Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report
for 17 July 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports the top official at Interpol has said that groups like al Qaeda and Hezbollah have turned to trafficking in counterfeit consumer goods, like fake Nike shoes, Sony stereo equipment and Calvin Klein jeans. (See item 5)
- Microsoft has released "Security Bulletin MS03−026: Buffer Overrun In RPC Interface Could Allow Code Execution (Critical)," and a patch is available on the Microsoft Website. (See item 22)
- Microsoft has released "Security Bulletin MS03−027: Unchecked Buffer in Windows Shell Could Enable System Compromise (Important)," and a patch is available on the Microsoft Website. (See item 23)
- Microsoft has released "Security Bulletin MS03−028: Flaw in ISA Server Error Pages Could Allow Cross−Site Scripting Attack (Important)," and a patch is available on the Microsoft Website. (See item 24)
- The Department of Homeland Security, FedCIRC has issued "DHS/FedCIRC Advisory FA−2003−15 Cisco IOS Interface Blocked by IPv4 Packet." (See item 25)
- Internet Security Systems has raised AlertCon to Level 2, with a need for increased alertness.
- SecurityFocus has raised ThreatCon to Level 2, with a need for increased alertness.

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web 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://esisac.com]

1. *July 16, Reuters* — **Twenty−two pounds of low−grade Iraqi uranium dispersed. The United Nations nuclear watchdog said on Wednesday it had accounted for most of the looted nuclear material at Iraq's main nuclear facility, but at least 22 pounds of low−grade uranium may have been dispersed. The International Atomic Energy Agency (IAEA) announced these conclusions in a report sent to the UN Security Council on Tuesday about its inspection of the Location C storage facility outside of the Tuwaitha complex near Baghdad.** In the post−war chaos in Iraq, looters broke into Tuwaitha's Location C and at least six other nuclear sites in Iraq and emptied out the contents of hundreds of containers of nuclear material. Most of the material and containers were recovered. "The quantity and type of uranium compounds dispersed are not sensitive from a proliferation point of view," IAEA Director General Mohamed ElBaradei wrote in the report. **This low−grade natural uranium would also be of little use in a so−called dirty bomb, which is the dispersion of radioactive material over a wide area with a conventional explosive like dynamite.** The IAEA first warned the United States and Britain in April that it was necessary to secure all of Iraq's nuclear facilities to prevent an environmental, medical and humanitarian emergency. The IAEA inspectors did not get to Iraq until early June.
Source: http://www.nytimes.com/reuters/international/international−i raq−nuclear.html

2. *July 15, Birmingham Post (UK)* — **Huge wind farms given go−ahead for Britain.** The biggest offshore wind farms in the world are to be built around the coast of Britain after the Government gave the green light yesterday to speed up the development of green power. **Huge areas off the coasts of Essex, Norfolk and the North West will be opened to farms each containing up to 300 turbines, which could be powering one in six households by the year 2010. Up to 20,000 new jobs will be created by the decision, which campaigners described as the dawn of a new clean energy era.** The new turbines will have 80 metre high towers and 50 metre long blades, the biggest ever to be used anywhere in the world, but they will be sited five miles out to sea to lessen the visual impact. Ministers are confident that the massive expansion will not affect bird migration routes or interfere with military radar. **The Government decided to step up its commitment to provide 10 per cent of Britain's energy from renewable sources by the year 2010 after a huge amount of interest from companies three years ago which led to 17 proposals to develop offshore wind farms.** The first project, by National Wind Power, involves 30 turbines off the North Wales coast, and is expected to start producing power later this year.
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3992056

3. *July 15, PR Newswire* — **Pepco assures customers that power supply will continue despite Mirant bankruptcy filing.** Pepco said today there is no interruption of power supply to its 700,000 customers in the Washington, DC area as a result of yesterday's bankruptcy filing by Mirant Corp. Mirant operates several power plants in the region and supplies power to Pepco customers under a contract with Pepco, a subsidiary of Pepco Holdings, Inc. **Mirant is continuing to supply power to Pepco under the terms of its contract and prices to Pepco's Standard Offer Service customers are unaffected.** These prices can be changed only by order of the Public Service Commissions in Maryland and the District of Columbia. **If at a later time Mirant moves to terminate the contract, Pepco has other options to ensure power supply is continued.**

Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=comtex_2003_07_15_pr_0000−2835−dc−pepco−mirant−power&SMContentSet=0

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *July 16, U.S. Department of Defense* — **National Guard and Reserve mobilized as of July 16, 2003.** This week, the Army, Air Force, Navy and Marine Corps each announce a decrease of reservists on active duty in support of the partial mobilization. The net collective result is 3,001 fewer reservists than last week. **The total number currently on active duty in support of the partial mobilization for the Army National Guard and Army Reserve is 136,835; Naval Reserve 8,853; Air National Guard and Air Force Reserve, 32,443; Marine Corps Reserve, 20,143; and the Coast Guard Reserve, 2,825. This brings the total Reserve and National Guard on active duty to 201,099 including both units and individual augmentees.** Source: http://www.dod.mil/releases/2003/nr20030716−0197.html

[Return to top]

Banking and Finance Sector

5. *July 16, New York Times* — **Fake goods support terrorism, Interpol official is to testify. Groups like al Qaeda and Hezbollah have turned to trafficking in counterfeit consumer goods, like fake Nike shoes, Sony stereo equipment and Calvin Klein jeans, says the top official at Interpol, who is scheduled to testify about the issue on Wednesday at a Congressional hearing.** "The link between organized crime groups and counterfeit goods is well established," states the written testimony by Ronald K. Noble, the secretary general of Interpol, to be presented at the House Committee on International Relations. "But Interpol is sounding the alarm that intellectual property crime is becoming the preferred method of funding for a number of terrorist groups." **The booming international trade in phony consumer goods has long been known and its links to terrorist groups often suspected by government agencies. But Congressional officials said that Noble's testimony was the first by a senior law enforcement official to conclude emphatically, on a global basis, that the trade in counterfeit consumer products financed terrorism.** Noble's appearance is the first time an Interpol secretary general has testified to a Congressional panel. A former senior official at the Justice and Treasury Departments, Noble took over in 2000 at Interpol, which coordinates information among police and security services in 181 countries. Source: http://www.nytimes.com/2003/07/16/national/16TERR.html

[Return to top]

Transportation Sector

6. *July 16, Financial Times* — **American halves flights from St Louis hub. American, the world's largest airline, underlined the problem of over−capacity in the U.S. market when it moved to halve the flights from its St Louis hub, as part of its effort to return to profitability.** The decision to shrink the hub from 417 flights a day to 207 flights, comes amid fierce last minute lobbying from Bob Holden, Governor of Missouri to protect service. **The decision also reflects the fact that American misjudged potential demand with its badly timed takeover of Trans World Airlines in 2000, whose headquarters were in St Louis.** The need to reduce operations comes amid continued losses in the airline industry. American said it lost $357m in the second quarter, a sharp improvement on its first quarter losses of $1.04bn and losses of $720m a year ago. Gerard Arpey, chief executive, warned, "we have a lot of work to do before we're able to achieve sustained profitability at acceptable levels." **American's net loss for the quarter was lifted by a $358m cash payment from the federal government, part of a package agreed to reimburse airlines for security costs.** The airline said it had also started to reap the benefits of its wage concessions, evident in the 12 per cent drop in salaries and benefits during the quarter to $1.9bn.
Source: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1057562466163

7. *July 16, Associated Press* — **Gov. Kulongoski tours the Oregon's bridges to promote repair bill. On Tuesday, the governor visited sites in Eugene and Portland, aiming to boost enthusiasm for what he calls the largest public works project since Interstate 5 was built in Oregon in the 1960s. Kulongoski made plugs for the project on two fronts: repairing crumbling roads and bridges necessary for transport, and putting thousands of unemployed Oregonians back to work.** The state's faltering bridges and highways would be repaired over the next decade with $2.5 billion package of bonds backed by revenue from higher auto registration and title fees and increased truck fees and weight mile taxes. Construction companies estimate the work would produce 4,700 jobs per year. **Bruce Warner, director of the transportation department, says that without major repairs, by 2010 more than one−third of the state's 660 bridges won't be traversable by large trucks. An economic analysis by the department found that such bridge deterioration would cost the state $125 billion in business and 80,000 jobs over the next 25 years, he said.** "If you look around at businesses, you see that sooner or later everything comes in on a truck," Warner said. "This is a big deal for the people of Oregon."
Source: http://www.theworldlink.com/articles/2003/07/16/news/news08. txt

8. *July 16, Cambridge Chronicle (Cambridge, MA)* — **Massachusetts bridges flunk test.** The short Walden Street overpass in North Cambridge doesn't look much different from any other bridge in the city − which is to say, it's in need of minor repairs. Aside from superficial problems, though, the bridge appears fine, especially considering it was built in 1914. **But identical signs on both ends of the bridge hint at a bigger, but more hidden, problem − one that is plaguing bridges throughout the state. The signs read, "Weight limit 6 tons." Presumably, heavier vehicles would put the structure at risk. The Walden Street bridge isn't alone. More than half of the 2,505 bridges in Massachusetts are considered deficient, the second−worst ratio in the nation behind Rhode Island, according to recent federal**

statistics. However, just the Walden Street bridge is categorized as "structurally deficient," while the other seven deficient bridges are "functionally obsolete." **Bridges are structurally deficient if they have been restricted to light vehicles, require immediate repairs or are closed. Functionally obsolete bridges are those that don't meet current size and safety standards. There are 645 structurally deficient bridges in Massachusetts and 1,860 functionally obsolete bridges. "Massachusetts has one of the oldest infrastructures in the country by virtue of being one of the oldest states," Carlisle said.**
Source: http://www.townonline.com/cambridge/news/local_regional/cam_covccbridgesmsgr07162003.htm

9. *July 16, Rocky Mountain News* — **More layoffs at United. United Airlines told its pilots union that it expects to furlough another 600 to 800 pilots by next July as part of its restructuring efforts, a union official said Tuesday.** The furloughs would come on top of 201 layoffs planned in the next six weeks and 1,555 since the September 11, 2001, attacks. United's projection "is their best guess" as airline executives draft a business plan to emerge from bankruptcy protection, said Scottie Clark, a spokesperson for United's pilots union. United, which filed for bankruptcy December 9, has about 8,400 active pilots. Its furlough projections take into account its plans to shift more capacity to its United Express commuter carriers, as well as other schedule changes, Clark said. **United, its United Express carriers and the pilots union are in talks on an agreement that would require the commuter affiliates to hire furloughed United pilots to fly any 70−seat regional jets, Clark said.**
Source: http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN_4_2112492,00.html

[Return to top]

Postal and Shipping Sector

10. *July 16, Associated Press* — **Post office finds powder in letters. A postal worker found white powder in about 20 letters addressed to politicians around the country early Tuesday, but Florida state health officials said preliminary tests found the material was harmless.** Samples of the powder were sent to a state Health Department testing laboratory in Jacksonville, agency spokesman Rob Hayes said. He did not expect final results of the powder's composition for two or three days. The letters, found at the city's main post office near downtown Tallahassee, were addressed to several members of Congress, Tallahassee Fire Department spokeswoman Pat Teague said. Postal workers immediately secured the area after discovering the powder and called 911, Teague said. A hazardous materials team decontaminated the area, and no postal workers are thought to have been contaminated by the powder.
Source: http://www.sptimes.com/2003/07/16/State/Post_office_finds_po w.shtml

11. *July 15, Financial Times* — **Investors complete DHL Airways deal. DHL Airways said on Monday that a group of U.S. investors led by John Dasburg, chief executive, had completed a buy−out, putting the air cargo carrier under the firm control of U.S. shareholders. DHL Airways argued that Dasburg's move should put paid to claims that the Miami, FL based carrier is foreign−controlled.** The U.S. Department of Transportation (DOT), at the behest of United Parcel Service and FedEx, is examining DHL Airways'

ownership structure to ascertain if it violates foreign ownership laws. **Under U.S law, a foreign company cannot control a U.S. air carrier. Both UPS and FedEx have claimed that DHL Airways, through a series of complicated partnerships and financing arrangements, is in effect controlled by German postal operator Deutsche Post.** The DOT's administrative law judge is expected to issue a decision on the ownership structure by October 31.
Source: http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1057562394021

[Return to top]

Agriculture Sector

12. *July 16, Japan Today* — **WTO rules Japan's apple import rules illegal. Japanese health rules on imported U.S. apples that include a 545−yard buffer zone around orchards and regular inspections are illegal under international trade law, the World Trade Organization (WTO) said Tuesday. A panel of trade experts found that Japan's measures, designed to protect its own apple trees from fire blight, are not based on scientific evidence.** The ruling was made following a complaint by the United States. Fire blight is a bacterial infection that affects apples, pears and roses. It is carried between trees by rain, wind and insects and is widespread in the United States. Japan, which does not have fire blight, imposed a series of strict rules on imports of U.S. apples to ensure that they could not carry the bacteria either on their surfaces or internally. The United States last year brought a complaint to the WTO, claiming that the restrictions are unnecessary and are preventing U.S. apple growers from selling their crops to Japan.
Source: http://www.japantoday.com/e/?content=news&cat=3&id=266517

13. *July 15, University of Wisconsin−Madison* — **Scientists find gene that protects against potato blight. Scouring the genome of a wild Mexican potato, scientists have discovered a gene that protects potatoes against late blight, the devastating disease that caused the Irish potato famine.** The identification of the gene, found in a species of wild potato known as Solanum bulbocastanum, holds significant potential. **All of the varieties now cultivated commercially on more than 1.5 million acres in the United States are highly susceptible to potato late blight, a family of fungal pathogens that wreaks havoc in the field, turning tubers to mush and invariably killing any plant it infects. With the blight−resistant gene in hand, the Wisconsin team was able to engineer plants that survived exposure to the many races of Phytophthora infestans.** The insertion of a single gene effectively protects plants from the range of late blight pathogens. **Prior to the 1990s, chemical fungicides were available in the United States and effectively held the disease at bay. But new strains of the pathogen have emerged, testing the limits of the technology and requiring American farmers to treat potato fields as many as a dozen times a season at a cost of up to $250 per acre.** In warmer climates such as Mexico, fields may be treated as many as 25 times a year with the costly and toxic chemicals.
Source: http://www.sciencedaily.com/releases/2003/07/030715090635.ht m

14. *July 15, Associated Press* — **Wheat rust causes concern in Washington state. A new strain of a disease that turns wheat the color of rust is hurting the crop in eastern Washington this summer.** Researchers at Washington State University (WSU) are scrambling to create a

wheat variety that is resistant to the new strain, or race, of stripe rust. "The new race showed up last year," said WSU agronomist Diana Roberts in Spokane. "It overcame the resistance in the varieties we have." Farmers are spending some $20 per acre to spray chemicals to fight the stripe rust, Roberts said. But spraying with fungicides does not make economic sense if crop yields are not high, she said. **"You can't get rid of the pathogen," Roberts said. "You have to develop varieties that are resistant to it." That can take as long as five years, she added.** Rust stripe can reduce crop yields by 60 percent, but the scope of the problem in Washington is not clear, Roberts said. **Last summer, farmers spent an estimated $2 million on chemicals and crop−dusters to save susceptible spring wheat.**
Source: http://www.theolympian.com/home/news/20030715/northwest/5233 6.shtml

[Return to top]

Food Sector

15. *July 15, Food and Drug Administration* — **FDA to review ways to reduce the risk of food contamination. As part of its continuing effort to ensure the safety and security of the nation's food supply, the Food and Drug Administration Tuesday announced it has contracted with the Institute of Food Technologists (IFT) to conduct an in−depth review of preventive measures that food processors may take to reduce the risk for an intentional act of terrorism or contamination.** As part of this contract, IFT will provide information about temperature, technology, chemical treatments, and other ways that may reduce or mitigate the risk. The review will assess ways to prevent or reduce the risk of contamination of processed food either through natural or intentional acts and will provide information on various research needs that might be used for eliminating or reducing the risk. **The review will include information on how these research needs technologies work, optimization of the method or processes, effectiveness, limitations in use, and equipment or methods for monitoring to ensure method and processes efficiency throughout the entire operation.**
Source: http://www.fda.gov/bbs/topics/NEWS/2003/NEW00925.html

16. *July 15, CIDRAP* — **UN commission adopts new standard for irradiated foods. The United Nations' food standards body announced last week that it would allow higher kiloGray (kGy) doses for irradiating food.** The Codex Alimentarius Commission, the highest international body on food standards, will now allow irradiation doses greater than 10 kGy when "necessary to achieve a legitimate technological purpose." The new standard also states, "The minimum absorbed dose should be sufficient to achieve the technological purpose, and the maximum absorbed dose should be less than that which would compromise consumer safety, wholesomeness, or would adversely affect structural integrity, functional properties, or sensory attributes." **Higher doses of irradiation would also mean that previously radiation−resistant pathogens, including Clostridium botulinum, could be eliminated.** "This is a really important breakthrough," said Alan Randell, the Codex Alimentarius Commission secretary. "For the consumer it means a potential for higher levels of food safety because of the protection offered by food irradiation. For example, it can be applied to spices which can carry bacteria resistant to other treatments."
Source: http://www.cidrap.umn.edu/cidrap/content/fs/irradiation/news /july15codex.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *July 16, Advocate* — **CDC: West Nile likely worse now.** The head of the U.S. Centers for Disease Control and Prevention (CDC) sounded the alarm Tuesday that this year's round of the mosquito−borne West Nile virus may be worse than last year's. The CDC has confirmed four human cases this year: three in Texas and one in South Carolina. **On Tuesday, CDC Director Dr. Julie Gerberding held a news conference saying more West Nile activity is being reported so far this year than by the same time last year. She said 34 states have reported some form of West Nile virus activity this year, compared to "about 20" by the same week in 2002. Gerberding said officials are not sure whether this year will wind up being worse than last.** Gerberding said CDC expects the new, quick test to diagnose more cases this year, but the agency will not count the results as official unless confirmed by state health departments. **Also, Dr. James Meegan, virology program officer for the National Institute of Allergy and Infectious Diseases, said scientists are working on vaccines and therapy drugs. One concept is creating a new vaccine based on a well−established yellow fever vaccine, "which has been around 70 years and has an excellent safety record," Meegan said.**
Source: http://www.2theadvocate.com/stories/071603/new_cdc001.shtml

18. *July 16, New York Times* — **Broad study finds significant resistance to AIDS drugs. The biggest study so far of resistance to AIDS drugs finds that about 10 percent of all newly infected patients in Europe are infected with drug−resistant strains.** The researcher who led the study called the level "surprisingly high." Other scientists at the conference agreed that the findings had worldwide public health implications and made the hunt for new classes of AIDS drugs even more critical. **They said the figure suggests that an "order of battle" approach to prescribing AIDS drugs, like that used for tuberculosis medicines, should be adopted in place of the current free−for−all.** For example, a drug like nevirapine, which can prevent mother−child transmission with just one dose, might be restricted to that use only, so resistance to it cannot grow as it would if thousands of patients were put on it for life. Also, public health authorities could tell doctors which drug combinations to prescribe first, second, and third as resistance was encountered. **Some doctors said the study suggested that all new AIDS patients should be tested to determine the drug resistance of the strains infecting them. Those tests can cost from $200 to $800 each and take from a week to a month to complete. Those factors could greatly raise the price of plans to bring inexpensive AIDS drugs to poor countries.**
Source: http://www.nytimes.com/2003/07/15/health/16CND−DRUG.html

19. *July 16, Associated Press* — **SARS travel alert to Taiwan lifted. U.S. officials Tuesday lifted a Severe Acute Respiratory Syndrome (SARS) related travel alert for Taiwan, the only area remaining on a federal health alert list.** The U.S. Centers for Disease Control and

Prevention (CDC) said the Taiwan alert was lifted because more than 30 days had elapsed since the last SARS case there. "Currently, no areas in the world are reporting ongoing transmission of the disease," the CDC said. A CDC travel alert is not a recommendation against travel to an area, but it advises travelers of a health concern. Hong Kong was dropped from the list Thursday.
Source: http://www.sunherald.com/mld/sunherald/news/breaking_news/63 11859.htm

[Return to top]

Government Sector

20. *July 16, Baltimore Sun* — **FAA's approval sought for drones.** Unmanned planes have proved their worth in wars in Iraq and Afghanistan, and now those who build them are thinking beyond the battlefields to a day when pilotless drones may fly in the nation's civilian airspace. **Defense industry and government officials taking part in a symposium on robotic technology and unmanned flight met at the Baltimore Convention Center on Tuesday to begin an effort to bring that day closer. They hope to develop uniform standards and regulations for unmanned aircraft, with the goal of convincing the Federal Aviation Administration that the planes can fly safely alongside commercial helicopters and passenger jets.** FAA approval − likely years away − is regarded as a critical step in exploiting the commercial potential of unmanned aerial vehicles, which have so far found prominence only as government research platforms and military surveillance and strike planes.
Source: http://www.sunspot.net/technology/bal−bz.unmanned16jul16,0,2 288152.story?coll=bal−technology−headlines

21. *July 15, Government Executive* — **IRS official to head Homeland Security procurement.** A senior procurement official with the Internal Revenue Service has been tapped to become procurement chief of the Homeland Security Department, IRS officials said Tuesday. **Greg Rothwell, who currently serves as the deputy chief of agencywide shared services at IRS, is widely regarded as one of the most seasoned and innovative procurement executives in the federal government. He will take a position that has sat vacant at the new department since it was established in March. Since then, Homeland Security Department officials have debated over how to structure the procurement function, according to sources close to the discussions.** The debate has often centered on the role of procurement versus acquisition −− the longer−term process of crafting purchasing strategies to meet an agency's needs. It has become so contentious at times that some observers felt only a widely respected and admired executive would stand a chance of making headway in the job. Some of Rothwell's former colleagues said he fits that bill, and that his appointment is a signal to the Homeland Security leadership that procurement will be given a high priority.
Source: http://www.govexec.com/dailyfed/0703/071503h1.htm

[Return to top]

Emergency Services Sector

Nothing to report.

[Return to top]

Information and Telecommunications Sector

22. *July 16, Microsoft* — **Microsoft Security Bulletin MS03−026: Buffer Overrun In RPC Interface Could Allow Code Execution.** Remote Procedure Call (RPC) is a protocol used by the Windows operating system which provides an inter−process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. **There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP** which results because of incorrect handling of malformed messages. This vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines to the server. **To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135. If successful, an attacker could then run code with Local System privileges on an affected system and then be able to take any action on the system**, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. **Microsoft has assigned a risk rating of "Critical" to this issue** and recommends that system administrators install the patch immediately.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−026.asp

23. *July 16, Microsoft* — **Microsoft Security Bulletin MS03−027: Unchecked Buffer in Windows Shell Could Enable System Compromise. An unchecked buffer exists in one of the functions used by the Windows shell to extract custom attribute information from certain folders**. An attacker could seek to exploit this vulnerability by creating a Desktop.ini file that contains a corrupt custom attribute, and then host it on a network share. **If a user were to browse the shared folder where the file was stored, the vulnerability could then be exploited. A successful attack could have the effect of either causing the Windows shell to fail, or causing an attacker's code to run on the user's computer in the security context of the user. This vulnerability only affects Windows XP Service Pack 1. Microsoft has assigned a risk rating of "Important" to this issue** and recommends that system administrators install the patch at the earliest opportunity.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−027.asp

24. *July 16, Microsoft* — **Microsoft Security Bulletin MS03−028: Flaw in ISA Server Error Pages Could Allow Cross−Site Scripting Attack.** ISA Server contains a number of HTML−based error pages that allow the server to respond to a client requesting a Web resource with a customized error. **A cross−site scripting vulnerability exists in many of these error pages that are returned by ISA Server under specific error conditions**. To exploit this flaw, an attacker would have to first be aware of a specific ISA server and its access policies or host an ISA server of their own and create specific access policies designed to exploit this vulnerability. The attacker could then craft a request to trigger a page refusal and host a Web site containing the link, or send the link to the user in the form of an HTML e−mail. After the user previewed or opened the e−mail, the malicious site could be visited automatically without further user interaction. **The vulnerability would not normally enable an attacker to gain**

any privileges on an affected ISA Server computer, breach the firewall, or compromise any cached content, unless the user is operating on the ISA server itself and is using the Web Proxy service to access the Internet. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch at the earliest opportunity.
Source: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03−028.asp

25. *July 16, U.S. Department of Homeland Security, FedCIRC* — **DHS/FedCIRC Advisory FA−2003−15 Cisco IOS Interface Blocked by IPv4 Packet. A vulnerability in many versions of Cisco IOS could allow an intruder to execute a denial−of−service attack against a vulnerable device.** Cisco IOS is a very widely deployed network operating system. A vulnerability in IOS could allow an intruder to execute a denial−of−service attack against an affected device. Cisco has published an advisory on this topic, available at http://www.cisco.com/warp/public/707/cisco−sa−20030717−block ed.shtml According to Cisco, a device receiving specially crafted IPv4 packets will force the inbound interface to stop processing traffic. This issue can affect all Cisco devices running Cisco IOS software. **This vulnerability may be exercised repeatedly resulting in loss of availability until a workaround has been applied or the device has been upgraded to a fixed version of code.** The solution to this vulnerability is to **apply the appropriate patch from Cisco.** Until a patch can be applied, you can mitigate the risks presented by this vulnerability by **judicious use of access control lists (ACLs).** For more information, see http://www.cisco.com/warp/public/707/cisco−sa−20030717−block ed.shtml#workarounds
Source: http://www2.fedcirc.gov/advisories/FA−2003−15.html

26. *July 15, Government Accounting Office* — **GAO−03−987T: Polar−Orbiting Environmental Satellites: Project Risks Could Affect Weather Data Needed by Civilian and Military Users.** Polar−orbiting environmental satellites that provide the data and imagery used by weather forecasters, climatologists, and the military to map and monitor changes in weather, climate, the ocean, and the environment. In the future, the National Polar−orbiting Operational Environmental Satellite System (NPOESS) is to merge the two current satellite systems. **The Government Accounting Office (GAO) found that the NPOESS program faces key programmatic and technical risks that may affect the successful and timely deployment of the system**. The NPOESS was supposed to be available to serve as a backup to the March 2008 launch of the final satellite in one of the two current satellite programs−−the Polar−orbiting Operational Environmental Satellite (POES) system. However, **the first NPOESS satellite will not be ready in time, resulting in a potential gap in satellite coverage should the satellite fail. If the final POES launch fails and if existing satellites are unable to continue operations beyond their expected life spans, the continuity of weather data needed for weather forecasts and climate monitoring will be put at risk**.
Source: http://www.gao.gov/highlights/d03987thigh.pdf

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 137 (netbios−ns), 445 (microsoft−ds), 1434 (ms−sql−m), 113 (ident), 4662 (eDonkey2000), 139 (netbios−ssn), 25 (smtp), 0 (−−−), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *July 16, Fox News* — **Terrorists may be eyeing North Americans.** Law enforcement officials are increasingly concerned about terrorist groups' recruitment efforts that seem to be targeting North Americans, officials told Fox News. None of the September 11 hijackers carried American or Canadian passports but terrorism analysts believe al Qaeda and other terror rings may be adapting to tighter security in the United States. **"They're [terror rings] looking for westernized Muslims, westernized operatives who are able to slip by law enforcement, who don't fit that traditional model," said Evan Kohlman, a senior terrorism analyst with the Washington−based Investigative Project. "Al Qaeda is not stupid, they know what we're looking for and they're looking to get around it."** Kohlman noted that someone with a Canadian passport could get in to the United States "with little suspicion." **Senior administration officials told Fox News that the United States sees potential repercussions of Canada's leniency for security within U.S. borders.**
Source: http://www.foxnews.com/story/0,2933,91984,00.html

28. *July 16, Associated Press* — **Claudette weakens after slamming Texas coast.** Hurricane Claudette slammed the Texas coast on Tuesday with high winds and heavy rains, causing widespread damage before weakening to a tropical storm as it moved inland. What had been a slow−moving tropical storm strengthened into a hurricane with 80−mph winds shortly before landfall at midmorning near Matagorda Bay, 80 miles southwest of Houston, and struck with surprising fury. **It was the third named storm of the 2003 Atlantic hurricane season, but the first hurricane. From the island city of Galveston to Port O'Connor, 110 miles to the southwest, Claudette left a trail of destruction, but no known casualties.** The National Hurricane Center downgraded Claudette to a tropical storm and said it would likely be a tropical depression by day's end.
Source: http://www.nytimes.com/reuters/news/news−weather−claudette.h tml

29. *July 16, Associated Press* — **Thousands flee blaze on Arizona reservation.** The governor of Arizona declared a state of emergency in two counties as a forest fire swept across an Indian reservation, forcing thousands of people to leave their homes as a precaution. Elsewhere in the Southwest, Mesa Verde National Park in Colorado was closed to visitors for the second time in two years because of wildfires. **As many as 5,000 people had fled their homes in Whiteriver, headquarters of the White Mountain Apache Tribe, and other communities on the Fort Apache Indian Reservation.** The 12,600−acre Kinishba fire chased off firefighters in some areas Tuesday with flames shooting 250 feet in the air. **The fire was started by lightning Sunday east of the starting point for last summer's Rodeo−Chediski fire, the largest wildfire in state history. Last year's fire charred 469,000 acres and destroyed 491 homes.** Source: http://www.washingtonpost.com/wp−dyn/articles/A64344−2003Jul 16.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.