1. Cyber Espionage Trace: Information Warfare Monitor

   Ref Link: http://www.networkworld.com/news/2010/040610-researchers-track-cyber-espionage-ring-to.html

Researchers track cyber-espionage ring to China

Attackers mostly targeted Indian government and military groups, as well as journalists and academics

By Sumner Lemon, IDG News Service
April 06, 2010 03:01 AM ET

Researchers in the U.S. and Canada have tracked and documented a sophisticated cyber-espionage network based in China, dubbed Shadow, that targeted computers in several countries, including systems belonging to the Indian government and military.

The Shadow network of compromised computers was detailed in a report released Tuesday by the Information Warfare Monitor -- a project involving researchers at the University of Toronto's Munk Center for International Studies and The SecDev Group -- and the Shadowserver Foundation. Information Warfare Monitor is the group that uncovered and documented GhostNet, a similar cyber-espionage ring, last year.

The release of the latest report, which details the scope of the Shadow network and discusses some of the Indian government documents that were stolen, was first covered by The New York Times.

"We were able to document another network of compromised government, business, and academic computer systems in India, the Office of the Dalai Lama, and the United Nations as well as numerous other institutions, including the Embassy of Pakistan in the United States," wrote Nart Villeneuve, the SecDev's chief research officer and a research fellow at the Citizen Lab at the University of Toronto's Munk Center for International Studies, in a blog post.

Shadow is the latest example of cyber-espionage efforts linked to China, including attacks on Google's Gmail system that ultimately led the company to close the censored search engine it built for China. Like other such networks, like GhostNet, targeted malware is believed to have allowed the attackers to compromise specific computer systems.

The cyber-espionage ring behind the Shadow network, which was traced to Chengdu, in China's Sichuan province, used social media and blogs to control computers they had compromised using malware.

"In total, we found three Twitter accounts, five Yahoo Mail accounts, 12 Google Groups, eight Blogspot blogs, nine Baidu blogs, one Google Sites and 16 blogs on blog.com that were being used as part of the attacker's infrastructure," the report said, noting that these services were being misused and were not compromised.

These services helped the attackers to circumvent efforts that might otherwise have blocked their access to compromised systems.

"The use of social networking platforms, blogs and other services offered by trusted companies allows the attackers to maintain control of compromised computers even if direct connections to the command and control servers are blocked at the firewall level," it said.

The primary focus of the attackers appears to be the Indian government.

The "vast majority" of the 44 compromised computers identified by the researchers are either in India or belong to Indian government and military organizations, the report said, citing an analysis of stolen documents recovered from the Shadow network.

"Having reported this incident to the China CERT -- which handles security incidents in China -- I look forward to working with them to shut down this malware network," Villeneuve said, referring to China's National Computer Network Emergency Response Technical Team (CNCERT).

mostly targeted Indian government and military groups, as well as journalists and academics

By Sumner Lemon, IDG News Service
April 06, 2010 03:01 AM ET

But CNCERT said in a statement that it had not received any reports of a security incident from the University of Toronto, where some of the researchers behind the Shadow report are based. The reason for the contradictory statements was not immediately clear.

"During our investigation, we recovered documents that are extremely sensitive from a national security perspective as well as documents that contain sensitive information that could be exploited by an adversary for intelligence purposes," the report said.

Several documents recovered were labeled "secret," "restricted" or "confidential" and originated from India's National Security Council Secretariat and Indian embassies abroad.

In addition, the Shadow network targeted Indian academics and journalists with a "keen interest" in China, the report said, citing the recovery of stolen documents discussing Chinese military exports, Chinese policy on Taiwan and Sino-Indian relations, as well as other topics related to China.

The Shadow network also collected personal information on individuals belonging to Indian government and military organizations that could be used in future attacks, it said.

The report concludes that Shadow was controlled from China and attributes responsibility for the network to "one or more individuals with strong connections to the Chinese criminal underground." However, it didn't rule out the possibility of a connection between these individuals and the Chinese government.

"Given the often murky relationships that can exist between this underground and elements of the state, the information collected by the Shadow network may end up in the possession of some entity of the Chinese government," it said.

2. Cyber Espionage Report – Information Warfare Monitor

Reference Link: http://www.sciencedaily.com/releases/2010/04/100406093508.htm

Groundbreaking Cyber Espionage Report Released; Identifies Dalai Lama as Target

ScienceDaily (Apr. 7, 2010) — The Information Warfare Monitor (Citizen Lab, Munk School of Global Affairs, University of Toronto and the SecDev Group, Ottawa) and the Shadowserver Foundation announce the release of "Shadows in the Cloud: An investigation into cyber espionage 2.0."

The report documents a complex ecosystem of cyber espionage that systematically targeted and compromised computer systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries.

Members of the research team held a news conference on April 6, to discuss their latest findings and to answer questions from the media.

The investigation recovered a large quantity of stolen documents -- including sensitive and classified materials -- belonging to government, business, academic, and other computer network systems and other politically sensitive targets. These include documents from agencies of the Indian national security establishment, and the Offices of the Dalai Lama. The stolen data included information voluntarily provided to Indian embassies and consulates by third-party nationals, including Canadian visa applications, as well as those belonging to citizens of other countries. Additionally, sensitive personal, financial, and business information belonging to Indian officials was systematically harvested and exfiltated by the attackers.

The report analyzes the malware ecosystem employed by the Shadows' attackers. The system leveraged multiple redundant cloud computing systems, social networking platforms, and free web hosting services in order to maintain persistent control while operating core servers located in the People's Republic of China (PRC). Although the identity and motivation of the attackers remain unknown, the report provides evidence that the attackers operated or staged their operations from Chengdu, PRC.

Summary of main findings:

Complex cyber espionage network -- Documented evidence of a cyber espionage network that compromised government, business, and academic computer systems in India, the Office of the Dalai Lama, and the United Nations. Numerous other institutions, including the Embassy of Pakistan in the United States, were also compromised. Some of these institutions can be positively identified, while others cannot.

Theft of classified and sensitive documents -- Recovery and analysis of exfiltrated data, including one document that appears to be encrypted diplomatic correspondence, two documents marked "SECRET," six as "RESTRICTED," and five as "CONFIDENTIAL." These documents are identified as belonging to the Indian government. However, we do not have direct evidence that they were stolen from Indian government computers and they may have been compromised as a result of being copied by Indian officials onto personal computers. The recovered documents also include 1,500 letters sent from the Dalai Lama's office between January and November 2009. The profile of documents recovered suggests that the attackers targeted specific systems and profiles of users.

Evidence of Collateral Compromise -- A portion of the recovered data included visa applications submitted to Indian diplomatic missions in Afghanistan. This data was voluntarily provided to the Indian missions by nationals of 13 countries as part of the regular visa application process. In a context like Afghanistan, this finding points to the complex nature of the information security challenge where risks to individuals (or operational security) can occur as a result of a data compromise on secure systems operated by trusted partners.

Command-and-control infrastructure that leverages cloud-based social media services -- Documentation of a complex and tiered command and control infrastructure, designed to maintain persistence. The

infrastructure made use of freely available social media systems that include Twitter, Google Groups, Blogspot, Baidu Blogs, blog.com and Yahoo! Mail. This top layer directed compromised computers to accounts on free web hosting services, and as the free hosting servers were disabled, to a stable core of command and control servers located in the PRC.
Links to Chinese hacking community -- Evidence of links between the Shadow network and two individuals living in Chengdu, PRC to the underground hacking community in the PRC.

About the Researcher Collaboration:

This investigation is a result of a collaboration between the Information Warfare Monitor and the Shadowserver Foundation. The Information Warfare Monitor (infowar-monitor.net) is a joint activity of the Citizen Lab, Munk School of Global Affairs, University of Toronto, and the SecDev Group, an operational consultancy based in Ottawa specialising in evidence-based research in countries and regions under threat of insecurity and violence. The Shadowserver Foundation (shadowserver.org) was established in 2004 and is comprised of volunteer security professionals that investigate and monitor malware, botnets, and malicious attacks. Both the Information Warfare Monitor and the Shadowserver Foundation aim to inform the field of cyber security through accurate, evidence-based assessments and investigations.

3. US Electric Grid Penetrated by spies: Wall Street Journal Report
   Reference Link: http://online.wsj.com/article/SB123914805204099085.html

WASHINGTON -- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war.

"The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."

Many of the intrusions were detected not by the companies in charge of the infrastructure but by U.S. intelligence agencies, officials said. Intelligence officials worry about cyber attackers taking control of electrical facilities, a nuclear power plant or financial networks via the Internet.

Authorities investigating the intrusions have found software tools left behind that could be used to destroy infrastructure components, the senior intelligence official said. He added, "If we go to war with them, they will try to turn them on."

Officials said water, sewage and other infrastructure systems also were at risk.

"Over the past several years, we have seen cyberattacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts," Director of National Intelligence Dennis Blair recently told lawmakers. "A number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure."

Officials cautioned that the motivation of the cyberspies wasn't well understood, and they don't see an immediate danger. China, for example, has little incentive to disrupt the U.S. economy because it relies on American consumers and holds U.S. government debt.

But protecting the electrical grid and other infrastructure is a key part of the Obama administration's cybersecurity review, which is to be completed next week. Under the Bush administration, Congress approved $17 billion in secret funds to protect government networks, according to people familiar with the budget. The Obama administration is weighing whether to expand the program to address vulnerabilities in private computer networks, which would cost billions of dollars more. A senior Pentagon official said Tuesday the Pentagon has spent $100 million in the past six months repairing cyber damage.

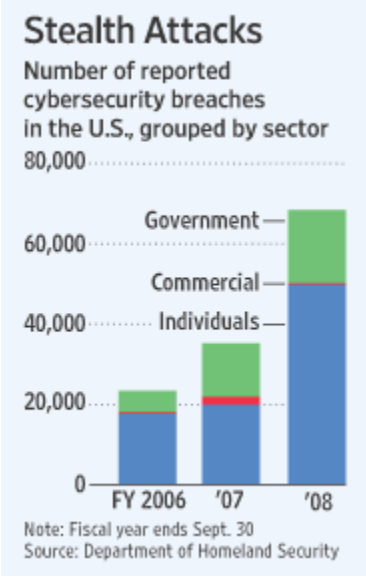
U.S. Intelligence Detects Cyber Spies

WSJ's Intelligence Reporter Siobhan Gorman says that Intelligence officials have found cyber spies lurking in the U.S. electrical infrastructure.

Overseas examples show the potential havoc. In 2000, a disgruntled employee rigged a computerized control system at a water-treatment plant in Australia, releasing more than 200,000 gallons of sewage into parks, rivers and the grounds of a Hyatt hotel.

Last year, a senior Central Intelligence Agency official, Tom Donahue, told a meeting of utility company representatives in New Orleans that a cyberattack had taken out power equipment in multiple regions outside the U.S. The outage was followed with extortion demands, he said.

The U.S. electrical grid comprises three separate electric networks, covering the East, the West and Texas. Each includes many thousands of miles of transmission lines, power plants and substations. The flow of power is controlled by local utilities or regional transmission organizations. The growing reliance of utilities on Internet-based communication has increased the vulnerability of control systems to spies and hackers, according to government reports.



The sophistication of the U.S. intrusions -- which extend beyond electric to other key infrastructure systems -- suggests that China and Russia are mainly responsible, according to intelligence officials and cybersecurity specialists. While terrorist groups could develop the ability to penetrate U.S. infrastructure, they don't appear to have yet mounted attacks, these officials say.

It is nearly impossible to know whether or not an attack is government-sponsored because of the difficulty in tracking true identities in cyberspace. U.S. officials said investigators have followed electronic trails of stolen data to China and Russia.

Russian and Chinese officials have denied any wrongdoing. "These are pure speculations," said Yevgeniy Khorishko, a spokesman at the Russian Embassy. "Russia has nothing to do with the cyberattacks on the U.S. infrastructure, or on any infrastructure in any other country in the world."

A spokesman for the Chinese Embassy in Washington, Wang Baodong, said the Chinese government "resolutely oppose[s] any crime, including hacking, that destroys the Internet or computer network" and has laws barring the practice. China was ready to cooperate with other countries to counter such attacks, he said, and added that "some people overseas with Cold War mentality are indulged in fabricating the sheer lies of the so-called cyberspies in China."

Utilities are reluctant to speak about the dangers. "Much of what we've done, we can't talk about," said Ray Dotter, a spokesman at PJM Interconnection LLC, which coordinates the movement of wholesale electricity in 13 states and the District of Columbia. He said the organization has beefed up its security, in conformance with federal standards.

In January 2008, the Federal Energy Regulatory Commission approved new protection measures that required improvements in the security of computer servers and better plans for handling attacks.

Last week, Senate Democrats introduced a proposal that would require all critical infrastructure companies to meet new cybersecurity standards and grant the president emergency powers over control of the grid systems and other infrastructure.

Specialists at the U.S. Cyber Consequences Unit, a nonprofit research institute, said attack programs search for openings in a network, much as a thief tests locks on doors. Once inside, these programs and their human controllers can acquire the same access and powers as a systems administrator.

4. Cyberwar impacting Smart Grid? - WSJ Report
   Reference Link: http://blogs.wsj.com/digits/2009/04/08/will-a-smart-grid-repel-or-open-doors-to-a-cyber-attack/

Will a Smart Grid Repel or Open Doors to a Cyber Attack?

By WSJ Staff

From Environmental Capital's Keith Johnson:

Is it a good idea to put the U.S. electricity system on the same footing as your spyware-addled computer?

Least of your worries (AP)

As momentum gathers for the creation of an Internet-like "smart grid" that will do for the electricity grid what the Internet did for home shopping, the WSJ reports the cyberspace wars have begun:

Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials.

The spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war. "The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians."

So far the damage is more theoretical than real, the paper notes. But the intrusions underscore the vulnerability of a key component of the nation's infrastructure.

Cybersecurity has been in the spotlight since last year, when the Center for Strategic and International Studies prepared a big report on how the new administration should deal with the threat of cyber attacks, which do "more real damage every day to the economic health and national security of the United States than any other threat." The Senate just introduced a bill largely based on the recommendations in that report that would put responsibility for U.S. cybersecurity increasingly in the hands of the federal government, rather than in the hands of private-sector companies.

The big question is whether the move to a smart grid would increase the country's vulnerability to such attacks, or serve as the best form of defense. The Center for American Progress, in its latest study on the electricity transmission system, said the smart grid was the solution—not the problem—because it would represent the chance to finally upgrade vulnerable old, jury-rigged technology currently cobbled together in the electric grid. Greater regulation and government oversight could also push through costlier but more effective security technologies that might otherwise not pass muster with the market, the report said.

- Maybe so—but that still leaves open the question of how the new smart grid should be designed. Should it have open standards, like the Internet Protocol, understood by everyone from hackers to software developers? Or should the smart grid rely on a closed, closely-held, standard specially-created by companies building smart grid gear?
- The CSIC report found that old Internet protocols are responsible for much of the U.S. weakness in cyberspace—the 1970s really were a more trusting era. But that doesn't rule out open standards, as Earth2Tech has noted: The more developers there are speaking a given language, as it were, the likelier it is that the private sector will respond with a spate of security improvements.
- Either way, much of that task will now fall to the California-based Electric Power Research Institute, which was picked today by the Commerce Department to draw up the "roadmap" of the new smart grid. Its main task will be figuring out just what standards should prevail in that brave new world.

5. Department of Energy's Control Systems Security Program:
   Reference Link: http://www.oe.energy.gov/controlsecurity.htm

Control Systems Security

About the Control Systems Security Program

A key mission of the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) is to enhance the security and reliability of the nation's energy infrastructure. Improving the security of control systems, which enable the automated control of our energy production and distribution, is critical for protecting the energy infrastructure and the integral function that it serves in our lives.

OE designed the Control Systems Security (CSS) program to assist leading utilities and energy companies in actively pursuing security solutions for control systems through integrated planning and a focused research and development effort.

CSS co-funds projects with industry partners to make advances in energy control systems that benefit the security of the government, the industry, and the public.

Critical Importance of Energy Control Systems

An efficient, secure, and reliable energy infrastructure is imperative as the energy sector confronts a convergence of physical and cyber systems.

Energy control systems are the brains that operate and monitor our energy infrastructure. Two examples of such systems are the Supervisory Control and Data Acquisition (SCADA) and the Distributed Control Systems (DCS). Most early SCADA system designs did not anticipate the security threats posed by today's reliance on common software and operating systems, public telecommunication networks, and the Internet. Control systems have become more productive and efficient, but the energy sector is faced with an unprecedented challenge in protecting systems against cyber assault.

Image provided courtesy of Kansas City Power & Light

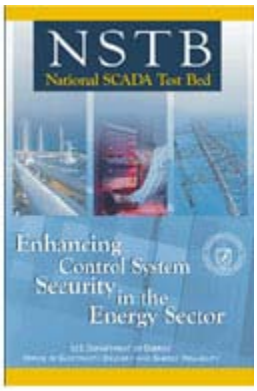
Control Systems Security (CSS) is a unique program under the U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE). Since its inception, the program has formed valuable links between the government, the energy sector, and national laboratories to conduct research and development in the area of cyber security. The aim of the program is to reduce the risk of energy disruptions due to cyber attacks, and so far the program's projects have uncovered a multitude of knowledge that has already increased the security of our energy control systems around the country.

CSS program activities fall under four project areas, guided by a risk-based approach to improving cyber security. They are:

- **Next Generation Control Systems**. Involving research and development that concentrates on accelerating the development and deployment of hardened control systems with built-in security.
- **System Vulnerability Assessments**. Through rigorous tests, exploitable systems vulnerabilities are revealed and through this we can encourage development of system fixes.
- **Integrated Risk Analysis**. Used to develop means for stakeholders to assess their security posture that will hasten the ability to mitigate potential risks.
- **Partnership and Outreach**. Through active partnerships, we can engage all stakeholders and encourage collaborative developments and dissemination of critical security information.

DOE is helping to address the critical security challenges of energy control systems through a focused R&D effort and integrated planning.

R&D: National SCADA Test Bed

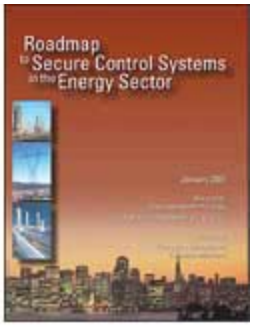


Securing control systems is essential for protecting energy infrastructure. The National Research Council identified "protecting energy distribution services by improving the security of SCADA systems" as one of the 14 most important technical initiatives for making the Nation safer across all critical infrastructures. In addition, the *National Strategy to Secure Cyberspace* (2003) (PDF 980 KB) states that "securing DCS/SCADA is a national priority".

The National SCADA Test Bed provides testing environments to help industry and government identify and correct vulnerabilities in SCADA equipment and control systems within the energy sector.

More about the National SCADA Test Bed >

Planning: Roadmap to Secure Control Systems in the Energy Sector



Asset owners and operators, government agencies, and other stakeholders are pursuing various strategies to improve control systems security. In the absence of a unifying framework, DOE has partnered with the industry to develop a *Roadmap to Secure Control Systems in the Energy Sector* to help focus these diverse efforts.

The Roadmap identifies critical needs and priorities for improving the security, reliability, and functionality of control systems in the energy sector. DOE coordinated this roadmap development with DHS and relied on the energy sector to guide the process and ensure that the priorities reflect the needs of the electric, oil, and gas companies.

In a report to the president, the National Infrastructure Advisory Council (NIAC) recognized the Roadmap's success in developing and implementing cyber security solutions for control systems. The report recommended that all critical infrastructures adopt the Roadma''s goal of securing control systems against loss of critical function from intentional cyber attack by 2015. It also recommended that the Department of Homeland Security and other sector-specific agencies collaborate with their partners to create their own sector-specific roadmaps using the energy sector's Roadmap as a model.

More about the Roadmap to Secure Control Systems in the Energy Sector >

To enhance the Roadmap's effectiveness, CSS created the interactive energy Roadmap (ieRoadmap), an online database where industry can map its R&D efforts for achieving Roadmap goals, evaluate its progress, and discover collaborative opportunities for future projects.

Highlight YOUR organization's activities to implement the Energy Sector Roadmap.

News

January 2011: DOCUMENT
"DNS as a Covert Channel Within Protected Networks" has been released by the National Electric Sector

Cybersecurity Organization (NESCO), an organization supported by OE. View PDF >

January 2011: DOCUMENT FOR COMMENT
DRAFT ROADMAP TO SECURE ENERGY DELIVERY SYSTEMS
The Energy Sector Control Systems Working Group is seeking comments on the draft document that updates the 2006 "Roadmap to Secure Energy Delivery Systems." View PDF >
Comments are due 2/11/2011 and may be submitted here >

NEWS ARCHIVE

Publications Library

DOE National SCADA Test Bed FY 2009 Work Plan (PDF 261KB)

INL Common Vulnerabilities Report (PDF 458 KB)

AMI System Security Requirements (PDF 826 KB)

Roadmap to Secure Control Systems in the Energy Sector (PDF 2.2 MB)

Fact Sheet: DOE National SCADA Test Bed (PDF 155 KB)

PUBLICATIONS LIBRARY

U.S. DEPARTMENT OF
ENERGY
1000 Independence Ave., SW Washington, DC 20585
t / 202-586-5000 f / 202-586-4403

6. **State Engagement with the Energy Sector to Improve Cyber Security : NGA Center for best practices**

State Engagement with the Energy Sector to Improve Cyber Security

Executive Summary

The state-owned computer networks used to deliver state and federal programs, benefits, and services are besieged by a variety of cyber criminals intent on stealing or manipulating the sensitive private information those systems contain. State information technology and homeland security offices are engaged full-time in fighting off those attacks by tracking new threats, protecting Internet portals, and securing databases.

But state officials also have one eye on the security of the networks that run private infrastructure operations: the telecommunications systems, electrical grids, gas and oil pipelines, and transportation networks on which modern society relies. That infrastructure is so interconnected and interdependent that a successful attack on any one component of the infrastructure could have a cascading effect on several others. A reliable supply of energy, for example, is essential to the operation of transportation systems, water and wastewater treatment facilities, hospitals, and 911 dispatch centers. A successful cyber attack on the electrical grid not only could knock out power, but could also debilitate those other essential services. In such an event, state and local governments would be expected to respond in the same way, and with the same efficiency, that they would for any other disaster.

But states cannot easily ensure the security of cyber systems owned and operated by the energy sector, or by any other sector of the economy. The majority of the infrastructure is privately owned, and legislative or other mandates often are strongly resisted. In addition, the cyber threat is so pervasive, and is evolving so rapidly, that the private sector often has the best information about the nature of the threat but does not share that information with government. Finally, a number of private sector-led initiatives and federal programs are already under way to improve cyber security in the energy sector, leaving the states to determine on their own what their appropriate role should be.

This Issue Brief examines those challenges and reviews the approaches that several states have used to work with the energy sector to improve cyber security. Those efforts take into account the programs, policies, standards, and practices already in place that contribute to a reliable energy supply. In general, states are playing an active role in improving the cyber security of the energy sector by:

Facilitating coordination and cooperation among and within state agencies, the energy sector, and other interdependent sectors with which the energy sector directly interacts;

Collaborating with private energy firms to improve their - and the state's - cyber security and overall information sharing; and

Participating in federal and private sector cyber security initiatives to build partnerships and monitor new initiatives.

7. NERC Reponse to Cyber Security Threat: NERC Press Release
   Referene Link: http://www.nerc.com/news_pr.php?npr=101

PRINCETON, N.J., July 14, 2008 — Rick Sergel, president and CEO of the North American Electric Reliability Corporation (NERC), recently announced the organization's plans to improve its response to cyber security and critical infrastructure protection concerns for the bulk power system in North America. Revealed to NERC's board of trustees and stakeholders in a letter last week, the plan outlines six specific actions that will lay the foundation for improving grid reliability by enabling faster and more effective action to protect critical assets from cyber or physical threats.

These actions arise from NERC's recent interaction with various organizations, notably including the House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the House Homeland Security Committee, whose efforts have been instrumental in emphasizing the urgency and priority of this critical issue.

"Cyber security is a critical component of grid reliability, but is, by its nature, fundamentally different from any other reliability concern we currently address through our standards, analysis, or enforcement programs," commented Rick Sergel, president and CEO of NERC. "It therefore requires a different approach; one that allows for more expedient treatment of critical information, urgent action on standards, and more thorough threat analysis and risk assessment."

"As the Electric Reliability Organization in the U.S. and home to the Electric Sector Information Sharing and Analysis Center (ES-ISAC), we are seeking to enhance and focus our existing efforts by putting the organizational structure in place to better support a more comprehensive treatment of these critical issues," he continued. "One of our key initiatives in this area is the recent formation of the Electric Sector Steering Group (ESSG), comprised of five industry chief executives, a NERC board member, and of which I am the Chairman. The group will be instrumental in guiding NERC as we execute the plans announced today."

Commenting on today's announcement, Barry Lawson, Chair of NERC's Critical Infrastructure Protection Committee (CIPC), stated "NERC's ongoing efforts to improve its ability to respond quickly and efficiently to cyber and physical security threats are critically important to reliability of the bulk power system and the CIPC continues to be supportive of their successful execution."

Specific actions, as detailed in last week's letter, include:

Increasing NERC Expertise on Critical Infrastructure Protection and Cyber Security — NERC will formally establish the Critical Infrastructure Protection program as one of NERC's program functions, alongside existing standards development, compliance and enforcement, and reliability assessment program areas. The establishment of this program will include the staffing of a Chief Security Officer position, who will serve as the single point of contact for the industry, the ESSG, and government regulators and stakeholders seeking to communicate with NERC on cyber and infrastructure security matters.

Consider Alternative Standard Setting Process for Cyber Security Standards —NERC will establish a task force to review, and where appropriate recommend, a standard setting process for cyber security that will include an emergency/crisis standards setting process. This process must provide a level of due process and technical review, but also provide the

speed necessary to establish standards quickly and respond seamlessly to government agencies in the U.S. and Canada.

Expedited Review of Existing Cyber Standards —Working through the Standards Committee, NERC also seeks to accelerate the comprehensive review of its eight existing critical infrastructure protection standards to fully incorporate the directives from FERC, including the consideration of the extent to which elements of the National Institute of Standards and Technology (NIST) standards should be incorporated therein or within new standards.

Facilitate Joint Collaboration on Cyber Security — NERC, working with the Federal Energy Regulatory Commission in the U.S. and relevant governmental authorities in Canada, will organize a briefing for the ESSG, the NERC CEO, and senior level utility executives across all stakeholder groups on cyber security threats.

8. SCE Cyber Security Program:
    a. SCE Smart Grid Program –
    Reference Link: www.cpuc.ca.gov/NR/rdonlyres/...A6A3.../**SCE**DistributionWorkshop.pdf
    b. SCE Advanced Metering Infrastructure Program –
    Reference Link:
    http://www.sce.com/NR/rdonlyres/898F9ADC-8F0F-4BF0-A833-75E1EE28CE6A/0/PRESAMITAB82406.ppt.
    c. Emerging Technology Solutions at SCE –
    Reference Link:
    http://ewh.ieee.org/cmte/pes/etcc/GD_Rodriguez_Emerging_Technology_SCE_GM_2010.pdf