Office of Electric Reliability Director Joseph McClelland
Platts Energy Week
April 23, 2011

Platts Chief Editor Chris Newkumet: *We have with us Joe McClelland, director of the Office of Electric Reliability with the Federal Energy Regulatory Commission. Thanks for coming, Joe.*

Joe McClelland: Thank you, Chris.

CN: *Give me a little Cybersecurity for Dummies. We have these facilities – we have the electric grid and transformers, oil and gas pipeline interconnections, LNG tankers and terminals. We think of these enormous facilities as relatively secure, with redundant systems. How could a cyber attack bring these things down?*

JM: Well let's start with the power grid. Over the past couple of decades the power grid has become increasingly dependent on remote operations. These remote operations depend on secure communication facilities, in other words, cyber-secure communication facilities. If an attacker or a criminal decided to interrupt the flow of information or manipulate that information or, worse yet, take control of these facilities they could not only cause outages, but they may actually be able to damage the very equipment that provides the electricity to the consumers.

This is especially important to consider as we move toward even greater levels of automation, for instance Smart Grid. It is therefore essential that cybersecurity stay ahead of deployment for these systems.

CN: *The threat is not limited to hackers, right Joe?*

JM: That's right. Although there are some people that are intent on interrupting or damaging equipment in the power grid, there are also financial incentives for criminals. Folks can, for instance, manipulate data on their user account. They may be able to lower their bills. Or perhaps they'd like to exfiltrate information – important information – about the way a company operates or even about its product line. There are also instances where two companies are in negotiations, perhaps a buyout negotiation, and a company is able to exfiltrate important information about the status of the financial health of the [other] company, thereby compromising those negotiations.

It is also interesting to note that many of these penetrations come from insiders, trusted employees who have access to this type of information or these control systems.

CN: *We've had a lot of testimony recently, a lot of reports from OMB, GAO – there was a bi-partisan commission – and they characterize this threat as severe, and our vulnerability as pretty high. Talk about what companies should be doing now.*

JM: Well the good news is that some of the best practices that one can deploy are already tried and true practices. For instance, user accounts that may be expired, employees that may have been terminated, it is important to quickly stop those user accounts so that disgruntled or former employee or employees that shouldn't have access to sensitive information can't gain that access through normal means.

Software. Every company is dependent upon the functionality of software, and important updates are issued frequently and regularly by their software vendors. Many of those updates address critical vulnerabilities to the security of those platforms. So companies need to be vigilant as far as performing those software patches.

It is also important to access and monitor network traffic. Are there unusual patterns of activity? Are there network activities that are occurring during off hours? Suspicious activities? Are there accounts that are accessing perhaps areas of the company they wouldn't normally access?

All of these things together don't guarantee that you won't be a target of cybersecurity perpetration, but they help to improve the posture and a hacker, perhaps at a less sophisticated level, may look for an easier target.

CN: *Of course the other very important piece of this is the potential for catastrophic damage from high-altitude events – electromagnetic pulse from a nuclear device or severe solar flares. Some pretty scary scenarios there, aren't there Joe?*

JM: Yes, I'd say there are pretty dire scenarios indeed. Electromagnetic pulse effects can originate from a couple of different sources. One might be man-made weapons and the other is solar magnetic disturbances, the routine activity that our sun generates. In either case, the outages from these types of events can be wide ranging and last for a long period of time, have an extreme duration. This could have dire and devastating consequences for our nation.

CN: *I heard you speak the other day and you mentioned four to 10 years to recover?*

JM: Yes. There was a study that the Federal Energy Regulatory Commission, the Department of Homeland Security and the Department of Energy jointly commissioned, or joint sponsored a study. We gave that work to the Oak Ridge National Lab. We asked them to evaluate the effects of either a solar magnetic disturbance or man-made weapons on the power grid. What areas of the power grid are most vulnerable and what pieces of equipment are most likely to fail.

One of the scenarios they evaluated was a 1921 solar event; it's been termed a one-in-100 year event. The results of the study were staggering. It's estimated that over 300 bulk power system transformers could be damaged or destroyed by this event, resulting in a loss of power to 130 million customers for perhaps as long as four to 10 years.

CN: *Joe, we have about 10 seconds. There is a call for some more FERC authority and there is a bill in Congress. We'll keep an eye on that. Thank you so much for coming, Joe McClelland.*

JM: Thank you.