Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 18 May 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Network World reports criminals are increasingly targeting corporations with distributed denial−of−service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies. (See item 4)
- The Associated Press reports that for the second time in a week, an international flight headed for Boston has landed instead in Bangor, Maine, because a passenger's name matched one on the government's no−fly list. (See item 5)
- Government Technology reports homeland security alerts and other critical information will now be sent to Pennsylvania State Police troopers directly through e−mails under a technology enhancement. (See item 21)

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. *May 17, Associated Press* — **BP says personnel failures led to blast.** BP PLC, one of the world's largest oil companies, said Tuesday, May 17, that failures by its staff led to the March explosion and fire that killed 15 workers and injured more than 170 others. "The mistakes made during the startup of this unit were surprising and deeply disturbing," Ross Pillari, president of BP Products North America Inc., said in a statement. The oil company released Tuesday its

interim fatal accident investigation report on the March 23 blast at the Texas City, TX, plant's isomerization unit, which boosts the octane level of gasoline. The investigation determined that the fluid level in the tower of the raffinate splitter, which separates chemicals for gasoline production, was 20 times higher than it should have been.
Texas City Refinery Investigation Interim Report:
http://www.bp.com/liveassets/bp_internet/globalbp/STAGING/global_assets/downloads/T/texas_city_investigation_report.pdf
Source: http://biz.yahoo.com/ap/050517/bp_plant_explosion.html?.v=2

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

2. *May 17, Finextra Research* — **Nearly half of U.S. adults have been phished.** Consumer studies conducted by First Data indicate that 6.8% of U.S. adults have been victimized by identity theft and 43.4% have direct personal experience of phishing fraud. The research, conducted in late 2004 by Synovate on behalf of First Data's Star Network, found that more than one−third of consumers surveyed had received a phishing e−mail, while 19% had taken a phishing phone call. On average five percent of consumers contacted fell for the scam and divulged personal details. Of those, 45% reported that the information was used to make an unauthorized transaction, open an account, or commit another type of identity theft. Nearly one−third of consumers said that the phisher had posed as a financial institution, while one in 10 reported that the phisher had impersonated a credit card company. Debra Janssen, president, First Data Debit Services, describes the survey results as worrying. "Close to five percent of phishing attempts are successful, despite significant efforts by the financial community to raise awareness and educate consumers about phishing. It's clear that more remains to be done."
Research: http://www.star.com/pdf/IDTheft_Research_3_3_05.pdf
Source: http://www.finextra.com/fullstory.asp?id=13681

3. *May 17, San Diego Business Journal* — **More employees vulnerable to phishing, study finds.** Spammers and phishers are infiltrating computer systems of more businesses than ever as their methods of luring Internet users get more sophisticated, according to a recent survey done for Websense, Inc., the San Diego maker of Internet filtering software. Eighty−two percent of information technology decision−makers surveyed said employees at their companies have received phishing attacks via e−mail or instant messaging. But only four percent of the employees surveyed admitted they have actually been deceived. “Phishers are becoming more

sophisticated in their deception techniques to lure employees to spoofed Websites, as most employees cannot determine which is a valid site and which is a fake," said Dan Hubbard, senior director of security and technology research for Websense. "By simply clicking on a phishing URL, the site can install spyware, such as a malicious keylogger, on the employee's computer which has the ability to capture data such as network passwords or Social Security numbers without their knowledge," said Hubbard. In the company's recent survey, only a third of employees even heard of the phishing phenomenon. The survey was taken in February of 354 IT decision−makers, and in late February−March of 500 employees, who work at organizations with at least 100 employees.
Detailed Findings: http://ww2.websense.com/global/en/PressRoom/PressReleases/PressReleaseDetail/index.php?Release=050516932
Source: http://www.sdbj.com/industry_article.asp?aID=06392975.7368738.1144130.7675701.8927053.303&aID2=88001

4. *May 16, Network World* — **Extortion via distributed denial of service attacks on the rise.** Criminals are increasingly targeting corporations with distributed denial−of−service (DDoS) attacks designed not to disrupt business networks but to extort thousands of dollars from the companies. Those targeted are increasingly deciding to pay the extortionists rather than accept the consequences, experts say. While reports of this type of crime have circulated for several years, most victimized companies remain reluctant to acknowledge the attacks or enlist the help of law enforcement, resulting in limited awareness of the problem and few prosecutions. The FBI aggressively works daily on cases involving DDoS attacks and extortion, says bureau spokesperson Paul Bresson. "Almost all of them have an international connection," he says. "There aren't many cases where people doing this are from the U.S, and many times it is a juvenile subject to the laws of another country," said Bresson. An indeterminable number of victims are choosing to meet the demands of extortionists rather than turn to law enforcement for fear of negative publicity. The law does not prohibit paying, says Kathleen Porter, an attorney at Robinson & Cole in Boston. "It's something companies are doing because the cost of denial−of−service attacks are so expensive," said Porter. "The problem is if companies keep paying, the attacks will continue," said Porter.
Source: http://www.networkworld.com/news/2005/051605−ddos−extortion. html

[Return to top]

Transportation and Border Security Sector

5. *May 17, Associated Press* — **Another Boston−bound plane diverted to Maine.** For the second time in a week, an international flight headed for Boston has landed instead in Bangor, ME, because a passenger's name matches one on the government's no−fly list. Alitalia Flight 618 was scheduled to land at Boston's Logan International Airport at 1:10 p.m. EDT. Instead, it landed about 20 minutes earlier at the Bangor International Airport. The Transportation Security Administration said federal law enforcement officials were on hand to greet the flight. There were no reports of any unusual activity on the plane. The Alitalia flight originated in Milan. Canadian and American military jets escorted the plane to Maine, reported Boston TV station WCVB. The passenger in question was to be removed from the plane and the flight would then be allowed to continue to Boston, the TV station said. Last week, an Air France flight bound for Boston was diverted to Bangor because a passenger's name and birth date was

nearly identical to that of a man on the government watch list. The man on the plane turned out not to be that person.
Source: http://www.nbc6.net/news/4498095/detail.html

6. *May 17, Department of Transportation* — **National Rail Safety Action Plan announced.** A new plan to improve safety along the nation's railroads was unveiled on Monday, May 16, by Department of Transportation Secretary Norman Y. Mineta during a visit to Columbia, SC. The plan will help prevent train accidents caused by human error, improve the safety of Hazmat shipments, minimize the dangers of crew fatigue, deploy state−of−the−art technologies to detect track defects, and focus inspectors on safety trouble spots. Mineta outlined the new National Rail Safety Action Plan, which represents the Department of Transportation's aggressive new approach to improving safety throughout the railroad industry. The plan will target the most frequent, highest−risk causes of accidents, focus federal oversight and inspection resources, and accelerate research into new technologies that can vastly improve rail safety. One of the primary safety issues addressed in the plan is human error, the largest single factor accounting for 38 percent of all accidents over the last five years. Preliminary findings from the tragic accident in Graniteville, SC, this January point to human error as the cause −− the failure of a train crew to properly line a switch back to the mainline track. The safe transport of hazardous materials by rail is also a major focus of the action plan.
National Rail Safety Plan: http://www.fra.dot.gov/downloads/Safety/action_plan_final_051605.pdf
Source: http://www.dot.gov/affairs/dot7805.htm

7. *May 17, Department of Transportation* — **United States, Ethiopia sign Open−Skies aviation agreement.** U.S. Deputy Department of Transportation Secretary Maria Cino and Haile Asegide, State Minister of Ethiopia's Ministry of Infrastructure, on Tuesday, May 17, signed a full Open−Skies agreement that will permit U.S. and Ethiopian airlines to operate air services between the two countries without restriction. The agreement was reached after two days of talks last week in Washington. "Open Skies will allow Ethiopia to serve as a vital gateway into and from Africa, connecting travelers, trade and friendship across both sides of the Atlantic," Department of Transportation Secretary Norman Y. Mineta said. "Ethiopia joins a growing list of countries that understand that removing artificial restrictions on international travel to, from, and between countries is the best way to increase travel and stimulate economic growth to the benefit of all parties." Open−Skies agreements permit unrestricted air service by the airlines of both sides between and beyond the other's territory, without restrictions on how often the carriers can fly, the prices they charge, or the kind of aircraft they use. The accord with Ethiopia also will allow all−cargo carriers to fly between the other country and third countries without directly connecting to their homeland. The United States now has Open−Skies relationships with 70 aviation partners, including 15 in Africa.
Source: http://www.dot.gov/affairs/dot8005.htm

8. *May 17, Department of Transportation* — **Highway bill would help ports fight congestion.** Traffic congestion outside the main gates of America's seaports would be reduced in the President's highway bill awaiting action in Congress, Department of Transportation Secretary Norman Y. Mineta said on Tuesday, May 17, during a visit to Jacksonville, FL's port docks. He said the President's bill, known as the Safe, Accountable, Flexible, and Efficient Transportation Equity Act (SAFETEA), would provide funding for port−related road projects to reduce

congestion as trucks hauling hundreds of thousands of trailers headed for market leave their docks each day. He said the President is committed to working with Congress to pass a bill that would spend a record $284 billion on highway and transit projects, but warned the Administration would not “give in to pressure to approve irresponsible plans that would no doubt lead to higher deficits or new gas taxes.” Mineta said the SAFETEA proposal is the first to include provisions that would help pay for better highway connections to ports.
Source: http://www.dot.gov/affairs/dot7405.htm

9. *April 15, Government Accountability Office* — **GAO−05−394: Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention (Report).** Sharing information with nonfederal officials is an important tool in federal efforts to secure the nation’s ports against a potential terrorist attack. The Coast Guard has lead responsibility in coordinating maritime information sharing efforts. The Coast Guard has established area maritime security committees—forums that involve federal and nonfederal officials who identify and address risks in a port. The Coast Guard and other agencies have sought to further enhance information sharing and port security operations by establishing interagency operational centers— command centers that tie together the efforts of federal and nonfederal participants. The Government Accountability Office (GAO) was asked to review the efforts to see what impact the committees and interagency operational centers have had on improving information sharing and to identify any barriers that have hindered information sharing. To help ensure that nonfederal officials receive security clearances in a more timely fashion, GAO recommends that the Coast Guard (1) develop formal procedures to use data as a tool to monitor the security clearance program and (2) raise the awareness of nonfederal officials about the process of applying for a clearance. The Department of Homeland Security and the Coast Guard concurred with these recommendations.
Highlights: http://www.gao.gov/highlights/d05394high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−394

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

10. *May 17, USAgNet* — **Above normal hurricane season may impact soy rust potential.** Forecasters at the National Oceanic and Atmospheric Administration (NOAA) are predicting another above−normal hurricane season on the heels of last year's destructive and historic hurricane season. "NOAA's prediction for the 2005 Atlantic hurricane season is for 12 to 15 tropical storms, with seven to nine becoming hurricanes, of which three to five could become major hurricanes," said retired Navy Vice Adm. Conrad C. Lautenbacher, Ph.D., undersecretary of commerce for oceans and atmosphere and NOAA administrator at a news conference Monday in Bay St. Louis, Miss. "Forecaster confidence that this will be an active hurricane season is very high." The above−normal hurricane forecast could have an impact on soybean

rust infestations along the Gulf Coast later this summer. So far, active soybean rust infestations have been found in extreme southern Georgia and Florida. Last year, Hurricane Ivan was blamed for bringing soybean rust spores from South America into and along the U.S. Gulf Coast.
U.S. Department of Agriculture Soybean Rust Information Site:
http://www.usda.gov/soybeanrust/
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=5 08&yr=2005

[Return to top]

Food Sector

11. *May 17, Government Accountability Office* — **GAO−05−549T: Overseeing the U.S. Food Supply: Steps Should be Taken to Reduce Overlapping Inspections and Related Activities (Testimony).** The Government Accountability Office (GAO) has issued many reports documenting problems resulting from the fragmented nature of the federal food safety system−−a system based on 30 primary laws. This testimony summarizes GAO's most recent work on the federal system for ensuring the safety of the U.S. food supply. It provides (1) an overview of food safety functions, (2) examples of overlapping and duplicative inspection and training activities, and (3) observations on efforts to better manage the system through interagency agreements. It also provides information on other countries' experiences with consolidation and the views of key stakeholders on possible consolidation in the United States.
Highlights: http://www.gao.gov/highlights/d05549thigh.pdf
Source: http://www.gao.gov/new.items/d05549t.pdf

12. *March 30, Government Accountability Office* — **GAO−05−213: Oversight of Food Safety Activities: Federal Agencies Should Pursue Opportunities to Reduce Overlap and Better Leverage Resources (Report).** GAO has documented many problems resulting from the fragmented nature of the federal food safety system and recommended fundamental restructuring to ensure the effective use of scarce government resources. In this report, GAO (1) identified overlaps in food safety activities at USDA, FDA, EPA, and NMFS; (2) analyzed the extent to which the agencies use interagency agreements to leverage resources; and (3) obtained the views of stakeholders. Several statutes give responsibility for different segments of the food supply to different agencies to ensure that the food supply is safe. In carrying out their responsibilities, with respect to both domestic and imported food, these agencies spend resources on a number of overlapping activities, such as inspection/enforcement, training, research, or rulemaking. Ultimately, inspection and training resources could be used more efficiently. GAO identified 71 interagency agreements that the agencies entered into to better protect public health and to coordinate their food safety activities. However, the agencies have weak mechanisms for tracking these agreements that, in some cases, lead to ineffective implementation. GAO spoke with selected industry associations, food companies, consumer groups, and academic experts, and they disagree on the extent of overlap and on how best to improve the food safety system.
Highlights: http://www.gao.gov/highlights/d05213high.pdf
Source: http://www.gao.gov/new.items/d05213.pdf

[Return to top]

Water Sector

13. *May 13, Environmental Protection Agency* — **Ninety percent of population served by community water systems that meet drinking water standards.** Ninety percent of the 272 million people served by 53,000 community water systems across the country received water that met health−based drinking water standards in fiscal year 2004. Through effective treatment, source water protection, and state and federal cooperation, EPA is working to meet its goal of having 95 percent of the population by 2008 served by community water systems in compliance with health−based drinking water standards. Water systems meeting the standards do not exceed the maximum allowable levels for contaminants such as nitrate and meet treatment technique requirements that ensure protection against microbial pathogens such as Giardia and viruses. Each year EPA releases a Summary of Drinking Water and Ground Water Statistics. The statistics in the summary are based on data from the Safe Drinking Water Information System, which is EPA's official record of inventory, violation, and enforcement data for public water systems.
Summaries of Drinking Water and Ground Water Statistics are available at:
http://www.epa.gov/safewater/data/getdata.html
Source: http://yosemite.epa.gov/opa/admpress.nsf/b1ab9f485b098972852562e7004dc686/03a586d96a599a1e852570000070df68!OpenDocument

[Return to top]

Public Health Sector

14. *May 17, Agence France−Presse* — **Second human bird flu case in Vietnam in a week.** A second human case of bird flu has been identified in under a week in Vietnam where 36 people have died from the disease since late 2003, a health official said. A 58−year−old man from northern Vietnam's Thanh Hoa province was admitted to the Institute of Tropical Diseases in Hanoi late last week and tested positive to the H5N1 virus, said Cao Van Vien, deputy director of the institute. Doctors said the patient and another 52−year−old man from Vinh Phuc province, also in the north, were in stable condition. Health officials in the two provinces said they had quarantined the patients' houses. Recent research showed the virus would be extremely difficult to eliminate in Vietnam's poultry population. Health experts have said there could be another full−blown outbreak of bird flu in Vietnam this year, urging the disinfection of areas containing poultry. They have also warned the H5N1 virus could lead to a pandemic if it mutated into a form that could be easily transmitted between humans.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20050517/wl_asia_afp/healthfluvietnam_050517080027

15. *May 17, Mercury News (CA)* — **Tracking outbreaks of illness.** Health officials across the country are trying to turn scattered wisps of health information into a way to identify outbreaks −− whether natural or the work of terrorists −− at the earliest possible stage so they can take action. The idea, known as syndromic surveillance, has been around for at least a decade, increasing momentum after the September 11 attacks and the delivery of anthrax−laden letters through the mail. It monitors the kinds of things people might do when they start feeling sick,

for example, buy tissues, call 911, or go to the emergency room. After identifying information is removed, the information is combined and sent to a health expert for analysis. “If something unusual is happening, it might merit digging a little more −− going down to the hospital to see what is going on −− or it might merit a full−scale investigation,” said Dr. James Buehler of the Center for Public Health Preparedness and Research at Emory University. On the national level, the Centers for Disease Control and Prevention has created an automated monitoring system called BioSense. It pulls in data from military and Veterans Administration hospitals, medical laboratories and drug stores, and makes it immediately available to local health departments.
BioSense: http://www.cdc.gov/phin/component−initiatives/biosense/index .html
Source: http://www.kentucky.com/mld/mercurynews/living/health/11665928.htm?source=rss&channel=mercurynews_health

16. *May 17, Voice of America* — **WHO urges action on public health crises.** The director−general of the World Health Organization (WHO), Lee Jong−wook, is calling for greater international coordination and more effective use of modern technology to deal with epidemics and threats from newly emerging diseases. Lee made a number of sweeping health proposals to delegates attending the opening of this year's World Health Assembly in Geneva, Switzerland. Lee told representatives of WHO's 192 member−states that the capacity to respond to health threats quickly with well−coordinated action is indispensable for public health in the 21st century. He said that capacity is growing. He pointed to the organization's Global Outbreak Alert and Response Network, which, since it started five−years ago, has responded to more than 50 major disease outbreaks. Lee said the Network's capabilities have been enhanced with the establishment of the Strategic Health Operations Center last year. He said it serves as the nerve center for bringing together the logistics and health information needed to respond to public health emergencies. The Center, he said, provides instant communication between member states and technical partners.
Source: http://www.voanews.com/english/2005−05−17−voa2.cfm

17. *May 16, Reuters* — **Death toll climbs from Marburg fever.** The World Health Organization (WHO) said on Monday, May 16, that Angola's Marburg fever outbreak was not over as the death toll from the disease climbed. "We've seen new cases in new municipalities that don't have obvious links to earlier cases of Marburg. We are very concerned about the situation," said WHO spokesperson Aphaluck Bhatiasevi. The death toll in the worst recorded outbreak from the rare hemorrhagic fever has risen during the past 10 days to 292 from 277, officials said. Overcoming cultural barriers remains the biggest obstacle in the battle to contain the Ebola−like disease, Deputy Health Minister Jose Van Dunem said. “We have some cultural problems. People think if they don't bathe the dead body then they are not properly putting them to rest," Van Dunem said. The fever is spread by bodily fluids like blood, saliva, tears and sweat. Experts say protection is essential when dealing with corpses. Bodily fluid secretions increase after death, meaning the corpses of Marburg victims are highly contagious. There is no cure.
Source: http://www.cnn.com/2005/WORLD/africa/05/16/marburg.angola.re ut/index.html

[Return to top]

Government Sector

18. *May 16, Federal Computer Week* — **Hill renews calls for emergency preparedness.** House Government Reform Committee Chair Rep. Tom Davis (R−VA) has asked the Government Accountability Office (GAO) once again to investigate if federal employees are prepared to relocate or telework in the event of another terrorist attack or natural disaster. Davis requested a third report on continuity of operations (COOP) plans after GAO officials delivered worrisome findings. "We remain concerned that many agencies are not adequately prepared to continue providing vital services during emergencies," Davis wrote to U.S. Comptroller General David Walker two weeks ago. Davis held a hearing on April 28 to review agencies' COOP progress. In a critical report last year, GAO officials found that agencies' guidelines for designating essential personnel were inadequate. Linda Koontz, director of information management issues at GAO, testified at the hearing that, as of May 2004, many of the 23 agencies under review reported using sound practices for identifying essential functions, but few provided enough documentation to corroborate the claim. Koontz said 10 agencies reported plans to use telework in emergencies, but did not provide any information that they were prepared to do so. Such efforts would require preparing and training staff members, ensuring that necessary technology is available and providing technical support and testing.
Source: http://fcw.com/article88848−05−16−05−Print

[Return to top]

Emergency Services Sector

19. *May 17, USA TODAY* — **Cellphones can now get AMBER Alerts.** AMBER Alert, the public notification system that has helped return 201 abducted children safely since 1997, will be expanded today so that most people with a cell phone or other wireless device can get alerts in their area. More than 182 million people use cell phones or other wireless devices, such as BlackBerrys. About 90% of the users in the country, those who subscribe to big carriers, can get an alert on an abducted child free by signing up at http://www.wirelessamberalerts.org. They can select the areas for which they want notification. Subscribers to smaller phone services will be able to sign up in about two months, says Steve Largent, president of CTIA−The Wireless Association. The cell phone alert builds on the existing AMBER Alert system that broadcasts descriptions of the missing children and the suspects who may have taken them in all 50 states and Washington, DC. AMBER stands for America's Missing: Broadcast Emergency Response.
Source: http://www.usatoday.com/news/nation/2005−05−16−amber−cells_x .htm

20. *May 17, The Collaborative for Disaster Mitigation* — **Conference: Disaster Resistant California 2005.** The California Governor's Office of Emergency Services and The Collaborative for Disaster Mitigation is holding its fifth annual Disaster Resistant California (DRC) Conference from May 15−18, 2005, at the Hyatt Regency Hotel in Sacramento, CA. This unique conference series will continue its tradition of offering an exciting and highly dynamic exploration of disaster mitigation, planning, preparedness, response and recovery through plenary panels, workshops and professional development courses. The goal of the conference is to increase coordination between federal, state, and local governments, and the private sector in the implementation of hazard mitigation measures in the state of California. The DRC Conference is designed to bring together emergency management professionals, local, state and federal government representatives and private business partners to share ideas,

technology and resources for the purpose of mitigating disasters. This year's program will include compelling cases from local, state and federal authorities and national and international experts offering innovative solutions for today's emergency management environment.
Source: http://www2.sjsu.edu/cdm/drc05/main.html

21. *May 17, Government Technology* — **System delivers homeland security e−mails to Pennsylvania troopers.** Homeland security alerts and other critical information will be sent to Pennsylvania State Police troopers directly through e−mails under a technology enhancement announced on Monday, May 16, by State Police Commissioner Jeffrey B. Miller. "Important messages will be delivered to desktop and wireless devices so that our personnel get the information in a timely manner no matter where they are carrying out their duties," Miller said. Official homeland security messages from the federal government are transmitted from the National Law Enforcement Telecommunications System to Pennsylvania through the Commonwealth Law Enforcement Assistance Network (CLEAN), which is operated by State Police. CLEAN is the computer system that provides criminal−record, driver− license, motor−vehicle and other data to all Pennsylvania law enforcement agencies.
Source: http://www.govtech.net/news/news.php?id=94013

22. *May 11, Southwest Nebraska News (NE)* — **Annual Emergency Medical Services Week to be observed.** The American College of Emergency Physicians (ACEP) has announced that the 32nd annual Emergency Medical Services (EMS) Week will be observed throughout the nation May 15−21, 2005. This year also marks the 20th anniversary of the first grants awarded by the federal Emergency Medical Services for Children (EMSC) program, which will be celebrated during EMSC Day on May 18. Hundreds of grassroots activities coast−to−coast will be planned around this year’s theme, which celebrates the 3 R’s that describe EMS: Ready, Responsive and Reliable. EMS is ready because it is available anywhere and any time. It is responsive to all kinds of medical emergencies despite weather conditions or hazards. And EMS is reliable, serving the public with well−trained paid and volunteer professionals. The National Highway Traffic Safety Administration (NHTSA) and Health Resources and Services Administration (HRSA) join ACEP as organizational sponsors of EMS Week. ACEP is a national emergency medicine medical specialty society with more than 23,000 members.
American College of Emergency Physicians: http://www.acep.org/emsweek
Source: http://www.swnebr.net/newspaper/cgi−bin/articles/articlearch iver.pl?157403

[Return to top]

Information Technology and Telecommunications Sector

23. *May 17, Associated Press* — **DHS Study: Revenge is often the reason for computer sabotage.** Corporate insiders who sabotage computers so sensitive they risk endangering national security or the economy commonly are motivated by revenge against their bosses, according to a Department of Homeland Security (DHS) funded study released Monday, May 16. The study, conducted by the U.S. Secret Service and the U.S.−funded CERT Coordination Center at Carnegie Mellon University, examined dozens of computer−sabotage cases over six years to determine what motivates trusted insiders to attack and how their actions damage the country's most sensitive networks and data. The review described most attackers as disgruntled workers or former employees−−typically working in technology departments−−who were angry

over disciplinary actions, missed promotions, or layoffs. The attacks included deleting vital software or data, posting pornography on an employer's Website, or crippling whole networks. The study said most saboteurs showed troubling signs before the attacks: truancy, tardiness, arguments with co−workers, or shoddy performance. Nearly all the employees took some steps to conceal their identities online as they plotted their attacks. All the attacks studied occurred between 1996 and 2002. The study said it did not examine insider attacks where employees sought to steal information to sell for profit or blackmail.
Report: http://www.cert.org/archive/pdf/insidercross051105.pdf
Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=163104819

24. *May 17, Government Accountability Office* — **GAO−05−383: Information Security: Federal Agencies Need to Improve Controls over Wireless Networks (Report).** The Government Accountability Office (GAO) was asked to study the security of wireless networks operating within federal facilities. GAO found that federal agencies have not fully implemented key controls such as policies, practices, and tools that would enable them to operate wireless networks securely. Further, tests of the security of wireless networks at six federal agencies revealed unauthorized wireless activity and “signal leakage”—wireless signals broadcasting beyond the perimeter of the building and thereby increasing the networks’ susceptibility to attack. Without implementing key controls, agencies cannot adequately secure federal wireless networks and, as a result, their information may be at increased risk of unauthorized disclosure, modification, or destruction. GAO recommends that the Director of the Office of Management and Budget (OMB) instruct the agencies to ensure that wireless network security is incorporated into their agencywide information security programs in accordance with the Federal Information Security Management Act. OMB generally agreed with the contents of this report.
Highlights: http://www.gao.gov/highlights/d05383high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−383

25. *May 17, vnunet* — **Lax security leaves networks wide open.** Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. Over 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus websites. Lack of awareness is key to this problem, according to the poll. Two thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training.
Source: http://www.vnunet.com/vnunet/news/2135301/lax−security−leavi ng−networks−wide−open

26. *May 16, SecurityFocus* — **Apache HTDigest realm command line argument buffer overflow vulnerability.** A buffer overflow vulnerability exists in the htdigest utility included with Apache. The vulnerability is due to improper bounds checking when copying user−supplied realm data into local buffers. By supplying an overly long realm value to the command line options of htdigest, it is possible to trigger an overflow condition. This may cause memory to be corrupted with attacker−specified values. This issue could be exploited by

a remote attacker; potentially resulting in the execution of arbitrary system commands within the context of the web server process. See Source link for any vendor supplied solutions. Source: http://www.securityfocus.com/bid/13537/info/

27. *May 16, SecurityFocus* — **Mozilla Suite and Firefox multiple script manager security bypass vulnerabilities.** Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross−site scripting, and other attacks are also likely possible. Original advisory and updates: http://www.mozilla.org/projects/security/known−vulnerabiliti es.html
Source: http://www.securityfocus.com/bid/13641/discussion/

28. *May 16, SecurityFocus* — **Mozilla Suite and Firefox DOM property overrides code execution vulnerability.** Mozilla Suite and Mozilla Firefox are affected by a code execution vulnerability. This issue is due to a failure in the application to properly verify Document Object Model (DOM) property values. An access validation error the attacker may leverage this issue to execute arbitrary code with the privileges of the user that activated the vulnerable Web browser, ultimately facilitating a compromise of the affected computer. Original advisory and updates: http://www.mozilla.org/projects/security/known−vulnerabiliti es.html
Source: http://www.securityfocus.com/bid/13645/info/

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received numerous reports of spam messages containing German and/or English text. It is believed that the spam messages are generated by a variant of the Sober worm family. The spam arrives with politically−themed messages in German and contains links to news articles on German Web sites.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 27015 (halflife), 6881 (bittorrent), 135 (epmap), 80 (www), 1433 (ms−sql−s), 139 (netbios−ssn), 53 (domain), 1025 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

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

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

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[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:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

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

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

DHS/IAIP Disclaimer