Election Glitches 'Could Get Ugly'
USA Today (09/14/06) P. 1A; R. Wolf

With the crucial midterm elections just eight weeks away, state and local governments are scrambling to prepare voting machines and train poll workers to fix the problems that are expected to arise. Glitches have already occurred this year in numerous states, and election officials warn that this year's election has more potential for technological difficulty than any other since 2000, with some 30% of the nation's precincts using new equipment. "If you're ever going to have a problem, it's going to be that first election," said K. Brace, president of Election Data Services. Almost half of all US counties have upgraded their voting systems to optical-scan or electronic voting since 2000, but they are still largely dependent on poll workers with an average age of 72 who are generally not experienced computer users. The principal concerns that observers voice are a shortage of technical support staff with both the precincts and the vendors, heightened demand for equipment delaying deliveries, and the touch-screen machines that have a paper backup for audits and recounts. "There are so many potential failure points this year that some of it could get ugly," said R.D. Lewis of the Election Center.

Simulated IT Attacks Reveal Response Flaws
eWeek (09/13/06), R. Hines

The US Dept. of Homeland Security has released the results of its Cyber Storm exercise, outlining the areas where government agencies and enterprises need to shore up their responsiveness to new IT threats. The exercise found that communication between the public and private sector in the event of an attack on IT infrastructure is insufficient, and that those groups could be hampered by their inability to discern the full scope of an attack. The results did indicate that progress is being made on those two fronts, however. Cyber Storm was intended to assess the information-sharing capabilities and level of readiness for an attack throughout the federal, state, and local levels of government. The testing conditions were designed to be a controlled environment where participants could simulate the coordination that would be required during a major cyber event. More than 100 public and private organizations at more than 60 locations in five countries participated in the exercise, which aimed to recreate the adverse effects that an attack or disaster could have on critical infrastructure. "In many ways, this exercise was designed to push the system to the maximum edge. That allows you to identify the greatest points of vulnerability, and we're fundamentally working to update and take lessons from Cyber Storm and Katrina and look at how we can improve coordination," said A. Purdy, acting director of the National Cyber Security Division at the Dept. of Homeland Security. Cyber Storm participants simulated cyberattacks against the nation's energy, transportation, and IT infrastructures that would have the potential to cause ripple effects throughout the government, economic, and social environments of participating countries. Responders tended to handle single threats effectively, but had trouble correlating multiple incidents occurring throughout public and private infrastructure. The report did find, however, that the existing communication platform between international governments is relatively effective.

Researchers Reveal 'Extremely Serious' Vulnerabilities in E-Voting Machines
Princeton University (09/14/06), T. Riordan

A team of Princeton University computer scientists claims to have developed software that can manipulate ballot counts in e-voting machines and be installed in under a minute in the most commonly deployed systems. "We have created and analyzed the code in the spirit of helping to guide public officials so that they can make wise decisions about how to secure elections," said E. Felten, director of Princeton's new Center for Information Technology Policy. In their examination of the Diebold AccuVote-TS machine, Felten and his colleagues found that the machine is vulnerable to numerous serious threats. In a brief video on their Web site, the researchers outline how the vote-stealing software can disrupt a mock election. The researchers show how the systems can fall prey to viruses that can automatically transmit themselves from one machine to another without being detected. Felten said that policymakers should take the threat of malicious software infecting the machines seriously, and that there is reason to be worried about other e-voting machines, in addition to the one that was tested. "There is reason for concern about other machines as well, even though our paper doesn't directly evaluate them," Felten said. "Jurisdictions using these machines should think seriously about finding a backup system in time for the November elections."

UA Scientists Probe 'Dark Web' to Uncover Potential Terrorist Threats
KVOA 4 (Tucson, AZ) (09/12/06), T. McNamara

For the past four years, scientists at the University of Arizona have been aiding US government intelligence agencies in their efforts to make sense of the terrorist-related information that is floating around on the Web. As part of the Dark Web project, University of Arizona Eller College of Management professor H. Chen and his colleagues have worked out formulas and algorithms for measuring social interactions of terrorists online, and the degree of hatred and violence that is expressed in their communications. Dark Web is now the largest computer database on terrorist Web sites and chat forums, with Chen adding that the number of terror Web sites has grown from hundreds when he started the project to about 5,000. Chen, who is currently tracking about 400 known terrorists, weeds out information that is unlikely to be useful to government agents, but passes along relevant information to intelligence agency experts to conduct sophisticated analysis on his leads. "This could be like a 'myspace' for the terrorist group, how they're interlinking with each other on the Web," Chen says of Dark Web. "It's on the Web, but you need more sophisticated technology to understand this phenomena." Chen is also assisted by advanced computer science students, and some of the students and his staff have been hired by the CIA and other agencies.

Techies Hot on Concept of 'Wisdom of Crowds,' But It Has Some Pitfalls
USA Today (09/13/06) P. 4B; K. Maney

The idea behind J. Surowiecki's popular 2004 book, "The Wisdom of Crowds," is that thousands or millions of people make better collective decisions than individual experts. The theoretical foundation for democracy, the idea is not a new one, but its implications are magnified when applied to the Internet. "The Internet provides a mechanism to get lots of diverse opinions and aggregate it in a quick and cost-effective way," says Surowiecki. By extension, the theory holds that Wikipedia, which is the product of tens of thousands of unpaid contributors, should be a better encyclopedia written by experts. Likewise, Internet mechanisms such as Digg, which allows readers to vote stories to the front page, should do a better job of finding the best stories than professional editors. The problem that Digg ran into was that groups

of savvy users began conspiring to artificially boost the popularity of certain stories. In response, Digg has adopted programs to undermine the effectiveness of block voting, a move that has drawn the ire of its regular users. The notion that the wisdom-of-crowds principle needs structure to be effective was demonstrated when the UK's Dept. of Food and Rural Affairs enlisted the public to help write environmental contracts in the form of a wiki. Despite the shortcomings of the theory, there remains a high level of enthusiasm for the wisdom-of-crowds philosophy. Google, for instance, employs the principle when ranking search results, and the forecasts of the Hollywood Stock Exchange site, where users buy "stocks" of movies and stars, are far more accurate predictors of a movie's success than the internal predictions of studios.

Microsoft Building Security Language for Grids
eWeek (09/13/06), D. Taft

Microsoft is developing a new language to improve the security of grid environments through features such as decentralized authorization policies, according to the company's B. Dillaway. The Security Policy Assertion Language (SecPAL) is a product of an ongoing Microsoft initiative to develop solutions for access control in large-scale grid environments. The need for tight control over trust relationships and delegated access rights has become more important than ever with the development of broad-based, decentralized distributed computing. The SecPAL prototype mimics a multidomain grid environment, incorporating existing Microsoft products and industry standards such as XML. The need for a new language to express security policies comes from the difficulty of describing the multitude of entities and relationships in large-scale grid environments. In addition to access control, SecPAL is also a tool "for expressing trust relationships, authorization policies, delegation policies, identity and attribute assertions, capability assertions, revocations, and audit requirements," Dillaway said in a white paper. The language also lessens the reconciliation requirements for disparate security technologies and the need for semantic translation. SecPAL enables a grid user to temporarily delegate a subset of access rights to another user who needs them for a particular job while keeping the rest of the rights restricted. Dillaway claims that SecPAL is more efficient and usable than existing technologies. In the future, SecPAL could be applied to automated access delegation, job management rights, and constrained trust management, Dillaway said.

RFID Security Consortium Receives $1.1 Million NSF Grant
RFID Journal (09/08/06) M. O'Connor

The NSF has issued a $1.1 million grant to the RFID Consortium for Security and Privacy (CUSP) to explore the security and privacy implications of RFID technology. CUSP is made up of academics and representatives from the private industry who will work together to examine the ways that RFID technology can affect consumer privacy and security, as well as potential deployment options that are safe for both customers and corporations. The CUSP researchers will also attempt to develop cryptographic protocols and partner with standards groups to improve the quality of data-protection tools. "Our plan is to look at ongoing [RFID] deployments and how to make them strong in respect to privacy and authentication," said K. Fu, assistant computer science professor the University of Massachusetts and the leader of the consortium. Any security tools that the group develops will be open source, Fu added. UMass and The Johns Hopkins University will be the two academic institutions hosting the research. RSA Laboratories, which has been researching security risks in RFID payment and identification systems, will also be an integral part of the project. While RFID technolo-

gy can be used for security purposes such as key fobs and contactless smart cards, the tags that are currently deployed are insufficiently protected, according to RSA's Ari Juels. Adding cryptography to tags will not be easy, however, particularly with passive tags that only have a small amount of processing power. RSA and California's Bay Area Rapid Transit (BART), which is interested in improving the security of smart cards, are currently the only two members of the consortium's advisory committee.

Will Your Vote Count?
CIO Insight (08/06)No. 71, P. 43; D. D'Agostino

Many problems with electronic voting systems persist six years after the 2000 presidential election illustrated the need for voting modernization, and the government faces a tough challenge in improving confidence levels in e-voting. Among the factors that have shaken people's faith in e-voting's reliability is the miscounting or deletion of votes due to malfunction; the potential of voter fraud because of insufficient security measures; and error-rife statewide registered-voter databases. Johns Hopkins University computer science professor A. Rubin says, "The problem is that technology makes it easier to manipulate elections in an invisible way. Because the systems are less transparent, the attacks can scale." But perhaps the most damaging contributor is a widespread feeling among US voters that the electoral process is broken. Experts say a voting system that is truly fair and accurate is not an impossibility if certain precautions are taken, most notably a voter-verifiable paper trail, random post-election audits, parallel testing of systems on election day, a prohibition on wireless capabilities, and stringent compliance with detailed chain-of-custody procedures. There is disagreement among states regarding which steps are actually needed. Rep. R. Holt (D-NJ) is supporting federal legislation that would make all steps mandatory, but whether such measures fly or fall may depend on American taxpayers' willingness to foot the bill. Holt says, "I suspect there are many thousands--maybe even millions--of Americans who don't believe the results of some recent election or other. We have to do everything we can to restore confidence in the mechanism of democracy." Carnegie Mellon University's M. Shamos argues that there is little money left for additional voting systems security, since the bulk of the Help America Vote Act's funding has been spent already.

Major Problems at Polls Feared
Washington Post (09/17/06), P. A1; D. Balz; Z. Goldfarb

The revamping of how state and local elections are conducted set in motion by the debacle in Florida six years ago could see the same problems that plagued Election Day in Maryland last week play out on a national scale, election experts warn. In that election, some computers failed to relay data to the state's central election office and incorrectly identified the party affiliation of some voters. More than 80 percent of voters will cast their ballots electronically in the Nov. 7 election, with a third of the precincts rolling out the technology for the first time. The Help America Vote Act of 2002 called for the replacement of old punchcard machines with new electronic systems, and the creation of centralized databases for registered voters. In last Tuesday's election in Maryland, human errors and technological glitches conspired to form long lines at the polls and delay vote counts. Similar problems in earlier elections in Ohio, Illinois, and other states have fueled concern among experts about the reliability of the systems and the ability of election officials to use them. In a time of tense political polarization, when elections often end up mired in litigation and charges of incompetent administration or even tampering, some observers are worried that the Florida scenario could play out anew in November. "What we know is, these technologies require significant testing

and debugging to make them work," said Richard Celeste, the former governor of Ohio who is now president of Colorado College. "Our concern--particularly as we look to the November election, when there is a lot of pressure on--is that election officials consider what kinds of fallbacks they can put in place." Among the central challenges in the upcoming election are ensuring the accuracy of electronic counts with paper audit trails, and the standards used to keep registration rolls current. In addition to technical bugs, computer scientists have long warned that e-voting machines could be vulnerable to hackers who could access the systems and manipulate vote totals.

Grant to Fund Fight Against Digital Crime
Pittsburgh Post-Gazette (09/17/06), J. Crompton

The US Justice Department wants to develop a national standard for investigating and preventing electronic and digital crime, and has awarded a $500,000 grant to Waynesburg College to take a leading role in this effort. Waynesburg will be called on to review current training practices, which is uneven and sometimes nonexistent at military agencies and police departments across the country, develop national standards, and create training modules that work with computers, the Internet, PDAs, and other forms of digital media. The training program would focus on collecting and preserving digital evidence, and provide techniques for managing digital equipment and data sources. Waynesburg will also use the money to buy equipment and software for a computer forensics lab, and with data collecting from government databases likely to begin in January officials hope to complete the project in a year and a half. "We're going to teach [investigators] how to handle evidence and investigations in digital form," says R. Leipold, a professor of computer science who chairs the mathematics and computer science department. In a statement, US Rep. J. Murtha (D-Pa.), adds "these same techniques can be helpful in detecting and tracking terrorist activity."

Lawmakers Question DHS Preparedness for Fighting Cyberattacks
IDG News Service (09/13/06), J. Vijayan

Department of Homeland Security (DHS) Secretary M. Chertoff announced last October that he was creating a position for an assistant secretary for cybersecurity and telecommunications, but the position has yet to be filled, to the dismay of lawmakers who say the delay may be harmful to the agency. During a recent hearing on cybersecurity for the national infrastructure, Rep. J. Dingell (D-Mich.) said DHS' failure to fill the position "conveys a lack of appreciation" for US cybersecurity threats. Dingell warned DHS against waiting for an attack before a plan is implemented. D. Powner at the US Government Accountability Office (GAO) agreed and said terrorists, criminals, and foreign intelligence services have already launched cyberattacks. Powner called the DHS' effort to work with private industry to develop an attack response initiative "immature," and noted that they do not even have a deadline. A recent GAO report found that the government is not equipped to recover from a major cyberattack. Cybersecurity issues were previously handled by a director-level position within DHS before Chertoff decided to create a new vacancy. The House Commerce Committee Subcommittee on Telecommunications and the Internet conducted the hearing.