To whom it may concern – NIST Developing a Framework to Improve Critical Infrastructure Cybersecurity,

Protecting critical infrastructure from cyber threats requires a dynamic and agile response. No static standard will protect critical infrastructure from the creative and evolving threats faced today. For this reason, adoption of measurable requirements that can be adjusted and incorporated into business improvement processes is needed. The 20 Critical Secure Controls is one mechanism to defend against this dynamic threat. Asset owners can develop and select which controls and to what level to match the threat posture currently. Control levels can be reduced or increased as exposure decreases or new vulnerabilities and exploits are made public. The 20 Critical Cyber Controls have been used successfully in Information Technology environments. Some entities have used the 20 Critical Cyber Controls for electric utilities.

Below are the most common vulnerabilities discovered from the 10 years of vulnerability assessments done by the Department of Energy Office of Electricity Delivery and Energy Reliability. These vulnerabilities are analyzed the common vulnerability reports produced the by National SCADA Test Bed at the Idaho National Laboratory (INL) ("Vulnerability Analysis of Energy Delivery Control Systems", July 2011). This report scored the vulnerabilities discovered based on the Common Vulnerability Scoring System (CVSS) version 2 that includes temporal and environmental factors.

Rank	**Vulnerability**	**SCADA Impact**
1	Unpatched Published Vulnerabilities	Most Likely Access Vector
2	Web Human-machine Interface (HMI) Vulnerabilities	Supervisory Control Access
3	Use of Vulnerable Remote Display Protocols	Supervisory Control Access
4	Improper Access Control (Authorization)	Access to SCADA Functionality
5	Improper Authentication	Access to SCADA Applications

6	Buffer Overflows in SCADA Services	SCADA Host Access
7	SCADA Data and Command Message Manipulation and Injection	Supervisory Control Access
8	SQL Injection	Data Historian Access
9	Use of Standard IT Protocols with Clear-text Authentication	SCADA Credentials Gathering
10	Unprotected Transport of SCADA Application Credentials	SCADA Credentials Gathering

Table 1 – Top 10 SCADA Vulnerabilities

Below is the analysis of the most common vulnerabilities in SCADA mapped against the 20 Critical Security Controls. The control priorities change - due to feasibility to incorporate and other factors. Penetration testing to discover the most likely attack vector has a higher priority in these control environments than applying anti-virus (malware defenses) since some of those applications many not fit in legacy systems. Securing configurations for software and equipment and continuous vulnerability assessment is problematic for control systems hence the lower ranking. Controlled access, boundary defenses and limiting services is feasible and ranks higher than the traditional IT application of the 20 critical controls. Skill set is rating high for the need for response.

	20 Critical Security Control	**Attack Mitigation Ranking**	**INL Control System Ranking**	**Challenges**	**Related Common Control System Vulnerabilities**
1	Inventory of Authorized and Unauthorized Devices	Very High	High	Feasibility – shared equipment at geographically disperse locations	4- Improper Access Control
2	Inventory of Authorized and Unauthorized Software	Very High	High	Feasibility – most providers do not know the full integration affects of settings for security configuration	1-Unpatched Published Vulnerabilities
3	Secure Configuration for SW, SW on Laptops, WS and Servers	Very High	Medium or Low	Feasibility – most providers do not know the full integration affects of settings for security configuration and the added complexity of embedded devices	2-Web HMI Vulnerabilities 4- Improper Access Control 5- Improper Authentication 8- SQL Inject
4	Continuous Vulnerability Assessment and Remediation	Very High	Medium or Low	Feasibility of patching on a 24/7 application	1-Unpatched Published Vulnerabilities
5	Malware Defenses	High Medium		Feasibility Embedded Systems – Guidance from NIST and NERC CIP	N/A

	20 Critical Security Control	**Attack Mitigation Ranking**	**INL ICS Ranking**	**Challenges**	**Related Common Control System Vulnerabilities**
6	Application Software Security	High		Legacy and new applications mixed in most infrastructures	All
7	Wireless Device Control	High		Ubiquitous in distribution energy – exists in many different configurations for one installation	4-Improper Access Control/Authorization 5- Improper Authentication 7- SCADA Data Command Message Manipulation and Injection 9-Use of Standard IT Protocols with Clear-text Authentication 10-Unprotected Transport of SCADA Application Credentials
8	Data Recovery Capability	Medium	Medium High	Forensics to support incident response needed. Infrastructure configuration data leaks primary concern . Open source analysis and egress filtering used.	N/A
9	Security Skills Assessment and Appropriate Training to Fill Gaps	Medium	Very High	Tailored nature of installations requires specialized skill sets	N/A
10	Secure Configurations for Network Devices such as FW, Routers and Switches	High Medium		Whitelist used often due to static nature of most networks	1-Unpatched Published Vulnerabilities 3-Use of Vulnerable Remote Display Protocols 4-Improper Access Control/Authorization 5-Improper Authentication 7-SCADA Data and Command Message Manipulation and Injection 9-Use of Standard IT Protocols with Clear-text Authentication 10-Unprotected Transport of SCADA Applications Credentials

	20 Critical Security Control	Attack Mitigation Ranking	INL Control System Ranking	Challenges	Related Common Control System Vulnerabilities
11	Limitation and Control of Network Ports, Protocols and Services	High Medium	Very High	Static nature of inner control system configurations allows for more limitations on services ports and protocols	No longer an assessment focus
12	Controlled Use of Administrative Privileges	High Medium		Feasibility – few control systems applications are maintained with roles and privileges down to control functions	4-Improper Access Control/Authorization 5-Improper Authentication
13	Boundary Defense	High Medium	Very High	Isolation of control system configurations from external and reliance on highly distributed devices required Boundary Defenses	3-Use of Vulnerable Remote Display Protocols 4-Improper Access Control/Authorization 5-Improper Authentication 7-SCADA Data and Command Message Manipulation and Injection 9-Use of Standard IT Protocols with Clear-text Authentication 10-Unprotected Transport of SCADA Application Credentials
14	Maintenance, Monitoring and Analysis of Security Audit Logs	Medium		Feasibility of coordinating logs	N/A
15	Controlled Access Based on the Need to Know	Medium	High	Feasibility – few control systems applications are maintained with roles and privileges – legacy systems not built for	4-Improper Access Control/Authorization 5-Improper Authentication 7-SCADA Data and Command Message Manipulation and Injection

				RBAC. Authentication on communication is top weakness	
	20 Critical Security Control	**Attack Mitigation Ranking**	**INL Control System Ranking**	**Challenges**	**Related Common Control System Vulnerabilities**
16	Account Monitoring and Control	Medium		Feasibility with limited RBAC	N/A
17	Data Loss Prevention	Medium Low	High	Transient nature of control signals changes focus to set point configurations and other configuration specific data for loss prevention – exception process intellectual property. Egress filtering used. Historian databases used.	9-Use of Standard IT Protocols with Clear-text Authentication 10-Unprotected Transport of SCADA Application Credentials
18	Incident Response Capability	Medium	Very High	Reliability and availability of critical infrastructure may demand up time in the 5 9’s Where’s Forensics?	N/A
19	Secure Network Engineering	Low	Very High	Lack of physical control of most end device requires robust network designs and barriers	3-Use of Vulnerable Remote Display Protocols 4-Improper Access Control/Authorization 5-Improper Authentication 7-SCADA Data and Command Message Manipulation and Injection 9-Use of Standard IT Protocols with Clear-text Authentication

					10-Unprotected Transport of SCADA Application Credentials
20	Penetration Tests and Red Team Exercises	Low	High	Penetration tests and red team exercises are useful tools to identify the weakest parts of configurations	All

Further analysis of the 20 Critical Security Controls deals with the most sensitive critical infrastructures for nuclear generation facilities.

For control system architectures, where maintenance of components that are 20 years old is common, some of these controls are more difficult to implement. Preliminary analysis applying these cyber security defensive controls to industrial control systems has been done with a change in the ranking of the controls based on feasibility (lack of quick patching) and priority to known security defenses in a mainly static and deterministic environment.

The bottom three priorities in the 20 critical security controls become the top.

1) Secure Network Engineering – due to the lack of ability to patch in an operational environment, understanding and maintain the network security is paramount.
2) Incident Response Capability – Safety and operations in a nuclear facility dictate all activity, incident response during a cyber event cannot be managed by an outside entity.
3) Penetration Tests and Red Team Exercises – until the configurations are so agile to allow continuous patching in an operational environment, periodic penetration test are needed to validate the most likely attack path. These attack paths or opportunities for an adversary to gain access change as the tactics, techniques and procedures (TTP) evolve.
4) Secure Skills Assessment and Appropriate Training to Fill Gap – Creativity and agile response are needed to respond to cyber attacks – investment in skills development is critical.
5) Limitation and Control of Network Ports, Protocols and Services – to reduce the attack surface.
6) Boundary Defenses – Needed in conjunction with the secure network design and limitation on ports and services.
7) Secure Configurations for Network Devices such as Firewalls, Routers and Switches – again needed in conjunction to secure network design, limitations on ports and boundary defenses.

8) Inventory of Authorized and Unauthorized Devices – Nuclear industry does this well as configuration management, and still has importance to be in the top 10 controls.

9) Inventory of Authorized and Unauthorized Software – same as devices above.

10) Applications Software Security – Requesting applications from provides that understand secure coding practices and procedures are proactive in the mainly reactive response mode of cyber security.

11) Data Loss Prevention – in all critical infrastructures, the implementation and configuration specifics are the data needed for a targeted cyber attack. Egress filtering techniques can be applied to identify if data are lost. Operational security (OPSEC) of information that is release in public formats also needs to be controlled (i.e. conferences and job postings)

The other Critical Security Controls fall into priorities as listed, Malware Defenses, Wireless Devices Control Data Recovery Capability, Controlled Use of Administrative Privileges, Maintenance, Monitoring and Analysis of Security Audit Logs, Controlled Access Based on the Need to Known and Account Monitoring and Control.