay for cleaner technology. Source: http://www.dallasnews.com/sharedcontent/dws/news/texasouthwest/stories/DN-emissions_23tex.ART.State.Edition1.4c56cf7.html

COMMERCIAL FACILITIES

(New York) Security stepped up at Comedy Central following threats against 'South Park'. The New York Police Department has stepped up security at the headquarters of the Comedy Central cable channel after an Islamic extremist Web site posted apparent threats to the creators of South Park for making fun of the Prophet Muhammad. The NYPD deputy commissioner and chief spokesman says that his department for some time has been aware of the small group, which appears to organize around a now-unreachable Web site called RevolutionMuslim.com, at least one of whose purported leaders posted threats against South Park after the cartoon series made fun of icons of several major religions in a two-part story celebrating the program's 200th episode. "We were aware of the threat before it surfaced and took precautions to safeguard the offices of Comedy Central," the deputy

UNCLASSIFIED

UNCLASSIFIED

commissioner says. He declined to discuss the security measures in further detail or to disclose how NYPD managed to get advance warning that the cartoon and its producers were going to be threatened. A law-enforcement official who asked to remain unnamed due to the sensitivity of the information and private experts who monitor extremist Islamic Web sites say that there is no evidence that the Web site or its supporters have ever engaged in actual violence or have access to any weapons. "It's all talk," the law-enforcement official says. Nevertheless, law-enforcement agencies are concerned that the implied threats that the Web site posted condemning the latest South Park lampoon of Muhammad "might inspire someone else," says the official. Source: <http://blog.newsweek.com/blogs/declassified/archive/2010/04/23/security-stepped-up-at-comedy-central-following-threats-against-south-park.aspx>

(Washington) Full scale simulated terrorist event at the Sundome. Operation Eagle Eye is conducting a full scale exercise of a terrorist event at Yakima State Fair Park April 22. The exercise scenario is a simulated fictitious event at the Sundome. It deteriorates into a hazardous materials and hostage situation for responders to deal with. The exercise will involve about 60 volunteer from the community who will be playing roles. Organizers say they can not predict exactly how the event will play out because emergency responders have been asked to respond as if it was real. Source: <http://www.kndo.com/Global/story.asp?S=12357429>

COMMUNICATIONS SECTOR

Questions prompt strong defense of broadband program. A Democrat on the Senate Small Business Committee raised concerns on Tuesday that federal regulators are wasting taxpayer dollars by funding duplicative broadband infrastructure projects as part of the \$7.2 billion broadband stimulus program. A New Hampshire senator also pressed the heads of agencies within the Agriculture and Commerce departments on whether their awarding of grants to bring high-speed Internet service to certain parts of the country may have driven up commercial broadband deployment costs in some markets. An assistant commerce secretary who directs the National Telecommunications and Information Administration, responded by saying any claims that duplication exists are "not serious objections." The assistant commerce secretary said his agency uses data on broadband penetration and speeds when choosing where to allot money, arguing that the need for broadband spending may not be apparent in certain areas where consumers have strong Internet connections in their homes but anchor institutions, including hospitals and schools, continue to lack the necessary infrastructure. Source: http://www.nextgov.com/nextgov/ng_20100428_8219.php

FCC seeks information on survivability and security of nation's broadband nets. The Federal Communications Commission (FCC) is taking the first steps toward a proposed, voluntary security-certification program for service providers and a study of the survivability of the nation's broadband infrastructure, both of which were recommended in the National Broadband Plan. The commission April 22 approved notices of inquiry seeking comment on each of these programs. "As network attacks and the level of risks increase, it is beyond important that we fully understand the implications of this evolution in communications and that we take all necessary and appropriate steps to ensure the survivability of our voice and broadband communications networks," the FCC chairman said in announcing the inquiries. The FCC has not proposed any rules on broadband security and the inquiries do not involve proposals for mandatory programs. The goal is to encourage better security

UNCLASSIFIED

UNCLASSIFIED

practices and provide consumers with more information about the security status of service providers. Source: <http://gcn.com/articles/2010/04/22/fcc-inquiries-042210.aspx>

DEFENSE INDUSTRIAL BASE SECTOR

Future UAVs must multitask, Air Force says. The Defense Department is reassessing its view of unmanned aerial vehicles – a key component of modern combat operations – and deciding what the military needs from UAVs beyond their traditional use as a platform to gather intelligence and fire weapons. The next-generation UAVs will need to take on additional duties including cargo transport, refueling and possible medical applications, and they will need to be interoperable with different platforms, users and military services, DOD officials said at an Institute for Defense and Government Advancement summit on UAVs the week of April 26 in Vienna, Va. “UAVs are 99 percent [intelligence, surveillance and reconnaissance] today. In the future, they need to be multipurpose – ISR and [target acquisition], aerial network layer, attack capabilities, sustainment and cargo,” said the deputy director at the Army Unmanned Aerial Systems Center of Excellence. The military should concentrate on developing modular, plug-and-play aircraft built on standardized interfaces – one aircraft for multiple missions, similar frames for one platform, according to the director of the Air Force Unmanned Aerial Systems Task Force. “We need to define interoperable architecture. And right now we’re working with [the Office of the Secretary of Defense] to define what that interface will look like,” the director said. He added that capabilities for “sense-and-avoid” aircraft detection technology, interoperable command and control, multi-access controls and enhanced human-system interfaces are among the most important short-term enablers in developing next-generation UAVs. Source: <http://defensesystems.com/articles/2010/04/29/unmanned-aerial-vehicle-versatility.aspx?admgarea=DS>

Report says U.S. military vulnerable to bad parts. The U.S. Defense Department lacks sufficient quality-controls to prevent substandard parts from ending up in its weapons and other hardware, U.S. congressional auditors said on Thursday. “Existing procurement and quality-control practices used to identify deficient parts are limited in their ability to prevent and detect counterfeit parts in DoD’s supply chain,” the Government Accountability Office said in its report. It cited as an example what it described as substandard Global Positioning System oscillators used for navigation on more than 4,000 Air Force and Navy systems. Also cited were substandard titanium used in fighter jet engine mounts; brake shoes made from ersatz materials, including seaweed; and electronics from a personal computer repackaged and labeled as a \$7,000 military-grade circuit for a missile guidance system. It said counterfeit parts had the potential to cause a serious risk to military supply chains, delay wartime missions and impair weapon systems. GAO, Congress’s audit and investigative arm, said the Defense Department draws from a complex network of global suppliers and manages more than four million different parts at a cost of more than \$94 billion. It recommended the department step up its efforts to establish anti-counterfeiting guidelines for all Defense Department components and defense contractors. Source: <http://www.reuters.com/article/idUSN2911653820100429>

Sikorsky plans unmanned test for Black Hawk. The Army is collaborating with an aircraft maker to develop a UH-60 Black Hawk helicopter that can fly without a pilot. Sikorsky announced the project April 15 and plans to fly the aircraft later this year in two demonstrations, said the program manager for Sikorsky’s advanced programs. Plans for the first demonstration, scheduled for this summer, will have an unmanned Black Hawk with a safety pilot on board flying in formation with a manned Black

UNCLASSIFIED

UNCLASSIFIED

Hawk. Later in the year, the goal is to fly an unmanned cargo resupply mission with the aircraft. The Army is looking at aircraft that can go pilotless as one capability for the 2016 to 2035 time frame, according to the service's newly released unmanned-aircraft-systems road map. The intention is to increase reconnaissance coverage and support without increasing manned -light hours, according to the road map. Source: http://www.militarytimes.com/news/2010/04/army_black_hawk_042510w/

DOD can achieve better outcomes by standardizing the way manufacturing risks are managed. DOD faces problems in manufacturing weapon systems — systems cost far more and take much longer to build than estimated, according to a new study from the Government Accountability Office. The GAO found that billions of dollars in cost growth occur as programs transition from development to production, and unit-cost increases are common after production begins. Several factors contribute to these problems including inattention to manufacturing during planning and design, poor supplier management, and a deficit in manufacturing knowledge among the acquisition workforce, the study found. Essentially, programs did not identify and resolve manufacturing risks early in development, but carried risks into production where they emerged as significant problems, it continued. Manufacturing readiness levels (MRLs) have been proposed as new criteria for improving the way DOD identifies and manages manufacturing risks and readiness. A GAO analysis of DOD's technical reviews that assesses how programs are progressing show that MRLs address many gaps in core manufacturing-related areas, particularly during the early acquisition phases. Several Army and Air Force centers that piloted MRLs report these metrics contributed to substantial cost benefits on a variety of technologies and major defense acquisition programs, the government watchdog agency found. The commercial firms GAO visited use a disciplined, gated process that emphasizes manufacturing criteria early in development. The practices they employed focused on gathering sufficient knowledge about the producibility of their products to lower risks, and include stringent, manufacturing-readiness criteria to measure whether the product is sufficiently mature to move forward in development. A key difference is that commercial firms, prior to starting production, required their manufacturing processes to be in control — that is, critical processes are repeatable, sustainable, and consistently producing parts within the quality standards. Source: <http://www.gao.gov/products/GAO-10-439>

CRITICAL MANUFACTURING

Toyota recalling older Sequoia SUVs. Toyota, which has already recalled the Lexus GX 460 SUVs sold in the U.S. to fix a stability-control issue, is now recalling 50,000, 2003 Toyota Sequoias to address a stability issue. The recall comes a few weeks after the Lexus recall, but nearly a year and a half after the National Highway Traffic Safety Administration opened a probe, in response to 50 complaints, about unexpected braking. Toyota said the VSC system can help control a loss of traction in turns as a result of front or rear tire slippage during cornering. In vehicles without the upgrade, the VSC system could, in limited situations, activate at low speed for a few seconds after acceleration from a stopped position and, as a result, the vehicle may not accelerate as quickly as the driver expects. There have been no reported injuries or accidents as a result of this condition, according to Toyota. Toyota said it instituted a running production change during the 2003 model year and published a Technical Service Bulletin to address this issue when it was first identified in fall 2003. Since that time, Toyota said it has been responding to individual owner concerns by replacing the Skid Control Engine Control Unit (ECU) in Sequoias impacted by this condition. Of the approximately 50,000 vehicles included in this

UNCLASSIFIED

UNCLASSIFIED

recall, approximately half have already been serviced under warranty. Source:

http://www.consumeraffairs.com/news04/2010/04/toyota_sequoia_recall.html

Ford to recall 33,256 vehicles to fix seat fault. Ford Motor Co will recall 33,256 of its 2010 model year cars and SUVs to replace potentially faulty front seat recliner mechanisms that could lead to injuries in an accident, according to a notice filed with U.S. safety regulators. Ford notified the U.S. Highway Traffic Safety Administration of the potential defect by letter dated April 16. Ford said it knew of no reports of accidents or injuries due to the defect as of April 14. The automaker said it expects to begin notifying owners of the recall by letter on April 30. The recall covers some 2010 Ford Fusion and related Mercury Milan sedans built from December 11 through February 3 in Hermosillo, Mexico, and some 2010 Ford Explorer and Mercury Mountaineer SUVs built from December 15 through February 3 in Louisville, Kentucky. The recall notice was posted on the NHTSA website within the past day.

Source: <http://www.reuters.com/article/idUSTRE63M3YT20100423>

Report: FAA to require Boeing 737 inspections. A new federal directive will require Boeing to conduct speedy inspections to prevent potentially dangerous vibrations affecting certain flight-control surfaces on the tails of some of its 737 models, The Wall Street Journal reported Saturday. The Federal Aviation Administration was expected to issue a new safety directive as early as Monday that requires inspections of the mechanisms that control part of the elevators on about 125 of Boeing's aircraft, the report said. The inspections of the elevators, which help control a plane's pitch, must be completed in the next six to 30 days, depending on the age of the aircraft, the Journal said.

Source:

<http://www.reuters.com/article/idUSTRE63N1QC20100424?feedType=RSS&feedName=domesticNews>

EMERGENCY SERVICES

DOD civil support guidance outdated. The chairman of the House Homeland Security Committee Thursday released a pair of reports from the Government Accountability Office (GAO) that recommend the Department of Defense (DOD) make improvements in its homeland defense and civil support operations. "These complimentary GAO reports demonstrate that significant gaps still exist in these vital support missions. From outdated strategies to a lack of coordination with federal partners, GAO describes a number of challenges that must be addressed immediately by DOD and its federal partners," he said in a statement. The Homeland Security Committee held a hearing on response to threats posed by weapons of mass destruction earlier this month, highlighting the need for coordinated and well-planned homeland defense capabilities in response to a large-scale disaster. In the first report, Homeland Defense: DOD Needs to Take Actions to Enhance Interagency Coordination for Its Homeland Defense and Civil Support Missions, GAO recommended that the Defense Department update its guidance for working with other agencies and produce a guide for how agencies can work with it. The department also should improve its management of its liaisons with homeland defense and civil support authorities. The second report, Homeland Defense: DOD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters, recommended that the Defense Department update its civil support guidance, clearly define the roles and responsibilities of personnel who manage civilian requests for assistance, set up an official system for tracking civil support requests across the department, and assess the needs of staffing for its defense

UNCLASSIFIED

UNCLASSIFIED

coordinating officers, who manage assistance requests in the event of large-scale disasters. Source: <http://www.hstoday.us/content/view/13107/128/>

(Alabama) Bomb-like device used to attack Irondale policeman. Investigators are looking for a suspect they say tried to attack a police officer with a bomb-like device just before 7:00 at Colonial Village at Trussville Apartments in Irondale, Alabama. The officer was not hurt. The officer was sitting in his patrol car, which was parked in the apartment complex. He was working a security guard shift. At some point, a plastic bottle wrapped in aluminum foil was tossed at his car by someone on foot. The device hit the pavement next to the officer's car and exploded, sounding like a shotgun blast. The homemade device is described by authorities as dangerous and similar to a chemical bomb. The officer was not able to get a good look at the suspect as the person fled on foot. Police will take the device and process it for evidence. If the officer had his window down with the device landing inside his car, he could have been seriously hurt. The Bureau of Alcohol, Tobacco, Firearms and Explosives was asked to assist in the investigation. Source: <http://www.myfoxa.com/Global/story.asp?S=12402273>

(Texas) Federal agent impersonator indicted. A Lewisville, Texas man arrested by the Collin County Sheriff's Office for trying to pass himself off as a federal agent, received a multi-count indictment Thursday. The man received five, felony indictments from a Collin County grand jury on two counts of impersonating a public servant, two counts of unlawful possession of a firearm by a felon, and one count of tampering with a government record, according to court records. The man went to the Collin County Sheriff's Office's administrative building on Community Avenue in August 2009 and identified himself as a federal agent with U.S. "Homeland Security, Customs and Border Protection." He also presented credible-looking credentials to back up his claims. Even the clothes the man had on at the time seemed to indicate he worked for the government, a Collin County Sheriff's Office official said. The man's "credentials were very realistic, and the shirt was possibly an actual Customs issue — but an old version," the official said by e-mail. Source: http://www.lewisvilleleader.com/articles/2010/04/25/plano_star-courier/news/907.txt

Legislators unhappy with national, disaster plan. Even as forecasters are predicting a potentially fierce Atlantic hurricane season, the U.S. Federal Emergency Management Agency has gotten no further than finishing a draft of a national disaster recovery strategy, which officials released in February. Under the reform act, that plan was supposed to be finished within 270 days of its enactment in October 2006. Top Democrats and Republicans on the Senate's Homeland Security and Governmental Affairs Committee are not pleased, not only at the delay but also at what they found in the draft. In a joint letter of criticism, the senators charge the suggested plan is extremely fuzzy, ambiguous, full of holes, and unspecific about who would be in charge of what. FEMA says it has devoted substantial time and effort to reaching out to state, local, and federal agencies, as well as private organizations. The agency also received new directions for disaster recovery after the current administration took office, which presumably contributed to the delay. Source: <http://www.kypost.com/content/middleblue3/story/Disaster-Plan-Overdue/QOhSjLMwYUa6TpWUwyMFvA.csp>

UNCLASSIFIED

ENERGY

ESC: Smart grid faces security, consumer challenges. An array of hurdles ranging from making communications gear secure to understanding consumer behaviors stand in the way of flipping on smart electric grids, according to a panel of experts at the Embedded Systems Conference. “Going forward a myriad of issues need to be worked,” said the national coordinator for smart grid standards at the National Institute of Standards and Technology (NIST). “One area we do need more work in is dealing with electro-magnetic events” such as so-called suitcase nuclear bombs or solar storms, he said on the ESC panel. “The military has systems to deal with EM pulses but they are just not practical, so we do need better physical and electrical designs to deal with these effects,” he added. He and others expressed confidence engineers are adequately focused on making the future digital, networked electric grid secure. “The problem I see is not in designing the products, but the operations practices — that’s where the gap is,” he said. Source:

<http://www.eetimes.com/news/semi/showArticle.jhtml?articleID=224700267>

(West Virginia) Gas still keeping investigators out of W.Va. mine. High levels of two, potentially explosive gases have been detected inside the Upper Big Branch mine, and investigators now say it could be a month before they can get inside to determine what caused an explosion that killed 29 workers. Neither ethylene nor acetylene is normally present in underground air, a federal Mine Safety and Health Administration spokeswoman said Friday. However, she said it is not unusual to find them after an explosion. The source is unclear, she said, noting, that it could mean a fire is burning somewhere inside the Massey Energy mine in Montcoal, West Virginia. State and federal investigators met Friday and will begin work on a plan to diffuse the gases. However, it may be another month before teams can enter the mine, said a spokeswoman for the state Office of Miners’ Health Safety and Training. Once state and federal teams devise a re-entry plan, they will present it to Massey. The prospect of a fire was first raised during the search and rescue operation that lasted several days after the April 5 explosion. Source: <http://www.washingtonexaminer.com/breaking/gas-still-keeping-investigators-out-of-wva-coal-mine-where-explosion-killed-29-workers-91924009.html>

FOOD AND AGRICULTURE

Walmart to test for Non-O157 E. coli. Retail giant Walmart announced April 29 it will require additional food safety measures from its beef suppliers, including specialized testing for dangerous pathogens like E. coli O157:57 and Salmonella — as well as non-O157 strains of E. coli, strains that are not currently defined by the U.S. Department of Agriculture (USDA) as adulterants. “In light of recent beef recalls, we determined it was prudent to require an additional layer of protection for our customers,” Walmart’s vice president for food safety said in a statement. A managing partner of Marler Clark, a food-safety litigation firm, said he would soon publish results of a 5,000-sample test for non-O157 strains in grocery-store meat that his firm sponsored. According to Walmart, suppliers who do not operate slaughterhouses must be in compliance with the new standard by June 2011. For beef slaughterhouse suppliers, there is a two-step approach with the first step to be completed by June 2011 and the second by June 2012. The new policy — which will also apply to meat sold to Sam’s Club — has been reviewed by consumer groups, regulators, academics, beef suppliers, and industry associations, and the company is making it clear that it will be implemented without

UNCLASSIFIED

additional costs to consumers. Source: <http://www.foodsafetynews.com/2010/04/wal-mart-boosts-beef-safety-with-non-o157-ecoli-testing/>

FDA takes steps to increase safety of foods during transport. The U.S. Food and Drug Administration wants commercial food transporters to follow new guidance to reduce the chances of physical, chemical, biological and other risks during transportation of foods while the agency reviews current food-safety transportation regulations. In an advance notice of proposed rulemaking (ANPRM) published in the April 30 Federal Register, the FDA has requested input on writing the new rules from all interested parties, including the food and transportation industries and consumer-interest organizations. The ANPRM is the first step in creating new regulations to govern sanitary practices by shippers, carriers by motor vehicle or rail vehicle, receivers, and others engaged in the transportation of food products for people and animals. The new industry guidance covers safety measures that should be employed while the regulations are being written and finalized. They include ensuring that food in transit is maintained at appropriate temperatures; that such food is closely monitored for pests; that the vehicles used to transport foods are sanitary and in proper working condition; that pallets used are of good quality; and that sanitary measures are followed in the loading and unloading of foods. “Our aim is to look at every component of the system to assess hazards, and to take science-based action where appropriate to maximize the safety of our food from farms all the way to consumers’ tables,” said FDA’s associate commissioner for food protection. “Although contamination of food product during commercial transport is relatively infrequent, the potential harm can be widespread and serious.” After evaluating comments received in response to the ANPRM, the FDA will propose specific regulations. The FDA will coordinate with the U.S. departments of Agriculture and Transportation in the rulemaking process. Source: <http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm210265.htm>

Two mixes added to HVP recall list. MiDAS Foods International has announced a recall of its Instant Beef Soup dry mix and Instant Beef Stroganoff sauce mix because they may contain salmonella-contaminated, hydrolyzed vegetable protein (HVP). Oak Park, Michigan-based MiDAS said it learned from a vendor that a flavor it was using in its soup mix contained the HVP produced and recalled by Basic Food Flavors in North Las Vegas. In a statement, MiDAS said testing of the flavor by an independent lab was negative for salmonella, but the company was proceeding with its own recall notice “for precautionary food-safety reasons.” The dry soup and dry sauce mixes were distributed to food-service establishments in Florida and Tennessee. Retailers sold none. No illnesses have been associated with this or previous, HVP-related recalls. The salmonella problem with HVP at Basic Food Flavors dates back to September 17, 2009. The company said the contamination was limited to a single, 10,000-pound lot. Food and Drug Administration (FDA) investigators in February found salmonella inside the North Las Vegas facility and production was halted for a time. Source: <http://www.foodsafetynews.com/2010/04/two-mixes-added-to-hvp-recall-list/>

Dying honeybee population threatens U.S. agriculture. A Pennsylvania bee expert is warning of a nationwide honeybee crisis after a survey released April 29 revealed that one-third of commercial beekeepers’ colonies died over the winter, the fourth consecutive year that’s happened. “These numbers are all indicators that a crisis is coming. It will reach a perfect storm, the way the credit crisis did,” said Pennsylvania Department of Agriculture bee researcher. Nearly 34 percent of the country’s managed honeybee colonies were lost over the winter, according to the survey of 4,331 beekeepers conducted by the Apiary Inspectors of America, and the Agricultural Research Service. That figure

UNCLASSIFIED

UNCLASSIFIED

compares to losses of 29 percent in 2008-09, 35.8 percent in 2007-08 and 31.8 percent in 2006-07. Honeybees are used to pollinate everything from apples to pumpkins to blueberries and add \$15 billion each year to agricultural output in the United States, according to the USDA. Crop production could be at risk if honeybees are found in increasingly short supply and if cash-strapped beekeepers leave the business, which some insist they might be forced to do. "All told, the rate of loss experienced by the industry is unsustainable," the survey stated. Not all of the losses stemmed from colony collapse disorder, a syndrome identified three years ago that is characterized by the death of an entire bee colony, the Pennsylvania bee researcher said. Bees also are under great threat from a variety of mites and viruses, and also from poor nutrition. The impact of pesticides on honeybees also is under increasing scrutiny. Source:

http://www.pittsburghlive.com/x/pittsburghtrib/news/breaking/s_678719.html

Stung by fraudsters, honey execs hold secret talks. For the nation's leading honey packers and sellers, smuggled and laundered foreign honey presents a vexingly sticky problem. Monday, they gathered for a secret meeting convened by the National Honey Packers & Dealers Association to discuss the impact it is having on their businesses. The meeting comes as federal investigators and the offices of the U.S. attorney in at least four states continue to hone in on packing companies, honey brokers and importers allegedly involved in facilitating or purchasing intentionally mislabeled or bogus honey. The crime, which some major suppliers say may involve 50 percent or more of all imported honey, is carried out by foreign hucksters and shady importers who take cheap but abundant Chinese honey, move it to a country with a reputation for a quality product, change the country of origin on the shipping papers, then market the bogus load to brokers in the U.S. Importers charge that most of the Chinese honey is adulterated, containing traces of an illegal, animal antibiotic called chloramphenicol. This drug, purchased from India, was first used years ago to stem an epidemic of disease that was laying waste to most of China's bee colonies. While chloramphenicol (CAP) is not harmful to most who consume the small amount in contaminated honey, some people can become seriously ill from any amount of the drug, and the Food and Drug Administration (FDA) has banned it from all food products. Source: <http://www.aolnews.com/crime/article/stung-by-chinese-fraudsters-honey-exec-hold-secret-talks/19454876>

(Michigan) Investigation food-borne illness outbreaks is expensive. Investigating the 13 Michigan cases in a recent outbreak from contaminated raw milk, and identifying the source of the infection, cost about \$22,500, according to experts at the Food Poison Journal. The breakdown consisted of \$1,697 in lab costs for personnel and supplies, \$12,201 for follow-up at the state level, and \$8,600 for Michigan Department of Agriculture personnel costs, the magazine said. This was a relatively small-scale outbreak that, fortunately, did not sicken too many people. Also, the epidemiological circumstances were fairly clear from the start, as health officials investigating outbreaks of E. coli, campylobacter, and salmonella routinely ask about raw-milk consumption for all such illnesses in initial interviews with the sick people. Thus, in this outbreak, health officials were probably able to hone in on the Family Farms Cooperative raw milk product early on in their investigation, thus eliminating lots of costs that are frequently associated with investigations of food-poisoning or "milk-poisoning" illnesses, the journal noted. Nonetheless, the costs attributable to the investigation of this outbreak are part and parcel of a problem — i.e. food- and milk-poisoning generally — that costs the U.S. an estimated \$152 billion annually. In addition to the personal-injury lawsuits that arise from such outbreaks, should state and local health officials seek reimbursement of the costs associated with food, water, and milk-poisoning? Why not? Sometimes, no injury claims emerge from outbreaks,

UNCLASSIFIED

UNCLASSIFIED

even when a specific food or milk product is conclusively identified as the outbreak vehicle. In those cases, what other mechanism is there to force accountability upon the manufacturers of the contaminated products? Source: <http://www.foodpoisonjournal.com/2010/04/articles/foodborne-illness-outbreaks/raw-milk-outbreak-investigation-costs/>

(California) Grape moth causes Napa County quarantine. A tiny grapevine moth, a light green or brown pest smaller than a fingernail, is threatening 219 square miles of the most valuable farmland in California, home to award-winning, three-digit Napa Valley Cabernet Sauvignon. The European grapevine moth, or *Lobesia botrana*, was first spotted in the Oakville area in September, during the 2009 harvest. Because of its proliferation, the federal government put the entire Napa Valley under quarantine as of April 21, said the county's public information officer. The area, stretching from the county line north to Calistoga, has dealt with pests in the past. What makes this moth particularly pesky is that it undergoes three generations. It is during the second flight — in the summer — that serious damage occurs and mating begins, so county officials anxiously await insecticides that will halt mating and eradicate the moths before the most damaging third generation, when they web and feed inside berries. If the pest isn't contained before September, when harvest begins, growers and wineries may suffer devastating losses. It costs at least \$6,000 to farm an acre of vines in the wine region, said the vineyard manager for Napa's Clos Du Val winery and former president of the Napa Valley Farm Bureau. "If this guy gets in the early season of the flower, the larvae grows inside the grape," he said. "So when you squeeze the grape, a worm comes out." So far, the state department of food and agriculture has captured moths from Calistoga to Carneros by setting up 25 traps per square mile, said the executive director of the Napa Valley Grapegrowers. Source: http://www.mercurynews.com/travel/ci_14939917

Salmonella outbreak traced to raw tuna. The Hawaii State Department of Health announced yesterday that it has confirmed 10 cases of *Salmonella Paratyphi B* infection related to the consumption of previously frozen internationally imported raw ahi tuna at various locations on Oahu. According to the Hawaiian Health Department, at least 13 laboratory-confirmed *S. Paratyphi B* cases have been reported in five other states: California (7), Maryland (2), Pennsylvania (2), Massachusetts (1), and New York (1). Public health agencies in all states are working with the Centers for Disease Control and Prevention (CDC) to determine whether all ill individuals were exposed to raw ahi prior to becoming ill with salmonellosis. "The Department of Health is concerned about these cases that are similar to a cluster of cases we investigated two years ago," said Hawaii's health director. "With the help of the [U.S. Food and Drug Administration], we hope to identify the source so we can prevent any further illness." The Hawaii health department investigated a similar salmonella outbreak in between October 2007 and February 2008. Source: <http://www.foodsafetynews.com/2010/04/salmonella-outbreak-traced-to-raw-tuna/>

(Michigan) State will test cattle for TB. After discovering a free-ranging deer infected with bovine tuberculosis in southeaster Cheboygan County, Michigan Department of Agriculture (MDA) officials are making plans to test cattle and bison in the area where the deer was taken. The MDA has designated a Potential High Risk Area within a 10-mile radius of the location where the deer was discovered. Officials have identified 15 cattle and bison farms within the Potential High Risk Area that require testing for bovine TB within six months of the official designation. These farms have been notified by telephone and will receive notice in the mail. Source: <http://www.cheboygannews.com/news/x932352238/State-will-test-cattle-for-TB>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Texas) Texas ‘terrorist’ posts death threat against Obama. A Dallas man describing himself as a terrorist threatened to kill the U.S. President in an online posting because he was upset about health care reform, according to a criminal complaint. The 43-year-old faces one count of making threats against the president. He made the death threats March 21 on Craigslist under a posting titled “Obama must die.” The posting said he was following through on a promise to become a terrorist if the federal health care bill passed. “I am dedicating my life to the death of Obama and every employee of the federal government,” the posting said. It ended with a call to arms: “This is war. Join me. Or don’t. I don’t care. I’m not laying down anymore.” He said, “Today I become a terrorist.” In a separate post the same night, he essentially dared others to turn him in to the Secret Service. A resident of Arlington, Texas reported the threats to the Secret Service. Agents tracked down the suspect at his Dallas home, where he lives with his mother. Police arrested him and seized his computer. They found no weapons in the residence. Source:

http://www.google.com/hostednews/ap/article/ALeqM5hfnLVdpsv5FulQzy-0zUNd_fdUugD9FCSEL01

(Texas) Texas Digest: Capitol security tapes confidential, court rules. A Texas publication is not entitled to videotapes recorded from security cameras at the Capitol, the 3rd Court of Appeals ruled Thursday. The Texas Observer had requested the recordings, made during the 2005 legislative session, to determine whether prominent Republican campaign donor pressed lawmakers to pass a school voucher pilot program while standing outside the House chamber. Lobbying in that area is against House rules. In a 3-0 opinion, the appeals court said the images are exempt from open records laws, which allow government agencies to withhold information relating to the specifications of security systems. Viewing DVD copies of the security tapes, the court reasoned, would reveal the Capitol security system’s capabilities, such as the quality and clarity of images. The state attorney general’s office had said the tapes should be released because their contents had nothing to do with security, but the Department of Public Safety fought the release, arguing that the information could compromise safety at the Capitol. Source: <http://www.statesman.com/news/texas-politics/texas-digest-capitol-security-tapes-confidential-court-rules-647855.html>

(Massachusetts) 6 charged with making bomb threats in Wareham. Six separate bomb scares in Wareham, Massachusetts public schools over the last several weeks have resulted in charges against six people, five of whom are younger than 18. The Wareham Fire Department responded to two separate calls about bomb threats Tuesday and Wednesday at Wareham Middle School. On Tuesday, a handwritten note was found on the wall of a bathroom at the middle school. On Wednesday, two more threats were found in a bathroom. Both times the school was evacuated while the building was combed for bombs. Three people who are younger than 18 were charged with making false bomb threats and disturbing school assembly. On April 14, another juvenile was charged with making a false bomb threat after a bomb scare at the Decas School. The day before, an 18 year-old student was charged with making a false bomb threat after a note was found in the hallway of Wareham High School. Another person under 18 was charged in a separate incident March 25 at the Minot Forest School, when a bomb threat in note form was found in the bathroom. The Wareham Fire Department is still investigating an April 6 bomb threat at the Wareham Middle School. Making a false bomb threat is a felony that carries a penalty of up to 20 years in state prison. Source:

UNCLASSIFIED

<http://www.enterpriseneews.com/news/x457997384/Six-charged-with-making-bomb-threats-in-Wareham>

(Kansas) Woman arrested after making 9 bomb threats. Wichita, Kansas police have arrested a woman they said called in numerous bomb threats to a school. The most recent was Tuesday, April 27 when Payne Elementary School officials reported receiving a call from a woman saying there was a bomb inside the school set to blow up. Parents said they have been concerned over the past few weeks. After bomb scare number eight was called into the school, police investigators were waiting at the school to try and catch the suspect. It turned out that the 27-year-old suspect had a child at the school. She is now under arrest after police said they found her near the school ... watching the police response to the bomb threat. Parents said they can now breathe easier. The suspect was expected to be formally charged Thursday. The school was evacuated after each threat except for Tuesday, and no bombs were ever found. No motive has been released by police. Source:

<http://www.ksn.com/mostpopular/story/WPD-Woman-arrested-after-making-nine-bomb-threats/gBIVP9exx0C7XsPgnO8FIA.csp>

(Washington) Pipe bomb found at Rainier View Elementary in Federal Way. A suspicious object found at the Rainier View Elementary School playground in Washington Monday turned out to be a six-inch pipe bomb, according to a King County sheriff's spokesman. The pipe bomb was found during morning recess. The school was put into lockdown at 10:20 a.m. and the lockdown was lifted at 12:22 p.m. The King County Sheriff's Department was called to the school at 3015 S. 368th St. in unincorporated King County. The bomb squad came in and picked up the bomb. Students and staff were all safe. Shortly after the all clear was given Monday at Rainier View, a bomb threat was reported at Todd Beamer High School at 35999 16th Ave. S. The school was evacuated. Police inspected the school and found nothing suspicious. Staff and students were able to return to the school at 1:30 p.m. Federal Way Police are continuing to investigate the threat, which came from a phone call. Source: http://www.pnwlocalnews.com/south_king/fwm/news/92115179.html

(California) Bomb threat sparks search on UOP campus. A bomb threat against the University of the Pacific in Stockton, California sparked a search by authorities Sunday, but investigators have since issued the all-clear. The Stockton Police Department said they received the threat by phone from an unidentified individual claiming that an explosive device had been placed on campus and was set to detonate at 10 p.m. Sunday. Stockton authorities notified the UOP Police Department, who sent an e-mail to students to be alert for any suspicious objects or activities. Authorities searched through the buildings but did not evacuate the campus. Some students left campus as a precaution, while others gathered at the baseball field to watch television on the big screen. No explosions were reported and police issued the all-clear after searching the university's buildings. Police have not released any information on potential suspects in the incident. Source:

<http://cbs13.com/local/uop.bomb.threat.2.1655996.html>

(North Carolina) Ohio man arrested with gun near Air Force One. A Coshocton, Ohio, man was arrested in Asheville, North Carolina, after authorities said he was carrying a firearm near Air Force One, which was transporting the U.S. President to Beckley for the miner's memorial April 25. The 23-year-old suspect was arrested and charged with going armed to the terror of the public. According to the Asheville Regional Airport Police, the suspect pulled into the airport rental car return parking lot in a Pontiac Grand Prix with Ohio plates. Police said the vehicle was equipped with LED law-

UNCLASSIFIED

UNCLASSIFIED

enforcement style lights in the front and rear, as well as a mounted digital camera and four large antennas on the trunk lid. According to the release, the suspect appeared to be listening to a radio/hand-held scanner when he exited the vehicle. Officers approached the suspect and removed his firearm. Police said he told them he heard the President was in town and he wanted to see him. Police said there was a siren box located under the dash of the vehicle and a note with rifle-scope formulas in the cup holder. Source: <http://www.wtrf.com/story.cfm?func=viewstory&storyid=78869>

(Nevada) Security boulders put up to guard Nevada Capitol. Nevada officials said boulders recently placed on sidewalks at entrances to the state capitol grounds were put there to improve security following a March 29 letter warning that the Nevada governor and other governors around the nation would “be removed” if they did not resign. “We needed to act quickly,” said the governor’s deputy chief of staff. “The rocks will sit there for now, while we decide what to do next.” In addition to the boulders to keep vehicles from the capitol grounds, a metal detector was installed at the capitol’s main entrance. All side entrances were closed, and employees and visitors must enter and exit through the front doors. No other governor had a similar reaction to the letter from Guardians of the Free Republics, according to news accounts. And new precautions weren’t put in place at the nearby state supreme court, legislative building or attorney general’s office. Source: <http://www.rgi.com/article/20100426/NEWS/4260326/1321/Security-boulders-guard-Nevada-Capitol>

Survey: 45 percent of local governments use cloud computing. Local government officials’ trepidation about cloud computing could be easing, as evidenced by a survey of IT decision-makers released April 20, that found 45 percent of local governments are using some form of cloud computing for applications or services. The survey, conducted during the first two weeks of April by the nonprofit Public Technology Institute (PTI), aggregated the opinions of 93 local, government IT executives. The findings revealed that an additional 19 percent of local governments plan to implement some form of cloud computing within the next 12 months, while 35 percent don’t intend to do so at all. Most public-sector CIOs are still reluctant to put critical data in public clouds because of security concerns, said PTI’s executive director, and some jurisdictions are limited by statutes that restrict where and how data is stored. Source: <http://www.govtech.com/gt/articles/755798>

Federal cybersecurity monitoring goes real-time and digital. Federal agencies soon will be required to digitally monitor the security of their computer systems and feed summaries of their findings to a central Web site under new, federal information security rules the White House issued Wednesday. The continuous reporting requirements outlined in an Office of Management and Budget memorandum are intended to improve the execution of the 2002 Federal Information Security Management Act. Critics said FISMA demands too much burdensome reporting and takes attention away from security. Several lawmakers are pushing to update the law, but for the time being the White House is working within the confines of the statute to alleviate reporting hassles. “We’re automating the process,” said the White House Cybersecurity Coordinator, noting that reports to the Office of Management and Budget and Congress will be “based on real-time information as opposed to a snapshot in time.” The key to this new approach will be software that transmits data on the status of controls directly from each division of an agency. The data feeds will include information about an agency’s inventory of systems and software, external connections, security training and user access. Source: http://www.nextgov.com/nextgov/ng_20100421_5175.php

UNCLASSIFIED

UNCLASSIFIED

Are cyberattacks coming from Brazil? Although most of the government-targeted cyberattacks that occurred last year were launched from China, targeted Chinese cyberattacks were actually less likely to be directed at governments than those launched from Brazil, said a cybersecurity analyst. In fact, less than a quarter of cyberattacks launched from China in 2009 specifically targeted governments, said the director of the Global Intelligence Network, which tracks worldwide Internet threat data for security software developer Symantec. In contrast, 48 percent of targeted cyberattacks launched from Brazil were directed at governments, he said, citing a private Symantec report on government Internet security. But the director cautioned that in the murky world of hacking, attackers hide their tracks easily, making it difficult to name the culprit. According to a summary of the report, the United States was the country most frequently targeted by denial-of-service attacks — accounting for 56 percent of the worldwide total. Source:

http://cybersecurityreport.nextgov.com/2010/04/cyberattacks_from_brazil.php

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Microsoft SharePoint bug exposes credentials, sensitive data. Microsoft says it's investigating a security flaw in older versions of its SharePoint Server product that an independent researcher says can easily expose sensitive data and user authentication credentials. The XSS, or cross-site scripting, vulnerability has been confirmed in SharePoint Server 2007 and is likely also present in earlier versions of the content management system software, an advisory from High-Tech Bridge warned. It allows adversaries to inject malicious javascript into the application by appending commands to the address of the targeted system. "The vulnerability exists due to failure in the '/_layouts/help.aspx' script to properly sanitize user-supplied input in 'cid0' variable," the advisory states. "Successful exploitation of this vulnerability could result in a compromise of the application, theft of cookie-based authentication credentials, disclosure or modification of sensitive data." A Microsoft spokeswoman said on April 29 that researchers are in the process of drafting a security advisory that includes mitigation and workaround details. With 17 days notice, it's unclear why Redmond's security team did not already have that information ready to go. Source:

http://www.theregister.co.uk/2010/04/29/microsoft_sharepoint_security_bug/

Easy-to-get Web certs undermine online trust. "Get ready a credit card and a free Web mail account that is registered as 'ssladmin.' Go to a certificate authority (CA), such as VeriSign's RapidSSL. Now, register online for a secure Web certificate for a domain that may not necessarily be owned by the registrant." This simple process of attaining a legitimate Web security certificate is a security flaw made known and described in detail by a security expert in a March report on blog site Betanews. It is not a new security concern, either, according to a strategic solutions consultant at RSA, the security division of EMC. In an e-mail interview with ZDNet Asia, he said this is a "well-recognized problem" that security practitioners have known for a "fairly long time". "The commercial pressures [faced by CAs] led some of these companies to introduce 'domain validated (DV) only' SSL certificates, for which minimal verification is made of the details in the certificate," the consultant elaborated. Another industry player gave further insight into the CA industry. Source:

<http://www.zdnetasia.com/easy-to-get-web-certs-undermine-online-trust-62062987.htm>

Microsoft reissues Windows 2000 Server security fix. On April 28, Microsoft released an updated critical fix for Windows Media Services on Windows 2000 Server. The revamped bulletin, MS10-025, addresses a "privately disclosed" bug that could enable remote code execution attacks. The bulletin

UNCLASSIFIED

UNCLASSIFIED

was reissued less than a week after Microsoft pulled the initial fix from its April monthly security-patch rollout. Microsoft explained at that time that the fix did not “address the underlying issue effectively.” The company added that it was not aware of active attacks seeking to exploit the vulnerability. Some security experts believe that Microsoft recently received private, third-party reports that the patch did not correctly address the vulnerability and therefore pulled it for a reconfiguration last week. For its part, Microsoft said that the new update remedies the remote code execution exploit, which takes advantage of stack overflow in Windows Media Services. Windows Media Services is an option in Windows Server 2000 that supports streaming media applications. Source: <http://gcn.com/articles/2010/04/28/microsoft-reissues-windows-2000-server-security-fix.aspx>

India now the primary producer of viruses. India has pushed Korea into second place and taken over the mantle of the world’s largest producer of Internet viruses, according to analysis of Internet threats in April by Network Box. India now accounts for just under 10 percent of the world’s viruses, ahead of Korea at 8.24 per cent and the U.S. at 6.7 percent. India is also becoming a more dominant force in spam production and intrusions: 7.4 percent of the world’s spam now originates from India; and the country is responsible for 8.6 percent of intrusions. This trails the U.S., which still produces more spam than any other country (11.9 percent). It was revealed earlier in the month that computer networks in India were compromised by Chinese hackers using social networking sites to compromise computers in India, and also attack the India High Commission in the UK. Source: http://www.net-security.org/malware_news.php?id=1320

Russia dominating automated-malware kit market. Russia is dominating the market for automated malware creation kits that are sold online to phishers and data thieves. A new report from M86 Security, entitled “Web Exploits: There’s an App for That,” found that the majority of new malware-creation kits, such as Adpack and Fragus, are being sold in Russia. The company had seen a big increase in the size and complexity of such kits, and said that more than a dozen had launched in the past six months. “People can launch attacks without even knowing a line of code, and the infrastructure now exists to pay the attacker per exploit achieved,” said the vice president of technology strategy at M86 Security. “With an attack kit, there is literally ‘an app for that’ and it is driving the explosive growth in Internet-borne threats such as spam and zero-day attacks with new kits popping up every day.” Software to automatically generate malware has been around for some years, but has now evolved into a complex business. Some kits just offer code generation, while others sell full-service packages that update the creation engine to keep ahead of security companies. The report also found a thriving trade in third-party payments, where attackers receive a commission based on the amount of third-party malware installed on a victim’s system. Source: <http://www.v3.co.uk/v3/news/2262206/russia-dominating-automated>

New twist on old scam defrauds Facebook users. A new phishing fraud is a frenzy on Facebook. Thousands of folks have fallen victim to an old scam with a new twist. The Colorado attorney general wants to change Facebook liability rules. “This is the very first time I have seen it but I am not surprised,” the CEO of Vertical IT Solutions in Tampa, Florida said. The CEO was an intended target himself. He got an e-mail from what he thought was Facebook. It asked him to “reset his password” by clicking on an attachment. But being an Internet-security expert, he knew better. “No organization can send you an e-mail requesting you to change your password. No organization does that,” he said. He said that this policy was put in place after the Bank of America phishing scam that hit thousands of

UNCLASSIFIED

UNCLASSIFIED

Americans last year. That scam was a more direct route to get to people's personal information, like passwords, account information and ultimately money. This Facebook scam is a more roundabout route but still effective, since most people tend to use the same password for everything. "Spoofing Facebook and having them capture that confidential information, I mean, it is ingenious," the CEO said. Source: <http://www.9news.com/money/consumer/article.aspx?storyid=137672&catid=103>

Costs of data breaches much higher in U.S. than in other countries, study says. A data breach in the United States could cost enterprises twice as much as the same breach costs companies in other countries with less stringent disclosure and notification laws, according to a study published April 28. The study, conducted by the Ponemon Institute and sponsored by security vendor PGP, is an extension of the companies' previous cost-of-breach research that examined regional differences in the costs inflicted by compromises of enterprise data. In a nutshell, the study finds breaches are much more expensive in countries that have stringent regulations than in countries that do not. "The overarching conclusion from this study is the staggering impact that regulation has on escalating the cost of a data breach," said the chairman and founder of The Ponemon Institute. "The U.S. figures are testament to this, and it is clear that as breach-notification laws are introduced across the rest of the world, other countries will follow the same pattern, and costs will rise." The study examined breach costs in five countries: the United States, the United Kingdom, Germany, France, and Australia. In the U.S., where 46 states have introduced laws forcing organizations to publicly disclose the details of breach incidents, the cost per lost record was 43 percent higher than the global average. In Germany, where equivalent laws were passed July 2009, costs were second highest — 25 percent above the world-wide average. In Australia, France, and the U.K., where data-breach notification laws have not yet been introduced, costs were all below the average. Source: http://www.darkreading.com/vulnerability_management/security/management/showArticle.jhtml?articleID=224700013

Qakbot worm steals 2 GB of confidential data per week, researchers say. An emerging worm is turning up more frequently in enterprises across the Web, and researchers now estimate that the malware is stealing as much as 2 GB of confidential data per week. According to a report by Symantec's security research team, the W32.Qakbot worm continues to pick up steam, infecting large batches of business computers as well as home users. More than 1,100 computers at the U.K.'s National Health Service are among the enterprise victims, according to news reports. "One unusual aspect of Qakbot is that even though its purpose is to steal information associated with home users, it has also been successful at compromising computers in corporate environments as well as government departments," Symantec said. The research also found more than 100 compromised computers on a Brazilian regional government network. "Whoever is behind Qakbot has not put much effort into securing the stolen information," Symantec reported. "Anyone with a sample of this threat who knows what they are doing will be able to access this data quite easily," it continued. "At the time of this writing, we have only observed Qakbot stealing consumer-based information. But since Qakbot also functions as a downloader, corporate environments compromised by Qakbot could find themselves defending a more serious attack if appropriate action is not taken now." Source: http://www.darkreading.com/vulnerability_management/security/antivirus/showArticle.jhtml?articleID=224600309

Microsoft admits MS10-025 patch didn't fix vulnerability. Microsoft has yanked security updates shipped in the MS10-025 bulletin after realizing the patch did not fix the underlying security

UNCLASSIFIED

UNCLASSIFIED

vulnerability. The withdrawal of the bulletin means that affected Windows 2000 Server users should immediately consider applying mitigations and workarounds to avoid malicious hacker attacks. The company did not explain why the bulletin was shipped with an inadequate patch. The issue only affects Windows 2000 Server customers who have installed Windows Media Services (a non-default configuration). A Microsoft spokesman urged affected users with Internet facing systems with Windows Media Services installed to evaluate and use firewall best practices to limit their overall exposure. The MS10-025 bulletin is rated "critical" because attackers could launch remote code execution if an attacker sent a specially crafted transport information packet to a Microsoft Windows 2000 Server system running Windows Media Services. Source:

<http://blogs.zdnet.com/security/?p=6298>

Twitter issues alert about phishing scam. Twitter issued a warning April 23 about phishing e-mails that tell users they have unread messages on the micro-blogging site. The e-mails, coming from a support@twitter.com e-mail address, tell members they have unread, delayed, or undelivered messages, and ask them to click a link in the e-mail to view the mystery messages. Twitter denied sending out the e-mails. The e-mail itself does not appear to contain malware, Twitter said. The link in the e-mail actually takes users to a pharmaceutical site, though to get to that site, users are re-routed through several other sites, which could contain malware. "We're actively pursuing measures to get these sites shut down; in the meantime, we recommend that you not click on the link and instead just delete any such e-mails you receive," Twitter said. Source:

<http://www.pcmag.com/article2/0,2817,2363006,00.asp>

Backdoor malware targets Apple iPad. Apple iPad users are being warned of an email-borne threat which could give hackers unauthorized access to the device. The technology writer for anti-virus firm BitDefender, wrote in a blog post Monday that the threat arrives via an unsolicited e-mail urging the recipient to download the latest version of iTunes as a prelude to updating their iPad software. "A direct link to the download location is conveniently provided. As a proof of cyber-crime finesse, the Web page the users are directed to is a perfect imitation of the one they would use for legitimate iTunes software downloads," the writer said. "Unfortunately for these users, following the malicious link means opening up a direct line to their sensitive data, as instead of the promised iTunes update they get malware on their systems." The Backdoor.Bifrose.AADY malware opens up a back door which could let the perpetrator gain unauthorized access to the device, warned the technology writer. It also tries to read the keys and serial numbers of the software installed on the device, and logs the passwords to any Webmail, IM or protected storage accounts. Source:

<http://www.v3.co.uk/v3/news/2261993/malware-targets-ipads>

Crippling McAfee virus update could have long-term fallout. As organizations worldwide scramble to restore their Windows XP S3 machines from crashes or repeated reboots due to a faulty virus definition update issued by McAfee Thursday, some security experts worry that additional machines could be affected weeks or months from now. McAfee has apologized publicly for pushing the defective 5958 virus definition file, which caused some Windows XP Service Pack 3 systems to crash or continuously reboot; the company said less than 1 percent of its enterprise customers were affected. The faulty update, which passed McAfee's quality assurance testing process, generated a "false positive," the company said, incorrectly detecting and quarantining XP S3's svchost.exe as a virus. According to a FAQ issued to McAfee corporate customers today, the company did not include XP SP3 with VSE 8.7 in its testing, resulting in "inadequate coverage of Product and Operating System

UNCLASSIFIED

UNCLASSIFIED

combinations in the test systems used.” The faulty AV update was removed from McAfee’s download servers, and a new version has been released. But there are still plenty of unanswered questions about the error — what exactly went wrong in McAfee’s quality assurance testing process, why McAfee was not testing sufficiently for the pervasive XP SP3 configuration, and what happens to XP SP3 machines that have not yet been affected by the bad update, but could be later. “It could have been anything from sabotage to just carelessness,” said a security expert. “What scares me a little is haven’t they tried this in a test environment before launching? And if they did, they have a serious problem on how they test their products.” Organizations that do not apply the replacement DAT file McAfee issued could end up suffering crashes and repeated reboots. “Those customers should exclude svchost.exe from being scanned until they can apply the appropriate McAfee DAT file, which is now available,” the CTO at BigFix and the former director of engineering at McAfee who helped develop the AV company’s DAT testing process said. Source:

http://www.darkreading.com/vulnerability_management/security/client/showArticle.ihtml?articleID=224600179

1.5 million stolen Facebook IDs up for sale. A hacker named Kirillos has a rare deal for anyone who wants to spam, steal or scam on Facebook: an unprecedented number of user accounts offered at rock-bottom prices. Researchers at VeriSign’s iDefense group recently spotted Kirillos selling Facebook user names and passwords in an underground hacker forum, but what really caught their attention was the volume of credentials he had for sale: 1.5 million accounts. IDefense does not know if Kirillos’ accounts are legitimate, and Facebook did not respond to messages April 22 seeking comment. If the accounts are legitimate, the hacker has data on about one in every 300 Facebook users. His asking price varies from \$25 to \$45 per 1,000 accounts, depending on the number of contacts each user has. To date, Kirillos seems to have sold close to 700,000 accounts, according to the VeriSign director of cyber intelligence. Hackers have been selling stolen social-networking credentials for a while — VeriSign has seen a brisk trade in names and passwords for Russia’s VKontakte, for example. But now the trend is to go after global targets such as Facebook, the director said. Source:

http://www.computerworld.com/s/article/9175936/1.5M_stolen_Facebook_IDs_up_for_sale

Fake fast food survey with cash reward leads to phishing site. Scammers often use the familiarity of a brand as a means of lessening the victims’ tendency to be cautious when perusing unsolicited e-mails. In this latest e-mail scam, this method is coupled with the offer of \$80 to whomever takes a short survey. The e-mail supposedly comes from a globally well-known fast food chain, and claims that the company is planning major changes to the establishments in order to improve the quality of service. In order to do so, they are asking the customers to fill out a survey and they offer the cash as an incentive. Symantec reports that to access the survey, the victims are encouraged to follow the link in the e-mail, which will then take them to a bogus page ostensibly belonging to the company. After the survey is completed, the victims are redirected to a fake user-authentication page where they are asked to enter their name, e-mail address, credit card number, expiration date, verification number and personal identification number, in order to get the money. but the survey is fake, and the page is a phishing page. Source: <http://www.net-security.org/secworld.php?id=9182>

NATIONAL MONUMENTS AND ICONS

Gulf Islands National Seashore: oil spill landfall update, NPS preparations continue. The National Park Service (NPS) is continuing to make preparations for the oil spill that is predicted to reach Gulf

UNCLASSIFIED

UNCLASSIFIED

Islands National Seashore's Mississippi District shores probably no later than Saturday night and possibly sooner. The unified command for response to the Deepwater Horizon explosion, sinking, and oil spill is predicting that landfall along the Mississippi River delta will come tonight. On the map above the Mississippi District of the national seashore is positioned at the center top just under the words "Jackson County." Yesterday, NOAA revised the estimation of the amount of oil that continues to flow from the sunken oil rig, putting it at five thousand barrels a day, up from one thousand barrels. To date, there have been no identified impacts to vulnerable natural and archeological resources or visitor services at Gulf Islands. NPS personnel continue to prepare to deal with the effects from the oil spill landfall and subsequent clean-up. More personnel are coming on board as needed and as it becomes more evident that this will be a long, on-going response operation. Some containment booms were put in place yesterday, with more scheduled to be deployed today. However, bad weather may restrict some of the work planned. The Gulf Islands team is coordinating with other national park areas including Jean Lafitte National Historical Park and Preserve, Padre Island National Seashore, De Soto National Memorial, Everglades National Park and the Dry Tortugas National Park. Source: <http://www.examiner.com/x-4661-National-Parks-Travel-Examiner~y2010m4d29-Gulf-Islands-National-Seashore-Oil-spill-landfall-update-NPS-preparations-continue>

(California) Bomb squad explodes military bomb at Fort Funston. Fort Funston in San Francisco is open again after a bomb squad detonated a leftover military bomb someone found along the rugged, coastal park south of Ocean Beach, Sunday. The bomb was discovered in the stretch of the headland that belongs to the National Park Service just after noon, according to the police department. U.S. Park Police closed a perimeter for a couple hours so they could set it off, according to the park service. No one was injured. "It was safe. It just takes just a couple minutes," a Golden Gate National Recreation Area spokesman said. "They know what they're doing." Source: <http://www.sfexaminer.com/local/Bomb-squad-explodes-military-bomb-at-Fort-Funston-92056669.html>

POSTAL AND SHIPPING

(Maine) No one hurt when bombs hit Windham mailboxes. Windham, Massachusetts police have charged two juveniles and one adult with six counts of criminal use of explosives, Class C felonies, in connection with six bomb detonations in Windham Tuesday afternoon. Two mailboxes were damaged in the incidents. No other property was damaged, and no one was injured. An 18-year-old suspect from Westbrook was being interviewed at the Windham Police Department Tuesday night after he was charged with criminal use of explosives. The two juveniles are male and are teens, said a Windham police sergeant. The bombs were chemical bombs that were held in plastic bottles. Windham police said that at least 11 devices were found in different locations in the South Windham area, and that they believed additional bombs that did not explode may be found. The three suspects may face more charges if police find more devices. Source: <http://www.wmtw.com/mostpopular/23281133/detail.html>

PUBLIC HEALTH

FDA urges industry to take additional steps to prevent cargo theft. The U.S. Food and Drug Administration (FDA) April 28 sent a letter to companies and a wide range of other key stakeholders

UNCLASSIFIED

UNCLASSIFIED

detailing the agency's concern over cargo and warehouse thefts of FDA-regulated products. The products stolen have included prescription and over-the counter medicines, medical devices, and infant formula. In its letter, the FDA seeks to raise awareness among industry about each firm's responsibility to review and strengthen their security practices. The missive also seeks to inform industry of the actions the FDA will take when it becomes aware of a large-scale theft, and outlines preventative steps firms should take. And the letter emphasize the importance of notifying and informing members of the supply chain and the public after thefts occur. The FDA believes every company should have a clear plan developed on how to respond to these incidents. It also believes prevention of cargo theft is critical. The FDA said it will continue to work closely with manufacturers and wholesalers to find ways to better secure the nation's supply chain, which protects the public health. Source: <http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm209911.htm>

FDA warns on Cardiac Science devices, shares fall. U.S. health regulators warned Tuesday about faulty components in more than a dozen types of external defibrillators made by Cardiac Science Corp. The agency cited 14 models, some of which are sold by other companies such as General Electric Co's GE Healthcare unit. About 280,000 external defibrillators used worldwide to try to rescue people having heart attacks could malfunction, the agency said. A spokesman for Cardiac Science had no comment. The FDA said Cardiac Science had already recalled some models, but that other models marketed under GE and Nihon Kohden brands have similar problems. A Cardiac Science software update issued for some models detects some, but not all defects, it added, noting that similar software upgrades are planned for other models. Source: <http://www.reuters.com/article/idUSN2711575520100427>

Study links 1976 "Swine Flu" shot to stronger immune response to current strain. New evidence shows immunization against "swine flu" in 1976 might provide individuals with some protection against the 2009 pandemic H1N1 influenza virus, according to new research from investigators at St. Jude Children's Research Hospital. Researchers found that individuals who reported receiving the 1976 vaccine mounted an enhanced immune response against both the 2009 pandemic H1N1 virus and a different H1N1 flu strain that circulated during the 2008-09 flu season. The work appears in the April 23 online issue of the journal, *Clinical Infectious Diseases*. "Our research shows that while immunity among those vaccinated in 1976 has waned somewhat, they mounted a much stronger immune response against the current pandemic H1N1 strain than others who did not receive the 1976 vaccine," said an associate member of the St. Jude Infectious Diseases Department and the study's lead author. He said it is unclear if the response was enough to protect against the 2009 H1N1 virus, but the study points to a lingering benefit. The findings also raise hope that those vaccinated against the 2009 H1N1 pandemic strain might also enjoy a similar, long-term advantage. Source: <http://www.medicalnewstoday.com/articles/186529.php>

Potentially deadly fungus spreading in US, Canada. A potentially deadly strain of fungus is spreading among animals and people in the northwestern United States and the Canadian province of British Columbia, researchers reported Thursday. The airborne fungus, called *Cryptococcus gattii*, usually only infects transplant and AIDS patients and people with otherwise compromised immune systems, but the new strain is genetically different, the researchers said in the study, published in the *Public Library of Science* journal *PLoS Pathogens*. "This novel fungus is worrisome because it appears to be a threat to otherwise healthy people," said the Duke University researcher who led the study. The new strain appears to be unusually deadly, with a mortality rate of about 25 percent among the 21 U.S.

UNCLASSIFIED

UNCLASSIFIED

cases analyzed, they said. The spore-forming fungus can cause symptoms in people and animals two weeks or more after exposure. They include a cough that lasts for weeks, sharp chest pain, shortness of breath, headache, fever, nighttime sweats and weight loss. It has also turned up in cats, dogs, an alpaca and a sheep. Freezing can kill the fungus and climate change may be helping it spread, the researchers said. Source: <http://www.alertnet.org/thenews/newsdesk/N22129903.htm>

Review: Many sick airline passengers aren't reported. Hundreds of people at major U.S. airports each year are severely ill with symptoms of potentially contagious diseases, yet few are reported to health officials as intended under U.S. regulations and international guidelines, a USA TODAY review of ambulance records and federal data shows. To detect diseases such as pandemic flu, tuberculosis and measles, federal regulations require airlines to notify health officials of passenger illnesses involving diarrhea or fever plus rash, swollen glands or jaundice. The International Civil Aviation Organization, a United Nations agency, also includes persistent vomiting or coughing in its guidelines. Concerns about fliers spreading dangerous diseases have been fueled by the 2003 SARS outbreak, high-profile tuberculosis patients and the H1N1 flu pandemic. In 2009, the Centers for Disease Control and Prevention's (CDC) 20, U.S. regional-quarantine stations received 1,623 reports of illnesses or deaths involving airline passengers, data obtained under the Freedom of Information Act show. Yet in some CDC regions, ambulance records at a single airport show far more people receiving emergency medical treatment for illnesses than were reported from multiple states. Most illnesses reported to the CDC don't require intervention, the agency's quarantine director said. Under-reporting is a concern because the CDC cannot assess what it does not know about, and in some cases it has learned of unreported deaths, the director said. Source: http://www.usatoday.com/news/health/2010-04-21-sick-passengers_N.htm

TRANSPORTATION

Europe to lift airplane liquids ban in 2013. Travelers in Europe will be able to bring water bottles and other liquids aboard airplanes again starting in April 2013 after screening technology is installed. Europe's air passengers will be able to take on board water bottles, sprays and gels from April 2013 on when a general ban on liquids will be replaced by better screening technology, the European Commission said on April 29. "This package takes a significant step forward in signaling the beginning of the end for the current restrictions on liquids in cabin baggage, with a clear and final deadline of April 2013," said the commission vice president in charge of transport. In the upcoming three years, EU airports will be required to install new technology capable of detecting liquid explosives, so as to allow for the current ban to be lifted. Source: http://www.businessweek.com/globalbiz/content/apr2010/gb20100430_265233.htm

NTSB chairman discusses data driven systems to improve aviation safety. The National Transportation Safety Board Chairman said on Thursday that the use of data to manage and improve safety in the aviation industry has had a positive effect on the world's improving aviation safety record but she cautioned against over-reliance on these systems to the neglect of forensic investigation. Addressing a conference of the International Society of Air Safety Investigators in Chantilly, Virginia, the chairman noted that "we have reached an era when aviation accidents are extremely rare..." One reason is the use of data - particularly, but not exclusively, Safety Management Systems (SMS) - in accident prevention and investigation. "The Board has been advocating the use of SMS for a decade, having issued 17 recommendations in favor of implementing SMS in the aviation

UNCLASSIFIED

UNCLASSIFIED

industry. When implemented correctly, she said, "SMS holds real promise in a variety of scenarios." She noted several instances where SMS helped eliminate potential unsafe conditions, notably a corporate flight operation that used flight data to determine that high bank angles occurred on repositioning flights, and a review of commercial aircraft approach data that indicated a high rate of TCAS (Traffic Alert and Collision Avoidance System) warnings at a particular airport. In these instances, she said, "data management adeptly identified a clearly measurable set of information and allowed for a relatively simple and effective solution." Source:

http://avstop.com/news_april_2010/NTSB_Chairman_Discusses_Data_Driven_Systems.htm

New rule should reduce airport tarmac wait times. The Department of Transportation (DOT) plans to put into effect more aggressive passenger protection rules concerning tarmac wait times. The DOT's tarmac-delay rule subjects airlines to stiff fines if passengers are stuck on the tarmac for more than three hours. It was prompted by a string of long delays dating back to December 2006, which DOT documents say caused passengers "undue discomfort and inconvenience." Passengers reported subsisting on rationed Pringles potato chips and said the toilet stopped working. "There was no common sense used, no decency towards people that were sitting on a plane," the DOT secretary said April 27 at a news conference. The tarmac-delay rule has been widely discussed and debated since it was announced in December, but it is only one of a series of new DOT regulations designed to protect commercial airline passengers. Source:

<http://www.cnn.com/2010/TRAVEL/04/29/airline.passenger.protections/index.html>

(New Mexico) Disruptive plane passenger taken into custody. A Delta Air Lines flight was rerouted April 23 after a passenger threatened to blow up the plane, screamed "get behind me Satan" and sprayed passengers with water from a beverage-cart bottle, according to a complaint filed in federal court. Flight attendants and other passengers on Delta Flight 2148 struggled to restrain the "erratic and dangerous" passenger with seat belts and plastic handcuffs while pilots rerouted the plane to Albuquerque, New Mexico, an FBI Special Agent said. The plane, which was flying from Los Angeles to Tampa, Florida, landed in Albuquerque at 3:37 a.m. ET, the Transportation Security Administration said. The passenger was taken into custody shortly afterward. Law enforcement swept the plane and found nothing suspicious, TSA said. The flight landed in Tampa at about 9:20 a.m. ET, more than three hours after its scheduled arrival. The complaint said the man, 46, was heading back to his first-class seat from the plane's bathroom when he grabbed a 2-liter water bottle from a drink cart, began spraying passengers and shouted "get behind me Satan." The complaint said that after a flight attendant asked him to return to his seat the man threatened: "I am going to bring this plane down. ... You need to land this plane or I'm going to blow it up [and] I will blow up this plane and take you all with me." Passengers "engaged [the man] in a struggle and restrained him" when he approached the cockpit door, the complaint said. Source:

<http://www.cnn.com/2010/TRAVEL/04/23/unruly.passenger/>

(Puerto Rico) US detains NY-bound passenger in Puerto Rico. A man on a flight from West Africa to New York City was removed from the plane and detained Thursday after authorities apparently added him to a no-fly list during the trip. Customs and Border Protection agents detained the man while the Delta Air Lines jet stopped to refuel in San Juan, Puerto Rico after an overnight trip from Dakar, Senegal. The flight originated in Nigeria, the native country of a man accused of boarding a Detroit-bound airplane from Amsterdam in December with a bomb hidden in his underwear. The man detained in Puerto Rico was not immediately charged with any crime. Customs and Border

UNCLASSIFIED

UNCLASSIFIED

Protection issued a statement identifying him only as a “potential person of interest,” who was removed from the flight for questioning. Passengers told the Associated Press that the captain announced over the intercom that the man had been added to a roster of people banned from travel to the U.S. while the plane was in flight. Source:

http://www.google.com/hostednews/ap/article/ALeqM5g-8LccJgack50fQj13kx_1BmZ5wgD9F8H5080

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7): 866-885-8295**; email: ndslic@nd.gov ; FAX: **701-328-8175**

State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455

US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

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

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



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED