

Background Materials for June 2, 2011 WIRAB Cybersecurity Webinar

These background materials are derived from multiple sources. The information is organized into three sections:

1. Cybersecurity Terms;
2. Organizations and Initiatives;
3. Proposed Legislation.

To access specific items of interest, drag your mouse's cursor to the appropriate heading under the "Table of Contents" section below, press the "Control" button on your keyboard and then click the right key of your mouse (i.e. the "control + click" function). You will then be directed to that specific subject heading.

Table of Contents

1.0 Cybersecurity Terms	2
1.1 Aurora vulnerability	2
1.2. Hacking the 'smart grid'	3
1.3 Phishing	4
1.4 Stuxnet	5
1.5 Firewall	7
1.6 Viruses	9
1.7 Trojan Horse	12
1.8 Cloud Computing	15
1.9 Advanced Persistent Threats (APTs)	19
1.10 DCS (Disturbance Control Systems) & SCADA (Supervisory Control and Data Acquisition)	22
1.11 High-Impact, Low-Frequency Risk to the.....Bulk Power System	24
1.12 NERC Hosts Geomagnetic Disturbance Workshop	26
2.0 Organizations and Initiatives.....	27
2.1 Selected Remarks of Gerry Cauley, NERC CEO (April 15, 2011).....	27
2.2 Electricity Sub-Sector Coordinating Council (ESCC): Strategic Roadmap (November 2010).	28
2.3 NERC Critical Infrastructure Protection Standards	29
2.4 Network "Hydra": Connecting Electric Industry Subject Matter Experts	31
2.5 NERC Announces Grid Security Exercise (May 3, 2011).....	32
2.6 DOE Cybersecurity Initiatives (Announced Sept. 23, 2010).....	32
2.7 DOE-EPRI Cybersecurity Collaborative (Announced Sept. 27, 2010).....	34
2.8 NESCO: National Electric Sector Cybersecurity Organization	35
2.9 NISTIR 7628 (NIST Interagency Report)	36

2.10 Comment on NISTER 7628, from GraniteKey (Sept. 5, 2010)	36
2.11 DHS National Infrastructure Protection Plan (NIPP)	40
2.12 DHS: Critical Infrastructure Partnership Advisory Council (CIPAC).....	42
2.13 DHS CSSP: Control Systems Security Program	42
2.14 US CERT: Computer Emergency Readiness Team	43
2.15 National Association of State Energy Officials (NASEO)	44
Smart Grid & Cyber Security for Energy Assurance (Dec. 2011).....	44
3.0 Proposed Legislation	48
3.1 The Grid Reliability and Infrastructure Defense (“GRID”) Act	48
3.2 Protecting Cyberspace as a National Asset Act of 2010	49
3.3 The American Clean Energy Leadership Act	49
3.4 The Cybersecurity Enhancement Act of 2010.....	49
3.5 Senate Energy Committee Joint Discussion Draft (April 2011).....	50
3.6 Administration Cybersecurity Legislative Proposal.....	51

1.0 Cybersecurity Terms

1.1 Aurora vulnerability¹

Aurora is a vulnerability to cyber attacks that could sabotage critical systems that provide electricity including the nationwide power grid. This vulnerability effects control systems that operate rotating machinery such as pumps, turbines and so on. The vulnerability of the nation's electrical grid to computer attack is due in part to steps taken by power companies to transfer control of generation and distribution equipment from internal networks to supervisory control and data acquisition, or SCADA, systems that can be accessed through the Internet or by phone lines.

The move to SCADA systems boosts efficiency at utilities because it allows workers to operate equipment remotely. But this access to the Internet exposes these once-closed systems to cyber attacks. So far, incidents of hackers breaking into control systems to cause damage or outages have been scarce although there have been a few. However, the threat of such damage makes control systems an alluring target for extortionists, terrorists, unfriendly governments and others.

Electric utilities, pipelines, railroads and oil companies use remotely controlled and

¹ Frank Saxton, Computer Network Security Engineer, Portland, OR. Saxton white papers are the source for sections 1.1-1.8.

² Damballa

³ NERC Announcement, Jan. 23, 2009

⁴ An ISAC is an Information Sharing and Analysis Center. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other

monitored valves, switches and other mechanisms that are vulnerable to attack.

In a dramatic video-taped demonstration of the Aurora vulnerability recorded in 2006, engineers at Idaho National Labs showed how the weakness could be exploited to cause any spinning machine connected to the power grid -- such as a generator, pump or turbine -- to self-destruct. These attacks could easily be carried out on vulnerable equipment using the Internet.

Costs and time are frequently given as the reasons for not locking down these complex networks. Many plant operators consider it unlikely that an attacker would be able to manipulate or damage control systems, as most of these systems run on obscure hardware powered by highly specialized communications standards. However, this "security-by-obscurity" defense is gradually eroding, as a number of utilities are upgrading from older, legacy systems to operating systems more familiar to the average hacker, such as Microsoft Windows and Linux.

The GAO issued a vulnerability report on May 21, 2008 regarding the Tennessee Valley Authority, the nation's largest public utility company. The GAO found that TVA's Internet-connected corporate network was linked with systems used to control power production, and that security weaknesses pervasive in the corporate side could be used by attackers to manipulate or destroy vital control systems. As a wholly owned federal corporation, TVA must meet the same computer security standards that govern computer practices and safeguards at federal agencies. As of 5/21/2008 it apparently did not. The GAO also warned that computers on TVA's corporate network lacked security software updates and anti-virus protection, and that firewalls and intrusion detection systems on the network were easily bypassed and failed to record suspicious activity.

The task of gauging the electric sector's true progress in mitigating the Aurora vulnerability has fallen to the Federal Energy Regulatory Commission. In January 2008, FERC approved eight mandatory reliability standards to protect bulk power systems against disruptions from cyber-security breaches. The agency has the authority to fine plants up to \$1 million a day for violations of those standards, but the industry has until 2010 to demonstrate compliance with the new rules.

Security experts contend that existing standards contain loopholes and don't adequately protect critical power systems. For example, telecommunications equipment is excluded, even though there are documented cases of computer worms shutting off service from control systems to substations. There are security experts in the power industry who recognize the threat from cyber vulnerabilities like Aurora, but who claim they don't have the funding or the authority to do much about it.

1.2. Hacking the 'smart grid'

The race to build a "smarter" electrical grid could have a dark side. Security experts are starting to show the dangers of equipping homes and businesses with new meters that enable two-way communication with utilities.

There are many benefits to upgrading the nation's electricity networks, which is why a smart-grid movement was already revving up before the recent economic recovery package included \$4.5 billion for the technology. Smarter grids could help conserve energy by giving utilities more control over and insight into how power flows. But there are potential problems with moving too fast.

The risks are similar to what happens when computers are linked over the Internet. By exploiting weaknesses in the way computers talk to each other, hackers can seize control of innocent people's machines. In the case of the power grid, better communication between utilities and the meters at individual homes and businesses raises the possibility that someone could control the power supply for a single building, an entire neighborhood, or worse. For example, a computer worm could give miscreants remote control of the meters, which would let them take advantage of a utility's ability to, for example, disconnect someone's power for not paying his bill. A key vulnerability has been found in devices made by an unnamed manufacturer. But once infected, a worm could spread to other manufacturers' products that use the same communications technologies and can be used to remotely disconnect people's power.

To get the computer worm going, a hacker might have to get physical access to one of the meters in order to program it with malicious code. That could start a chain reaction in which the worm spreads meter to meter over the grid's communication network. This hack might also be done remotely, if the traffic on the network isn't encrypted.

More than 50 million smart meters are expected to be deployed by U.S. electric utilities by 2015, according to a list of publicly announced projects kept by The Edison Foundation. More than 8 million have already been deployed.

1.3 Phishing

The following is an unsubstantiated report that was published on the Internet. The report declines to identify the energy company involved so I will take these "facts" with a grain of salt. However, the described attack and its aftermath is certainly plausible so I will include it here as a potential attack vector that needs to be defended against.

Using a Microsoft zero-day vulnerability and a bit of social engineering, hackers compromised a workstation and threatened critical SCADA systems. It began with an e-mail sent to an employee at an energy company, and ended with a security breach that exposed critical systems to outside control. The attack began to unravel April 3, 2007. That's when a fraudulent user account, complete with administrative privileges, was detected by the energy company. Tracing backwards, it turned out that random administrative accounts were being added in the internal network because another machine inside their corporate network had been compromised due to a successful phishing attack. The reason why I am repeating this story is to underscore that fact that the number one security risk to networks is people.... in some cases, employees can be fooled into going to a web site that has been infected with malware and once that

happens, it's all over but the crying. But in this example, the attack was even less sophisticated than that.

The employee machine sat on the same segment where the SCADA (Supervisory Control And Data Acquisition) controllers were. This, of course, was a fundamental network security gaffe. Soon, evidence appeared that the attackers had leapfrogged off this network and broken into the domain controller. The source of the breach? A relatively simple phishing attack. The phishing e-mail contained a pitch for a new health care plan, something that caught an employee's eye. The e-mail claimed to be about benefits for a family with two or more children, and the employee had three. The message also contained a malicious .chm file attachment. When the employee opened the attachment, it reached out to a server in the Asia-Pacific region and pulled out a malicious executable that gave the attackers a foothold on the employee's machine. This particular attack took advantage of MS07-029, a Windows DNS (Domain Name System) vulnerability that at the time was unpatched. This, of course, is also a fundamental network security gaffe. Strike three! You're out... Using the vulnerability as an entry point, the attackers ended up with control of the employee's account. With the level of access they gained, the attackers could potentially control, view and modify everything related to the business.

Our advice? Put a proxy in place for Web browsing, obviously. But more critical is the subject of segregation. No workstation sharing a critical network segment such as SCADA should be connected to the Internet. Patch management, employee security training and the other preventative measures described in this series of white papers are also vital to protecting your network.

1.4 Stuxnet

The Stuxnet worm is included here because, like Aurora, it is used to penetrate and infect SCADA PLC systems. However Aurora is an opportunistic, "all purpose" worm which attacks motors, motor generators and Programmable Logic Controllers generally. Stuxnet is far more specialized and was designed specifically to attack Iran's nuclear capability. The creator(s) of Stuxnet are currently unknown. But given how complicated, selective and sophisticated this worm is, one can make some logical guesses. The short list would most likely include any International Government with the technical wherewithall and desire to shut down Iran's nuclear weapons program.

Stuxnet is the first [suspected] Government [sponsored] attack on another Government that does not involve Military action, bombs, death, a declaration of war and so on. I suspect that Stuxnet is the first salvo in a Global trend towards Cyber Warfare that will continue, grow and escalate for decades (at least) to come. IMHO, it's just a question of when, not if, Terrorists deploy some sort of Aurora/Stuxnet attack against the USA and other free Nations around the World. These attacks can, and probably will eclipse the 9/11 World Trade Center attacks in terms of disruption and destruction to infrastructures that we depend on for our daily existence. The emergence of cyber warfare is more significant, in my opinion, than the creation of the atomic bomb in 1945. The Planet is on the cusp of the greatest "arms race" ever known.

The worm's target seems to be high value infrastructures in Iran that use Siemens control systems and specific hardware components. Stuxnet has also infected other SCADA systems (an estimated 6 million computers in China, for example) but seems to be disinterested in anything that does not use the narrow band of equipment found in Iran's nuclear facilities. According to news reports the infestation by this worm might have significantly damaged Iran's nuclear facilities in Natanz and has delayed the start up of Iran's Bushehr Nuclear Power Plant. Although Siemens has stated that the worm has not caused any damage, on November 29, 2010, Iran confirmed that its nuclear program had indeed been damaged by Stuxnet.

The Stuxnet worm was first reported by the security company VirusBlokAda in mid-June 2010, and roots of it have been traced back to June 2009. Stuxnet contains a component with a build time stamp from 3 February 2010. In the United Kingdom on 25 November 2010, Sky News reported that it had received information that the Stuxnet worm, or a variation of the virus, had been traded on the black market. The name is derived from some keywords discovered in the software.

The complexity of Stuxnet is very unusual for malware, and consists of attacks against three different systems: The Windows operating system, an industrial software application that runs on Windows, and a Siemens programmable logic controller (PLC). This type of attack required in-depth knowledge of industrial processes and an interest in attacking industrial infrastructure. Developing the capabilities in Stuxnet would have required a team of people to program, as well as check that the malware would not crash the PLCs.

Stuxnet attacked Windows systems using four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm). It initially spread using infected removable drives such as USB flash drives, and then used other exploits and techniques such as peer-to-peer RPC to infect and update other computers inside private networks that are not directly connected to the Internet. The number of zero-day Windows exploits used is unusual, as zero-day Windows exploits are valued, and hackers do not normally waste the use of four different ones in the same worm. Stuxnet is unusually large at half a megabyte in size, and written in different programming languages (including C and C++) which is also irregular for malware. The Windows component of the malware is promiscuous in that it spreads relatively quickly and indiscriminately.

The malware has both user-mode and kernel-mode rootkit capability under Windows, and its device drivers have been digitally signed with the private keys of two certificates that were stolen from separate companies, JMicron and Realtek, that are both located at Hsinchu Science Park in Taiwan. The driver signing helped it install kernel-mode drivers successfully and remain undetected for a relatively long period of time. Both compromised certificates have since been revoked by VeriSign.

Two websites were configured as command and control servers for the malware, allowing it to be updated, and for industrial espionage to be conducted by uploading information. Both of these websites have subsequently been taken down as part of a

global effort to disable the malware.

Once installed on a Windows system, Stuxnet infects project files belonging to Siemens' WinCC/PCS 7 SCADA control software, and subverts a key communication library of WinCC called s7otbxbx.dll. The purpose of this subversion is to intercept communications between the WinCC software running under Windows and the target Siemens PLC devices that the software is able to configure and program when the two are connected via a data cable. In this way, the malware is able to install itself on PLC devices unnoticed, and subsequently to mask its presence from WinCC if the control software attempts to read an infected block of memory from the PLC system. The malware furthermore used a zero-day exploit in the WinCC/SCADA database software in the form of a hard-coded database password.

The complete Stuxnet code has not yet been decrypted, but among its peculiar capabilities is a fingerprinting technology which allows it to precisely identify the systems it infects. Stuxnet requires specific slave variable-frequency drives (frequency converter drives) to be attached to the targeted Siemens S7-300 system and its associated modules. It only attacks those PLC systems with variable-frequency drives from two specific vendors: Vacon based in Finland and Fararo Paya based in Iran. Furthermore, it monitors the frequency of the attached motors, and only attacks systems that spin between 807Hz and 1210 Hz. The industrial applications of motors with these parameters are diverse, and may include pumps or centrifuges. Stuxnet installs malware into memory block DB890 of the PLC that monitors the Profibus messaging bus of the system. When certain criteria are met, it periodically modifies the frequency to 1410 Hz and then to 2 Hz and then to 1064 Hz, and thus affects the operation of the connected motors by changing their rotational speed. It also installs a rootkit that hides the malware on the system - the first such documented case on this platform.

Stuxnet removal: As stated earlier, you don't have to be running a nuclear facility in Iran to become infected with Stuxnet! Siemens has released a detection and removal tool for Stuxnet. Siemens recommends contacting customer support if an infection is detected and advises installing Microsoft patches for security vulnerabilities and prohibiting the use of third-party USB flash drives. Siemens also advises immediately upgrading password access codes. The worm's ability to reprogram external programmable logic controllers (PLCs) may complicate the removal procedure. Fixing Windows systems may not completely solve the infection; a thorough audit of PLCs is recommended. Despite speculation that incorrect removal of the worm could cause further damage, Siemens reports that in the first four months since discovery, the malware was successfully removed from the systems of twenty-two customers without any adverse impact.

1.5 Firewall

Why are firewalls needed? Firewalls have been around for decades. However it was not uncommon to visit a data center that did not have firewall protection as recently as 2004 or so. Prior to around 2000, hackers, crackers, virus attacks and so on were

typically viewed by IT Managers as more of a nuisance than as a serious threat to the safety, security, reliability and integrity of their enterprise. Dealing with these activities was (and still is, to some degree) viewed as "unproductive" work, since blocking unwanted access to a network is generally related more to revenue protection than it is to revenue generation. However, these days, the decision of whether to assign resources and spend money to protect against hackers, crackers, viruses, denials of service and so on is no longer open to discussion. Once the realm of so-called "script kiddies", hacking, phishing and other illegal activities is now big business. Serious criminal organizations are now involved in many of these attacks. Consequently, IT Managers have been forced to allocate much more money and resources for network and data center security than ever before. Current estimates are that about one third of today's IT budget goes towards protecting the network from illegal intrusions and attacks. Helping IT Managers select and deploy enterprise security mechanisms and best practices has kept Consultants like myself quite busy in recent years.

What is a firewall? In its simplest form, a firewall is a mechanism that prevents unauthorized access to or from a computer or a computing network. This methodology is typically implemented by placing a firewall computer, appliance, device or capabilities at the entry point into the IT data center. The firewall is typically set to block ports and services that are not allowed anywhere within the enterprise. For example, most IT organizations do not allow Telnet access to anything. Therefore, port 23 (Telnet) would typically be blocked from any IP address to any address. Some Data Centers, such as remote colo, have the need for Administrators to be able to connect to servers remotely, so the main firewall might be set to allow SSH (port 22), but only for packets originating from specific IP addresses belonging to authorized Admin computers. Many IT Organizations will also block all UDP packets, no matter where they originate from. This type of firewall methodology is very effective in keeping the meteor sized chunks of mal-intended traffic out of a network.

There are, however, some services that simply cannot be blocked at the border. An example would be SMTP (port 25) which is used to transmit e-mail. There are ways to get around this that are beyond the scope of this paper, but for now, suffice it to say that blocking all incoming SMTP packets is not realistic. So networks have all of these SMTP packets running around looking for vulnerabilities to exploit and ads for Viagra looking for e-mail addresses to spam. This is an over- simplified example, to be sure. But the way to effectively block unwanted traffic on a computer to computer basis is with an "on the box" firewall. This would be implemented using IPF, IP Tables, IP Chains or in the case of a PC, with something like Zonealarm. The "on the box" firewall" in our example case would be set to block everything except for required services such as port 25, port 22 and possibly POP (port 110), IMAP Webmail and so forth. In this way, even if a hacker was able to get past the main firewall, the intrusion attempt would be blocked further down the line. Of course the best strategy is to block bad people as soon as possible so that's where "best practices", Intrusion Detection Systems (IDS), utilizing a "DMZ" and things of that nature come in.

As an example, a very simple but often overlooked best practice is to turn off all services that are not needed on every computer and server in the network. There are literally thousands of "port scans" going on at any given time, looking for vulnerabilities

in your network to exploit. Firewall port blocking and turning off unneeded services will greatly reduce your risk of having a vulnerability exploited.

However, all of that aside, in our simple, one mail server network example, the objective would be to set the on the box firewall rules so tight that even if the main firewall wasn't there, the mail server would still be protected. It would also be a wise best practice to keep the e-mail application service patched to the latest revision and to protect against having a lax server configuration setup that begs to be exploited by a clever hacker.

Will implementing firewalls as described protect my network 100%? Unfortunately, no. Not even close, although this was a common misperception when IT Managers first started deploying firewalls some ten years ago. Installing a firewall is sort of like putting a "kill switch" in your car. It's still easy enough to steal the car... it's just that the crooks have to work a little to do so. Even with aggressive firewall deployment, networks are still beaucoup exposed.

This issue is further clouded by sales people, in some cases. IT Managers are sometimes led to believe that security is an issue that technology alone can solve. Spend enough money (buying products that this salesman sells) and poof! The problem goes away! Consider this: you can purchase the biggest and very best firewall product that's out there. But if it's installed haphazardly and if it is configured with a silly, ineffective rule set, you're pretty much as vulnerable as if you had no firewall at all! In my opinion, IT managers would do better investing in making sure that the core security fundamentals are in place before pulling out their checkbook.

So then what? IT managers need to understand the problem before they can fix the problem. I would recommend doing an audit and testing the network for vulnerabilities as a first step. Once management understands where the biggest holes are, a responsive and sensible project plan can be developed to address the greatest areas of weakness. If a comprehensive testing methodology is in place, it will be a lot easier to measure how effective various security initiatives have been in tightening up the network. Laying solid groundwork is key to implementing projects that deliver effective results.

1.6 Viruses

What is a Computer Virus? In its simplest form, a computer virus is unwanted software that can be downloaded, often unknowingly, and will then execute arbitrary code on the host (infected) computer. Viruses frequently have the ability to replicate and to mask their presence. Many viruses can harm computers. Some can and do cause serious harm. Many viruses cause the infected computer to operate as a "bot", seeking to infect other computers inside your data center and elsewhere. Infected computers can be used to send out millions of SPAM e-mails and can be used to coordinate denial of service (DoS) attacks at the whim of the people who have access to the bot's "back door" portal. Viruses typically infect computers when a person opens up an e-mail attachment that contains a virus. Viruses can also be unknowingly downloaded by visiting

web sites that have compromised web servers. Depending on the virus type, the software typically tries to trick the user into clicking on a pop-up that then activates and subsequently propagates the virus. Anti-virus software has varying degrees of effectiveness preventing the downloading and/or activating of viruses. Having anti-virus software installed on every computer in your network is no guarantee that computers in your charge won't become infected. However, deploying anti-virus software is the minimum required strategy for dealing with blatant virus attacks.

Viruses started out as something that anti-social techo-geeks with too much time on their hands created and deployed for amusement. These days, infecting computers with viruses is big business that represents substantial revenue for SPAMMERS, porn site operators, criminal organizations and others. It is unlikely that virus attacks will get anything but worse and more frequent any time soon. In fact, now that organized criminals are involved, virus attacks have become increasingly more sophisticated and difficult to defend against. There are now viruses out there that are extremely difficult to remove from infected computers short of formatting the disk. Once little more than an annoyance, virus attacks now present a significant liability to business continuity and data integrity. Once again, IT Managers ignore the risks of virus attacks at their peril.

The types of viruses out there, their "payloads", how they operate, how they gain access to computers and how you get rid of them is a lengthy and detailed topic. Again, this white paper seeks to hit just the high points on this subject. [Easyrider LAN Pro](#) is a Systems and Network Engineering Consultancy that can audit your data center for vulnerabilities and can make recommendations on things IT Managers can do to reduce their exposure to risk. In many cases, implementing at least some of our recommendations can be done easily and inexpensively. Any reduction in risk can help delay the day that some clever hacker breaks into your network and does a lot of very embarrassing harm!

So what can I do about virus attacks without spending piles of money? As mentioned earlier, installing a good quality anti-virus software product, anti-spyware software and an on-the-box firewall are all good first steps in any network security plan. And once again, keeping virus attacks on the Internet side of your border router is the most effective strategy. User training and education is important, but even with training and AV software installed, it's just a matter of time before some user downloads a virus that winds up travelling through your data center like wildfire.

Many viruses communicate (call home) using non-standard IP ports. Infected computers running bots can send out non-stop pings to denial of service (DoS) targets. Others will send out tens of thousands of SPAM e-mails every hour. Having aggressive firewall deployment strategy and tight firewall rules will help to at least confine the subsequent damage that infected computers will cause inside and outside your data center.

It is a common misperception that all viruses gain access to computers through e-mail. While this is true for the majority of infections, e-mail is not the only exploit method. Visiting a rogue or compromised web site can also cause an infection as can installing an infected removable media such as a floppy or CDROM. There have been many documented cases of Vendor software distribution CDROMs that left the factory

infected with viruses. Assuming that such products couldn't possibly be infected, installing a driver or another piece of software often resulted in some virus immediately racing through the network, infecting every computer it came in contact with. This is why it is an important best practice to virus scan ALL removable media before doing ANYTHING with it, although I know of very few IT organizations that enforce this policy. Some IT groups do not allow users to have Administrator or even Power User rights on their own PCs which does help prevent at least some viruses from getting completely out of hand.

Another inexpensive precaution to take is deploying a web proxy server. This can be done easily and there is a lot of very good proxy software out there that's free! There are other advantages to using proxy servers, such as the browsing performance boost gained by page caching. User web site visits can be easily monitored so that if Users are spending an inordinate amount of work hours surfing the web or visiting questionable web sites, there is an audit trail available to use to have a discussion with errant Users. Most proxy server software is rich in tools and capabilities that block viruses, dangerous sites, phishing attempts and so on. As an additional benefit, since all browsing is being done effectively by the proxy server, HTTP and HTTPS can be blocked pretty much everywhere else in the enterprise.

Another thing worth considering is moving Users from Internet Explorer to Mozilla. Or at least giving them the option to do so. IE has always been a magnet for hackers, mostly because there are so many "dumb (non-technical) users" running it. Exploiting IE is often "easy pickings" for hackers, especially if the target user is not diligent about keeping up with patches and security updates. Microsoft products are frequently under sustained attack from new exploits even before a CERT bulletin is issued. Not so much with non-Microsoft products, primarily because these have much smaller installed bases and therefore are much less juicy as targets. Mozilla has quite a few security provisions built into the core product (which is free). Plus, there is an ever-growing list of nifty plug-ins available to add on to Firefox. Again, an easy and essentially free option that could offer substantial security benefits.

However, having said all of that.... I am a VERY knowledgeable, extremely cautious Computer Engineer who is suspicious of even Verisign certified sites and downloads. I run Zonealarm, AVG anti-virus software and Microsoft Defender as well as the Firefox web browser with every security plug-in known to man. I have a WEP encrypted wireless network with a wireless router that also has firewall capabilities. But even with all of that, I recently had a Zlob trojan virus download onto my Windows XP SP3 100% up to date patch-wise PC by visiting a web site that was apparently compromised. I was smart enough to kill the popup using the task manager and not by being suckered into clicking "cancel" or the close button (which would have instantly installed, deployed and propagated this VERY destructive trojan), but.... this recent event underscores the fact that even if you do everything possible to protect your network, you are still just one mis-step away from disaster. And if you haven't done everything possible to protect your enterprise (which is the case with almost all of the data centers I have visited, well.... you're just asking for judgment day, in my opinion.

1.7 Trojan Horse

What is a Trojan Horse? A Trojan horse, also known as a Trojan, describes a class of computer malware that appears to perform a desirable function but in fact performs undisclosed malicious functions. These could include allowing unauthorized access to the host machine, logging the user's keystrokes (spyware) and even permitting complete control over the computer.

Trojan Horses (not technically a virus) can be easily and unwittingly downloaded. This is usually done by tricking the user into downloading and activating malevolent software under the guise of being an ActiveX plug-in, driver, game or some other "desired" piece of software or function. The Trojan, once activated, opens a back door that allows a hacker to control the computer of the user. In recent years, sophisticated designs have made it increasingly easier to trick users into installing Trojans onto their computers. Additionally, the Trojan removal process has become correspondingly more difficult. The term is derived from the classical story of the Trojan Horse.

A program named "waterfalls.scr" serves as a simple example of a Trojan horse. The author claims it is a free waterfall screen saver. When running, it instead unloads hidden programs, scripts, or any number of commands without the user's knowledge or consent. Malicious Trojan horse programs conceal and install a malicious payload on an affected computer.

The Zlob Trojan is another, much more insidious and destructive Trojan. When visiting a web site, the user is asked if they want to install an ActiveX control so that the user can view the site content (often videos). At this point, the Trojan has already been downloaded to the user's computer. Clicking anywhere on the request pad (not just the "OK" button) will install and activate the Trojan.

Once installed, it displays popup ads with appearance similar to real Microsoft Windows warning popups, informing the user that their computer is infected with spyware. Clicking these popups trigger the download of a fake anti-spyware program (such as Virus Heat) in which the Trojan horse is hidden.

Some variants of the Zlob family, like the so-called DNSChanger, adds rogue DNS name servers to the Registry of Windows-based computers, network settings of Macintosh computers and attempts to hack into any detected router to change the DNS settings and therefore could potentially re-route traffic from legitimate web sites to other suspicious web sites.

The Trojan has also been linked to downloading atnvrinstall.exe which uses the Windows Security shield icon to look as if it is an Anti Virus installation file from Microsoft. Having this file initiated can wreak havoc on computers and networks. One symptom is random computer shutdowns or reboots with random comments. This is caused by the programs using Scheduled Tasks to run a file called "zlberfker.exe".

PHSDL - Project HoneyPot Spam Domains List tracks and catalogues Zlob spam Domains. Some of the domains on the list are redirects to porn sites and various video watching sites that show a number of inline videos. Clicking on the video to play activates a request to download an ActiveX codec which is malware. It prevents the user from closing the browser in the usual manner. Other variants of Zlob Trojan installation are in the form of computer scan that comes as a Java cab.

There is evidence that the Zlob Trojan might be a tool of the Russian Business Network or at least of Russian origin.

The Gumblar Trojan: A recent attack known as Gumblar is continuing to blow all previous web-based malware out of the water, with a new infected web page found every 4.5 seconds. Troj/JSRedir-R is now found six times more often than its nearest rival Mal/Iframe-F. JSRedir-R, which has been found on high traffic legitimate Web sites, loads malicious content from third-party sites (including one called Gumblar.cn, inspiring some security vendors to dub the threat 'Gumblar') without users' knowledge. The malware can then be used to steal sensitive information for financial gain, to commit identity theft or to meddle with search-engine results. The core security problem is that most computer users still think there's no danger in surfing the web. But with legitimate sites often falling victim to these attacks, it's time to change that thinking. As a first step, it's essential to scan every Web site for malicious code before visiting it. However, a green check mark is no guarantee of safety. I recently clicked on a legitimate-looking link on a legitimate-looking web site and INSTANTLY received a pop-up message from my web shield antivirus software that a threat had been detected. Poof.. like that the trojan was on my PC. Luckily for me, AVG immediately dumped it in the quarantine vault. But had I not been using professional grade AV software that I automatically update every four hours, it could have been a much sadder story.

So how is that so many websites are being compromised lately? Often it is due to SQL injection errors or direct hacking into the back end of the hosting companies. But the most prevalent method seems to be compromised FTP passwords that belonged to the people that administer these websites. There is also a major vulnerability in the Microsoft IIS server software that is being exploited.

SpySheriff is malware that disguises itself as an anti-spyware program, in order to trick the owner of the infected computer to buy the program, by repeatedly informing them of false threats to their system. SpySheriff often goes unnoticed by actual anti-spyware programs, and is difficult to remove from an infected computer.

SpySheriff cannot be simply deleted, as it reinstalls itself through hidden components on the computer. Trying to remove it with the Add/Remove programs feature has similar results, or may result in a system crash. A blue screen of death may occur. The program will stop the computer from connecting to the internet or a limited internet connection, and will display an error message reading "The system has been stopped to protect you from Spyware."

The desktop background can also be replaced with a blue screen of death, or a notice reading: "SPYWARE INFECTION! Your system is infected with spyware. Windows

recommends that you use a spyware removal tool to prevent loss of data. Using this PC before having it cleaned of spyware threats is highly discouraged." SpySheriff has been known to create another user account, at the administrator level, to block access to programs and utilities for other users. If logged in as an administrator, it is sometimes possible to delete the SpySheriff account. It also acts to stop any attempt to do a System restore by preventing the calendar and restore points from loading. This prevents the user from being able to revert their computer to an earlier usable state. A System restore is however often possible after booting in Safe mode.

It blocks several websites, including the ones that have downloadable anti-spyware software, locks the user's Internet Explorer options, and It has also been implemented in pirated versions of Norton Antivirus. It will likely create the need for the use of a recovery disk in order to restore original factory specs.

The Vundo Trojan (also known as Virtumonde or Virtumondo and sometimes referred to as MS Juan) is a Trojan horse that is known to cause popups and advertising for rogue antispyware programs, and sporadically other misbehavior including performance degradation and denial of service with some websites including Google and Facebook.

A Vundo infection is typically caused either by opening an e-mail attachment carrying the Trojan, or through a variety of browser exploits, including vulnerabilities in popular browser plug-ins, such as Java. Many of the popups advertise fraudulent programs such as Sysprotect, Storage Protector, AntiSpywareMaster, WinFixer, AntiVirus 2009, and AntiVirus 360.

Since there are many different varieties of Vundo Trojans, symptoms of Vundo vary widely, ranging from the relatively benign to the severe. Almost all varieties of Vundo feature some sort of pop-up advertising as well as rooting themselves to make them difficult to delete.

Most antivirus programs are not able to block this infection. Some antivirus programs such as McAfee VirusScan and VundoFix may be able to remove the Trojan, however sometimes it is not able to, depending on what happens and how much damage the Trojan did.

Think you may have the Vundo Trojan infection? We are currently getting dozens of hits per hour by people looking for information about a green screen and popup saying that their system has been halted. I suspect this is due to the currently (as of 1/16/10) unpatched vulnerability in Microsoft Internet Explorer that hackers are gleefully taking advantage of. Here's what the trojan looks like when you are infected: Desktop screen becomes all green with a box in the middle displaying the following message: "Your system is infected! System has been stopped due to a serious malfunction. Spyware activity has been detected. It is recommended to use spy ware removal tool to prevent data loss. Do not use the computer before all spy ware removed"

Clearing this trojan (Trojan.Vundo.H) is a pain but it can be done. First step is to do a scan using whatever AV software you happen to already have installed. Make sure your definitions are up-to-date although Vundo has been around for a while. You could get

lucky and your existing AV software will get rid of it. However.... if your AV software was doing it's job you wouldn't have gotten infected in the first place, right? Failing that, try the following:

We've heard of good results using MBAM - Malwarebytes free Anti-Malware tool. You can download it from <http://www.malwarebytes.org/mbam.php> or alternately from http://www.majorgeeks.com/Malwarebytes_Anti-Malware_d5756.html. Follow the instructions to install and run MBAM, taking the defaults. Reboot in normal mode after the scan is completed. Run the scan a second time and verify that the system is now clean. You may also want to run something like ATF Cleaner to get rid of lingering temp files and other garbage. I've had good results from CCleaner. Both are free. If you still have problems or want to go really crazy, you can download and run SUPERAntiSpyware at <http://www.superantispyware.com>

1.8 Cloud Computing

What is cloud computing? In a sentence, cloud computing is software that's hosted centrally in a shared environment that can be leased.

More specifically, cloud computing is a computing model in which virtualized resources are provided as a service over the Internet. The concept incorporates infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) as well as Web 2.0 and other recent technology trends that have the common theme of reliance on the Internet for satisfying the computing needs of the users. Cloud computing services usually provide common business applications online that are accessed from a web browser.

Cloud computing characteristics: Customers engaging in cloud computing do not own the physical infrastructure that hosts the software service. Instead, they rent usage from a third-party provider. They consume resources as a service, paying for only the resources they use or on a subscription basis. Sharing computing power among multiple customers can reduce costs significantly. A cloud application often eliminates the need to install and run the application on the customer's own computer, thus alleviating the burden of software maintenance, ongoing operation, and support.

Cloud computing economics: Cloud computing users can avoid capital expenditure on hardware, software and services, rather paying a provider only for what they use. Consumption is billed based on resources consumed or on a subscription basis with little or no upfront cost. Other benefits of this time sharing style approach are low barriers to entry, shared infrastructure and costs, low management overhead and immediate access to a broad range of applications. Users can generally terminate the contract at any time (thereby avoiding return on investment risk and uncertainty) and the services are often covered by service level agreements with financial penalties. One of the key advantages that cloud computing offers is infrastructure agility. IBM, Amazon, Google, Microsoft and Yahoo are some of the major, more well known cloud computing

service providers.

Cloud computing risks: Customers wishing to avoid data access and data loss problems should research vendors' policies on data security before using those services. The Gartner Group lists seven security issues which one should discuss with a cloud-computing vendor:

- Privileged user access: who has root/Administrator access to data?
- Regulatory compliance: will vendor undergo external audits and security certifications?
- Data location: Does the provider allow for any control over the location of data?
- Data segregation: Is encryption available at all stages and were these encryption schemes designed and tested by experienced professionals?
- Recovery: What will happen to data in the case of a disaster? Do they offer complete restoration and, if so, how long that would take?
- Investigative Support: Does the vendor have the ability to investigate any inappropriate or illegal activity?
- Long-term viability: What will happen to your data if the company goes out of business; how will data be returned and in what format?

In practice, one can best determine data-recovery capabilities by experiment: asking to get back old data, seeing how long it takes, and verifying that the checksums match the original data. Determining data security is harder.

Probably the biggest risk relating to cloud computing is the obvious: a total dependency that the Internet will always be available. Operations that are highly mission critical could become vulnerable to service availability problems if the Internet is disrupted in any meaningful way. This possibility certainly exists due to State sponsored or rogue terrorism or several other methods described in other white papers in this series.

Cloud computing key benefits: Cost is greatly reduced and capital expenditure is converted to operational expenditure. Pricing uses utility resource usage or subscription options. Minimal or no IT skills are required for implementation.

Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using, e.g., PC, mobile. Since the infrastructure is typically provided by an off site third-party and accessed via the Internet the users can connect from anywhere.

Security typically improves due to centralization of data, increased security-focused resources, etc., but raises concerns about loss of control over certain sensitive data. Security may be as good as or even better than traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. Providers typically log accesses and transactions, but accessing the audit logs themselves can be difficult or impossible.

Cloud computing security issues:

- 1) Every breached security system was once thought secure

SaaS (software as a service) and PaaS (platform as a service) providers all trumpet the robustness of their systems, often claiming that security in the cloud is tighter than in most enterprises. But the simple fact is that every security system that has ever been breached was once thought infallible.

Google was forced to make an embarrassing apology when its Gmail service collapsed in Europe, while Salesforce.com is still smarting from a phishing attack in 2007 which duped a staff member into revealing passwords.

While cloud service providers face similar security issues as other sorts of organizations, analysts warn that the cloud is becoming particularly attractive to cyber crooks. The richer the pot of data, the more cloud service providers need to do to protect it.

2) Data and information security

In the realm of multi-tenant data, you need to trust the cloud provider that your information will not be exposed. For their part, companies need to be vigilant about how passwords are assigned, protected and changed as examples. Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data. However, realistically, this could be easier said than done.

An important measure of security often overlooked by companies is how much downtime a cloud service provider experiences. Ask to see service providers' reliability reports to determine whether these meet the requirements of the business. Exception monitoring systems is another important area which companies should ask their service providers about.

An important consideration for cloud service customers, especially those responsible for highly sensitive data, is to find out about the hosting company used by the provider and if possible seek an independent audit of their security status.

Customers typically do not seem to be as stringent about data and information security as one might think they should in many cases.

3) Distributed cloud computing issues

Let's say that you use a particular cloud provider for your eCommerce web presence. But your checkout and credit card transaction capabilities may be carried out using different servers in different data centers or even by different cloud providers. This may be happening with or without the customer's knowledge. This type of computing distribution is a very common cloud provider model. Cloud providers may have dozens of servers in dozens of data centers in dozens of Countries. If communications between the various cloud provider services is not strongly encrypted and extremely secure, your data and information could be at risk.

We maintained all of our own web and mail servers for many years (decades, actually). But the web page you are reading now is hosted on a cloud provider server. We were very careful to locate a provider that has strong ethics, is very competent and is likely to

not go out of business tomorrow. We were particularly fortunate to find a provider that has its offices and data center right here locally. But in our research, we found that this situation is the exception rather than the rule. Many cloud providers are located in Third World Countries and have questionable competency to say that least. One large provider that we looked at was so bad that their entire netblock was blacklisted by most SPAM e-mail black list authorities. We don't know (or care) whether this is because the cloud provider in question has a lot of open relay servers that have been hacked or whether they actively sell services to known spammers. And as for support... you'll come to value USA-based cloud providers and support teams the first time you have to contact them with issues or questions. Personally, we would think that trusting vital service applications to a company that was in Russia, China or India (as examples) would be a fundamentally bad idea. And just because the company headquarters are in the American heartland is no guarantee that the computers that are hosting your services aren't in Bangalore!

4) Security standards

In most SaaS offerings, the applications are constantly being tweaked and revised, a fact which raises more security issues for customers. Companies need to know, for instance, whether a software change might actually alter its security settings. The cloud is still very much a new frontier with very little in the way of specific standards for security or data privacy. In many ways cloud computing is in a similar position to where the recording industry found itself when it was trying to combat peer-to-peer file sharing with copyright laws created in the age of analogue. In terms of legislation, there's very little that is specifically written for cloud computing. As is frequently the case with disruptive technologies, the law lags behind the technology development for cloud computing. What's more, many are concerned that cloud computing remains at such an embryonic stage that the imposition of strict standards could do more harm than good. IBM, Cisco, SAP, EMC and several other leading technology companies created an 'Open Cloud Manifesto' calling for more consistent security and monitoring of cloud services. But the fact that none of the main cloud providers agreed to take part suggests that broad industry consensus may be some way off.

There are a handful of existing web standards which companies in the cloud should know about. Chief among these is ISO27001, which is designed to provide the foundations for third party audit, and implements OECD principles governing security of information and network systems. The SAS70 auditing standard is also used by cloud service providers.

5) Local law and jurisdiction where data is held

Possibly even more pressing an issue than standards in this new frontier is the emerging question of jurisdiction. Data that might be secure in one country may not be secure in another. In many cases though, users of cloud services don't know where their information is held. Currently in the process of trying to harmonise the data laws of its member states, the EU favors very strict protection of privacy, while in America laws such as the US Patriot Act invest government and other agencies with virtually limitless powers to access information including that belonging to companies.

Companies need to be confident that they have immediate access to all of their data should their cloud provider contract be terminated for any reason, so that their information can be quickly relocated. Part of this includes knowing in which jurisdiction the data is held.

European concerns about US privacy laws led to creation of the US Safe Harbor Privacy Principles, which are intended to provide European companies with a degree of insulation from US laws. Some suspect that "Counter terrorism legislation" is increasingly being used to gain access to data for other reasons.

Cloud computing data privacy: Everything communicated on the web has a long shelf life. A really, really long shelf life, making it virtually impossible to leave the past in the past. Once someone uses the Internet to send a message or document, they have little to no control over the data. Cloud computing is becoming more common as more people opt to use web-based word processors and e-mail programs, such as Google's online word processor, Docs, or Microsoft's forthcoming online version of Office. People tend to put a lot, and perhaps too much trust in the Internet.

People go online to write notes to themselves, manage their calendars, share photos and manage contacts. And although storing information online means it's accessible from any computer, it also means it's in the "cloud," an enormous data center in cyberspace. In the Internet world, data never disappears. It has a potential to stay around forever. Much of the data is stored by third parties and because storage is so cheap, there's no reason to ever delete data. Hackers could potentially breach the stored data, compromising thousands of people's personal information. And as soon as that data has left the servers, where it goes could be anyone's guess.

In July, 2009, a hacker calling himself Hacker Croll successfully infiltrated 310 business documents belonging to social networking site Twitter that were stored in Google Docs. The hacker then sent that information, including what he claimed were PayPal, Gmail, and Amazon accounts, to various technology blogs. And while a person has some control over information contained on their home computers, they should never believe that deleting a file actually means it's gone. The truth is that bits from the file still remain in the computer and can be recovered. The Internet is even more indestructible, leaving people with little control over information transmitted online.

1.9 Advanced Persistent Threats (APTs)²

What are Advanced Persistent Threats? APTs are a [cybercrime](#) category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and

² Damballa

initial goals reached.

Definitions of precisely what an APT is can vary widely, but can best be summarized by their named requirements:

Advanced – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

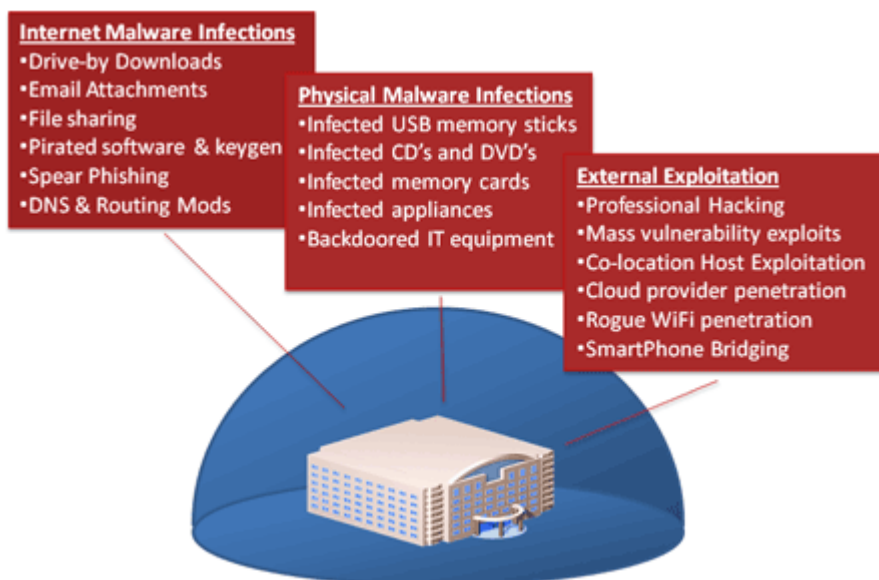
Persistent – Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful.

Threat – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

How Advanced Persistent Threats Breach Enterprises:

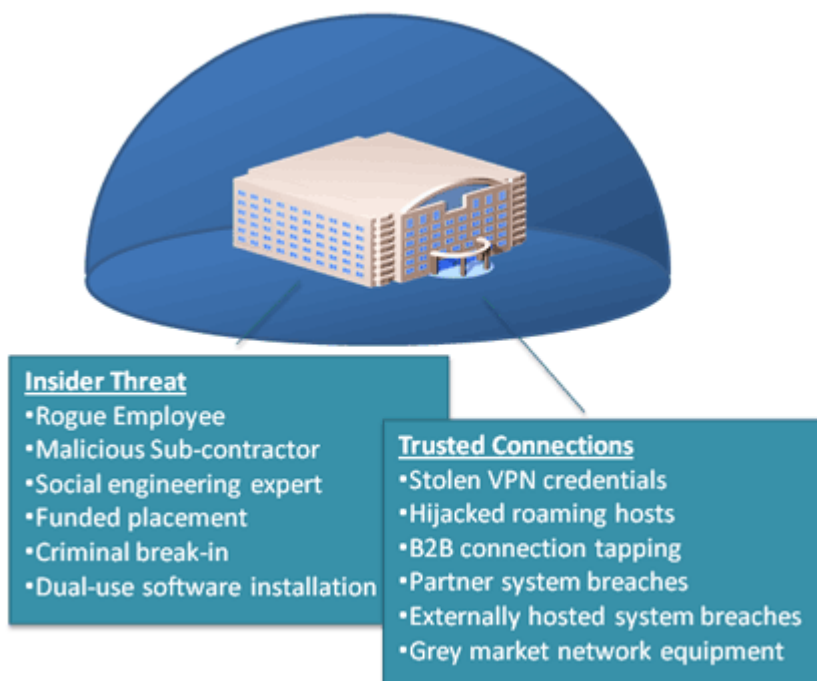
APTs breach enterprises through a wide variety of vectors, even in the presence of properly designed and maintained defense-in-depth strategies:

- Internet-based malware infection
- Physical malware infection
- External exploitation



Well funded APT adversaries do not necessarily need to breach perimeter security controls from an external perspective. They can, and often do, leverage “insider threat” and “trusted connection” vectors to access and compromise targeted systems.

Abuse and compromise of “trusted connections” is a key ingredient for many APTs. While the targeted organization may employ sophisticated technologies in order to prevent infection and compromise of their digital systems, criminal operators often tunnel in to an organization using the hijacked credentials of employees or business partners, or via less-secured remote offices. As such, almost any organization or remote site may fall victim to an APT and be utilized as a soft entry or information harvesting point.



A key requirement for APTs (as opposed to an “every day” botnet) is to remain invisible for as long as possible. As such, the criminal operators of APT technologies tend to focus on “low and slow” attacks – stealthily moving from one compromised host to the next, without generating regular or predictable network traffic – to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.

Malware is a key ingredient in successful APT operations. [Modern “off-the-shelf” and commercial malware](#) includes all of the features and functionality necessary to infect digital systems, hide from host-based detection systems, navigate networks, capture and extricate key data, provide video surveillance, along with silent and covert channels for remote control. If needed, APT operators can and will use custom developed malware tools to achieve specific objectives and harvest information from non-standard systems.

At the very heart of every APT lies [remote control](#) functionality. Criminal operators rely upon this capability in order to navigate to specific hosts within target organizations, exploit and manipulate local systems, and gain continuous access to critical information.

If an APT cannot connect with its criminal operators, then it cannot transmit any intelligence it may have captured. In effect, it has been neutered. This characteristic makes APTs appear as a sub-category of botnets.

While APT malware can remain stealthy at the host level, the network activity associated with remote control is more easily identified. As such, APT’s are most effectively identified, contained and disrupted at the network level.

1.10 DCS (Disturbance Control Systems) & SCADA (Supervisory Control and Data Acquisition)

SCADA generally refers to industrial control systems: computer systems that monitor and control industrial processes (including power generation), infrastructure (including electrical power transmission and distribution), and public and private facility processes (including HVAC and energy consumption). Bob Byrne notes that DCS and SCADA were historically separate, but the recent convergence of technologies has blurred the distinctions.

The goals of DCS and SCADA are quite different. It is possible for a single system to be capable of performing both DCS and SCADA functions, but few have been designed with this in mind, and therefore they usually fall short somewhere. It has become common for DCS vendors to think they can do SCADA because the system specifications seem so similar, but a few requirements paragraphs about data

availability and update processing separates a viable SCADA system from one that would work OK if it weren't for the real world getting in the way.

DCS is process oriented: it looks at the controlled process (the chemical plant or whatever) as the center of the universe, and it presents data to operators as part of its job. *SCADA is data-gathering oriented:* the control center and operators are the center of its universe. The remote equipment is merely there to collect the data--though it may also do some very complex process control! A *DCS operator station* is normally intimately connected with its I/O (through local wiring, *FieldBus*, networks, etc.). When the DCS operator wants to see information he usually makes a request directly to the field I/O and gets a response. Field events can directly interrupt the system and advise the operator.

SCADA must operate reasonably when field communications have failed. The 'quality' of the data shown to the operator is an important facet of SCADA system operation. SCADA systems often provide special 'event' processing mechanisms to handle conditions that occur between data acquisition periods.

There are many other differences, but they tend to involve a lot of detail. The underlying points are:

- SCADA needs to get secure data and control over a potentially slow, *unreliable communications medium*, and needs to maintain a database of 'last known good values' for prompt operator display. It frequently needs to do event processing and data quality validation. Redundancy is usually handled in a distributed manner.
- *DCS is always connected to its data source*, so it does not need to maintain a database of 'current values'. Redundancy is usually handled by parallel equipment, not by diffusion of information around a distributed database.

These *underlying differences* prompt a series of design decisions that require a great deal more complexity in a SCADA system database and data-gathering system than is usually found in DCS. DCS systems typically have correspondingly more complexity in their process-control functionality.

The company I work for has both DCS and SCADA products. The operator stations for each product line can use the same *UNIX workstations*. The systems share data (and thus form a composite SCADA/DCS system), but the *SCADA database architecture* is significantly different from the DCS data architecture, to the extent that the SCADA master station database looks to the DCS operators very much like some directly-connected DCS I/O. The DCS people are (of course) keen to simplify this to cut costs. However, they do not yet have a viable alternative for the mechanisms required in SCADA systems to have communications redundancy and data redundancy to provide the sort of SCADA system reliability that our customers expect.

If you look at most customer's system requirements specifications, a careful analysis of the data collection and data quality requirements will indicate if SCADA-style or DCS-style systems are appropriate. In general: the more features a system provides the more it will cost, so if you do not need SCADA-type data gathering facilities it will usually

be more economical to use a DCS-type system. If you do need these facilities, you will pay for them.

The short answer: DCS and SCADA are still different things, it depends what the customer specifies as to which is appropriate for a particular installation.

I hope this has clarified more than it has confused. Also, it is my opinion based on my own experiences with DCS and SCADA. Others may have experience with systems that are designed to provide full SCADA and full DCS functionality in the one system.

SCADA Systems: NERC Industry Alert (Sept. 14, 2010)

The North American Electric Reliability Corp. released an industry alert Monday identifying malware that targets SCADA systems. The alert urges entities to closely review the information provided and recommends the implementation of mitigation methods as required.

The Stuxnet worm is a significant computer virus that exploits a previously unknown Microsoft Windows operating system vulnerability. While there have been no reported instances of Stuxnet in the United States, NERC is recommending that the industry take precautions in advance. Various versions of the Windows OS are widely deployed throughout the world's critical infrastructures, including the North American bulk power system, which means there is the potential for significant impact.

1.11 High-Impact, Low-Frequency Risk to the Bulk Power System

NERC & U.S. DOE (June 2010)

Full Report: <http://www.nerc.com/files/HILF.pdf>

While HILF risks can include other extreme events like major natural disasters, meteor strikes, and deliberate attacks or acts of war, the November (2009) workshop focused on three specific threats as identified by the HILF Steering Committee in the planning process: Coordinated Cyber/Physical Attack, Pandemic Illness, and Geomagnetic and Electromagnetic Events. Each section identifies the threat to the system, the system's vulnerabilities, and the consequences that could occur were these vulnerabilities to be exploited. This discussion is followed by a consideration of various mitigating options and *Proposals for Action*.

Coordinated Attack Risk: The risk of a coordinated cyber, physical, or blended attack against the North American bulk power system has become more acute over the past 15 years as digital communicating equipment has introduced cyber vulnerability to the system, and resource optimization trends have allowed some inherent physical redundancy within the system to be reduced. The specific concern with respect to these threats is the targeting of multiple key nodes on the system that, if damaged, destroyed, or interrupted in a coordinated fashion, could bring the system outside the protection provided by traditional planning and operating criteria. Such an attack would behave very differently than traditional risks to the system in that an intelligent attacker could

mount an adaptive attack that would manipulate assets and potentially provide misleading information to system operators attempting to address the issue.

While no such attack has occurred on the bulk power system to date, the electric sector has taken important steps toward mitigating these issues with the development of NERC's Critical Infrastructure Protection standards, the standing Critical Infrastructure Protection Committee⁶, and a myriad of other efforts. More comprehensive work is needed, however, to realize the vision of a secure grid. Better technology solutions for the cyber portion of the threat should be developed, with specific focus on forensic tools and network architectures to support graceful system degradation that would allow operators to "fly with fewer controls." Component and system design criteria should also be reevaluated with respect to these threats and an eye toward designing for survivability. Prioritization of key assets for protection will be a critical component of a successful mitigation approach.

Pandemic Risk. Pandemic risk differs from many of the other threats facing the system in that it is a "people event." The principal vulnerability with respect to a pandemic is the loss of staff critical to operating the electric power system. Without these personnel, operational issues on the system would increase as less-trained or less-experienced individuals work to operate generation plants, address mechanical failures, restore power following outages caused by weather and other natural events, and operate the system.

The sector recently experienced a mild pandemic through the 2009 A/H1N1 outbreak. This pandemic's effects on society were very limited and are not representative of the scenarios of concern to the electric sector. While many entities within the sector have developed advanced pandemic plans, the sector is ultimately reliant on government health authorities for quality and timely information on the spread and severity of a pandemic. Clear triggers from these authorities are needed for the sector to make appropriate response decisions in the event of a severe outbreak.

Geomagnetic Disturbances, High Altitude Electromagnetic Pulse Events, and Intentional Electromagnetic Interference Threats. Geomagnetic disturbances, the earthly effects of solar weather, are not a new threat to the electric sector. Recent analysis by Metatech and Storm Analysis Consultants suggests, however, that the potential extremes of the geomagnetic threat environment may be much greater than previously anticipated. Geomagnetically-induced currents on system infrastructure have the potential to result in widespread tripping of key transmission lines and irreversible physical damage to large transformers. The 1989 event that caused a blackout of the Hydro Québec system provided important lessons to the sector. Since that time, the sector has adopted operational procedures to reduce the vulnerability to geomagnetic storms and has installed certain protections in areas most prone to impact as recommended by Oak Ridge National Labs in their report on the March 1989 event.

More work is needed, however, to consider the potential impacts larger storms may have and develop viable, cost-effective mitigations, potentially at lower geographic latitudes than previously thought necessary. The high-altitude detonation of a large nuclear device or other electromagnetic weapon could have devastating effects on the

electric sector, interrupting system operation and potentially damaging many devices simultaneously. A coordinated attack involving intentional electromagnetic interference (EMI) could result in more localized and targeted impacts that may also cause significant impacts to the sector. The physical damage of certain system components (e.g. extra-high-voltage transformers) on a large scale, as could be effected by any of these threats, could result in prolonged outages as procurement cycles for these components range from months to years. Many of these components are manufactured overseas, with little manufacturing capability remaining in North America. The impacts of these events on the power system are not yet fully understood across the sector and warrant further collaborative work to identify the prioritized “top ten” mitigation steps that are both cost-effective and sufficient to protect the power system from the widespread catastrophic damage that could result from any of these events.

1.12 NERC Hosts Geomagnetic Disturbance Workshop (April 2011)

The objective of the workshop is to actively seek comments on industry recommendations that enhance preparations and lessen the risks to bulk power system reliability from severe geomagnetic disturbances.

The bulk power system is designed and operated to provide significant resilience to withstand substantial disruptive events, including geomagnetic disturbances that frequently occur during the year. The industry has been coordinating its efforts to determine if additional resilient measures are warranted to address severe solar storms that can produce disturbances over a wide geographic region. A severe solar storm could potentially impact North American bulk power system reliability, including damaging transformers and generators. This potential from a high impact, low frequency severe geomagnetic event was identified in a joint report published by NERC and the Department of Energy in June 2010.

The workshop will focus on additional operational and planning preparations, and precautionary mitigation steps that industry can take to counteract the most severe of these disturbances, building on the provisions currently in place to address normally anticipated levels of solar storms. Keynote speakers include.....William Murtagh, senior forecaster at the National Oceanic and Atmospheric Administration’s Space Weather Prediction Center.

2.0 Organizations and Initiatives

2.1 Selected Remarks of Gerry Cauley, NERC CEO (April 15, 2011)

House Homeland Security Subcommittee on Cybersecurity Infrastructure Protection.
Full testimony: http://www.nerc.com/news_pr.php?npr=741

In its position between industry and government, NERC embodies the often-invoked goal of creating effective partnerships between the public sector and the private sector.

The bulk power system in North America is one of the largest, most complex, and most robust systems ever created by man. It provides electricity to more than 334 million people, is capable of generating more than 830 gigawatts of power and sending it over 211,000 miles of high voltage transmission lines, and represents more than \$1 trillion in assets.The assets that make up the BPS are varied and widespread. Consequently, the architecture within the systems varies from operator to operator. However, the computer systems that monitor and control BPS assets are based on relatively few elements of technology. Due to increasing efficiencies and globalization of vendors, the universe of suppliers for industrial control systems is limited.

(T)he bulk power system could be as vulnerable to digital threats as IT systems, but with far more critical implications. As proprietary industrial control systems continue to integrate Commercial Off-The-Shelf (COTS) systems, these platforms could inherit the embedded vulnerabilities of those systems. The Stuxnet intrusion methods may serve as a blueprint for future attackers who wish to access controllers, safety systems, and protection devices to insert malicious code that could result in changes to set points and switches, as well as the alteration or suppression of measurements.

The bulk power system has not yet experienced wide-spread debilitating cyber-attacks due in large part to the traditional physical separation between the industrial control system environment and business and administrative networks. However, the increased sharing of Internet and computer networking by control systems and business and administrative networks means that digital infrastructures that were formerly physically separated are now becoming susceptible to common threats.

The NERC CIP standards require electric sector entities to develop a risk-based security policy based upon their specific assets, architecture and exposure. This policy, if properly implemented, will provide insight into the entity's systems and provide the opportunity to mitigate potential threats and vulnerabilities before they are exploited.The defensive security barriers mandated by CIP standards can be effective in frustrating ordinary hackers by increasing the costs and resources necessary to harm to the grid. They may not, however, stop the determined efforts of the intelligent, adaptable adversaries supported by nation states or more sophisticated terrorist organizations.

Electricity Sub- Sector Coordinating Council (ESCC). (NERC works) with industry CEOs and our partners within the government, including the Department of Energy, Department of Defense and Department of Homeland Security, to discuss and identify critical infrastructure protection concepts, processes and resources, as well as to facilitate information sharing about cyber vulnerabilities and threats.

The National Infrastructure Advisory Council (NIAC)). The most effective approach for combating sophisticated adversaries is to apply resiliency principles, as outlined in a set of nine recommendations the National Infrastructure Advisory Council delivered to the White House in October 2010.....Resiliency includes providing an underlying robust system; the ability to respond in real-time to minimize consequences; the ability to restore essential services; and the ability to adapt and learn. The industry is already resilient in many aspects, based on system redundancy and the ability to respond to emergencies. To further enhance resiliency, examples of the NIAC team's recommendations include: 1) a national response plan that clarifies the roles and responsibilities between industry and government; 2) improved information sharing by government regarding actionable threats and vulnerabilities; 3) cost recovery for security investments driven by national policy or interests; and 4) a national strategy on spare equipment with long lead times, such as transformers.

Partnership for Critical Infrastructure Security (PCIS). The PCIS is the senior most policy coordination group between public and private sector organizations. On the government side, PCIS is comprised of the National Infrastructure Protection Plan (NIPP) Federal Senior Leadership Council (FSLC) and the State, Local, and Tribal Government Coordinating Council (SLTGCC), as well as the chairs of all of the other Government Sector Coordinating councils. On the private side, PCIS is comprised of the chairs of all of the private sector coordinating councils.

Industrial Control Systems Joint Working Group (ICSJWG). The ICSJWG is a cross-sector industrial control systems working group that focuses on the areas of education, cross-sector strategic roadmap development, coordinated efforts on developing better vendor focus on security needs and cybersecurity policy issues.

NERC is working with DOE and the National Institute of Standards and Technology (NIST) to develop comprehensive cybersecurity risk management process guidelines for the entire electric grid, including the BPS and distribution systems. We believe this to be particularly important with the increasing availability of smart grid technologies. While the majority of technology associated with the smart grid is found within the distribution system, vulnerabilities realized within the distribution system could potentially impact the BPS.

2.2 Electricity Sub-Sector Coordinating Council (ESCC): Strategic Roadmap (November 2010).

Full report: <http://www.nerc.com/filez/escc.html>

The role of NERC's Electricity Sub-Sector Coordinating Council is to "foster and facilitate the coordination of sector-wide policy-related activities and initiatives to

improve the reliability and resilience of the electricity sector, including physical and cyber security infrastructure.” To help carry out that role, the ESCC has developed this Critical Infrastructure Strategic Roadmap (Roadmap) to recommend to NERC’s Board of Trustees that NERC’s Technical Committees and the industry place renewed emphasis on certain severe-impact risks to electricity system reliability.

In particular, the ESCC has identified three risks that merit increased attention by NERC and the electricity sub-sector. Each of these has the potential to severely impact large portions of the bulk power system, or disrupt electricity service for an extended period of time.

- Coordinated physical attack on significant electricity system equipment.
- Coordinated cyber attack on control systems needed to manage reliability.
- Severe geomagnetic disturbance

The ESCC acknowledges that significant cost and effort will be required to properly understand these risks and develop realistic and effective solutions, and has therefore prioritized initiatives that would deliver the greatest benefit to reliability as soon as possible.

Vision Statement

The Electricity Sub-Sector envisions a robust, resilient electricity infrastructure in which continuity of business and services are maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between sub-sector entities and government.

Information Sharing and Communication

Goal 1: Enhance situational awareness within the electricity sub-sector and with government through robust, timely, reliable, and secure information exchange.

Physical and Cyber Security

Goal 2: Use sound risk management principles to enhance physical and cyber measures that improve preparedness, security, and resilience.

Coordination and Planning

Goal 3: Conduct comprehensive emergency, disaster, and business continuity planning.

Conduct training and large-scale exercises involving electricity industry and government entities to enhance reliability and coordinated emergency response.

Goal 4: Clearly define critical infrastructure protection roles and responsibilities.

Goal 5: Enhance understanding of key interdependencies and collaborate with other critical infrastructure sectors to address them, and incorporate that knowledge in planning and operations.

Public and Regulatory Confidence

Goal 6: Strengthen public and government regulatory agency confidence in the subsector’s ability to manage risk and implement effective security, reliability and recovery efforts.

2.3 NERC Critical Infrastructure Protection Standards

A reliable Bulk Electric System increasingly relies on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data.

NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage BES reliability, and the risks to which they are exposed.

Details: <http://www.nerc.com/page.php?cid=2|20>

CIP-001-1a **Sabotage Reporting**

Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.

CIP-002-4 **Cyber Security - Critical Cyber Asset Identification**

Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1.

CIP-003-4 **Cyber Security - Security Management Controls**

Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

CIP-004-4 **Cyber Security - Personnel & Training**

Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

CIP-005-4 **Cyber Security - Electronic Security Perimeter(s)**

Standard CIP-005-4 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

CIP-006-4 **Cyber Security - Physical Security of Critical Cyber Assets**

Standard CIP-006-4 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

CIP-007-4 **Cyber Security - Systems Security Management**

Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

CIP-008-4 [Cyber Security - Incident Reporting and Response Planning](#)

Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009-4 [Cyber Security - Recovery Plans for Critical Cyber Assets](#)

Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

2.4 Network “Hydra”: Connecting Electric Industry Subject Matter Experts³

Modern threats to the bulk power system are swift, relentless, ever-changing and stem from an immeasurable number of offenders. Various threats extend from cyber activity to physical destruction to terroristic intimidation from offenders attempting to uncover vulnerabilities. NERC, operating as the ES-ISAC,⁴ is charged with identifying the latest vulnerabilities, determining mitigation plans and educating the industry on ways to secure their physical and cyber assets to avoid potential failure.

Enter Network ‘Hydra’, a program designed to engage the right people with the right process at the right time to dynamically protect the electric sector. Hydra will create a network of electric industry subject matter experts (SME) to handle modern fast-moving threats to the bulk power system. The program will identify and manage security knowledge resources as part of the ES-ISAC business processes and workflows. Hydra participants will be asked to assist the ES-ISAC to generate the highest quality threat warning and vulnerability management intelligence. Hydra embraces a set of tools and methods that allow SMEs to collaborate effectively in an expert social network. Hydra is seeking 200 individuals that are directly employed by bulk power system and electric sector entities with the following backgrounds:

- Cyber security
- Physical security
- Operations
- Infrastructure Support (technology and supply chain)

³ NERC Announcement, Jan. 23, 2009

⁴ An ISAC is an Information Sharing and Analysis Center. Each critical infrastructure industry has established an ISAC to communicate with its members, its government partners, and other ISACs about threat indications, vulnerabilities, and protective strategies. ISACs work together to better understand cross-industry dependencies and to account for them in emergency response planning. Presidential Decision Directive 63 - PDD 63 - was issued by President Bill Clinton in 1998. It defines eight infrastructure industries critical to our national economy and public well-being. (Electricity is one of the eight). It also proposes the creation of ISACs. All entities in the electricity sector are participants in the ES-ISAC. The electric sector (ES) ISAC is operated by NERC on behalf of the electricity sector.

There is an open invitation to anyone employed by an electric sector entity with an ES-ISAC performed verification. The ES-ISAC's goal is to complete all verifications in a one week timeframe. Hydra participants are expected to:

- Commit to adhere with information protection requirements
- Complete a skills and experience questionnaire
- Participate in readiness tests and receive ES-ISAC Hydra notices
- Participate if able (goal of participating in 4 calls a year)
- Actively contribute in calls to analyze/evaluate specific threats or vulnerabilities
- Advise the ES-ISAC as requested (e.g. bulk power system & electric infrastructure impact analysis)

In 2009 the ES-ISAC will attempt to consistently employ Hydra on every formal notification sent to the electric sector. Active Hydra members will routinely evaluate the effectiveness of the program and improve associated processes and methodologies. NERC will attempt to launch efforts to assemble a Hydra team in late March, 2009. More information will be provided via the NERC web site (<http://www.nerc.com/>) as the registration date approaches. (NERC News, Jan. 2009)

2.5 NERC Announces Grid Security Exercise (May 3, 2011)

The North American Electric Reliability Corporation (NERC) announced it will conduct a cybersecurity incident readiness exercise, called GridEx 2011, in November as part of its ongoing cyber readiness program.

The grid security exercise, scheduled for November 15-17, will test NERC's and the electricity industry's crisis response plans, and validate current readiness in response to a cyber incident. The exercise also will serve as an opportunity to enhance collaboration and strengthen industry security processes and capabilities.

"GridEx 2011 will involve bulk power system owners and operators from across North America," said Mark Weatherford, chief security officer for NERC. "This large-scale security exercise will continue our forward momentum in securing the grid by allowing NERC and the industry to identify any gaps and to better focus our resources."

The NERC exercise, modeled after the Department of Homeland Security's Cyber Storm exercise series, will allow participants to respond to scenario events as they would in the case of a real-time incident. This will enable participants and leadership to assess, test and validate existing crisis response plans.

Exercise participants will include NERC staff, Regional Entities, Reliability Coordinators, Registered Entities and selected federal partners. To participate in the exercise, contact Brian Harrell at FERC.

2.6 DOE Cybersecurity Initiatives (Announced Sept. 23, 2010)

1. Innovative Cybersecurity Solutions
2. National Electric Sector Cybersecurity Organization (NESCO)
3. 2010 U.S. Smart Grid Vendor Ecosystem Report

Speaking at the inaugural GridWise Global Forum, U.S. Energy Secretary Steven Chu today announced the investment of more than \$30 million for ten projects that will address cybersecurity issues facing the nation's electric grid.

1. Innovative Cybersecurity Solutions - \$20 million

As the energy infrastructure becomes more advanced, it must meet and address cybersecurity challenges along the way. These eight projects will research, develop, and commercialize a comprehensive range of cybersecurity solutions to strengthen the U.S. energy infrastructure against cyber intrusion and assist owners and operators in complying with cybersecurity regulations. Together, these projects will bring cyber security and privacy protection into the utilities, out to the substations, and to homes. One of the projects being funded is: Sypris Electronics - Centralized Cryptographic Key Management (Tampa, FL). This project will enhance the security of the Smart Grid meters at residences, by ensuring the data remains private through providing and managing electronic data keys that only allow trusted parties to access the data and prevent intruders from doing the same. This project will receive \$3.1 million in funding.

2. National Electric Sector Cybersecurity Organization - \$10 million

The National Electric Sector Cybersecurity Organization (NESCO) will be a broad-based, public-private partnership that will work to improve electric sector computer and network cybersecurity, including those used in the smart grid. Working with the DOE and other federal agencies, it will bring together domestic and international experts, software developers and users to focus research efforts; to assess and test the security of new cyber technologies, architectures, and applications; and analyze, monitor, and disseminate infrastructure weaknesses and threats.

Two organizations will receive awards to support this effort. One, described below, will form the organization, NESCO. The other recipient, the Electric Power Institute, Inc. (EPRI), will provide a research and analysis resource for NESCO. Energy Sector Security Consortium, Inc. (EnergySec) (Clackamas, OR) EnergySec will form the organization to be known as NESCO. It will work to improve electric system reliability by supplying data analysis and forensics capabilities for cyber-related threat. It will also assist in creating a framework to identify and prepare for challenges to grid reliability; share information, best practices, resources, and solutions to and from domestic and international electric sector participants; and encourage key electric sector supplier and vendor support and interaction. This project will receive \$5.9 million in funding.

3. 2010 U.S. Smart Grid Vendor Ecosystem Report

DOE released today the findings of a new research study, the 2010 U.S. Smart Grid Vendor Ecosystem Report, which highlights \$2.75 billion in annual product sales in three key smart grid categories: Advanced Metering Infrastructure (AMI), Demand Response, and Distribution Grid Management.

In addition to providing insight into spending patterns and market share in the sector, the report draws attention to a number of emerging industry dynamics shaping the future of the smart grid ecosystem. Key findings explored in the report include:

- The increasing data and communications sophistication of smart grid applications is driving dependence on integration and successful partnerships amongst a growing network of companies sharing the market
- \$1.7 billion in venture capital has been invested into smart grid companies between 2007-2010 with the majority flowing into suppliers of AMI and home and building energy management products
- While venture-backed innovators have played an important role in the market, the report finds that the broader smart grid vendor landscape is comprised of companies new and old, large and small, as well as domestic and international.

2.7 DOE-EPRI Cybersecurity Collaborative (Announced Sept. 27, 2010)

Protecting the U.S. Electric Sector Against Cyber Attacks:
Technologies, Best Practices, Metrics, and Standards

The Electric Power Research Institute (EPRI) said today that the U.S. Department of Energy has selected its cyber security collaborative to assess and develop technologies, best practices, metrics and standards to protect the U.S. electric sector against cyber attacks. The DOE's National Energy Technology Laboratory (NETL) and the collaborative will negotiate a funding level for the public-private research initiative.

The EPRI-led collaborative comprises national research and commercial research laboratories, universities, and subject matter experts in key areas of cyber security (see list of participants at the end of this press release). The participants bring diverse experience in technology, business, standards and policy. It was among 10 cyber security initiatives representing an investment of more than \$30 million that was announced last week in Washington by U.S. Energy Secretary Steven Chu.

Among the collaboratives tasks are: assessing requirements and results developed by the National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), and other organizations; reviewing power system and cyber security standards in meeting power system security requirements; and, testing grid security technologies protocols using laboratories and pilot projects.

The selection of the EPRI collaborative is part of a long-term program that will ultimately lead to the creation of a National Electric Sector Cyber Organization (NESCO). This federal government-electric sector partnership will analyze the cyber security status of the nation's transmission and distribution systems as smart grid technologies are incorporated to enable a low-carbon future.

"The Idaho National Laboratory (INL) brings knowledge gained from six years of cyber security vulnerability assessments on grid architectures in the energy sector," said Rita Wells, energy sector lead of the Critical Infrastructure Protection & Defense Systems of

the lab, a collaborative participant. “Emerging smart grid technologies are challenging traditional security and functional boundaries, and this is requiring us to pursue new approaches to cyber security.”

Up to \$10 million is expected to be available over three years to establish NESCO, fund research and development, and set up administrative and operational functions. It is expected that NESCO will become self-sustaining within the three years, utilizing key findings from the collaborative.

“This collaborative effort will play a critical role in addressing cyber security for the nation's -grid”, said Sami Ayyorgun, senior scientist at Telcordia Technologies. “Our decades of experience in cyber security, communications, and networking will be critical to the project’s success.”

The EPRI-led collaborative comprises Enernex, Flowers CCS, Xanthus Consulting International, N-Dimension, Palo Alto Research Center, SRI, Oak Ridge National Laboratory, Idaho National Laboratory, Sandia National Lab, National Renewable Energy Laboratory, Telcordia, University of Houston, Mladen Kezunovic (Texas A&M University), University of Minnesota Smart Grid consortium (including Adventium Labs and Honeywell), UCLA, UC Berkeley, Inguardians, and Arc Technical. Siemens and ABB are serving in industry advisory role in the collaborative.

2.8 NESCO: National Electric Sector Cybersecurity Organization

Mission: Lead a broad-based, public-private partnership to improve electric sector energy systems cyber security. Goals:

- Identify and disseminate common, effective cyber security practices
- Analyze, monitor and relay infrastructure threat information
- Focus cybersecurity research and development priorities
- Work with federal agencies to improve electric sector cyber security
- Encourage key electric sector supplier and vendor support

NESCO/NESCOR Partnership

- EnergySec = National Electric Sector Cybersecurity Organization (NESCO)
- EPRI = National Electric Sector Cybersecurity Organization Resource (NESCOR)

NESCO	NESCOR
Primary grant recipient; “EnergySec will form the organization to be known as NESCO”	R&D Partner; “EPRI led team will provide a research and analysis resource for NESCO to mitigate risks from imminent threats and vulnerabilities”
Emphasis on information and resource sharing, collaboration, situational/ tactical awareness, rapid notification, forensics and applied research	EPRI led team will harmonize cybersecurity requirements from NIST CSWG, DHS ICS, JWG, NERC and OpenSG Utilisec and assess cybersecurity posture of standards and technologies (including lab testing)
Asset owner participation is primary vehicle, supplemented by SME contractors.	EPRI led team includes 17 partners from research labs, academia and other SMEs

2.9 NISTIR 7628 (NIST Interagency Report)

By: U.S. Dept. of Commerce/Natl. Inst. Of Standards and Technology (August 2010)

Guidelines for Smart Grid Cyber Security

Vol. 1: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

Vol. 2: Privacy and the Smart Grid

Vol. 3: Supportive Analyses and References

Problem Statement (Vol. 1, pg. 1):

With the implementation of the Smart Grid has come an increase in the importance of the information technology (IT) and telecommunications infrastructures in ensuring the reliability and security of the electric sector. Therefore, the security of systems and information in the IT and telecommunications infrastructures must be addressed by an evolving electric sector. Security must be included in all phases of the system development life cycle, from design phase through implementation, maintenance, and disposition/sunset.

Cyber security must address not only deliberate attacks launched by disgruntled employees, agents of industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable ways. The need to address potential vulnerabilities has been acknowledged across the federal government, including the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Energy (DOE), and the Federal Energy Regulatory Commission (FERC).

Additional risks to the grid include:

- a) Increasing the complexity of the grid could introduce vulnerabilities and increase exposure to potential attackers and unintentional errors;
- b) Interconnected networks can introduce common vulnerabilities;
- c) Increasing vulnerabilities to communication disruptions and the introduction of malicious software/firmware or compromised hardware could result in denial of service (DoS) or other malicious attacks;
- d) Increased number of entry points and paths are available for potential adversaries to exploit;
- e) Interconnected systems can increase the amount of private information exposed and increase the risk when data is aggregated;
- f) Increased use of new technologies can introduce new vulnerabilities; and
- g) Expansion of the amount of data that will be collected that can lead to the potential for compromise of data confidentiality, including the breach of customer privacy.

2.10 Comment on NISTER 7628, from GraniteKey (Sept. 5, 2010)

The entire Smart Grid deployment and cyber security world has been waiting for NISTIR 7628 to move from "Draft" status to "Final" status for nearly one and a half years. This magnificent effort, which included over 400 participants from many industries, government agencies, public and private groups, and just plain interested individuals, has culminated in 3 volumes that essentially read like an encyclopedia of cyber security best practices and technical jargon, complete with tables, drawings, and lots of arrows pointing all over the place. It is an impressive compendium of knowledge.

So what does this all mean to the world of Smart Grid security? Does this make us more secure? Well, as things stand right now, not exactly.

First of all, let's understand something about NIST and NISTIR 7628. The title is both prescient and potentially misleading. Here is the title for Volume 1:

"Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements"

Look carefully at the first word and the title and bear in mind that, for all legal intents and purposes that is all that matters. It is a "Guideline". I know it says "Requirements" at the end of the sentence, but understand that NIST does not dictate requirements to anyone who has the authority to enforce anything. The only requirements NIST has any authority over is the requirements NIST sets forth to comply with NIST standards (i.e. there are certain specific requirements that an entity must meet in order to become FIPS certified).

Why do I say this is potentially misleading? Well, because unless an authoritative body passes a rule, law, or mandate of some sort that requires the adoption of all or part of the recommendations in NISTIR 7628, it is nothing more than a magnificent exercise. The simple existence of Smart Grid security guidelines does not make the Smart Grid more secure. The correct implementation of Smart Grid security standards, however, can.

Yet simply pointing at the NISTIR 7628 and saying "do this" will not suffice. This is because NISTIR 7628 is a collection of NIST standards and recommendations. While this may seem sufficient for some, it is still too open ended to serve as anything close to prescriptive. In fact, NISTIR 7628 is not intended to be prescriptive, and it says so in section 2.2 of Volume 1:

"This list of technologies and services is not intended to be prescriptive; rather, it is to be used as guidance."

This leads to the obvious conclusion that NISTIR 7628 is not intended to serve as "the rulebook", but to assist the rulemakers in writing "the rulebook".

So who are the rulemakers?

Well, that is a good question, and one that is not so easy to answer without first understanding that it all depends on what part of the Smart Grid we are talking about.

To try to simplify this as much as possible, and forgive me if this is oversimplified (or overly complicated as the case may be).

We can break the power Smart Grid into three categories:

1. Generation - Where the power is generated (i.e. the power plant)

2. Transmission - How the power gets from the power plant to the substations that send it to those who use it.
3. Distribution - The part of the organization that the user directly interfaces with (the ones who read your meter and send you a bill and shut off your power if you do not pay your bill).

So Generation and Transmission are generally not considered part of AMI (Advanced Metering Infrastructure). AMI is the part of the Smart Grid where smart meters live. Generation and Transmission currently fall under the jurisdiction of the Federal Government, and are therefore subject to the whims of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC). NERC is not a Federal agency, but is given authority by FERC to conduct audits, levy fines, and all sorts of interesting stuff that tends to keep utilities in various stages of insomnia and cold sweats.

Distribution, on the other hand, falls under the jurisdiction of the individual States, and consequently the Public Utility Commission (PUC) of a given state.

So what this means is that FERC, NERC, and the State PUC's must now take a long and hard look at NISTIR 7628 (not to say they have not already been doing so) and try to synthesize some specific regulations based upon what is contained in this very verbose 3 volume set. This is no easy task, as one can imagine. Let's examine one particular section, taken from Volume 1:

4.2.1.8 Physical Security Environment

...In determining the appropriate level of physical protections required for a device, it is important to consider both the operating environment and the value and sensitivity of the data protected by the device. Therefore, the specification of cryptographic module physical protections is a management task in which both environmental hazard and data value are taken into consideration. For example, management may conclude that a module protecting low value information and deployed in an environment with physical protections and controls, such as equipment cages, locks, cameras, and security guards, etc., requires no additional physical protections and may be implemented in software executing on a general purpose computer system. However, in the same environment, cryptographic modules protecting high value or sensitive information, such as root keys, may require strong physical security...

If, for example, you are the CPUC (California Public Utility Commission) and are attempting to create a requirement based upon this section for physical protection of cryptographic modules (and the data contained within them), one must first define what "high value or sensitive information is". The root key mentioned is a good example, but what about other information stored on the device? What is the information? Is it also sensitive? Who determines if it is sensitive or not?

If the CPUC then determines that the information stored is not overly sensitive (i.e. not a root key), then it is important to ensure that the scope of the information stored on such modules does not "creep" to a point where it may indeed become sensitive. This is no easy task, because sometimes what is deemed safe today does not always remain safe going forward. A good example of this is a Social Security Number. There was a time

when nobody had a problem sharing their Social Security Number with anyone. Heck! In many cases it was your ID number for school, work, military, etc. What happened, however, is that the scope of the Social Security Number expanded, and it was soon discovered that if you knew someone's number you could do all sorts of bad things with it.

If the CPUC determines that the information is indeed sensitive, then they are tasked with determining what standard for protection of such information must serve as a baseline (i.e. FIPS 140-2).

Providing they can accomplish these tasks, they must then determine if and how they are going to audit (and potentially certify) such requirements.

...but first they have to determine what is in scope and what is not in scope, and why. This in and of itself requires the PUC's (and FERC and NERC) to have an intimate understand of what parts of NISTIR 7628 (and potentially other guidelines, such as the excellent [work done by the UCAIUG AMI-SEC Task Force](#), which is specifically credited for their contributions to NISTIR 7628 within Volume 1) apply to their purview. Looking at this at the Federal level, one might conclude that they have enough resources to tackle this task, but having listened to FERC Commissioner Philip Moeller's keynote address at my [Smart Grid Cyber Security Summit](#) last month, in which he stated "We don't have all the answers, we need all of you to help.", I am led to believe that we still have a long way to go.

...and it is even more challenging for State PUC's. The CPUC is a fairly well staffed organization, being that California is indeed a very large State. Nonetheless, the CPUC does not currently have anything close to a comprehensive understanding of cyber security. To be fair, why would they? In its many years of existence they have never had to deal with cyber security issues with respect to regulation of utilities, and up until the passage of [California SB 17](#) it has never been their responsibility. However, being staffed with some very intelligent (and diligent) people, and now being responsible for making decisions relating to cyber security and the Smart Grid, the CPUC has indeed taken it upon themselves to rise to the occasion. I have personally attended two public hearings at the CPUC where Smart Grid security was discussed, contributed to requests for comments from the CPUC regarding cyber security, and the CPUC is planning a public hearing to specifically discuss NISTIR 7628 with the NISTIR 7628 team at the CPUC at the end of September, 2010 (currently planned for September 28th and 28th), as well as additional workshops to hash out the details of Smart Grid security.

This is all good stuff!.....but what about other PUC's? Some States (from what I have been told by members of the CPUC) have PUC's that could fit into a small room with plenty of space to spare for filing cabinets, chairs, and tables. In other words, they are woefully understaffed and underfunded. How are they going to manage cyber security?

Well, one answer is contained in one of my favorite sayings "As goes California, so goes The Nation." Their eyes are on California, and what California decides is quite likely to serve as a template for the rest of the nation. Some have also argued that

Texas is also serving as a template. While this may be true, I have a sneaking suspicion that California will likely prevail as a trendsetter. Only time will tell, I imagine.

The great news is that there seems to be no shortage of people who are willing to volunteer their time in working through these challenges. It may not be entirely altruistic in nature (hey, everyone wants a piece of the Smart Grid security market pie, including yours truly), but the fact remains that we are indeed well served by some of the great minds working on the effort. PG&E has a cybersecurity team currently led by [CISO Dave Tyson](#) (who came from the security team of eBay) and PG&E has been dealing with Smart Grid security for longer than just about any utility in the world. The UCAIUG AMI-SEC Task Force is still working hard and growing stronger with every meeting (I try to attend and contribute as often as possible). Many AMI vendors are currently specifically dedicating resources to cyber security efforts, and are working together in a spirit of "coopetition", where they cooperatively share information with each other despite being competitors. Anyone who attended my conference is well aware of just how many organizations are involved in this effort, and the list keeps growing.

We still have a lot of work to do, but we have come a long way, and I am not even close to tired yet! NISTIR 7628 is worthy of being celebrated for finally being completed, but now the real work begins.

2.11 DHS National Infrastructure Protection Plan (NIPP)

Protecting and ensuring the continuity of the critical infrastructure and key resources (CIKR) of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life. CIKR includes physical or virtual assets, systems, and networks so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

The National Infrastructure Protection Plan (NIPP) provides the coordinated approach that is used to establish national priorities, goals, and requirements for CIKR protection so that Federal resources are applied in the most effective and efficient manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified under the authority of Homeland Security Presidential Directive 7, and addresses the physical, cyber, and human considerations required for effective implementation of protective programs and resiliency strategies.

Risk Management

The NIPP specifies the key initiatives, milestones, and metrics required to achieve the Nation's CIKR protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security (DHS), Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, territorial, and private sector partners. The cornerstone of the NIPP is its risk management framework, which establishes the processes for

combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

NIPP Sector Partnership Model.

To be effective, the NIPP must be implemented using organizational structures and partnerships committed to sharing and protecting the information needed to achieve the NIPP goal and supporting objectives. DHS, in close collaboration with the SSAs, is responsible for overall coordination of the NIPP partnership framework and information-sharing network. The coordination mechanisms establish linkages among CIKR protection efforts at the Federal, State, regional, local, tribal, territorial, and international levels as well as between public and private sector partners. In addition to direct coordination between partners, the structures described below provide a national framework that fosters relationships and facilitates coordination within and across CIKR sectors.

- **Sector Partnership Coordination.** The CIKR Cross-Sector Council, the Government Cross-Sector Council (made up of two subcouncils: the NIPP Federal Senior Leadership Council and the State, Local, Tribal, and Territorial Government Coordinating Council), the Regional Consortium Coordinating Council, and individual Sector Coordinating Councils and Government Coordinating Councils create a structure through which government and the private sector can collaborate and develop consensus approaches to CIKR protection.
- **Sector Coordinating Councils (SCC).** The sector partnership model encourages CIKR owners and operators to create or identify an SCC as the principal private sector entity for coordinating with the government on a wide range of CIKR protection activities and issues. Specific membership will vary by sector, reflecting each sector's unique composition; however, membership should be representative of a broad base of owners, operators, associations, and other entities within a sector.
- **Government Coordinating Councils (GCC).** A GCC is formed as the government counterpart to the SCC to enable interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (Federal, State, local, tribal, and territorial) as appropriate to the security landscape of each sector.
- **Regional Consortium Coordinating Council (RCCC).** The RCCC brings together representatives of regional partnerships, groupings, and governance bodies to enable CIKR protection coordination among partners within and across geographical areas and sectors.
- **International Coordination.** The United States-Canada-Mexico Security and Prosperity Partnership, the North Atlantic Treaty Organization's Senior Civil Emergency Planning Committee, certain government councils such as the Committee on Foreign Investment in the United States, and consensus-based nongovernmental or public-private organizations enable a range of CIKR protection coordination activities associated with established international agreements.
- **Critical Infrastructure Partnership Advisory Council (CIPAC).** The CIPAC directly supports the sector partnership model by providing a legal framework for members of the SCCs and GCCs to engage in joint CIKR protection-related activities. The CIPAC serves as a forum for government and private sector partners to engage in a broad spectrum of activities including: planning, coordination, implementation, and operational

issues; implementation of programs; operational activities related to CIKR protection, response, and recovery; and development and support of national plans, including the NIPP and Sector-Specific Plans

2.12 DHS: Critical Infrastructure Partnership Advisory Council (CIPAC)

Website: http://www.dhs.gov/files/committees/editorial_0843.shtm

The Department of Homeland Security has established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments.

The CIPAC represents a partnership between government and critical infrastructure/key resource (CIKR) owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection.

CIPAC membership will encompass CIKR owner/operator institutions and their designated trade or equivalent organizations that are identified as members of existing Sector Coordinating Councils (SCCs). It also includes representatives from federal, state, local and tribal governmental entities identified as members of existing Government Coordinating Councils (GCCs) for each sector.

CIPAC Energy Sector

The Energy Sector consists of thousands of geographically dispersed electricity, oil, and natural gas assets that are connected by systems and networks. Collaboration is essential in order to secure such an interdependent infrastructure that is owned, operated, hosted, and regulated by numerous public and private entities. The sector's public-private partnerships address security issues and share information on threats, vulnerabilities, and protective measures. Private sector security partners are represented by the Electricity and the Oil and Natural Gas Sector Coordinating Councils (SCCs), and public sector security partners comprise the Energy Government Coordinating Council (GCC). The Electricity SCC represents 95 percent of the electric power industry, and the Oil and Natural Gas SCC represents 98 percent of the oil and natural gas industry. The U.S. Department of Energy serves as the Sector-Specific Agency of the Energy Sector.

2.13 DHS CSSP: Control Systems Security Program

The goal of the DHS National Cyber Security Division's CSSP is to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local, and tribal governments, as well as

industrial control systems owners, operators and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

Top 10 most accessed control systems documents and web pages

1. [ICS-CERT](#)
2. [Strategy for Securing Control Systems](#) (pdf)
3. [Catalog of Control Systems Security: Recommendations for Standards Developers](#) (pdf)
4. [Cyber Security Procurement Language for Control Systems](#) (pdf)
5. [Recommended Practices](#)
6. [Personnel Security Guidelines](#) (pdf)
7. [Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies](#) (pdf)
8. [Developing an Industrial Control Systems Cybersecurity Incident Response Capability](#) (pdf)
9. [Cyber Security Evaluation Tool](#)
10. [Secure Architecture Design](#)

2.14 US CERT: Computer Emergency Readiness Team

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

1. [Who runs US-CERT?](#) US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). It is a public-private partnership.
2. [Where is US-CERT located?](#) US-CERT is located in the Washington DC Metropolitan area.
3. [What is US-CERT's relationship to NCSD and DHS?](#) US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). The NCSD was established by DHS to serve as the federal government's cornerstone for cyber security coordination and preparedness, including implementation of the [National Strategy to Secure Cyberspace](#) (2003).
4. [Who are US-CERT's partners?](#) As it grows, US-CERT will include partnerships with private sector cyber security vendors, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local governments, and domestic and international organizations. Working together, these groups will coordinate national and international efforts to address key cyber security issues.
5. [How does the Protected Critical Infrastructure Information \(PCII\) Program work to protect submitted information?](#) The [PCII Program](#), established in response to the Critical Infrastructure Information Act of 2002 (CII Act), creates a new framework for protecting certain types of information. The PCII program enables members of the private sector to, for the first time, voluntarily submit confidential information regarding the nation's critical infrastructure to the Department of Homeland Security (DHS) with the assurance that the information will be protected from public disclosure. More details

about how information can be protected under the CII Act can be found on the [Department of Homeland Security](#) web site.

2.15 National Association of State Energy Officials (NASEO): Smart Grid & Cyber Security for Energy Assurance (Dec. 2011)

Planning Elements for Consideration in States' Energy Assurance Plans

<http://www.naseo.org/search.asp?q=Smart+Grid+and+Cyber+Assurance&sa=Search&cx=010282055925951439871%3Ahusilm6wiom&cof=FORID%3A9#1094>

Examples of Recent Attacks (pg. 15-16)

- In 2001, hackers penetrated the California Independent System Operator, which oversees most of the State's electricity transmission grid; attacks were routed through California, Oklahoma, and China.
- Ohio's Davis-Besse nuclear power plant safety monitoring system was offline for five (5) hours due to the Slammer worm in January 2003.
- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities electronic control systems.
- In April 2009, the Wall Street Journal reported that spies hacked into the U.S. electric grid and left behind computer programs that could allow them to disrupt service.
- Associated Press on August 4, 2010 reported "Hackers Try to Take over Power Plants." In September 2010, cyber experts discovered for the first time a malicious computer code, called a worm, specifically created to take over systems that control the inner workings of industrial plants.
- The Stuxnet Worm was reported in an Industrial Control Systems Cyber Emergency Response Team Advisory on September 29, 2010. Stuxnet is a Malware Targeting Siemens Control Software. It can be used to infiltrate industrial control systems used in the power grid, power plants and other infrastructure. It is reported to have the ability to damage or possibly destroy control systems.
- The North American Electric Reliability Corporation (NERC) and DOE released a report titled *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* (June 2, 2010)¹⁶ that identifies a certain class of high-impact, low-frequency risk shown to have the potential to significantly affect the reliability of the North American bulk power system. The report examines three high-impact, low-frequency risks in detail: coordinated cyber, physical, or blended attacks; pandemic illness; and geomagnetic disturbances and electromagnetic pulse (EMP) events.
- NERC issued a recommendation ¹⁷ to industry on the AURORA vulnerability¹⁸ in October 2010. The recommendation provides new sensitive and clarifying information regarding the nature of AURORA. The recommendation requires entities to report on efforts and progress by Dec. 13, 2010 with updates every six months until mitigation is complete.

Assessing the Status of State Smart Grid Developments_(pg. 10-12)

The first step in addressing smart grid as part of State energy assurance plans is to understand the current level of activity and investment in the State. Key questions include: what has been done, where and what types of investments have been made, and what projects and investments are planned for the future. Assessment Outline:

1. Describe the current status of smart grid implementation:

a. Purpose(s) and drivers for smart grid projects.

- Energy assurance aspects; emergency response, resiliency and risk mitigation.
- Business case developed by utilities and others.
- Other expected benefits.

b. Overall plan for smart grid implementation; technologies installed and planned.

c. Degree to which smart grid implementation has enabled or will enable:

- Improvements in security, reliability and resiliency.
- More rapid recovery from power outages.
- Demand management and energy efficiency programs.
- Integration of distributed generation and renewable energy.
- Integration of plug-in electric hybrid vehicles.
- Use of smart grid distribution automation.

d. Plans for evaluating performance and benefits, and comparing to initial estimates.

e. Digital meters (i.e. smart meters and advanced metering infrastructure (AMI)).

- Overview of meter investment plan, objectives, drivers.
- Relation to energy assurance plans.
- A description of the meter functional capabilities (the type of meter deployed may vary among utilities).
- Number and location of AMI/smart meters installed.
- Implementation of meter data management systems to support the large volume of data and make it available to other utility processes.
- Customer web portal for customers to access and view their own usage from as recent as prior day.
- Two-way communications through the AMI and related head-end management systems to provide services to customers, such as demand response and pre-pay services.
- Determination of whether the systems being deployed proprietary or standards or open-source based systems.
- Integration of meter outage notifications into utility outage management systems, to better and more rapidly identify the number and location of customers affected and the rate of recovery.

f. Distribution system.

- Overview of distribution system investment plan, objectives, drivers.
- Relation to energy assurance plans.
- Automated and remotely controlled capacitor banks for var (reactive power) and power factor control, to maintain voltage on feeders at optimum levels to save end-use energy and to reduce losses.
- Supervisory-controlled reclosers to speed restoration for faults that clear themselves, avoiding manual fuse replacements.
- Automated fault isolation and feeder reconfiguration equipment.

- Mobile workforce management systems that dispatch crews already in the field to new work assignments, such as outage repairs, in a timely and effective manner.
- Outage management systems that integrate smart meter “last gasp” outage information for better and more rapid identification of the number of customers affected (and their location) to speed restoration of power.
- Distribution management systems that incorporate seamless interface for operators and provide for fault location to speed crews to precise locations of outages.

g. Transmission system.

- Overview of transmission system investment plan, objectives, drivers.
- Relation to energy assurance plans.
- Phasor measurement units (PMUs) at key grid nodes.
- Dynamic line rating tools and methods for system operators.
- Condition monitoring of major transformers to allow operation at maximum safe loadings and detect emerging equipment problems.

2. Describe utility and other State and private sector plans for future smart grid deployment, including pilot and demonstration programs:

- a. The level and source of investments, including those funded by grants, stockholders, and those already approved by the State utility commission for inclusion in rates.
- b. Are there future investments which are pending approval?
- c. Any non-utility smart grid related investments that may integrate into the smart grid. For example, this could include storage for renewable projects such as compressed air, battery, pumped hydro, etc.

3. Identify any State public utility commission orders or administrative rules addressing smart grid, and any special conditions that may have been set by the commission.

4. Identify any pending cases that address smart grid in whole or in part.

5. Identify any future anticipated cases that may address smart grid investment.

6. Identify any projects that may be funded by other sources that may support smart grid, including the State Energy Program or the Energy Efficiency Conservation Block grants to local communities.

Development of Cyber Security Capability at the State Level (pgs. 16-21)

Step One – Understand the State’s internal cyber security profile.

- a) Understand cyber security risks at work and at home. Many States and organizations have guidance available. For an example see: <http://www.michigan.gov/cybersecurity>.
- b) Identify the individuals in the State who have the primary roles for addressing cyber security, and identify their roles and responsibilities.
- c) Determine which State agency, if any, has lead and/or supporting roles and responsibilities in cyber security as it directly relates to smart grid implementation.
- d) Become familiar with the State’s Continuity of Operations Plans (COOP)¹⁹ and disaster recovery strategies that pertain to the essential cyber security systems.²⁰

e) Determine if it may be helpful to become a member of the FBI's InfraGard Program: <http://www.infragard.net/>.

f) Become familiar with the U. S. Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber attacks for the Federal Civil Executive Branch, as well as information sharing and collaboration with State and local government, industry and international partners.

<http://www.us-cert.gov/>

Step Two – Understand the *current* cyber security requirements for the energy sector.

a) Electricity and smart grid:

- NERC -- Standards CIP-002 through CIP-009 (the Critical Cyber Asset Identification portion of the [Critical Infrastructure Protection Standards](#)).
- Section 1305 of EISA 2007 defines the roles of both Federal Energy Regulatory Commission (FERC) and NIST as they relate to the development and adoption of smart grid standards. Subsection 1305(d) defines the Commission's role.

b) Understand the cyber security requirement for other parts of the energy sector including natural gas (pipeline safety standards) and the petroleum sector, because of the interdependency effects that need to be considered.

c) Under EISA 2007, NIST has "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems..."

Step Three – Understand *future* standards and guidelines currently under discussion and development, and how they may affect utilities' plans for smart grid deployment.

a) The Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) is a utility-driven, public-private collaborative among DOE, EPRI, and a large group of leading North American utilities..... To date, ASAP-SG has produced three Security Profiles.

- The Security Profile for Advanced Metering Infrastructure (*AMI Security Profile*) has been ratified by the AMI-SEC Task Force within the UCAlug....
- The Security Profile for Third Party Data Access (*3PDA Security Profile*) has been ratified by a Usability Analysis team within the UCAlug SG Security Working Group.....
- The recently completed Security Profile for Distribution Management (*DM Security Profile*) has been handed over to the SG Security Working Group for review and ratification.....
- Publicly available versions of ASAP-SG documentation may be found on SmartGridiPedia at <http://www.smartgridipedia.org>.

b) Over the next three years, the National Electric Sector Cyber Security Organization (NESCO) will be working with the National Electric Sector Cyber Security Organization Resources (NESCOR) to lead a broad-based, public-private partnership to improve electric sector energy systems cyber security.

Step Four – Determine whether there are cyber security plans in place, and whether they are driven by State regulatory or Federal grants compliance.....States need to identify the best options for working with the private sector to address cyber security concerns.....The Smart Grid Investment Grants (SGIG) program under the American Recovery and Reinvestment Act required utilities proposing projects to develop cyber security plans.....The SGIG grant language requires a description of how cyber security concerns will be addressed with respect to the use of best available equipment and the application of procedures and practices involving system design, testing, deployment, operations and decommissioning, including at a minimum:

- A description of the cyber security risks at each stage of the system deployment lifecycle.
- Cyber security criteria used for vendor and device selection.
- Cyber security control strategies.
- Descriptions of residual cyber security risks.
- Relevant cyber security standards and best practices.
- Descriptions of how the projects will support/adopt/implement emerging smart grid security standards.

Another area to consider is whether the cost to meet cyber security requirements will be recovered. Public utility commissions need to address how regulated utilities will pay for the necessary infrastructure upgrades to meet the cyber security requirements. This is a necessary step because of the ubiquitous presence of legacy information systems that will require upgrades to meet the cyber security requirements.....

Step Five. Consider and address the human element of cyber security. While this step is last, in many ways it is also one of the most important.

- It represents a serious ongoing vulnerability, and therefore it is critical to assure that it is properly addressed.
- Understand what the insider threat is and what policies and procedures are in place to prevent intrusion and manipulation.
- Understand what social engineering is and how it can be used to access systems.
- Understand that technical solutions to security should account for human behavior, which can be driven by both cultural and psychological factors.
- Understand the nature of the threat from employees, contractors, consultants, or anyone with short or long term access to IT systems, and know about system vulnerabilities.
- Understand that the effect of new systems on consumer behavior could be both a plus and a minus. It could strengthen security or incite actions to attack the system.

3.0 Proposed Legislation

3.1 The Grid Reliability and Infrastructure Defense (“GRID”) Act⁵

The [GRID Act](#) was passed by the House of Representatives on June 9, 2010. This bill would amend the Federal Power Act to grant the Federal Energy Regulatory Commission (“FERC”) authority to issue emergency orders requiring critical infrastructure facility operators to take actions necessary to protect the bulk power system. Prior to FERC issuing such an order, the President would have to issue a written directive to FERC identifying an imminent threat to the nation’s electric grid. FERC would be required to consult with federal agencies or facility operators before issuing an emergency order only “to the extent practicable” in light of the nature

⁵ Hunton & Williams LLP 2010: Source for 3.1-3.4

of the threat. The GRID Act is being considered by the Senate Committee on Energy and Natural Resources at this time.

3.2 Protecting Cyberspace as a National Asset Act of 2010

The Senate Homeland Security and Government Affairs Committee passed the [Protecting Cyberspace as a National Asset Act of 2010](#) on June 24, 2010. The bill is a comprehensive, multi-sector bill requiring the Department of Homeland Security (“DHS”) to coordinate its response to cyber emergencies with agencies and regulators that have jurisdiction over critical energy infrastructure. The critical energy infrastructure to be protected would be classified and would require higher levels of security for assets that are at higher risk of a cyber attack. The Protecting Cyberspace as a National Asset Act of 2010 aims to leverage the utility expertise of public-private partnerships and the law enforcement and intelligence gathering expertise of DHS to assess threat levels before requiring action that could have operational consequences for the nation’s electric grid. A companion bill has not yet been introduced in the House of Representatives.

3.3 The American Clean Energy Leadership Act

The [American Clean Energy Leadership Act](#) was passed by the Senate Energy and Natural Resources Committee on July 16, 2009. It was a likely candidate for passage (either by itself or as part of a broader energy package) until climate change negotiations broke down in the Senate. The American Clean Energy Leadership Act would amend the Federal Power Act to grant FERC authority to issue emergency orders without notice or hearing in order to protect the electric grid from “cybersecurity vulnerabilities,” which are defined as weaknesses or flaws in design or operation that expose the energy grid to cybersecurity threats. The bill would grant the Secretary of Energy similar authority to issue emergency orders in the event of an imminent threat that could disrupt the operation of the nation’s electric grid. Unlike the GRID Act, The American Clean Energy Leadership Act would grant FERC the authority to issue orders only to electric infrastructure operators, and would not be contingent on a presidential directive.

3.4 The Cybersecurity Enhancement Act of 2010

The [Cybersecurity Enhancement Act of 2010](#) was the first major cybersecurity bill to reach the floor of either house in the 111th Congress. This bill, which has broad bipartisan support, passed the House of Representatives on February 4, 2010. This bill differs from other cybersecurity legislation because it does not create emergency government authority for cybersecurity threats, nor does it specifically address the energy or utility industries. Instead, the Cybersecurity Enhancement Act of 2010 charges the National Institute of Standards and Technology and the National Science Foundation with addressing several issues pertaining to cybersecurity, including: 1) public education and security awareness; 2) interoperability and standards; 3) research

and development investment objectives; and 4) cybersecurity workforce development. The Cybersecurity Enhancement Act of 2010 is currently under consideration in the Senate Committee on Commerce, Science and Transportation.

3.5 Senate Energy Committee Joint Discussion Draft (April 2011)

On April 15, 2011, Senators Bingaman and Murkowski released a joint staff draft of legislation addressing the cyber security of the bulk power system. The draft provided the basis for a Senate Energy Committee hearing in early May. Key provisions:

- The draft would add a new section (#224) to the Federal Power Act.
- It provides definitions of “critical electric infrastructure”⁶; “critical infrastructure information”; “cyber security information”; and “cyber security vulnerability”.
- It would authorize and require FERC to determine whether current reliability standards are adequate to protect critical electric infrastructure from cyber security vulnerabilities.
- If FERC finds that current standards are inadequate, it shall order NERC to propose adequate standards.
- If NERC fails to submit adequate standards, FERC shall issue an interim final rule that provides adequate protection.
- If DOE determines that immediate action is necessary, the Secretary may order, with or without notice, actions that DOE believes will best avert or mitigate the threat. (Under these circumstances, utilities are under the jurisdiction of DOE. Regarding such actions, FERC must establish a mechanism that permits utilities to recover “prudently incurred costs.”)
- The Dept. of Defense must develop a comprehensive plan to protect the reliability of the electric power supply of national defense facilities.

The draft does not appear to address:

- The definition of “adequate protection.” How and on what basis does FERC determine this? Does it consult with NERC and industry? Does it distinguish between vulnerabilities for which industry is responsible and those involving national security?
- How does DOE determine that immediate action is necessary? How does DOE determine the appropriate immediate actions?
- How and on what bases portion of distribution systems are included in “critical electric infrastructure.” On what authority does FERC make these calls?
- Can costs be “prudently incurred” only in response to DOE’s immediate action orders? Or might utilities prudently incur costs in advance of such orders?

May 5, 2011 hearing on Senate Energy Committee Joint Discussion Draft

⁶ “Critical electric infrastructure” includes systems and assets used for the generation, transmission or *distribution* of electric energy affecting interstate commerce whose incapacity or destruction would have a debilitating impact on national security. (Emphasis added.)

The hearing discussed the “joint staff draft” (previously summarized). The presenters were Patricia Hoffman (DOE/OE), Joe McClellan (FERC), Gerry Cauley (NERC), David Owen (EEI), and William Tedeschi (Sandia Natl. Lab).

McClellan noted that FERC authority is now limited to the bulk electric system, and that it depends on the ERO (NERC) to develop standards that it can only approve or remand. FERC commissioned a study by ORNL, which found that a 1921-like Electromagnetic Pulse (EMP) event could knock out 300+ transformers and affect 130 million customers over a 10-year period (due to the long queue for new transformers manufactured outside the US). He wants legal authority to take direct action regarding “imminent threats,” with scope extending to distribution systems, and with costs recovered from ratepayers.

Cauley said that NERC has CIP standards (pending FERC approval), and that NERC’s “ES-ISAC” (Information Sharing and Analysis Center, which communicates with federal intelligence agencies) issues alerts. These alerts (14 since July 2010) go to entities responsible for distribution as well as bulk power. Cyber threats will evolve—a dynamic, adaptive approach is required. Aurora and Stuxnet (as examples) present real risks, but NERC has assessed how to deal with Aurora, and patches and blocks protect against Stuxnet. Congress should refrain from trying to “fix this” once and for all. Therefore, Section 224b of the discussion draft (giving FERC more direct action authority) is not needed. If FERC authority *were* to be expanded, it should be aligned with that of NERC.

The discussion focused on three questions:

- The distinction between an “imminent threat” and a “vulnerability.” For Cauley, it’s difficult to draw a bright line, and it’s more about doing things right than doing them fast. FERC wants authority to compel targeted action (It decides which and who.), bypassing the stakeholder process and extending to distribution systems.
- The role of states, which regulate distribution systems and have responsibility to look at costs. (Cauley would argue, so does industry.) Smart Grid 2-way communications creates vulnerabilities that can propagate beyond distribution systems. Should FERC have authority to reach into distribution systems, bypassing the NERC stakeholder process?
- For Richard Burr (R-NC), we already have cyber authority in too many places. Yes, there is cyber risk, but we don’t have the luxury of doing everything. He probably has a good point, but he has no proposed solution, and any such would extend beyond the scope of the “joint staff draft.”

3.6 Administration Cybersecurity Legislative Proposal

On May 11, 2011, Howard Schmidt (White House Cybersecurity Coordinator) unveiled the Administration’s cybersecurity legislative proposal. Senator Jay Rockefeller observed that the proposal parallels objectives of the “Protecting Cyberspace As a National Asset Act,” which he and Senator Olympia Snowe introduced in 2010. (See Section 3.4 above.) The proposal notes that our critical infrastructure (including the

electricity grid) has suffered repeated cyber intrusions, and that cyber crime has increased dramatically. Key elements include:

- Standardizing “the existing patchwork of 47 state laws,” requiring businesses that have suffered an intrusion to notify owners.
- Application of the RICO (Racketeering Influenced and Corrupt Organizations) Act to cyber crimes.
- Enabling DHS to move more quickly help a private-sector company, state or local government in review/assessment of cyber intrusions.
- Providing immunity when such organizations share cybersecurity information with DHS.
- Requiring such organizations to make reasonable efforts to remove identifying information unrelated to cybersecurity threats when sharing cybersecurity information with DHS.
- Requiring each critical-infrastructure operator to have a third-party commercial auditor⁷ assess its cybersecurity risk mitigation plans.

⁷ Is not NERC-WECC the “auditor” for entities with BPS functions? See CIP standards regarding Sabotage Reporting, Security Management Controls, Personnel and Training; Physical Security; Systems Security Management; Incident Reporting and Response Planning; Recovery Plans. (Section 2.3 above.)