Department of Homeland Security Daily Open Source Infrastructure Report for 27 June 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The Associated Press reports that Saudi Arabian authorities have arrested this year 520 people with suspected ties to Al Qaeda. Some of those arrested and detained were plotting attacks against an oil installation and "security target." (See item **1**)
- The National Intelligence Council chairman warned that global climate change could sap the country's military forces – while fueling new conflicts around the world. He also reported that a number of active coastal military installations in the U.S. are at risk for damage, including two dozen nuclear facilities and numerous. (See item **12**)

DHS Daily Open Source Infrastructure Report Fast Jump

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. *June 26, Associated Press* – (International) **Saudis holding hundreds, citing links to Al Qaeda.** Saudi authorities have arrested and detained 520 people so far this year that are suspected of having links to Al Qaeda, the Interior Ministry said Wednesday. In a statement reported by the official Saudi Press Agency, the ministry said some of those arrested had been plotting bomb attacks against an oil installation and what it called a security target, but it provided no details. The ministry said police officers had found money, weapons, and ammunition owned by the suspects, who had buried some of it in remote areas. The men who are from Africa, Asia and other regions were organized into cells whose leaders were based outside Saudi Arabia, the statement added. One of the

men was reportedly found with a message from Al Qaeda's second in command, urging him to raise money and saying the terrorist group would provide militants from Iraq, Afghanistan, and North Africa "to target oil installations and fight security forces." The ministry said that 181 others had been arrested since January but released because there was no evidence linking them to Al Qaeda. Al Qaeda has called for attacks against the Saudi government, criticizing its alliance with the U.S. and hoping to disrupt the flow of oil to the West.
Source:
http://www.nytimes.com/2008/06/26/world/middleeast/26saudi.html?_r=1&ref=world&oref=slogin

2. *June 26, Agence France-Presse* – (International) **Nigerian militants release 11 crew of oil vessel: military.** Nigerian militants have released a Chevron supply vessel with its 11 crew members hijacked six weeks ago in the restive Niger Delta, a military source said Thursday. The nine Nigerians, one Portuguese, and one Ukrainian were released on Wednesday, the source told AFP, refusing to say if a ransom was paid. The attack on the Chevron vessel, Lourdes Tide, took place on May 13 between the oil city of Port Harcourt and Escravos in southern Nigeria. A Military Joint Task Force spokesman had told AFP that the attackers had asked for a ransom of 30 million naira ($260,000) for the hostages. A Pakistani and a Maltese working for Texas drilling company Lonestar, who were abducted on May 23, have also been released, a company spokesman said. The Maltese government said no ransom was paid.
Source:
http://news.yahoo.com/s/afp/20080626/wl_africa_afp/nigeriaoilunrest;_ylt=AjCWg4GH_KfNIIpghvMaC5u96Q8F

3. *June 26, Bloomberg* – (New York) **Consolidated Edison workers may strike.** Consolidated Edison Inc.'s unionized workers are preparing a strike that could begin Sunday morning at the utility owner's operations in most of New York and Westchester County. The two sides remain "miles apart" in round-the-clock talks on conditions for a new contract, said a negotiator for the 9,000-member Local 1-2 of the Utility Workers Union of America. Local members voted 97 percent in favor of a strike on June 13, he said Thursday. The New York Daily News reported Wednesday that there may be a strike.
Source:
http://www.bloomberg.com/apps/news?pid=20601072&sid=a3rDfbkxy_C8&refer=energy

4. *June 25, Business News Americas* – (International) **Drummond workers threaten to strike.** Employees at U.S. coal producer Drummond in Colombia's Cesar department are considering going on strike if they do not receive a satisfactory offer to their demands for higher salaries and better housing, education, and health benefits. "If the workers are not happy with the proposal, the only recourse they have is to put the law into motion and vote to strike," said a spokesperson for the Sintramienergetica union. The parties have until June 29 to reach an agreement and if negotiations fail, "we will call an employee assembly for July 6 or 8 and put the strike to a vote," he said, adding

the exact time and date of the strike would be decided afterward.
Source:
http://www.bnamericas.com/news/mining/Drummond_workers_threaten_to_strike

5. *June 25, Reuters* – (Washington) **Shell Washington refinery cited for safety violations.** Washington State's Department of Labor and Industries (DLI) said on Wednesday it found 23 serious safety and health violations at Shell Oil Co's 145,000 barrel per day refinery in Anacortes, Washington. Shell said it was weighing a possible appeal of the agency's citation, which could lead to fines totaling $109,600. DLI's findings came after inspectors spent two days a week for two months in the refinery and poured over 10,000 pages of documents. The inspection is part of the federal National Emphasis Program to conduct detailed safety inspections at U.S. refineries to prevent a repeat of the 2005 explosion at BP Plc's Texas City, Texas, refinery, which killed 15 workers and injured 180 other people. Among the serious violations found at the Shell Anacortes refinery were failures to identify and control hazards that could lead to releases of highly hazardous chemicals and deficiencies in the development of mechanical integrity programs, DLI said. A Shell spokesman said much of the citation concerned documentation of safety programs at the refinery.
Source:
http://www.reuters.com/article/rbssEnergyNews/idUSN2542088320080626?pageNumber=1&virtualBrandChannel=0

6. *June 24, Colorado Springs Gazette* – (Colorado) **Explosion causes power outage downtown.** Colorado Springs Utilities workers are trying to restore power to a widespread power outage caused by some type of explosion. The area stretching from Cache le Poudre Street downtown north to Fillmore Street is currently without power. Colorado Springs police said they did not know what caused the explosion but think it may have been a transformer.
Source:
http://www.gazette.com/news/power_37632___article.html/explosion_caused.html

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

7. *June 25, Reuters* – (International) **Greenpeace tries to delay French reactor work.** Greenpeace France activists on Wednesday blocked for the second day the entrances of three of the four quarries used by EDF to build its new-generation nuclear reactor, the environmentalist group said. But French power group EDF said the action was not preventing building of the 1,600-megawatts reactor. "The action is not hindering the works," an EDF spokeswoman said, without giving more details. Work at the building

site of Flamanville were partly halted at the end of May following an order from France's nuclear safety authority (ASN) due to several irregularities, but EDF was given the go-ahead to resume work last week. "We are asking the ASN to cancel its decision and we are issuing a warning on the choice of nuclear," said a Greenpeace France spokeswoman. Around 20 Greenpeace activists chained themselves early on Tuesday to the entrances of three out of four quarries, which are used by EDF to make concrete. "We have no plan to stop the action, we will carry on as long as it's necessary," Greenpeace said.
Source: http://uk.reuters.com/article/environmentNews/idUKL2580194620080625?pageNumber=1&virtualBrandChannel=0

8. *June 24, KNDO/KNDU 23/25 Yakima* – (Washington) **Explosives used to level part of N reactor.** Those living near the Hanford site may have heard three loud blasts on the site over the weekend. The U.S. Department of Energy (DOE) used explosives to take down two huge stacks and a tank at the N Reactor complex. DOE officials say the part of the reactor's three-foot thick walls make it almost impossible to take down without explosives. The teardowns are part of the process of cocooning the reactor.
Source: http://www.kndo.com/Global/story.asp?S=8543983&nav=menu484_5_4

[Return to top]

Defense Industrial Base Sector

9. *June 26, USA Today* – (National) **Military facing $100 billion in equipment repairs.** Pentagon leaders realize they face a choice between a larger military and improved equipment, said the chairman of the Joint Chiefs of Staff. More than five years of simultaneous wars in Iraq and Afghanistan have ground down military equipment. Humvees, for example, travel as much as 100,000 miles a year in Iraq, five times the peacetime rate. Heavy armor strains engines and axles. Repairs have skyrocketed in recent years. The Army repaired 6,000 rifles and handguns per year before the Iraq war. This year that number jumped to 200,000, said an employee with the Army Material Command. Just how high the bill will go depends on when U.S. troops leave Iraq and how much equipment is upgraded rather than repaired, said the executive director of the Center for Strategic and Budgetary Assessments. The Army wants $17 billion a year, for as many as three years after the wars in Iraq and Afghanistan end, to re-equip itself. The Marine Corps estimates it will cost $15.6 billion to replace its damaged or destroyed equipment, including light armored vehicles "lost in combat." The Air Force puts its costs at $10 billion.
Source: http://www.usatoday.com/news/military/2008-06-25-Military-repairs_N.htm

10. *June 26, Associated Press* – (National) **US military shoots down separating missile in test.** The military's ground-based missile defense system destroyed a missile launched from an airplane in the first successful test of the system's ability to destroy a warhead that separates from its booster, the Missile Defense Agency said. The interceptor missile launched off Kauai, Hawaii, on Wednesday had to differentiate between the warhead and the body of the missile before destroying the warhead above the Pacific Ocean, the

agency said. It was the fifth successful intercept in five attempts since 2005 for the Terminal High Altitude Area Defense system (THADD), according to the agency. The threat missile was launched from a U.S. Air Force C-17 aircraft flying over the Pacific Ocean. The interceptor missile was fired six minutes later. Like the Patriot anti-missile defenses, THADD is designed to knock out ballistic missiles in their final minute of flight. However, it is designed to intercept targets at higher altitudes, enabling it to defend a larger area. THADD is one of two missile defense systems being tested at the Navy's Hawaii missile range. The sea-based Aegis system completed its own successful test on June 5.
Source:
http://ap.google.com/article/ALeqM5gHrP8RITLNsb4YHaf36kDfqxF8EAD91HNP6G0

11. *June 26, Knoxville News Sentinel* – (Tennessee) **Y-12 workers celebrate milestone.** Workers at the Y-12 nuclear weapons plant have completed a years-long refurbishment project that is supposed to significantly extend the life of B61 bombs. The Oak Ridge work involved revamping the "canned subassemblies" that contain the second stage of the thermonuclear bomb. Y-12 workers built parts for two versions of the B61 bombs, according to information released by the National Nuclear Security Administration's (NNSA) Oak Ridge office. One of those versions, Mod 11, is reportedly designed to be a bunker-busting bomb, while the other is a strategic nuclear bomb. A spokesman for the NNSA said he could not discuss how many bombs were refurbished during the project, which began in 2005.
Source: http://www.knoxnews.com/news/2008/jun/26/y-12-workers-celebrate-milestone/

12. *June 25, Wired Blogs* – (National) **Climate change may sap military, intel chief says.** The National Intelligence Council chairman warned Congress that global climate change could sap the country's military forces – while fueling new conflicts around the world. But he warned that responding to global warming might be even more costly than the problem itself. "Climate change will have wide-ranging implications for U.S. national security interests over the next 20 years," he noted. But the biggest impact is likely to be overseas, where "climate change... will worsen existing problems — such as poverty, social tensions, environmental degradation, ineffectual leadership, and weak political institutions. [That] could threaten domestic stability in some states, potentially contributing to intra- or, less likely, interstate conflict, particularly over access to increasingly scarce water resources." China and the U.S. "share a common interest in maintaining stability and ensuring dependable access at reasonable prices." But an employee with the Army War College also warned that climate change could make the Middle East and Africa more fertile ground for terrorists. On the home front, responding to thawing in and around Alaska, water shortages in the Southwest, and storm surges on the East and Gulf Coasts will involve costly repairs, upgrades, and modifications. A number of active coastal military installations in the continental United States are at a significant and increasing risk of damage. In addition, two dozen nuclear facilities and numerous refineries along U.S. coastlines are at risk and may be severely impacted by storms.
Source: http://blog.wired.com/defense/2008/06/we-judge-global.html

[Return to top]

Banking and Finance Sector

Nothing to report

[Return to top]

Transportation Sector

13. *June 26, Washington Times* – (International; National) **U.S., Thais probe trafficking of passports.** U.S. and Thai security officials are probing Bangkok-linked international gangs after police in recent months seized thousands of U.S. and foreign passports. U.S. officials became especially concerned after an April raid uncovered hundreds of real U.S. passports – legally issued to Americans by the State Department – hidden among boxes of fake passports. No breakthrough was announced in the cases. Several U.S. and British passports bore photographs, names, birth dates, and birthplaces of people who apparently legally owned the passports. Some of the people may have lost their U.S. passports or had them stolen, police said. Others may have illegally sold their genuine passports for quick cash. Even though those passports had expired, officials said forgers could alter the dates and photographs, enabling criminals to use otherwise genuine documents for travel to countries where immigration officials might not notice the changes. Such destinations include countries where U.S. or European passport holders do not need to apply for visas in advance and are allowed entry upon arrival. Other seized passports were from Canada, Japan, Singapore, Malaysia, Indonesia, India, Peru, Malta, Britain, and other European countries. In a separate case, police arrested 12 gang members from Thailand, Burma, and Indonesia on May 11 in Bangkok and seized hundreds of additional counterfeit U.S., European, and Asian passports. American and Thai officials insisted no raids have ever uncovered newer U.S. passports with high-tech electronic components, such as radio frequency identification tags, antennas, or readers. The U.S. Government Printing Office, the congressional agency producing new passports, said the U.S. passport-production facility in Ayutthaya's Hi-Tech Industrial Estate is secure, and that the State Department checked the security of Thailand's plant. Source: http://www.washtimes.com/news/2008/jun/26/us-thais-probe-trafficking-of-real-counterfeit-pas/

14. *June 25, Reuters* – (New York) **N.Y. airport plot suspects extradited, plead innocent.** Three men accused of plotting to blow up New York's John F. Kennedy International Airport pleaded not guilty on Wednesday after they were extradited to the U.S. from Trinidad. At a hearing in Brooklyn federal court, the three men pleaded innocent to involvement in a plot to blow up buildings, fuel tanks, and pipelines at the top international air passenger gateway to the U.S. A fourth suspect was arrested in New York and is in jail pending trial. A naturalized U.S. citizen from Guyana who once worked as a cargo handler at the airport has also pleaded not guilty. The four men were indicted in New York a year ago on charges of plotting to blow up JFK. They face a maximum sentence of life in prison if convicted. Prosecutors say the four suspects are Islamic extremists. The charges include conspiring to attack a mass transportation

facility, to destroy a public building by explosion, and to destroy international airport facilities. U.S. authorities acknowledged previously that the plot – conceived between January and June 2007 – was more aspirational than operational.
Source: http://www.reuters.com/article/domesticNews/idUSN2549835520080626

15. *June 25, Associated Press* – (National) **Report warns of woes from visa-free travel rules.** U.S. congressional investigators say that the government could be overwhelmed by visa applications because of new requirements for visa-free travel. A report by the Government Accountability Office released this week said that the State Department does not yet have a plan to deal with a possible increase in visa applications after the new requirements are implemented within months. The concern involves changes to the U.S. visa waiver program. The U.S. will soon require visitors from closely allied countries like Britain and Japan, who can travel without visas, to register personal details online at least three days before they arrive. The U.S. plans to begin implementing the changes for some countries in August and to require online registration for all visa-free travel by January 12. The report warns that some travelers who are rejected for visa-free entry after registering online are likely to apply for visas. If even a small percentage of all travelers from visa-waiver countries apply for visas, they could overwhelm consulates with their applications. U.S. officials say the changes will help the U.S. to boost the security of its visa-free travel program by allowing the government to screen visitors before they travel. Currently, visitors fill out paper forms on route and are screened by U.S. customs agents on arrival.
Source: http://www.msnbc.msn.com/id/25371694/

16. *June 25, Houston Business Journal* – (Texas) **Harris County launches security effort along ship channel.** Harris County officials have created a Homeland Security Marine Unit in an effort to improve security along the Houston Ship Channel and its tributaries. The Harris County's Office launched the initiative in partnership with Harris County Commissioner's Court, the U.S. Coast Guard, and private industry. The project is being funded with $30 million in grants from the U.S. Department of Homeland Security. "The refineries and marine transportation facilities are basically the lifeblood of our petrochemical industry," notes a homeland security official for the Harris County Sheriff's office. The newly-formed marine unit's official main objective is to prevent potential terrorist attacks through identification, intervention, and investigation of potential security threats along the waterway and in specially designated security zones.
Source: http://www.bizjournals.com/houston/stories/2008/06/23/daily27.html

17. *June 25, Reuters* – (Texas) **Enterprise Products says Texas NGL pipeline shut.** Enterprise Products Partners L.P. on Wednesday shut its 125,000 barrel-per-day Seminole pipeline that transports propane and other natural gas liquids (NGLs) from West Texas to Mont Belvieu, Texas, after a leak was discovered in Pasadena, Texas, near Houston, a company spokesman said. The leak was detected at 10:30 a.m., and the section of the pipeline was isolated and crews dispatched, the company said. There were no injuries, according to an Enterprise spokesman. He said the cause of the leak was not determined and no restart estimate was available. The NGLs vaporize when exposed to air, so usually the products do not pool when leaked, he said. Shipping on the nearby

Houston Ship Channel was not affected, the U.S. Coast Guard said.
Source: http://uk.reuters.com/article/oilRpt/idUKN2525487920080625

[Return to top]

Postal and Shipping Sector

18. *June 25, Reuters* – (International) **Suspicious powder shuts U.S. embassy in Sri Lanka.** The U.S. embassy in the Sri Lankan capital, Colombo, was closed on Wednesday after a "suspicious powder" was found in the premises, the embassy said. "The suspicious substance will be sent to a laboratory for analysis. Until the results are received and a determination is made that the substance does not pose health or safety risks, the embassy will be closed to the public," it said in an e-mailed statement. The heavily-guarded embassy has thrice been closed in the past after suspicious powder was detected but on each occasion it was a false alarm.
Source: http://in.reuters.com/article/southAsiaNews/idINIndia-34228120080625

19. *June 25, Chicago Tribune* – (Illinois) **Release delayed for man accused of being mail bomber 'The Bishop.'** The man accused of being "The Bishop" mail bomber will remain in custody for at least a few more days despite being ordered released on bail by a federal judge earlier this week. The suspect has been held at the downtown Chicago Metropolitan Correctional Center for more than a year after being arrested on charges he sent pipe bombs in an attempt to inflate the prices of stocks in which he invested. A U.S. magistrate judge had ordered the suspect jailed last year, finding that he was a danger to the community. But the judge reversed himself Monday, siding with the suspect's lawyer, who has suggested that home detention and electronic monitoring would be enough to keep the community safe. Prosecutors said the suspect is still a threat and noted that he allegedly sent letters mentioning the Unabomber and the D.C. sniper case. He then escalated his conduct to mailing actual explosives.
Source: http://www.chicagotribune.com/news/local/chi-bishop-bond-web-jun26,0,6779176.story

[Return to top]

Agriculture and Food Sector

20. *June 26, Associated Press* – (Florida) **No-fishing zones studied for ecosystem protection.** A University of Miami marine biologist and others are studying whether putting large tracts of ocean off-limits to fishing in the Keys can help species rebound, and prove a way to help reverse the effects of overfishing worldwide. Some studies suggest the outcome could mean life or death for not only commercial and sport fishing, but for mass seafood consumption as it exists today. Florida has the largest contiguous "no-take" zone in the continental U.S. — about 140 square miles are off limits to fishing in and around Dry Tortugas National Park, a cluster of seven sandy islands about 70 miles west off Key West. Nearby, another 60 square miles are also off limits. The region is home to some 300 fish species and lies within a crucial coral reef habitat at the convergence of the Gulf of Mexico, the Caribbean Sea, and the Atlantic Ocean. Keeping

anglers away, scientists believe, will create havens where fish can feed, grow, and spawn, then migrate to areas that have been over-fished. The larger a fish grows, the more eggs it can produce. A 2006 report in the journal Science warned that nearly a third of the world's seafood species have declined by 90 percent or more and all populations of fished species could collapse by 2048 if current fishing and pollution trends continue.
Source:
http://ap.google.com/article/ALeqM5iiFCZBV6woXCsSpCpfMpfxwO_TYAD91HLDPO4

21. *June 25, Reuters* – (Ohio) **E.coli in beef linked to 19 illnesses in Ohio.** A sample of raw ground beef was found to contain the same harmful strain of E. coli O157:H7 bacteria that caused outbreaks in Ohio and Michigan in recent weeks, the state's departments of health and agriculture said in a statement on Wednesday. "Information submitted with the positive beef sample indicates the product was purchased at the Kroger Marketplace in Gahanna. It is important for consumers to realize beef purchased from other sources may also be tainted, and steps should be taken to protect themselves from food-borne illnesses," the statement said. "The department is working closely with the U.S. Department of Agriculture to perform a trace back investigation to find the source of this ground beef," the Ohio Department of Agriculture director said in the statement. The Ohio Department of Health and local health departments in six counties continue to investigate 19 Ohio cases of E. coli O157:H7 that have been linked genetically and epidemiologically to cases in Michigan.
Source:
http://www.reuters.com/article/healthNews/idUSN2548448620080625?feedType=RSS&feedName=healthNews

22. *June 25, USA Today* – (National) **Humane Society releases video of cattle being abused.** The Humane Society of the United States said a new investigation discovered dairy cattle being abused in May at a livestock auction in New Mexico. The group said an investigator watched three cows and calves "being mistreated and tormented in order to get them to stand and walk" into an auction ring. The group said state inspectors "were present at the auctions and apparently saw much of the abuse." The American Meat Institute president said, "Humane handling of animals "is both ethically appropriate and has real economic benefits in terms of safer workplaces and better meat quality." There is no evidence the downer cows were slaughtered or, if so, whether the meat found its way into the National School Lunch Program, a major buyer of ground beef, he said. A House representative said the Department of Agriculture should close a federal loophole that allows downer cattle to enter the food supply if they are ambulatory when they are initially inspected. Downer cattle generally have been prohibited from the U.S. food supply since 2004 because they carry a higher risk of mad cow disease, a fatal brain illness, and E. coli and salmonella contamination.
Source: http://www.usatoday.com/news/nation/2008-06-25-downer-cattle_N.htm

[Return to top]

Water Sector

23. *June 25, Register-Mail* – (Iowa) **Flood inspires plan for clean water.** The city of Galesburg is in line to be reimbursed for some money spent trying to protect its water plant in Oquawka if Knox County is declared a federal a disaster area. The county is one of 21 counties designated a state disaster area by the governor. Local leaders have discussed possible scenarios if FEMA money is made available. The fire chief and director of the Knox County Emergency Management Agency earlier suggested asking whether FEMA money could be used "to help us raise our pump stations in Oquawka, rather high. We could become a central point for clean water once the treatment plant is built." This past spring, the city began building a new water treatment plant on higher ground, outside of the 500-year flood plain. However, at this time, the collector well and other buildings at the site would still be in jeopardy when the Mississippi floods. Last week, the city of Galesburg imposed a boil order, although it continued to pump water from Oquawka, because AmerenIP shut off power to the facility because of the flood. The water from Oquawka was mixed with back-up well water in Galesburg, which is not chlorinated. The fire chief believes raising the other buildings high above the level of possible floodwaters would ensure Galesburg could guarantee a safe supply of water. Source: http://www.galesburg.com/news/x379975430/Flood-inspires-plan-for-clean-water

24. *June 25, Bloomberg* – (Florida) **Florida's $1.75 billion everglades deal quenches thirsty state.** Florida's planned $1.75 billion purchase of thousands of acres of wetland from U.S. Sugar Corp. will reconnect scattered parts of the Everglades to capture new water supplies for a thirsty state. In one of the largest environmental land deals in U.S. history, Florida will get the "missing link'' between Lake Okeechobee and the Everglades, the governor said yesterday. The state will regain control of water reserves that are being channeled to the sea to allow for real estate and industrial development. The conservation effort will help replenish groundwater needed for drinking supplies and buffer the area against hurricanes. It also will cut the flow of agricultural chemicals entering the region known for its alligators and crocodiles.
Source:
http://www.bloomberg.com/apps/news?pid=20601103&sid=aDZ_gjt0UxKE&refer=us

[Return to top]

Public Health and Healthcare Sector

25. *June 26, New York Times* – (New York) **City is pushing for H.I.V. tests for all in Bronx.** The New York City health department plans to announce on Thursday an ambitious three-year effort to give an H.I.V. test to every adult living in the Bronx. The Bronx has a higher death rate from AIDS than any other borough. The campaign will begin with a push to make the voluntary testing routine in emergency rooms and storefront clinics, where city officials say that cumbersome consent procedures required by state law have deterred doctors from offering the tests. "Routine would mean if you came into the emergency room for asthma or a broken leg, we test everyone for H.I.V.,

if they're willing," the health commissioner said in an interview on Wednesday. While Manhattan has long been the epicenter of the AIDS epidemic in New York, with the highest incidence of both AIDS and H.I.V., the Bronx, with its poorer population, has far more deaths from the disease. Public health officials attribute this to people not getting tested until it is too late to treat the virus effectively, thus turning a disease that can now be managed with medication into a death sentence. Several AIDS experts said on Wednesday that the Bronx campaign was the most aggressive testing effort they could recall in the nation.
Source: http://www.nytimes.com/2008/06/26/nyregion/26hiv.html?ref=health

26. *June 26, Search Engine Journal* – (National) **Google and others support online health record privacy framework.** The Common Framework for Networked Personal Health Information standard which was negotiated by Markle Foundation, a New York-based nonprofit group that focuses on uses for information technology, has gained the support of Google, Microsoft, and other online health care players. The newly formulated online health information privacy guidelines set forth the best practices in protecting and securing patient data online. With this policy in place, online health care players are hoping that the industry would gain major ground and earn consumers' trust in partaking in their online health services. The new framework includes guidelines to which participants must adhere and addresses issues on user authentication, audit trails, limiting scope of identifying data to third partie,s and securing data in transit and at rest. It also includes mechanism for enforcing policy and its parameters.
Source: http://www.searchenginejournal.com/google-and-others-supports-online-health-record-privacy-framework/7219/

27. *June 26, Asian News International* – (International) **Two global TB initiatives to be announced on Monday.** Two major health initiatives that will have a substantial impact in the fight against the global tuberculosis (TB) epidemic will be unveiled Monday in a joint announcement by Foundation for Innovative New Diagnostics (FIND), the Stop TB Partnership, UNITAID, and the World Health Organization. TB is one of the world's leading killers - second only to HIV/AIDS - with over 1.5 million deaths and nearly nine million people falling seriously ill every year. Almost half a million people a year develop multidrug-resistant TB (MDR-TB), a dangerous form of TB that is difficult to treat with standard drugs. The spread of drug-resistant strains, especially the recent emergence of virtually untreatable extensively drug-resistant TB (XDR-TB), threatens to push TB control back into a pre-antibiotic era.
Source: http://www.thaindian.com/newsportal/business/two-global-tb-initiatives-to-be-announced-on-monday_10064854.html

28. *June 25, Evertiq* – (International) **RFID chips interfere with medical equipment.** Fifty percent all electrical medical equipment in a Dutch study was so unstable that it put patients in danger when radio frequency identification (RFID) chips were in the vicinity. RFID can interfere with medical equipment at distances up to six meters from the device. The report is published by doctors from the Academic Medical Center at the University of Amsterdam. Two of the most widely used RFID chips have been put in single rooms without patients. Twenty-two risky disorders, two significant disruptions

and 10 less errors were registered. Studies have previously shown that alarm systems in supermarkets also can create electromagnetic interference for people with pacemakers.
Source: http://www.evertiq.com/news/read.do?news=11620&cat=2

29. *June 25, Kansas City Star* – (National) **Woman pleads guilty in identity theft scheme.** A woman pleaded guilty in federal court Wednesday to her role in an identity-theft scheme that sought more than $15 million in illegal tax refunds. The woman, a citizen of Kenya, said she stole the identities of nursing home residents and filed false tax returns in their names. She has been jailed since a grand jury indicted her and 16 others in July 2007. According to court records, she worked for five months beginning in November 2002 as an H&R Block tax preparer and after that prepared returns privately. In early 2005, she and others harvested personal data from residents of at least a dozen local nursing homes and assisted-care centers, according to court records. She then prepared false federal and state tax returns. The conspirators also filed false tax returns in 27 states, using the stolen identities of more than 300 people, most from the Kansas City area, officials said.
Source: http://www.kansascity.com/news/local/story/679618.html

[Return to top]

Government Facilities Sector

30. *June 25, News-Leader* – (Missouri) **Bomb squad checking on danger from chemical bottle.** In Springfield, Missouri, several government buildings are shut down or on lockdown as the fire department's bomb squad checks out a deteriorating bottle of picric acid at the Springfield-Greene County Health Department. City Hall and the Busch Municipal building have been evacuated along with the health department. The streets around the health department have been shut down while the squad assesses the danger. The nearby North Police Headquarters is on lockdown. The chemical was found as the laboratory was being cleaned. The concern is that encrusted material around the bottle's lid indicates the acid has deteriorated, making it potentially explosive.
Source: http://www.news-leader.com/apps/pbcs.dll/article?AID=/20080625/BREAKING01/80625012

31. *June 25, NextGov.com* – (National) **Phishing attacks becoming more sophisticated.** Hostile code attached to e-mail messages is one of the most significant cybersecurity problems federal agencies face today, said an industry analyst and former FBI investigator on Tuesday. Long recognized as a serious problem, phishing attacks send messages masquerading as notices from legitimate organizations or persons to computer users, with the expectation that they will click on a link and enter personal information, such as bank account numbers or passwords. Spear phishing attacks, however, target specific individuals, frequently using their name, and are therefore harder to spot and avoid. Phishing is the most common cyberattack that agencies experience. Of the nearly 63,000 cyber incidents reported to the Homeland Security Department's U.S. Computer Emergency Readiness Team between 2003 and 2006, almost 42,000 were phishing attempts. US-CERT was established in 2003 to coordinate the government's response to cyberattacks.

Source: http://www.nextgov.com/nextgov/ng_20080625_6504.php

[Return to top]

Emergency Services Sector

32. *June 26, Texarkana Gazette* – (Arkansas) **Little River hospital to have disaster drill today.** Little River Memorial Hospital in Ashdown, Arkansas, will sponsor a full-scale disaster drill from 9 a.m. to 1 p.m. Thursday. The drill is being conducted in part by TEC Solutions and the Arkansas Department of Health and is made possible by a federally funded grant. The grant, which has already provided equipment for hospitals statewide, also funded training to prepare health care providers and first responders in terrorism response and all-hazards preparedness. Thursday's drill is targeted to prepare additional responders, including health care providers and public safety organizations, in emergency preparedness. The disaster drill will be directed and critiqued by representatives of TEC Solutions of Pine Bluff, which specializes in this type of training. The full-scope drill offers local agencies the means to test their skills in real time, to gain the in-depth knowledge that only this type of realistic experience can provide, and to build coordinated capacity for disaster and terrorism response.
Source: http://www.texarkanagazette.com/news/WireHeadlines/2008/06/26/little-river-hospital-to-have-disaster-d-18.php

33. *June 26, Gazette.net* – (Maryland) **Pandemic flu drill tests city's readiness.** On June 18, Laurel, Maryland, conducted a pandemic flu drill, in which the flu hit hundreds of homes, forcing families to stay indoors and quarantine themselves. The drill, which tested Laurel's ability to respond to such an emergency, was part of statewide drill of responding to a 5- to 12-week-old pandemic flu epidemic. The group was briefed in the Laurel City Council Chambers before heading out in police cars, armed with electronic devices and bright yellow vests. Their mission was to identify residents with a highly infectious influenza strain and get them the medications they need before the flu spread any more. The city sent placards to 800 homes in three neighborhoods - Ashford, Laurel Hills, and section one of the Villages at Wellington. About 300 homes participated. Residents randomly chose to display placards that either said they were infected or not infected. Infected homes also listed the number of residents and who was sick. Volunteers in police cars used binoculars to read the information, which they marked down in a Juno, a personal digital assistant. The internet-capable device instantly transmitted the information to information technology professionals back at the emergency center set up at the Laurel Armory, who printed medication labels for infected residents. A point of distribution was then set up for infected residents to pick up medication. The department will analyze Laurel's reports in the next 60 days to determine how effective the methods were.
Source: http://www.gazette.net/stories/062608/laurnew174611_32357.shtml

34. *June 25, Sierra Sun* – (California) **Fires in Nevada, Placer counties are lower priority.** More than 1,000 wildfires raging in California have created competition for resources to battle the blazes choking Nevada, Sierra, and Placer counties. A fire official said Wednesday that an air inversion layer will have to lift before smoky conditions

improve. “We’re competing for resources,” said the incident commander for the Yuba River Complex of fires in Nevada and Sierra counties. On Wednesday, only 295 firefighters had been assigned to the complex because fire crews “are at a premium.” The commander was hoping for additional crews by this morning, but it was unclear whether they would arrive.
Source: http://www.sierrasun.com/article/20080625/NEWS/9131306/1051

[Return to top]

Information Technology

35. *June 26, IDG News Service* – (International) **Antispam group outlines defenses to block botnet spam.** A major anti-spam organization is pushing a set of new best practices for ISPs (internet service providers) to stop increasing volumes of spam from botnets. The guidelines, from the Messaging Anti-Abuse Working Group (MAAWG), were drawn up at a meeting in Germany last week and deal with forwarded e-mail and e-mail that is sent from dynamic IP (Internet Protocol) addresses. Many people forward their e-mail from one address to another, a relay that goes through their ISPs mail server. But many ISPs use automated tools that could begin blocking further e-mail to an address if a large volume of e-mail has come through. Legitimate messages would be blocked, too. ISPs can fix this by separating the servers that receive e-mail and ones that then forward e-mail. That way, ISPs can filter out spam coming into the accounts before forwarding, taking a look at the messages, and spotting which ones came from dodgy domains, he said. MAAWG’s second recommendation deals with the long-standing problem of PCs that have been infected with malicious software that sends spam. The PCs are part of botnets, or networks of computers that have been compromised by hackers. After a PC is infected, it will often start sending spam through port 25 straight onto the Internet. That contrasts with legitimate e-mail, which usually goes through the ISP’s mail server first before being sent on. MAAWG’s primary suggestion for ISPs is to block all machines on dynamic IP addresses that are sending e-mail on port 25 outside their own network unless there are special, legitimate circumstances. But MAAWG said that idea may not be possible for some ISPs, and its guidelines offer another alternative: ISPs should share information about their dynamic address space. That would let other ISPs refine their spam filters.
Source:
http://www.pcworld.com/businesscenter/article/147586/antispam_group_outlines_defenses_to_block_botnet_spam.html

36. *June 25, SC Magazine* – (International) **Szirbi botnet causes spam to triple in a week.** Malicious spam has tripled in volume in a week, most of it caused by the Srizbi botnet, according to research by the Marshal TRACE team. In the beginning of June, three percent of total spam was malware. However by the following week, that amount jumped to 9.9 percent. Malcious spam usually contains a URL linking to a malware-serving website. Since February, Srizbi has been responsible for nearly half of all spam, overtaking the previous record holder — the Storm botnet. Srizbi is a pernicious botnet, not just due to its size, but also because it implements an extremely fast mail-sending engine, a senior anti-spam technologist at messaging security vendor MessageLabs said.

With Srizbi, botnet authors "moved the engine into the Windows kernel" "This allows it to send more mail per hour than a regular botnet." Most of the recent malicious spam is capitalizing on two popular ways of social networking. One is to spoof the Classmates.com site by sending messages saying there is an update on friend information. The other is to send a video link with a message stating, "Here's a link of you doing something stupid." "The botnet is very good at keeping out of sight," he added. "It changes frequently, making it more difficult to detect with malware scanners."
Source: http://www.scmagazineus.com/Szirbi-botnet-causes-spam-to-triple-in-a-week/article/111720/

37. *June 25, Blocksandfiles.com* – (International) **USB thumb drives fingered as Trojan carriers.** The Japanese newspaper Yomiuri Shimbun reports a local Trend Micro survey that says USB-carried Trojans are on the rise. The most damaging Trojan is called MAL OTORUN1 along with its derivatives. There were 58 infections of this through flash drives in February, which rose to 138 in March, 110 in April, and 150 last month.
Source: http://blocksandfiles.com/article/5729

38. *June 25, ComputerWorld* – (International) **Cleaning Chinese malware sites a 'bigger challenge' than in U.S., says researcher.** More than half the sites spreading malicious code are hosted on Chinese networks, an anti-malware group said Wednesday. Of the over 213,000 malware-hosting sites analyzed last month by Stopbadware.org — a joint effort of researchers at Harvard University, Oxford University and several corporations, including Google Inc. and Sun Microsystems Inc. — 52% were hosted by servers running Chinese IP addresses. Of the top 10 networks serving malicious code, six are Chinese. The U.S. hosts 21% of the malware sites, giving it the dubious honor of second place. Stopbadware.org, which uses data collected by Google's crawlers, would not speculate on what proportion of the sites, Chinese or otherwise, are deliberately hosting malicious code and what fraction are actually legitimate sites that have been hacked. But the dramatic year-to-year growth in the number of sites serving up malware is likely due to a boom in site hacking. The problem has become so acute, said Microsoft Corp. Tuesday, that it and Hewlett-Packard Co. joined forces to launch free tools that site developers and administrators can use to search for vulnerable code and block incoming attacks
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9103378&taxonomyId=17&intsrc=kc_top

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: http://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]

Communications Sector

39. *June 26, Xinhua* – (International) **African countries meet over submarine fiber optic cables.** Ten African countries are meeting in Lome, Togo, to explore and work out ways to promote and enhance access to the deployment and use of fiber optic technologies across parts of West and Central Africa, according to official sources. The meeting, which began on Wednesday, will deliberate on ways to spur the implementation of the Agreement for Construction and Maintenance as well as contracts for the supply of the system, approved and signed by the governments of the ten countries. The ten countries, all member states of the Interim Committee for the Management Project of Fiber Optic Submarine Cables (WAFS), are scheduled to meet for two days in a bid to address the issue of communications in the sub-region, according to a statement issued by the organizers of the event. The WAFS project is intended to lay a series submarine fiber optic cables along the West African coast while passing through ten members, including Togo, Benin, Cameroon, Angola, the Republic of Congo, Gabon , Equatorial Guinea, the Democratic Republic of Congo, Botswana, and South Africa. These cables will be interconnected with other fiber optic cables, which are already existent in the West African sub-region. They will be used to provide broadband internet services in each of these countries.
    Source: http://news.xinhuanet.com/english/2008-06/26/content_8444681.htm

40. *June 26, New York Times* – (New York) **More delays for cameras in subways.** Aging fiber-optic cable in Brooklyn and Queens has become the latest obstacle to a planned high-tech system of surveillance cameras meant to safeguard the subway and commuter railroads, according to Metropolitan Transportation Authority officials. The system, which is expected to cost at least $450 million, is a crucial component of a larger program to thwart terrorist attacks on the region's transportation network, but it has met repeatedly with technical problems and delays. On Wednesday, the authority's board authorized the replacement of 84,000 feet of old fiber-optic cable, which was installed in the late 1980s. The replacement will cost $5 million and is being done as part of a separate project to build out the subway's data network. According to a board document, tests on the cable showed that it had "many broken fibers unsuitable to carry the high bandwidth required" to transmit large amounts of data, which hindered the surveillance camera project. The document did not say how long it would take to replace the cable.
    Source: http://www.nytimes.com/2008/06/26/nyregion/26security.html?ref=nyregion

41. *June 25, Network World* – (National) **Avaya, Cisco and Nortel face VoIP vulnerabilities.** Voice-over-IP (VoIP) customers of Avaya, Cisco, and Nortel should look Wednesday for patches that correct newly found vulnerabilities that, if exploited, can result in remote code execution, unauthorized access, denial of service, and information harvesting. The vulnerabilities were found by VoIPshield Laboratories, the research division of VoIPshield Systems Inc., and reported earlier to the three vendors to give them time to develop patches for the flaws, said the president and chief executive officer of VoIPshield. He would not reveal more details because his company and the affected VoIP vendors agreed to a simultaneous announcement. Details of the vulnerabilities and the vendor responses are scheduled to be released Wednesday at

noon Eastern Standard Time. The vulnerabilities affect voice servers -- VoIP PBXes -- and softphone software that runs on laptops and desktops. VoIPshield ranks most of the vulnerabilities found as either critical or high, the two most severe rankings on its four-step scale. Avaya, Cisco, and Nortel were chosen for vulnerability testing because they represent the bulk of IP PBX sales in North America.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9103318&taxonomyId=17&intsrc=kc_top

[Return to top]

Commercial Facilities Sector

Nothing to report

[Return to top]

National Monuments & Icons Sector

42. *June 25, Las Vegas Sun* – (Nevada) **New mining claims banned in region around Grand Canyon National Park.** The House Natural Resources Committee invoked rarely-used powers to ban new mining claims on about a million acres adjacent to Grand Canyon National Park. Between January 2003 and January 2008, the number of claims within five miles of Grand Canyon National Park increased from 10 to more than 1,100, according to Bureau of Land Management data compiled by the Environmental Working Group. The House resolution will not impact valid claims already staked; companies could still mine these claims even if their activities might threaten the Canyon or the Colorado River, according to Environmental Working Group. "The resolution is a critically important stopgap measure to temporarily halt a new wave of uranium mining near the Grand Canyon allowed under the antiquated 1872 mining law," said the air and energy director for the Grand Canyon Trust, in a statement. "It gives Congress time to pass legislation needed to permanently withdraw the lands from mining, prevent uranium mining from further threatening Grand Canyon's seeps and springs, and from diminishing the experience of millions of visitors from around the world."
Source: http://www.lasvegassun.com/blogs/news/2008/jun/25/new-mining-claims-banned-region-around-grand-canyo/

[Return to top]

Dams Sector

43. *June 26, Independent* – (International) **MI5: revealing areas at mercy of collapsing dams is a terror threat.** MI5 and flood risk experts are at odds over whether to publish inundation maps highlighting areas under threat if any of the United Kingdom's dams were to collapse. The Security Service says that the information could show terrorists where an attack on a dam might have the most impact. Experts in the Cabinet Office and the Environment Agency feel the time has come to make the information public, as the

risk of major flooding rises with climate change. Just how grave the threat is was illustrated yesterday when it was revealed that record rainfall nearly caused a Yorkshire dam to fail, with catastrophic consequences. Yet emergency services facing this crisis had no maps of potential inundation to work from and had to work it out themselves. He added that because of climate change, flooding in Britain was itself likely to become a risk as great as terrorism or an influenza pandemic. According to Cabinet Office and Environment Agency sources, the Water Act 2003 had specified that the maps should be made public, but this had not happened after MI5 objected.
Source: http://www.independent.co.uk/environment/climate-change/mi5-revealing-areas-at-mercy-of-collapsing-dams-is-a-terror-threat-854325.html

44. *June 25, Greater Milwaukee Today* – (Wisconsin) **Mukwonago dam finally stable.** With the Mukwonago dam stable, work is now going to be done to assess the damage, officials said Tuesday at a joint town and village protective services committee meeting. The Mukwonago fire chief said the dam is now being drained, which is causing Phantom Lake to be several inches under its normal level. The dam is being drained to allow one side to be shut down, so in the next few days dam experts from the state's Department of Natural Resources (DNR) can assess it, he said. There may be some Federal Emergency Management Agency funds coming to build concrete spillways on both sides of the dam, in case spillage occurs again. There used to be spillways, but the DNR requested they be taken out, he said.
Source: http://www.gmtoday.com/news/local_stories/2008/June_08/06252008_07.asp

[Return to top]