Thursday, March 20, 2014

MONTANA CRITICAL INFRASTRUCTURE BULLETIN

OFFICE: 406-444-1330 FAX: 406-444-1349 EMAIL: CIP@MT.GOV

WATER

(U) FLOODING SWELLS MONTANA RIVERS, WASHES OUT ROADS

(U) Swollen rivers and impassable roads left hundreds of people cut off in rural areas of Montana on Monday, while in neighboring Wyoming members of the National Guard joined the fight to protect two towns threatened by high water.

(U) Authorities warned the flooding could get worse with more rain and snow expected early Tuesday.

(U) Montana Gov. Steve Bullock declared a flood emergency late Monday after forecasters put 30 of the state's 56 counties under some type of high water warning.

(U) Musselshell County in central Montana appeared to be hardest hit: Dirt roads in rural areas turned to mud, some bridges were blocked by high water and the Musselshell River threatened to overcome protective dikes in Roundup.

(U) Warm weather over the past week unleashed massive amounts of water from record snowfalls that have blanketed the region. That pushed many streams and rivers over their banks, authorities said.

(U) Impassable roads cut off about 350 people south and east of Roundup, Musselshell County disaster coordinator Jeff Gates said.

(U) Officials advised residents to stay in place if possible, and were crafting plans to ensure sufficient food and medical supplies were available to any stranded residents.

(U) Hundreds more in the Dean Creek subdivision southwest of Roundup also were cut off for a time until the situation improved Monday evening. But officials advised residents to remain ready to leave if necessary.

(U) Temperatures were forecast to drop below freezing overnight as the rain turns to snow.

(U) "If it freezes and we get snow the roads will freeze and it will help us," Gates said.

(U) In Wyoming, Guard members stacked up sand bags in Manderson and Greybull. The National Weather Service says sandbags were used to divert water around the Manderson school and water treatment plant. No evacuations were reported.

(U) Seven homes were damaged in Greybull over the weekend but the extent of damage wasn't immediately clear, said Wyoming Office of Homeland Security spokeswoman Kelly Ruiz. Video posted by the homeland security office showed the river full of ice chunks on Sunday and a home protected by sand bags surrounded by water.

(U) Mountain snowpack across both states already is well above average, setting the stage for more high water when the spring runoff arrives. That's expected in May or early June, said National Weather Service forecaster Chauncy Schultz.

(U) Officials were keeping a wary eye on ice-jams along the Musselshell River west of Roundup, which has about 1,900 people. Ice jams also were reported on the Yellowstone, Big Horn and other rivers in Montana and Wyoming.

(U) If the ice jams break free, water levels downstream could rise and more people in low-lying areas evacuated on short notice, Gates said. A makeshift dike in Roundup built after flooding three years ago was successfully holding back the water.

(U) By late Monday, the Musselshell had risen to levels not seen since severe flooding damaged hundreds of homes in 2011.

(U) More than two dozen houses near the Musselshell River were evacuated. Schools in Roundup were canceled for Tuesday in anticipation that many teachers and students would not be able to make it.

(U) The National Weather Service said a powerful Pacific storm system moving into the region would bring rain and wet snow through early Tuesday. More than an inch of precipitation was forecast in some areas.

(U) Bullock's emergency declaration allows the Democrat to mobilize state resources - including the National Guard if necessary - to help local authorities.

(U) "We're quite concerned about the moisture that's going to drop in the Little Belt Mountains and the Snowy Mountains. That could add more issues along the Musselshell River and in Roundup," said Steve Knecht, chief of operations for Montana Disaster and Emergency Services.

(U) In Yellowstone County, high waters that flooded the basements of many homes were starting to dissipate, said county emergency services director Duane Winslow. Five homes south of Laurel remained evacuated.

(U) A boil water order was in effect in Clyde Park north of Livingston, the Billings Gazette reported.

(U) In the town of Manhattan, about 19 miles northwest of Bozeman, Mayor Dave Rowell said flooding in the downtown area late last week caused at least a million dollars in damages, television station KTVM reported. (Source - http://www.abc6.com, 11 March 2014)

ENERGY

(U) U.S. RISKS NATIONAL BLACKOUT FROM SMALL-SCALE ATTACK

(U) The U.S. could suffer a coast-to-coast blackout if saboteurs knocked out just nine of the country's 55,000 electric-transmission substations on a scorching summer day, according to a previously unreported federal analysis.

(U) The study by the Federal Energy Regulatory Commission concluded that coordinated attacks in each of the nation's three separate electric systems could cause the entire power network to collapse, people familiar with the research said.

(U) A small number of the country's substations play an outsize role in keeping power flowing across large regions. The FERC analysis indicates that knocking out nine of those key substations could plunge the country into darkness for weeks, if not months.

(U) "This would be an event of unprecedented proportions," said Ross Baldick, a professor of electrical engineering at the University of Texas at Austin.

(U) No federal rules require utilities to protect vital substations except those at nuclear power plants. Regulators recently said they would consider imposing security standards.

(U) FERC last year used software to model the electric system's performance under the stress of losing important substations. The substations use large power transformers to boost the voltage of electricity so it can move long distances and then to reduce the voltage to a usable level as the electricity nears homes and businesses.

(U) The agency's so-called power-flow analysis found that different sets of nine big substations produced similar results. The Wall Street Journal isn't publishing the list of 30 critical substations studied by FERC. The commission declined to discuss the analysis or to release its contents.

(U) Some federal officials said the conclusions might overstate the grid's vulnerability.

(U) Electric systems are designed to be resilient and it would be difficult for attackers to disable many locations, said David Ortiz, an Energy Department deputy assistant secretary who was briefed on the FERC study. The agency's findings nevertheless had value "as a way of starting a conversation on physical security," he said.

(U) The study's results have been known for months by people at federal agencies, Congress and the White House, who were briefed by then-FERC Chairman Jon Wellinghoff and others at the commission. As reported by the Journal last month, Mr. Wellinghoff was concerned about a shooting attack on a California substation last April, which he said could be a dress rehearsal for additional assaults.

(U) "There are probably less than 100 critical high voltage substations on our grid in this country that need to be protected from a physical attack," he said by email this week. "It is neither a monumental task, nor is it an inordinate sum of money that would be required to do so." Mr. Wellinghoff left FERC in November and is a partner at law firm Stoel Rives LLP in San Francisco.

(U) FERC has given the industry until early June to propose new standards for the security of critical facilities, such as substations.

(U) Executives at several big utilities declined to discuss the risks to substations but said they are increasing spending on security. Virginia-based Dominion Resources Inc., for example, said it planned to spend $300 million to $500 million within seven years to harden its facilities.

(U) A memo prepared at FERC in late June for Mr. Wellinghoff before he briefed senior officials made several urgent points. "Destroy nine interconnection substations and a transformer manufacturer and the entire United States grid would be down for at least 18 months, probably longer," said the memo, which was reviewed by the Journal. That lengthy outage is possible for several reasons, including that only a handful of U.S. factories build transformers.

(U) The California attack "demonstrates that it does not require sophistication to do significant damage to the U.S. grid," according to the memo, which was written by Leonard Tao, FERC's director of external affairs. Mr. Tao said his function was to help Mr. Wellinghoff simplify his report on the analysis.

(U) The memo reflected a belief by some people at the agency that an attack-related blackout could be extraordinarily long, in part because big transformers and other equipment are hard to replace. Also, each of the three regional electric systems—the West, the East and Texas—have limited interconnections, making it hard for them to help each other in an emergency.

(U) Some experts said other simulations that are widely used in the electricity industry produced similar results as the FERC analysis.

(U) "This study used a relatively simplified model, but other models come to the same conclusion," said A.P. "Sakis" Meliopoulos, professor of electrical and computer engineering at the Georgia Institute of Technology in Atlanta. He estimated it would take "a slightly larger number" of substation attacks to cause a U.S.-wide blackout.

(U) In its modeling, FERC studied what would happen if various combinations of substations were crippled in the three electrical systems that serve the contiguous U.S. The agency concluded the systems could go dark if as few as nine locations were knocked out: four in the East, three in the West and two in Texas, people with knowledge of the analysis said.

(U) The actual number of locations that would have to be knocked out to spawn a massive blackout would vary depending on available generation resources, energy demand, which is highest on hot days, and other factors, experts said. Because it is difficult to build new transmission routes, existing big substations are becoming more crucial to handling electricity.

(U) In last April's attack at PG&E Corp.'s Metcalf substation, gunmen shot 17 large transformers over 19 minutes before fleeing in advance of police. The state grid operator was able to avoid any blackouts.

(U) The Metcalf substation sits near a freeway outside San Jose, Calif. Some experts worry that substations farther from cities could face longer attacks because of their distance from police. Many sites aren't staffed and are protected by little more than chain-link fences and cameras.

(U) While the prospect of a nationwide blackout because of sabotage might seem remote, small equipment failures have led to widespread power outages. In September 2011, for example, a failed transmission line in Arizona set off a chain reaction that created an outage affecting millions of people in the state and Southern California.

(U) Sabotage could wreak worse havoc, experts said.

(U) "The power grid, built over many decades in a benign environment, now faces a range of threats it was never designed to survive," said Paul Stockton, a former assistant secretary of defense and president of risk-assessment firm Cloud Peak Analytics. "That's got to be the focus going forward." (Source - http://online.wsj.com, 12 March 2014)

(U) HOW TO HACK INTO A CITY'S POWER GRID

(U) Employees are the weakest link when securing industrial control systems that run power plants, municipal water supplies, electric grids and other pieces of critical infrastructure, a professional hacker said at the RSA conference here Friday (Feb. 28).

(U) Andrew Whitaker, director of the Cyber Attack Penetration Division at the Reston, Va.-based Knowledge Consulting Group, is paid by companies to penetration test or "pen test" their own systems — to try to break into corporate computers, just as a malicious attacker would."

(U) "The objective is simple — to gain access," Whitaker told the audience of information-technology professionals. "We target SCADA engineers. You know how to get into industrial control systems."

(U) SCADA, or supervisory control and data acquisition systems, are the largest form of computerized industrial control systems, and use both hardware and software to monitor and control large industrial processes.

(U) "So how do we gain access?" Whitaker asked. "We often just ask for an engineer's username and password."

(U) Whitaker said his team crafts simple phishing attacks, usually consisting of a brief email message that looks like it comes from a staffer in the company's IT department.

(U) "We're made some recent changes to our Web-based Outlook access," reads the message. "When you get a free minute, please try logging in using your network credentials and let me know if you have any problems."

(U) A link to the Outlook login page is included — but that link really goes to a fake Outlook page on a site controlled by Whitaker's company.

(U) "In our experience," Whitaker said, "18 percent of employees will give up their passwords when asked."

(U) That may not sound like a winning rate, but Whitaker said it was: "We email 20 people, and get four sets of credentials. That's all we need."

(U) Canned air and fence hopping

(U) Sometimes a company will have two-factor authentication enabled, requiring a second login device that the employee carries on his person and making remote break-ins much more difficult.

(U) How to Hack Into a City's Power Grid

(U) "Then we need physical access," Whitaker said. "We'll hop fences or figure out ways to walk into buildings."

(U) Doors that use electronic badge systems, he explained, can usually be defeated by a $10 can of compressed air.

(U) "Spray the canned air along the crack of the door" where the electronic lock is, he said, "and you can open the door."

(U) It's also quite easy to create a fake corporate badge, Whitaker explained — and then "tailgate" a group of legitimate employees who will glance at the badge and let the wearer in.

(U) "Thanks to all the smokers out there," he joked, "for leaving doors unlocked" and not looking too hard at a new employee who seems to cough a lot when he smokes.

(U) Once they're physically inside a facility, pen testers wander the halls, looking official even as they look for network closets and administrative rooms.

(U) Owning the network

(U) But getting into the company network is only the first step. Whitaker's pen testers then grab everything they can get from employee accounts to try to gain administrative power over the network.

(U) "Administrative passwords and other valuable information show up in archived emails," he explained.

(U) One of Whitaker's skilled hackers will take between two and four hours to gain administrative access, he explained, and then it's off to the races.

(U) "We take screenshots of engineers' desktops, inject keyloggers, use [protocols] to dump routing tables, compromise firewalls and create tunnels," he explained.

(U) Sometimes, Whitaker will hack into employees' webcams, just to see what they're looking at.

(U) "There was one guy who always sat a weird angle," Whitaker recalled. "I figured out he was looking at two screens — his corporate computer, and his air-gapped SCADA computer. Since I was already in the building, I just waited until he left and then walked over to his desk."

(U) End of the line

(U) Through monitoring engineers' email messages, hacking into their SCADA-connected machines or simply taking screenshots as engineers log in, Whitaker's team will almost always gain access to a critical-infrastructure company's SCADA system, even if that system is air-gapped, or not connected to any other network.

(U) "Once we're in, that's where we stop," he said. "We don't need to prove anything else."

(U) The real danger to the company, he explained, and to the public at large, is that it's almost always possible for an outside adversary to gain access to a SCADA system that controls an electrical utility, a railway or any other kind of critical infrastructure.

(U) "Most SCADA protocols are still transmitting in clear," or using unencrypted internal processes, Whitaker said. "That's a problem because a network attack upon an industrial control system can have a kinetic [physical] effect on the safety of others."

(U) But there's almost no amount of security software a company can buy, he said, that will protect it from human error and frailty. To that end, companies need to make sure their employees are informed and educated to resist social engineering attacks.

(U) "Here's how to make my job harder," Whitaker told the audience. "Secure your people. Involve your people. Invest in your people."

(U) Whitaker closed with an anecdote about how a simple practice using extremely time-tested technology was able to foil him.

(U) "There was one utility company where we couldn't get into the SCADA system," he admitted. "I finally asked an engineer how they kept us out. He told me they used floppy disks, which were kept in locked drawers, to transfer data between systems." (Source - http://news.yahoo.com, 28 February 2014)

(U) RADIOACTIVE DUMP SITE FOUND IN REMOTE NORTH DAKOTA TOWN

(U) Police and state health officials are investigating the illegal dumping of radioactive filter socks in an abandoned gas station in the tiny remote town of Noonan in Divide County.

(U) "This is a vacant building filled with toxic waste," said Divide County Sheriff's Deputy Zach Schroeder, lead investigator, who says the building's apparent owner is a fugitive on felony larceny charges in Wyoming and so far not traceable.

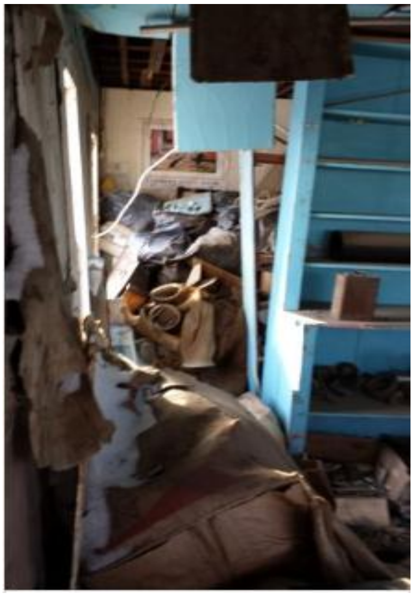
(U) The building's contents were reported two weeks ago to Divide County Emergency Manager Jody Gunlock, who said the situation was turned over to the state Health Department and Divide County law enforcement.

(U) Health Department waste division manager Scott Radig said the building contains at least twice as much filter sock material and is more than twice as radioactive as the open trailers loaded with the socks discovered near Watford City three weeks ago.

A
North Dakota
Montana

(U) Schroeder said six separate rooms in the old Mobil gas station contain industrial-sized black garbage bags of filter socks. He estimates at least 200 bags or more are piled into the dirt-floor structure's warren of rooms.

(U) Schroeder said he's trying to track down the building owner so the state can jointly develop a cleanup plan. He said county records show Ken Ward, or his wife, own the building as of January 2012, though property taxes for the year were paid by his mother, Edie Ward, who sells real estate in Montana. He said Ken Ward, who escaped police custody, is nowhere to be found.



(U) From records in the building, Schroeder said he has identified a filter sock supply company, Acceleration Production of Watford City, and hopes that will help identify the oil field service company that used them in oil field operations and ditched them in the building.

(U) He said residents of Noonan, population 120, don't have information and said it's likely that whoever dumped the garbage bags did so under cover of darkness.

(U) In the meantime, Gunlock said the building may be fenced off to prevent anyone from entering the property and the deputy said he planned to surround it with crime scene tape. Gunlock said the bags were dust-covered and may have been there for some time, though it's hard to tell how long.

(U) "I don't think this was ignorance, just deliberate," Gunlock said.

(U) Gunlock said tests done last week on the material show it is low-level radium that emits "big weak" particles that don't penetrate skin, but would be hazardous to inhale or ingest.

(U) "It's a pretty big mess," Gunlock said.

(U) Radig said tests of the Noonan material show it's at five times background rate of naturally occurring radiation. The Watford City material was around two times background.

(U) He said the people of Noonan are not at risk as long as the building is secure. The building has broken windows and old unsecured doors.

(U) Socks used to filter oil production fluids are banned from disposal in North Dakota because they concentrate naturally-occurring radiation.

(U) The Health Department is developing rules for tracking radioactive waste because of dumping incidents like this and because hundreds of them show up at oil patch landfills, where truckers are fined if the socks are found in a load.

(U) Radig estimates oil production results in 27 tons of the filter socks daily.

(U) He said the department will try to work with the Noonan property owner on clean up and disposal. Barring that, the state may have to tap the Industrial Commission's cleanup funds for abandoned well sites.

(U) "The health department has no cleanup fund," Radig said. (Source - http://bismarcktribune.com, 11 March 2014)

(U) Analyst Note: Oil companies can dispose of the socks in other states such as Montana, Colorado and Idaho, which allow a higher level of radioactivity in landfills. (MATIC – TH)

(U) EXPERTS CALL FOR A NEW ORGANIZATION TO OVERSEE GRID'S CYBERSECURITY

(U) In 2013, U.S. critical infrastructure companies reported about 260 cyberattacks on their facilities to the federal government. Of these attacks, 59 percent occurred in the energy sector. A new report proposes that energy companies should create an industry-led organization to deflect cyber threats to the electric grid. Modeled after the nuclear industry's Institute of Nuclear Power Operations, the proposed organization, to be called the Institute for Electric Grid Cybersecurity, would oversee all the energy industry players that could compromise the electric grid if they came under a cyberattack.

(U) In 2013, U.S. critical infrastructure companies reported about 260 cyberattacks on their facilities to the federal government. Of these attacks, 59 percent occurred in the energy sector.

(U) A new report, co-authored by former CIA and NSA director, Gen. (Ret.) Michael Hayden, proposes that energy companies should create an industry-led organization to deflect cyber threats to the electric grid. The organization would extend membership to power companies across North America, including large generators as well as local distribution utilities. Modeled after the nuclear industry's Institute of Nuclear Power Operations, the proposed organization, to be called the Institute for Electric Grid Cybersecurity, would oversee all the energy industry players that could compromise the electric grid if they came under a cyberattack.

(U) "We believe such an organization could substantially advance cybersecurity risk-management practices across the industry," the authors write. The report, released last week by the Bipartisan Policy Center, also evaluates current initiatives aimed at protecting the North American electric grid from cyberattacks.

(U) Critical infrastructure companies are increasingly concerned about cyberattacks, but NextGov reports that the energy sector has already made important strides in protecting the electric grid because it is subject to mandatory cybersecurity standards enforced by the U.S. government. These standards mainly focus on high-voltage transmission facilities and large generators, and often excludes distribution vendors which deliver power to residents and businesses. Distribution level cyberattacks, however, could disrupt power lines that affect critical utilities like telecommunications, water systems, and oil pipelines.

(U) "In some cases, cyberattacks on distribution system facilities could have consequences that extend beyond that system," the report's authors write. "Simultaneous attacks on multiple distribution utilities, or an attack on a single utility's distribution operations in multiple locations, could have broader ramifications for the bulk power system."

(U) The 2003 Northeast blackout cost $6 billion in economic loss, and while that incident was blamed on a tree branch in Ohio, a cyberattack combined with a physical attack could lead to greater losses.

(U) The proposed organization would not interfere with the industry standard-setting organization, the North American Electric Reliability Corporation (NERC), or the government agency that enforces industry standards, the Federal Energy Regulatory Commission (FERC). The authors of the report also assure that "at present, we do not believe that there is a sufficient case for expanding FERC's jurisdiction to encompass cybersecurity at the level of the distribution system."

(U) Similar to the cybersecurity framework issued by the National Institute of Standards and Technology (NIST), participation in the proposed organization would be optional, but the federal government would persuade companies to join by equating "participation in the institute — and satisfactory performance evaluations — as equivalent to adopting the cybersecurity framework to the extent adoption of the framework is required to be eligible for particular government programs or incentives going forward," the authors write.

(U) Other incentives for joining the organization include better insurance options against economic losses caused by cyberattacks. The federal government would initially guarantee coverage. "A federal backstop would increase carriers' willingness to offer cyber insurance and lower the cost of doing so," the authors write. "In addition, a federal backstop would give carriers time to gather and review data about cyber incidents as they seek to develop policies that appropriately share risk." (Source - http://www.homelandsecurityssi.com, 4 March 2014)

HEALTH AND PUBLIC HEALTH

(U) CYBERATTACKS ARE ON THE RISE. AND HEALTH-CARE DATA IS THE BIGGEST TARGET

(U) The recent spate of cyberattacks on retailers has scared shoppers and triggered debates on Capitol Hill about whether consumers' data is being properly protected. Despite its security flaws, the retail sector isn't the one most vulnerable to breaches. That dubious honor goes to health care.

(U) A study of all data breaches in 2013 (pdf) found that the health-care sector suffered the highest share of attacks last year, overtaking the business sector for the first time in almost a decade.

(U) The Identity Theft Resource Center, a nonprofit organization that tracks data theft, reported that health-care organizations suffered 267 breaches last year, or 43 percent of all attacks in 2013. That's significantly higher than the business sector (comprised of retailers, tech companies and others) which suffered 210 attacks, or 34 percent of all breaches. The financial sector was hit by 23 breaches, or 3.7 percent of all attacks.

(U) Unfortunately, the numbers don't come as a surprise. In 2012, a Washington Post investigation found that the health-care sector was far behind in addressing basic security flaws.

(U) Robert O'Harrow reported:

(U) As the health-care industry rushed onto the Internet in search of efficiencies and improved care in recent years, it has exposed a wide array of vulnerable hospital computers and medical devices to hacking.

(U) Security researchers warn that intruders could exploit known gaps to steal patients' records for use in identity theft schemes and even launch disruptive attacks that could shut down critical hospital systems.

(U) One caveat: The health-care number may be distorted because of a 2013 federal regulation that requires companies to publicly report breaches affecting 500 or more people. So there's more data out there on health-care breaches than there is on say, retail attacks. In fact, that's a practice the retail industry is talking about standardizing right now.

(U) But there's no doubt the number of data breaches across sectors has increased. Since ITRC began tracking figures in 2005, the number of reported breaches is up nearly 300 percent. In 2013 alone, the number of breaches was 30 percent higher than in 2012. And the leading cause of stolen data last year was hackers.

(U) Why would hackers want to steal your medical records? Well, there's no limit to the uses they could put it to, according to Sam Imandoust, legal analyst at the ITRC. They could steal your identity using the sensitive data contained in medical records, abuse prescriptions to buy narcotics, or sell your information on the black market.

(U) "If you have someone's medical records — with their name, social security number and everything else — you can commit any other kind of identity theft," Imandoust said.

(U) Most of the health-care breaches in 2013 happened at the state level, at hospitals and insurance providers. California was hit by some of the biggest breaches. More than 700,000 patients' records were compromised when two laptops were stolen from an AHMC Healthcare office near Los Angeles. In New Jersey, more than 830,000 records were stolen in a similar theft at Horizon Blue Cross Blue Shield.

(U) What this means is that while the conversation on protecting the data consumers share with retailers is a good step, there may need to be another one about the health-care system. (Source - http://www.washingtonpost.com, 5 February 2014)

(U) Analyst Note: Hackers have the potential to obtain a large amount of personally identifying information through medical records. A greater concern may be the potential impact to a victim if a hacker changed information in medical records. (MATIC –AD)

INFORMATION TECHNOLOGY

(U) LARAMIE COUNTY SHERIFF WARNS OF COMPUTER HELP DESK SCAMS

(U) Fake Help Desk Scams an Ongoing Problem.

(U) Law enforcement continues to see reporting of malicious cyber actors using fake help desk scams, also known as technical support scams. These scams, if successful, seek to compromise and take control of computer systems. Malicious cyber actors send users an e-mail or they make cold calls, purportedly representing a help desk from a legitimate software or hardware vendor. The malicious cyber actors try to trick users into believing that their computer is malfunctioning – often by having them look at a system log that typically shows scores of harmless or low-level errors – then convincing them to download software or let the "technician" remotely access the personal computer to repair it.

(U) Colleges, universities, and private organizations have reported attempts by fake help desks to gain personal information or access through e-mails spoofed to appear from the organization's real help desk. The e-mails request that users "click" on a URL and enter their personal information.

(U) On 8 April 2014, support and updates for Windows XP will no longer be available—including security updates, non-security hotfixes, free or paid assisted support options, and online technical content updates. This action could present an opportunity for malicious cyber actors to initiate a new round of fake help desk scams targeting XP users with malicious e-mails or phone solicitations that could lead to compromise of users' systems.

(U) Best Practices if You Suspect a Fake Help Desk Scam Employees and Individuals: Be suspicious of any e-mail that asks you to divulge personal or financial information, is poorly written, is urgent, or contains a link to a website that does not match the organization sending the e-mail. Never give control of your computer to a third party unless you can confirm the party is a legitimate representative of a computer support team with whom you are already a customer or member of the organization. If contacted with a perceived fake request, take the caller's information down and immediately report it to your organizational help desk or local authorities.

(U) Organizations and Individuals Should: Keep your software and security programs up to date. Block execution of embedded URLs within e-mails. (Source – http://www.kgwn.tv, 15 March 2014)

Please take a moment to provide feedback - https://www.surveymonkey.com/s/MATICCIP

//END//

(U//FOUO) Tracked by: MATIC-2.3-2014; MATIC-02.5-2014; MATIC-02.8-2014; MATIC-02.13-2014

PREPARED BY: TH REVIEWED BY: AD

SECURITY NOTE: Information contained in this document is limited to open source information only. Information submitted by readers is subject to further dissemination and shall not contain any information that is Classified, Law Enforcement Sensitive, or For Official Use Only.