Georgia System Operations Corporation
2100 East Exchange Place
Tucker, GA 30084-5336
phone 770-270-7200
fax 770-270-7872

FERC Annual Reliability Technical Conference June 1, 2016
Commission Offices 888 First Street NE
Washington D.C. 20426

Panel III Grid Security 2:30 p.m.

Comments of Gregory S. Ford (President and Chief Executive Officer - Georgia System Operations Corporation)

I am Gregory S. Ford, the President and Chief Executive Officer of the Georgia System Operations Corporation (GSOC) located in Tucker Georgia, which is near Atlanta. Georgia System Operations is an electric system operations company which is owned by 38 of Georgia's distribution Electric Membership Corporations (EMCs) that provide electricity to most of the rural parts of the state and some of the metro areas surrounding Atlanta. I am also the present Chairman of the Board of SERC which has a Delegation Agreement with NERC to enforce mandatory reliability standards for the Bulk Electric System and I am also a new member of the Electricity Subsector Coordinating Council (ESCC) and a member of the NERC Member Representatives Committee (MRC) representing the cooperative sector.

I appreciate the invitation from the Federal Energy Regulatory Commission to participate in this technical conference and the comments expressed here are mine representing the position of GSOC and those on behalf of the National Rural Electric Cooperative Association (NRECA).

The 38 EMCs also own both Oglethorpe Power Corporation which provides generation resources to them and Georgia Transmission Corporation (GTC) which provides high voltage transmission services to them over an integrated transmission system. The Integrated Transmission System (ITS) is owned by GTC, Georgia Power Company, Municipal Electric Authority of Georgia, and the City of Dalton, Georgia. The ITS participants coordinate transmission service planning and operational issues in Georgia and have the right to use the integrated transmission system. In addition, the EMCs procure additional generation supply resources from independent power providers to meet their load using the ITS via service agreements with GTC.

In its responsibility as the system operation control center for these 38 EMCs, their independent power providers, Oglethorpe Power and Georgia Transmission, GSOC must coordinate in real time with Georgia Power Corporation, Southern Company Services (GSOC's Reliability Coordinator) and independent power providers to assure coordinated electric reliability in the State of Georgia.

GSOC is registered with NERC as a Transmission Operator and has been required to comply with the Critical Infrastructure Protection (CIP) standards since 2007. Like other electric utilities in the United States and globally, GSOC has embraced the concept and responsibility of protecting our cyber assets and computer systems in an effort to assure our EMC customers receive reliable electric service each and every second of the day. We have expended considerable resources, in both manpower and tools in this effort.

With that being said, I would like to address some **Bulk Electric System Security** issues which are the subject of this technical conference:

The Cybersecurity Information Sharing Act of 2015 (CISA 2015) and the Fixing America's Surface Transportation (FAST) Act amendment 61003, both address cybersecurity. I would like to talk about how government, NERC and industry can use these new authorities to address cybersecurity risks and enhance information sharing. Further, I would like to address some of the questions presented at this FERC Technical Conference.

a. The CISA 2015 bill:
- Requires the Director of National Intelligence and the Departments of Homeland Security (DHS), Defense, and Justice to develop procedures to share cybersecurity threat information with private entities.
- Establishes a legal framework that would encourage private industry to voluntarily share cybersecurity information (cyber threat indicators and defensive measures) with the federal government to help bolster efforts to guard against cyber-attacks.
- Establishes the Department of Homeland Security (DHS) as the primary interface with the private sector and the main portal for the sharing of cyber information from industry to the federal government.

b. The 2015 FAST act:
- Adds a new section 215A to the Federal Power Act, which authorizes the Secretary of Energy to order emergency measures if the President finds a grid security emergency. In a grid security emergency, the Secretary of Energy can issue any order he or she deems necessary to protect or restore the reliability of critical electric infrastructure or defense critical electric infrastructure (electricity infrastructure serving designated critical defense facilities).

- Directs the Federal Energy Regulatory Commission (FERC) to provide a mechanism for cost recovery if costs for compliance with an order cannot otherwise be recovered. DOE must issue rules of procedure for exercising the new emergency authority, and must designate critical defense facilities. The law authorizes federal agencies to share classified information with key personnel at utilities subject to emergency orders.
- Creates a new information classification of "Critical Electric Infrastructure Information" ("CEII") and requires DOE to issue regulations that will establish procedures regarding the designation of CEII, prohibiting its disclosure.

Both of these new authorities can provide the electric industry with more real time and detailed threat information which can be used to increase the defensive measures to better ensure the Bulk Electric System (BES) is not adversely impacted by cyber events. Having a single point for submitting and receiving information about events that target the electric sector is critical for preventing and responding to Bulk Electric System emergencies.

Whereas both pieces of legislation lay the foundation for better communication with respect to cyber security incidents, turning this legislation into effective communication formats and channels which can be used by the electric industry still needs to be developed. These initiatives need to be coordinated with existing cyber security forums such as the Electricity Information Sharing and Analysis Center (E-ISAC) developed and hosted by NERC and the Electricity Subsector Coordinating Council (ESCC) which is a partnership between executives in the utility sector and the federal government. Also, other entities should be involved such as the Center for Internet Security (CIS) Security Operations Center in upper New York in which the New York Power Authority has partnered with and in which the Department of Homeland Security believes is a key cyber security resource. Other entities like the North American Transmission Forum (NATF), North American Generator Forum (NAGF) and the electrical trade associations also have a keen interest in cyber security and should be included.

The world of BES security, especially in cyber, happens in seconds, not minutes nor hours, neither days nor weeks. Control Centers, Generation Plants and Transmission Operations must respond immediately when attacks and intrusions are attempted so as to prevent cascading outages and equipment damage. These incidents need to be shared immediately with other utilities, their interconnections, the government, the industry and policing agencies.

With help from federal and state governments in coordinating, hosting and providing information concerning cyber security threats and vulnerabilities, the electric utility industry will be better prepared to protect our critical electric utility infrastructure from both cyber and physical attacks.

What can we learn from recent attacks? Let's talk about the Ukraine.

One of the most important lessons to take from the recent attacks is that our efforts associated with the NERC Standards to this point have been well directed at protecting the Bulk Electric System from cyber-attacks. Mitigation measures are already in place, such as multi-factor authentication, configuration management, Intermediate Systems for remote access, awareness training, and separation of BES Cyber Assets from corporate systems to mitigate attacks such as the one the Ukraine experienced. This event should not be used as justification for major changes in our approach to ensuring the reliability of the BES, when it actually provides compelling evidence that our current approach is providing effective protection of our Bulk Electric System. As an example, a key element of the Ukraine attack was the ability to gain remote access to control systems by stealing passwords. The CIP requirement for the utilization of an Intermediate System with two factor authentication is a highly effective approach to addressing this type of attack.

Following are some examples of how the standards developed under our current regulatory system are relevant to the Ukraine event:

- Cyber security training and awareness, as required by CIP-004, is the best available mitigation against phishing attacks
- Malware detection and protection measures required by CIP-007, mitigates the risk against the residual risks of BlackEnergy malware
- Isolation of networks, as required by CIP-005, protects against a pivot from an attack on a corporate network to one on the operations network
- Advance, latent compromise of devices with corrupt firmware is mitigated by the CIP-010 configuration management and monitoring standards
- Two factor authentication and Intermediate Systems required by CIP-005, mitigates the risk of theft of credentials and other potential misuse of remote access using VPN
- Incident response and recovery planning as required by CIP-008 and CIP-009, mitigates the impact of an incident such as this and enables industry to recover more quickly than Ukraine did
- Interpersonal communication capabilities necessary to maintain reliability as required by COM-001 mitigates the risk of telephone denial-of-service attacks on control centers

Another lesson is to ensure that the utility's operation technology systems are separated from its corporate IT systems using Electronic Security Perimeters, especially those open to the internet.

A third lesson is that interconnected utilities must be able to communicate with each other using the E-ISAC and above referenced government authorities in order to identify and communicate possible attacks so that the affected entities can take immediate action.

What should we do in response?

But to say that we have already responded appropriately to a large extent is not to say that there is nothing that should be changed. We should continue to closely examine this incident to determine whether there are other precautions or actions that should be taken. Identifying and implementing security measures require continuous effort in order to prevent an attacker from successfully exploiting any vulnerabilities. In addition to vulnerability testing, establishing penetration testing protocols where the results can be shared with the regulatory regime and industry in a constructive but non adverse manner might be a good method in preventing a potential problem before it can be exploited by people who desire to damage the BES or an individual Registered Entity's computer systems.

Are there ways to reduce risk by "simplifying" or even non-digitizing the technology used at certain critical points or locations?

The advantage of digitizing the technology has been demonstrated by the speed at which a Transmission Operator can respond to BES situations. Reverting back to old manual operating methods will only delay restoration during outages, but it can be done. It would be better to develop other safeguards at critical locations that require dual authentication to control breakers. But with that said, I do believe that it is critical that we retain the ability to operate our systems in a manual mode as a failsafe against worst case cyber scenarios. This will require not only ensuring that the design of new equipment continues to incorporate provisions for manual operation, but also that we continue to train our staff to operate in this manner.

Further, FERC and NERC are beginning concentrated reviews in the areas of restoration and recovery plans. Guidance and direction in this area with industry input will put the BES in a much better position when addressing cyber incidents.

Are there reasonable ways to further reduce the risk of lengthy outages from hostile actions?

We already prepare to prevent lengthy outages using incident response plans, backup plans and restoration plans. Based on the Ukraine situation, the best method to reduce lengthy outage is by immediately identifying the situation and responding while communicating with the others in the industry. This can only be accomplished with repeated and more intense incident response exercises.

Can new standards or changes to standards help?

If affected entities in the Ukraine had separation from the corporate network and internet from their control system, it is very unlikely that the outage would have happened. This is evidence that no major revisions to our standards are needed today based on the Ukraine situation, however we should look closely at the event, and other evolving information about threats to determine if there are areas where the standards or other

measures can be strengthened or clarified. As attackers become more sophisticated and their methods evolve, then new security measures may be needed.

How effectively does the current standards process address emerging or rapidly evolving reliability issues?

Even before standards can be developed, many entities begin developing mitigation strategies to address recently discovered vulnerability issues. The current standards process is effective in addressing known reliability risks, but there may not be enough understanding and knowledge of emerging or evolving risks to increase the attention and effort needed to mitigate new vulnerabilities. The CIP standards provide the framework that supports the utility's ability to react quickly to emerging or rapidly evolving reliability issues.

Can Reliability Standards be structured to change quickly for newly-identified security risks or new scientific or engineering analyses (e.g., of geomagnetic disturbances)? If so, how?

Reliability Standards should not be viewed as the sole, or even primary, avenue for responding to newly identified threats. The industry is highly motivated to secure assets critical to its core business and can and will respond quickly to industry alerts about new threats.

However, in cases where Reliability Standards are appropriate, NERC and the industry have shown that they are capable of moving quickly. As seen with the Metcalf event, the CIP-014 Physical Security Reliability Standard was quickly developed and approved. The electric sector is always willing to move quickly to prevent any serious risk to the BES, regardless of whether through a reliability standard or other action.

What is the status of research on whether or how electromagnetic pulses might affect the grid?

Industry, including Georgia Transmission, is working closely with the Electric Power Research Institute (EPRI) and the North American Transmission Forum (NATF) on this issue. The EPRI three year research plan began in April of this year. Additional time is needed to characterize the threat, assess the impact on the Bulk Electric System, cost-effectiveness and vet possible solutions to ensure they do not cause other unintended consequences.

What additional research would help address any uncertainties?

Industry and EPRI, in particular, needs access to existing research that the government has already conducted on electromagnetic pulses.

The CIP and PRC standards continue to be among the most-often violated Reliability Standards. What efforts are being made, or should be made, to improve compliance with these particular standards?

The frequency of violations of the CIP and PRC standards are driven by the nature and complexity of those standards. Industry has benefited from the additional clarity regarding performance expectations and measures of compliance evident in more recent versions of the PRC standards. This level of clarity is essential to reducing that risk. With the risk-based focus on compliance, more effective NERC outreach and stakeholder involvement have resulted in new and revised standards that focus on providing enhanced direction and guidance for operation and maintenance of protection systems. With recent changes to data reporting, NERC will have more ready access to information regarding actual causes of misoperations and protection system failures and the reliability risks they create. Effective utilization of the resulting metrics will better inform entities of strategies and actions to mitigate known risks. Risk based compliance also gives entities with lower risk profiles greater ability to allocate resources to effectively focus on internal controls and causal analysis as a means to avoid or mitigate the most serious risks applicable to their specific facts and circumstances.

The reliability standards predominantly codified already-in-place practices, whereas in some cases, the CIP standards have sought to fundamentally change the way companies operate. GSOC welcomes and agree with these changes, but the frequency of violations is going to be lower for the standards that seek to formalize existing practices when compared to those that seek substantial change in current practices.

The CIP standards, prior to version 5, have been based on zero tolerance of activities that take place hundreds or even thousands of times. It is one thing to put in a program that routinely identifies, evaluates, tests, and installs appropriate software patches; but with human error, it is very difficult for people to complete all the complex steps and never miss one of the thousands of patches processed in a month. It is more reasonable to expect some compliance exceptions to this type of standard when comparing to the traditional reliability standards that have been around for years.

The industry is aware that there are competing risks. There are reliability and availability risks to the Bulk Electric System associated with making security changes and there are security risks associated with not making changes. The balance of these risks is critical to prevent outages. Reliability standards and increasing frequency of software exploits have changed that balance of risks significantly. Those changes are unquestionably for the better, but they require a major shift in the processes and procedures that have been in place for years.

Industry entities agree and support the shift in the balance of risks to put more emphasis on security, but it appears in some cases that Industry's valid concerns regarding the installation of insufficiently vetted patches were not given sufficient weight. Industry is painfully aware of these violations and has been working diligently to address them. CIP version 5 and version 6 Standards provide the details needed for entities to better understand how to comply with each requirement. With the format of the new standards, entities will know which BES Cyber Assets apply, the actual requirement, and examples of the evidence needed to prove compliance. In addition, the Guidelines and Technical Basis of the Standards provide valuable information and diagrams.