



Department of Homeland Security Daily Open Source Infrastructure Report for 18 July 2007

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)
<http://www.dhs.gov/>

Daily Highlights

- The Washington Post reports air travelers should not expect authorities to ease restrictions on gels and liquids in carry-on luggage until sometime next year when new technology may give screeners the ability to more easily spot potential explosives in bags. (See item [12](#))
- According to a U.S. intelligence estimate released Tuesday, July 17, the al Qaeda terrorist network has regained enough strength to pose the largest part of a persistent and evolving terrorist threat to the United States over the next three years. (See item [35](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 17, Reuters* — **Officials: More leaks at nuclear plant after quake.** Officials at the world's biggest nuclear power plant acknowledged Tuesday, July 17, there had been more radiation leaks after an earthquake in Japan that killed nine people and forced thousands from their homes. The admissions by Tokyo Electric Power Co. (TEPCO) have reignited fears about nuclear safety in a country that relies on atomic power for one-third of its electricity but has faced repeated cover-ups of past accidents by atomic power utilities. "I believe that nuclear power plants can only be operated with the trust of the people," Prime Minister Shinzo Abe told reporters in Tokyo, about 250 km (155 miles) southeast of Niigata prefecture, where the quake

struck Monday morning. TEPCO had initially said that the lethal earthquake had not caused any leaks, but it revealed later on Monday night that radioactive water had sloshed into the sea from its Kashiwazaki–Kariwa plant in Niigata. The company added that the quake was stronger than its reactors had been designed to withstand. Then on Tuesday, a TEPCO official told a news conference that about 100 of the 22,000 drums containing nuclear waste at a warehouse had fallen over and "several" lost their lids.

Source: <http://www.cnn.com/2007/WORLD/asiapcf/07/17/japan.quake.reut/index.html>

2. *July 17, Platts Energy Bulletin* — **Iran oil minister: No need for OPEC to hold extraordinary meeting.** Iranian oil minister Kazem Vaziri Hamaneh said Tuesday, July 17, there is no shortage of oil on international markets, but because of shortages in refining products crude oil prices could climb to \$80/barrel, the oil ministry's Shana news agency reported. "Currently there is no shortage of oil in the international markets and there is no need for OPEC (Organization of Petroleum Exporting Countries) to hold an extraordinary session," Shana quoted Hamaneh as saying. The next scheduled meeting of OPEC ministers is on September 11 in Vienna.

Source: <http://www.platts.com/Oil/News/8160990.xml?sub=Oil&p=Oil/News&?undefined&undefined>

3. *July 16, Associated Press* — **BP Solar's Maryland expansion grows.** British energy company BP PLC said Monday, July 16, it will spend an additional \$27 million on a previously announced expansion of its solar–cell manufacturing plant in Frederick, MD — on Interstate 70 about 40 miles northwest of Washington, DC — to prepare for future growth. The additional investment raises the cost of the project to \$97 million from the \$70 million announced in November. The company said it expects to complete its expansion of the BP Solar plant in 2009. The expansion will nearly double the plant's capacity for casting and sizing — the first steps in the production process — to 150 megawatts. It will allow space for future increases in casting, sizing, and wafering to at least 400 megawatts, BP Solar said.

Source: http://biz.yahoo.com/ap/070716/md_bp_solar.html?.v=1

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

4. *July 17, Associated Press* — **Toxic cloud follows Ukraine derailment.** A train carrying yellow phosphorus derailed in western Ukraine, releasing a cloud of toxic gas into the air over 14 villages. Twenty people were hospitalized and hundreds evacuated on Tuesday, July 17, officials said. Rescuers extinguished a fire that broke out in the highly toxic substance, which can catch fire spontaneously on contact with air at temperatures higher than 104 degrees. It can cause liver damage if consumed. Ukraine's Deputy Prime Minister Oleksandr Kuzmuk, who was at the site, compared the accident to the explosion at the Chernobyl nuclear reactor in 1986. Of the 11,000 people living in the contaminated area, 815 were evacuated, said Ihor Krol, spokesperson for the emergency situations ministry. The poison cloud produced by the fire contaminated 35 square miles, Krol said. Local residents were advised to stay inside, not to use water from wells, eat vegetables from their gardens or drink the milk produced by their cows.

Source: <http://www.newsday.com/news/nationworld/world/sns-ap-ukraine-toxic-gas.0.7156575.story?track=rss>

5. *July 17, Foster's Online (NH)* — **Gas line leak causes evacuation of 15 homes.** Fifteen houses were evacuated and streets blocked off following a gas line leak on Monday afternoon, July 16, in Portsmouth, NH. The Portsmouth Fire Department responded to the area of Newcastle Avenue and Fernald Court at about 4:45 p.m. EDT after construction crews digging to install a new drainage structure hit a gas line, causing vapors to escape. Firefighters evacuated the houses and made sure windows were closed as a precautionary measure in case the gas was ignited. Police blocked off Newcastle Avenue from South Street to Pleasant Street and directed traffic to seek alternate routes. There were no injuries.

Source: <http://www.fosters.com/apps/pbcs.dll/article?AID=/20070717/FOSTERS01/107170223/-1/NEWS06>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

6. *July 17, TechWorld (UK)* — **Scam targets domain name holders.** A new scam has come to light using publicly available "whois" data to rip off domain name owners. The scam, like many other increasingly targeted attacks, uses contact information available in the publicly available "whois" database to direct its e-mails. The e-mails claim to originate from a company called Domain Renewal, which operates a professional-looking site and offers to renew users' or companies' domain names. Targets are sent an e-mail informing them that their domain name is about to expire, and offering to renew it. Many companies and users buy different domain names from different registrars, making the scam hard to spot. The e-mails direct users to a site that displays Microsoft, Oracle, Cisco and IBM logos, as well as those of major credit card makers. Payment is taken via a payment service called MultiCards. Industry experts advise users not to follow links from e-mails claiming to come from e-commerce Websites or authorities such as domain name registrars, since such e-mails are a common way of carrying out financial fraud.

Source: <http://www.techworld.com/security/news/index.cfm?newsID=9518&pagetype=samechan>

7. *July 17, Reuters* — **Hackers steal government, corporate data.** Hackers stole information from the Department of Transportation and several U.S. corporations by tricking employees with fake job-listings on ads and e-mail, a computer security firm said on Monday, July 16. The list of victims included several companies known for providing security services to government agencies. They include consulting firm Booz Allen, Unisys Corp., L-3 communications, Hewlett-Packard Co. and Hughes Network Systems, said Mel Morris, chief executive of British Internet security provider Prevx Ltd. Malicious programs were able to pass sophisticated security systems undetected because that software hadn't been instructed that they were dangerous. Hackers only targeted a limited group of personal computers. It was not clear

whether the hackers used information stolen from the personal computers, Morris said. A piece of software, NTOS.exe, probes the PC for confidential data, then sends it to a Website hosted on Yahoo Inc. That Website hosts data that had been stolen from more than 1,000 PCs and encrypted before it was posted on the site, according to Morris. He said that he believes the hackers have set up several "sister" Websites that are collecting similar data from other squadrons of malware.

Source: http://news.yahoo.com/s/nm/20070717/wr_nm/internet_attack_dc:_ylt=AnTMG7sas1Ry_1sYNRnDR8AjtBAF

8. *July 17, Federal Computer Week* — **OMB, DHS outline data security best practices.** The Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) on Tuesday, July 17, explained 10 common mistakes agencies make when securing data and personal information and offered a host of best practices to correct each mistake. In a new paper, "Common Risks Impeding the Adequate Protection of Government Information," OMB and DHS discuss common problems in areas such as training, contracting and records management. OMB and DHS developed this paper as a part of the President's Identity Theft Task Force recommendations.
OMB, DHS paper: <http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf>
Source: <http://www.fcw.com/article103240-07-17-07-Web>
9. *July 16, InfoWorld* — **Report: Vast majority of businesses do not meet data-handling regulations.** An overwhelming percentage of businesses still fall far short in their efforts to comply with industry data-handling regulations and reduce their likelihood of experiencing a serious leakage incident, according to a new survey. In a report to be published by the IT Policy Compliance Group on Wednesday, July 18, the consortium of IT compliance and security experts concludes that some 90 percent of all businesses still do not have sufficient policies in place to meet data governance regulations and adequately limit the risk of a breach. In the survey of 475 companies, a third of whom reported revenues of more than \$1 billion last year, the industry group found that an overwhelming majority of the firms expect to deal with at least six business disruptions related to major data incidents per year along with five or more instances of information loss or theft. While businesses continue to invest policy enforcement software, and other technologies aimed at helping them meet data-handling regulations, said James Hurley, managing director of IT Policy Compliance Group, most are still struggling to fill all the gaps left in their systems that leave them open to potential incidents.
Source: http://www.infoworld.com/article/07/07/16/9-of-10-companies-fail-compliance_1.html
10. *July 16, ComputerWorld* — **Hacking extortionist resurfaces.** "Ransomware" last seen in 2006 has reappeared and is trying to extort \$300 from users whose files the malware has encrypted, a Russian security researcher said Monday, July 16. GpCode, a Trojan horse which last made a run at users last summer, has popped up again, said Aleks Gostev, senior virus analyst with Moscow-based Kaspersky Lab Inc., in a posting to the research center's blog. Noting the long quiet time, Gostev added: "So you can imagine our feelings this weekend, when some of our non-Russian users told us their documents, photos, archive files etc. had turned into a bunch of junk data, and a file called 'read_me.txt' had appeared on their systems." The text file contained the "ransom" note. So-called ransomware typically follows the GpCode pattern: malware

sneaks onto a PC, encrypts files, and then displays a message demanding money to unlock the data.

Kaspersky Lab blog: <http://www.viruslist.com/en/weblog>

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027160&intsrc=hm_list

- 11. July 16, *Network World* — Thirty countries move to protect online consumers.** Spurred to find ways to protect consumers as online shopping grows, the 30 countries belonging to the international economic and social-development group Organization for Economic Co-Operation and Development (OECD) announced Monday, July 16, an accord on dispute resolution -- the "OECD Recommendation on Consumer Dispute Resolution and Redress." After two years of wrangling over the policy document, the Paris-based OECD said its 30 members -- which include the European countries, Japan, Korea, Mexico, the United States and the United Kingdom among others -- have signed off on a legal framework intended to lead to better policing and resolution of consumer complaints, particularly in cross-border disputes involving e-commerce. But it remains unclear whether concrete change will come from the policy agreement, which the OECD countries now must find a way to put into effect. The OECD's Committee on Consumer Policy is expected to monitor the progress to around the accord and report to the OECD's Council within five years.

Source: <http://www.networkworld.com/news/2007/071607-countries-protect-online-consumers.html>

[\[Return to top\]](#)

Transportation and Border Security Sector

- 12. July 17, *Washington Post* — Limits to stay on gels in carry-ons.** Air travelers should not expect authorities to ease restrictions on gels and liquids in carry-on luggage until sometime next year when new technology may give screeners the ability to more easily spot potential explosives in bags, according to federal security officials who are nearing the one-year anniversary of the rules. Authorities enacted the bans in August 2006, after British police said they uncovered a plot to blow up transatlantic flights using liquid explosives. The Transportation Security Administration (TSA) later eased the restrictions to allow small amounts of liquid and gel toiletries in carry-on bags, but many travelers still complain about the cumbersome rules that force them to check more bags. Passengers are generally restricted to carrying on a small plastic bag with containers holding three ounces or less of liquid and gel products. Some in Congress and outside experts complain that federal officials are taking too long to make use of new technology that might help counter liquid explosives. TSA administrator Kip Hawley and other TSA officials said the key to easing the ban would be the deployment of high-tech X-ray machines that would provide screeners with 3-D images of the contents of luggage.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/16/AR2007071601796.html?hpid=moreheadlines>

- 13. July 17, *Associated Press* — Five airlines want new China routes.** At least five major U.S. airlines have asked federal regulators for the right to operate new nonstop flights between the United States and China beginning in March 2009. American, the largest U.S. carrier, said it

applied Monday, July 16, for a route from Chicago's O'Hare Airport to Beijing. A similar bid failed several months ago, partly because American's management and pilots couldn't agree on work rules for the flights. Continental applied Monday to fly between Newark, NJ, and Shanghai. US Airways said it is seeking to offer nonstop service between its Philadelphia hub and Beijing, China. Delta Air Lines Inc. asked to fly from Atlanta to Beijing and Shanghai; and Northwest Airlines Corp. filed to offer service between Detroit and the same two Chinese cities.

Source: http://biz.yahoo.com/ap/070717/airlines_china.html?.v=1

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

14. *July 16, Animal and Plant Health Inspection Service* — USDA selects Kansas State University to lead a benefit–cost analysis of the National Animal Identification System. The U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service today announced the selection of Kansas State University to lead a multi–institutional benefit–cost analysis of the National Animal Identification System (NAIS). The analysis will be conducted with the assistance of co–contributors Colorado State University and Michigan State University. Montana State University will provide a comprehensive assessment of the economic benefits and costs of NAIS, including its three components, premises registration, animal identification and animal tracing. Several segments of the livestock industry will be a part of this analysis including small producers; commercial producers; marketing institutions; processing facilities and rendering operations. Kansas State and colleagues will study the benefits and costs of all components of NAIS across species. Also, the analysis will seek to determine the overall distribution of benefits and costs of NAIS among producers of various sized herds, marketing firms, processors, consumers and state and federal government agencies. NAIS is a federal–state–industry partnership designed to help producers respond to and minimize the impact of an animal disease outbreak.

Source: http://www.aphis.usda.gov/newsroom/content/2007/07/ksu_benefitcost_nais.shtml

15. *July 16, Illinois Ag Connection* — Illinois finds new ash borer infestation. A destructive, non–native pest that feasts on ash trees has been confirmed in LaSalle County, IL. The emerald ash borer (EAB) was discovered just north of Peru. Illinois Department of Agriculture staff made the discovery while identifying ash trees for removal later this year as part of a survey to determine the extent of the beetle infestation in Illinois. "Our staff now is surveying ash trees in the surrounding area to define the size of the infestation," Agriculture Director Chuck Hartke said. "We also are considering adjustments to an existing quarantine as a result of this new find to limit the artificial spread of this destructive pest." The emerald ash borer is a beetle native to Asia. Its larvae burrow into the bark of ash trees, causing the trees to starve and eventually die. Since the emerald ash borer was first confirmed in the Midwest in the summer of 2002, more

than 20 million ash trees have died.

EAB information: <http://www.emeraldashborer.info/>

Source: http://www.illinoisagconnection.com/story-state.php?Id=594&y_r=2007

16. *July 16, Agricultural Research Service* — **Gaining strides against a giant reed.** The tenacious and aggressive weed known as *Arundo donax*, also called Carrizo cane and giant reed, can easily grow three to seven inches a day and reach a height of 30 feet. Brought to North America in the 1600s from Mediterranean Europe, *A. donax* invades riparian habitats and irrigation canals, leading to loss of biodiversity, catastrophic stream bank erosion, and damage to bridges. It also necessitates costly chemical and mechanical controls along waterways, and it competes for water in arid regions. *Arundo* has been cited as a troublesome invasive weed in Kentucky, Virginia and other eastern states, the American Southwest, northern Mexico and the Rio Grande Valley. Taking a high-tech approach to control, Agricultural Research Service scientists are using remote sensing to delineate *Arundo*'s distribution and density along the Rio Grande and its tributaries. The specialists are assessing how much water *Arundo* actually uses. But the best option for long-term management of the weed may be biological control using insects from the native range of *A. donax*. So far, three insects—captured and identified by scientists at the ARS European Biological Control Laboratory in Montpellier, France—seem the most promising candidates.

Source: <http://www.ars.usda.gov/is/pr/2007/070716.htm>

17. *July 16, Stop Soybean Rust News* — **Soybean rust moves north in Texas.** Asian soybean rust has been found on soybeans in a sentinel plot in Burleson County, TX. This is the northernmost confirmed rust on soybean in Texas and the seventh county with rust in the state this year. Texas officials also reported that "Rust is widespread in Victoria and Calhoun counties. It is present in Wharton County, and there are preliminary reports of its presence in Jackson and Matagorda counties." Rust was confirmed late last week in commercial soybeans in Victoria and Calhoun counties. At this point in the season last year, only one Texas county was known to have soybean rust: Hidalgo, and it was no longer found there after March.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=1064>

[\[Return to top\]](#)

Food Sector

18. *July 16, Reuters* — **Confectioner fined over salmonella scandal.** A United Kingdom court fined Cadbury Schweppes, the world's largest confectionery group, two million dollars Monday, July 16, for selling unsafe chocolate in Britain and Ireland during 2006 in a salmonella health scare. Cadbury, which makes Dairy Milk chocolate, had pleaded guilty after a number of people were left ill and some victims spent a number of days in hospital. Cadbury accepted the outcome and admitted the factory process it had followed in Britain was unacceptable. In June 2006, Cadbury admitted to the salmonella problem at one of its plants and recalled more than one million chocolate bars in the UK and Irish markets, as they could contain minute traces of salmonella. Birmingham council prosecuted Cadbury under the UK General Food Regulations and Food Hygiene Regulations for, among other things, failing to immediately alert authorities that it had reason to believe some of its chocolate was infected with salmonella.

Source: <http://money.cnn.com/2007/07/16/news/international/cadbury.r.eut/>

19. July 16, Reuters — China blames foreign media for food health scares. Foreign media have fuelled unfounded fears about Chinese products, the nation's top quality official has said, as China blocked a U.S. protein powder shipment while the two countries sparred over safety worries. The deaths of patients in Panama from mislabeled drug ingredients from China, deadly toxins in pet food ingredients and food laced with additives and antibiotics have fanned public anxiety in the U.S. about the safety of China's surging exports. But foreign reports about tainted Chinese foods had presented isolated failings as the whole picture, said Li Changjiang, head of the General Administration of Quality Supervision, Inspection and Quarantine. "Some foreign media, especially those based in the U.S., have wantonly reported on so-called unsafe Chinese products. They are turning white to black," he said. "One company's problem doesn't make it a country's problem." Chinese inspectors announced that a protein powder from a U.S. supplier contained too much selenium and was being sent back, the official Xinhua news agency reported on Monday, July 16.

Source: <http://www.reuters.com/article/worldNews/idUSPEK10303520070716>

20. July 16, Associated Press — Food label warnings seen as confusing. More and more foods bear a mishmash of warnings that they might accidentally contain ingredients that could seriously sicken people with food allergies. Yet there are signs that the labels are creating confusion among families that should heed them. The disconnect is sparking calls for standards on what are now voluntary warning labels. The U.S. Food and Drug Administration plans to seek advice from consumers and food makers, perhaps by year's end, before considering whether to intervene. Worried the labels may be losing credibility, the industry's Grocery Manufacturers/Food Products Association already is preparing to update its own guidelines on when foods should carry the warnings. Consumers see the label "on so many products, they say, 'Oh heck, I'm going to ignore it,'" laments Steve Taylor, a food scientist at the University of Nebraska who co-authored a recent study about the confusion. About 12 million Americans have some degree of food allergy. Severe food allergies trigger 30,000 emergency room visits a year, and 150 to 200 deaths a year. Food labels help the allergic avoid ingredients that could sicken them.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2007/07/16/national/w120936D72.DTL&type=politics>

21. July 13, U.S. Food and Drug Administration — Toothpaste recalled. Dent Fresh U.S.A., Inc, of Miami, FL, is initiating a nationwide recall, in accordance with the U.S. Food and Drug Administration (FDA), of toothpaste made in China involving all DentFresh Fluoride Mint Toothpaste. This recall has been initiated because the products may contain the poisonous chemical diethylene glycol (DEG). DEG is used in antifreeze and as a solvent, and is a central nervous system depressant and potent kidney and liver toxin. FDA is not aware of any U.S. reports of poisonings from toothpaste containing DEG. However, the agency is concerned about potential risks from chronic exposure to DEG and exposure to DEG in certain populations, such as children and individuals with kidney or liver disease. DEG in toothpaste has a low but meaningful risk of toxicity and injury to these populations. No injuries or illnesses have been reported to date in connection with this problem.

Source: http://www.fda.gov/oc/po/firmrecalls/dentfresh07_07.html

[\[Return to top\]](#)

Water Sector

22. *July 15, Gannett Wisconsin Newspapers* — **Eleven failing septic systems found near restaurant.** Door, WI's inspection of septic systems surrounding the Log Den restaurant turned up at least 11 failing systems that could be feeding human feces to the groundwater. All 11 of the systems will need to be replaced. The Sanitarian's Office and Public Health Department asked the Board of Health for authority to order the owners to replace their failing systems within 60 days. The owners of the failing systems will have one year to install a replacement system. In late June, 81 wells were tested in the area both up and down stream of the Log Den. None of the wells tested positive for E. coli, an indicator of fecal contamination.

Source: <http://www.greenbaypressgazette.com/apps/pbcs.dll/article?AI=D=/20070715/GPG0101/707150686/1207/GPGnews>

[\[Return to top\]](#)

Public Health Sector

23. *July 17, Daily Herald (UT)* — **Tularemia in Utah.** A potentially nasty biological agent has infected 13 people in Utah. Tularemia, also known as rabbit fever, a naturally occurring Class-A biological agent, is being blamed for 13 cases of serious illnesses that have sent victims repeatedly to the emergency room. The victims were from three different counties spread across the state; however, they all have one thing in common. All 13 people are believed to have been camping on the west side of Utah Lake sometime between the end of June and the first week of July. The Utah Department of Health has only confirmed that two of the cases are Tularemia. The remaining 11 cases are "suspect" with the patients showing all appropriate clinical signs of the bacteria infection. Positive confirmation cannot be made until bacterial culture growths can be completed for testing.

Tularemia information: <http://www.bt.cdc.gov/agent/tularemia/index.asp>

Source: <http://www.heraldextra.com/content/view/228971/4/>

24. *July 17, Reuters* — **India seen winning fight against worst polio strain.** India may be winning the fight against the most dangerous strain of polio, with no cases reported this year in a badly hit region seen as a key global battleground against the paralyzing disease, officials said. India is the focus of concern among the global health community after an outbreak of 676 cases in 2006 — a tenfold jump over 2005 and a third of the world's total. The Indian strain caused countries such as Angola and then Namibia to be re-infected, and is thought to be the source of the first outbreak in seven years in neighboring Myanmar this year. Around 96 percent of India's cases in 2006 were of the virulent Type 1 strain, and the majority were reported from western Uttar Pradesh. Uttar Pradesh is India's most populous state, with 170 million people. India, which aims to eradicate polio by the end of 2008, has seen 103 cases of polio this year against 150 till the end of June last year, but, more importantly, Type 1 cases in the first six months have fallen to 39 against 145 year-on-year.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://in.today.reuters.com/news/newsArticle.aspx?type=topNews&storyID=2007-07-17T170821Z_01_NOOTR_RTRMDNC_0_India-285193-1.xml&archived=False

25. *July 16, CIDRAP News* — **Inhibiting cytokine response might not reverse H5N1 infections.** Scientists have hoped that disabling the body's destructive immune-system overreaction to the H5N1 avian influenza virus, known as "cytokine storm," could lead to new lifesaving treatments, but according to a new study, trials testing the strategy didn't protect mice infected with the disease. The study was conducted by Robert Webster, and colleagues at St. Jude Children's Research Hospital. They report that groups of mice genetically programmed to lack one of three important inflammatory cytokines died after they were exposed to a Vietnamese H5N1 virus strain. Also, they found that mortality rates were high in nonaltered mice that were given glucocorticoids to suppress cytokine production after exposure to the H5N1 virus. Scientists have suggested that the cytokine storm contributed to the high death rate in the 1918 Spanish flu pandemic and is playing a similar role in human cases of H5N1 infection today. Autopsies of some H5N1 avian flu victims in the current outbreaks have revealed lungs were choked with debris from excessive inflammation triggered by the virus. Similar severe lung damage was often reported in victims of the 1918 pandemic, which disproportionately killed young, healthy adults—those with the strongest immune systems.
- Source: <http://www.cidrap.umn.edu/cidrap/content/influenza/avianflu/news/jul1607cytokine.html>

[[Return to top](#)]

Government Sector

26. *July 17, Government Accountability Office* — **GAO-07-1098T: Federal Acquisitions and Contracting: Systemic Challenges Need Attention (Testimony).** In fiscal year 2006, the federal government spent over \$400 billion for a wide variety of goods and services, with the Department of Defense (DoD) being the largest purchaser. Given the large and growing structural deficit, the government must get the best return it can on its investment in goods and services. For decades, the Government Accountability Office (GAO) has reported on a number of systemic challenges in agencies' acquisition of goods and services. These challenges are so significant and wide-ranging that GAO has designated four areas of contract management across the government to be high-risk. This testimony highlights four key acquisition challenges agencies face: (1) separating wants from needs, (2) establishing and supporting realistic program requirements, (3) using contractors in appropriate circumstances and contracts as a management tool, and (4) creating a capable workforce and holding it accountable. While GAO is making no new recommendations in this testimony, GAO has made numerous recommendations through the years to improve government acquisitions, many of which have not been implemented.
- Highlights: <http://www.gao.gov/highlights/d071098thigh.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-07-1098T>

27. *July 16, Associated Press* — **Man declaring 'I am the emperor' killed at Colorado governor's office.** On Monday, July 16, just outside Governor Bill Ritter's Capitol office, a man who declared "I am the emperor" was shot and killed by a state trooper when he refused to

drop his gun, authorities said. Authorities said the unidentified man — described as wearing dark pants and a white shirt — had at least two verbal confrontations with state troopers in Ritter's security. The man had walked into the reception area of Ritter's office and was being escorted out before he produced a gun and refused orders to put it down, police spokesperson Sonny Jackson said. Before he was shot, the gunman said, "I am the emperor and I'm here to take over state government," said Evan Dreyer, the governor's spokesperson. The shooting occurred shortly after 2 p.m. MDT. The Capitol has no metal detectors. They are usually installed temporarily during the governor's annual State of the State address in January but then are removed.

Source: <http://www.cnn.com/2007/US/07/16/colorado.capitol.ap/index.html>

[\[Return to top\]](#)

Emergency Services Sector

28. July 17, *Whittier Daily News (CA)* — Emergency agencies in California drill for large earthquake. Officials from 60 law enforcement and emergency response agencies and the armed forces met Monday, July 16, near Los Angeles, CA, to polish their skills in case a magnitude 7.9 or greater earthquake ever hits California. The eight-day training exercise will involve thousands of members from Los Angeles and Orange County sheriff's and fire departments. It is part of a military operation, "Golden Phoenix," which will test the communication channels of law enforcement agencies in case the big one hits. Twenty communication channels will be used by law enforcement agencies, spanning satellite, cell phone, global positioning systems and data transfer. On July 24, there will be emergency drills at the Rose Bowl, the Forum in Inglewood, and a mall in Hawthorne involving 1,000 Marines playing the roles of displaced civilians and angry looters. The Red Cross and the sheriff's and fire departments will be on scene to test transportation and personnel equipment.

Source: http://www.whittierdailynews.com/news/ci_6389576

29. July 16, *Boston Globe* — Emergency officials in Connecticut seek access to DOT cameras on I-95. In Connecticut, municipal officials and the state Department of Transportation (DOT) are sparring over local access to images generated by traffic cameras along Interstate 95. Local officials are demanding more access to the images and may oppose a \$40 million state plan to replace the cameras in an upgrade. Weston First Selectman Woody Bliss, chairman of the South Western Region's Metropolitan Planning Organization, said, "It's inexcusable that this traffic information is not available to first responders in the towns. It needs to be an integral part of the design of the new cameras." Norwalk Fire Chief Denis McCarthy said municipal first responders need access to the images because information called in during an accident is often incorrect. DOT spokesperson Kevin Nursick said emergency first responders may access traffic camera feeds using the DOT Website. McCarthy and Robert McGrath, chief of Stamford Fire and Rescue, said DOT's Website feed doesn't always update in real time and views of serious accidents on the highway are often blacked out.

Source: http://www.boston.com/news/local/connecticut/articles/2007/07/16/local_emergency_officials_seek_access_to_dot_cameras_on_i_95/

30. July 16, *WWAY-TV (NC)* — North Carolina first responders say new 911 system has dangerous holes. The Brunswick County, NC, 911 center just got a new system, but first

responders say new doesn't necessarily mean better. First responders say the multi-million dollar system paid for by tax payers has dead zones and holes that are putting the community at risk. Fire and emergency medical services were switched over to the new system last October. The problems started shortly thereafter. Some of those problems include too much traffic on the emergency radio, making it difficult to understand instructions. Emergency crews also say tower problems make it difficult for them to get a signal in some places, especially inside buildings.

Source: http://www.wwaytv3.com/responders_say_new_911_system_has_dangerous_holes/07/2007

[\[Return to top\]](#)

Information Technology and Telecommunications Sector

31. July 17, VNUNet — Cross-browser Firefox/IE flaw worsens. The browser flaw which allows attackers to hijack a computer by using Internet Explorer (IE) to launch Firefox is affecting other applications as well. Security researchers Nate McFeters, Billy Rios and Raghav Dube have disclosed information and working exploit code for a similar vulnerability in Trillian. Like the Firefox attack, the Trillian exploit uses a Uniform Resource Identifier (URI) function as the point of attack. The URI allows the browser to launch a third-party application on the user's system in much the same way that a URL is used to access a Web page. When the user visits a specially-crafted page, the application is launched and attack code is run to crash the application and execute code. The attack could be used to remotely install malware on a user's system. The researchers claim that, while this attack only affects AIM clients, any application that allows for URI access could be targeted with similar attacks.

Trillian vulnerability information provided by McFeters, Rios, and Dube:

<http://www.xs-sniper.com/nmcfeters/Cross-App-Scripting-2.htm>

Source: <http://www.vnunet.com/vnunet/news/2194362/cross-browser-flaw-expands>

32. July 16, IDG News Service — Security firm: Don't use iPhone Web dialer. Security researchers at SPI Labs are warning iPhone users not to use a special feature that lets them dial telephone numbers over the Web using the iPhone's Safari browser. The feature was created to give iPhone users a simple way to dial phone numbers listed on Web pages, but according to SPI, the feature could be misused. Attackers could exploit a bug in this feature to trick a victim into making phone calls to expensive "900" numbers or even keep track of phone calls made by the victim over the Web, said Billy Hoffman, lead researcher with SPI Labs. The iPhone could even be stopped from dialing out, or set to dial out endlessly, he said. "Because this vulnerability can be launched from Websites, everybody who has an iPhone has the potential to get exploited," Hoffman said.

SPI Labs blog: <http://portal.spidynamics.com/blogs/spilabs/archive/2007/07/16/SPI-Labs-advises-avoiding-iPhone-feature.aspx>

Source: http://www.infoworld.com/article/07/07/16/Security-firm-says-to-not-use-iPhone-Web-dialer_1.html

33. July 16, ComputerWorld — Anonymous researcher boasts of building Mac worm. An anonymous security researcher claimed this weekend to have created a worm that exploits a vulnerability in the Mac OS X operating system which Apple Inc. missed in a May round of

patches. A poster on the Information Security Sell Out blog said Sunday, July 15, that he or she had written a proof-of-concept worm "in a few hours" that exploits a variation of a vulnerability patched in May by Apple. According to the researcher, he or she exploited a still-unpatched bug in mDSNResponder, a component of Apple's Bonjour automatic network configuring service, in the worm's code. "This vulnerability, as with the ones fixed, gives remote root access," the researcher said. Apple's May security update, 2007-005, included a fix for the mDSN bug.

Information Security Sell Out blog:

<http://infosecsellout.blogspot.com/2007/07/oh-look-apple-worm.html>

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027179&intsrc=hm_list

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

34. July 17, *Saginaw News (MI)* — Bomb scare prompts Meijer store evacuation. Bridgeport Township, MI, is the only community in Saginaw County with a \$60,000 HazID Kit, which in 30 seconds can recognize any of 30,000 hazardous materials. Monday, July 16, it did its job at the Meijer Inc. store at 3360 Tittabawassee in Kochville Township. Although it didn't tell emergency responders the whole story, it told them enough about a white substance someone found in two two-liter soda bottles in a trash container in the bottle return department. Meijer officials evacuated the store for about two hours. "We couldn't match the substance," said Bridgeport Township Assistant Fire Chief David J. Smigiel. "Whatever it is, it wasn't in our library." The computer picked up an "infrared signature" that Smigiel said he will forward to the HazID manufacturer for analysis.

Source: <http://www.mlive.com/news/sanews/index.ssf?base/news-5/1184682063240290.xml&coll=9>

[\[Return to top\]](#)

General Sector

35. July 17, *USA TODAY* — Report: Al Qaeda may use Iraqi network to attack U.S. The al Qaeda terrorist network has regained enough strength to pose the largest part of a "persistent and evolving terrorist threat over the next three years," according to a U.S. intelligence estimate released Tuesday, July 17. Al Qaeda, whose ranks were cut by U.S. and allied attacks after the September 11 terrorist strikes, has regained strength in its sanctuary in Pakistan, said the National Intelligence Estimate developed by U.S. intelligence agencies. At a news briefing,

David Shedd, deputy director of national intelligence, said Pakistan's inability to control its tribal region along the Afghanistan border has "created additional operating space" for al Qaeda. The main threat to the United States "comes from Islamic terrorist groups and cells, especially al Qaeda, driven by their undiminished intent to attack the homeland and a continued effort by these terrorist groups to adapt and improve their capabilities," the report said.

Approved by the heads of 16 U.S. intelligence agencies and Director of National Intelligence Mike McConnell on June 21, the estimate was released as Congress continues to debate a defense bill that includes provisions that would either cut or restrict the number of U.S. troops in Iraq.

Declassified report on terrorist threat to the United States:

http://hosted.ap.org/specials/interactives/wdc/documents/nie_071707.pdf

Source: http://www.usatoday.com/news/washington/2007-07-17-intelligence-estimate_N.htm

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.