CYBER SECURITY PROJECT PLAN

1. Background

High-Integrity, real-time computer systems, such as the safety-related digital instrumentation and control systems found at nuclear power plants, must be secure against physical and electronic threats. Computer systems are secure from such threats if the consequences of unauthorized and inappropriate access to and use of those systems are limited to assure that safety is not significantly impaired. Cyber assessments of hardware should include physical access control, modems, connectivity to external networks, data links, open ports, maintenance access, etc. Security of computer system software relates to the ability to protect against unauthorized, undesirable, and unsafe intrusions throughout the life cycle of the safety system. The security of computer systems is established by (1) designing into the systems the security features that will meet the licensee's security requirements, (2) developing the systems without undocumented codes (e.g., back doors), which includes adequate protection against the injection of malicious code at any time during the system life cycle (e.g., viruses, worms, Trojan horses, and bomb codes), and (3) installing and maintaining those systems in accordance with the station administrative procedures and the licensee's security program. Additionally, the design of the plant data communication systems that interface to the safety-related systems at nuclear power plants should ensure that the communications pathways do not present an electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators.

In January 2006, the NRC revised Regulatory Guide 1.152 to endorse the updated IEEE Std. 7-4.3.2-2003. Because IEEE Std. 7-4.3.2-2003 does not provide adequate guidance regarding security of computer-based safety system equipment and software systems, the NRC included Regulatory Positions 2.1 – 2.9 to provide specific guidance concerning computer safety system (cyber) security. These regulatory positions address cyber security of safety-related computer systems at the various stages of the system life cycle. More recently the NRC issued a proposed rule change to 10 CFR 73.55 that includes provisions for cyber security of critical digital systems at power reactors, such as safety systems, security systems, and emergency preparedness systems. This rule is anticipated to be final in late 2007.

Currently NUREG-0800, the Standard Review Plan (SRP) is being revised by the staff. Proposed revisions include adding guidance in Appendix7.1D on the application of the criteria of IEEE Std. 7-4.3.2-2003 as endorsed by Regulatory Guide 1.152, Revision 2. Section 10 of Appendix 7.1-D provides additional guidance on applying Cyber Security requirements of IEEE Std. 603-1991 on access control and the security guidance of Regulatory Position 2 of RG 1.152, Revision 2.

2. Scope

The following cyber security requirements will be addressed by the TWG:

1. Cyber security assessment of computer hardware, including physical access control, modems, connectivity to external networks, data links, open ports, maintenance access, etc.

ENCLOSURE 2

2. Security of computer system software relates to the ability to protect against unauthorized, undesirable, and unsafe intrusions throughout the life cycle of the safety system.
3. Protection of critical systems and digital assets to thwart cyber security attacks.
4. Installation and maintenance of those systems in accordance with each nuclear station's administrative procedures and the licensee's security program.
5. Prevention of communication pathways within the plant data communication systems that will permit unauthorized changes to plant safety systems or display erroneous plant status information to the operators.

The following are explicitly excluded from the scope of this task:

1. Evaluation of specific cyber security technologies, such as firewalls and IDS.

This task working group will be focusing its efforts in addressing inconsistencies within existing NRC and industry cyber security requirements. Specifically, the working group will be evaluating the differences between Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, revision 2, and NEI 04-04 "Cyber Security Programs for Power Reactors." The resulting deliverable will be used to modify these guidance documents to build a coherent set of requirements. In addition, this task working group will evaluate existing regulations, proposed rule 10CFR73.55, and standard review plan to address any conflicts, and to determine if the NRC needs to develop additional rules and guidance documents.

3. PROBLEM STATEMENT

In December 2005 the NRC Office of Nuclear Security and Incident Response (NSIR) endorsed Nuclear Energy Institute (NEI) guidance document NEI 04-04, "Cyber Security Programs for Power Reactors," Revision 1, dated November 18, 2005, as an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. In January 2006, the NRC published Revision 2 to Regulatory Guide 1.152 (RG1.152R2) as "acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and cyber security for the use of digital computers in safety systems of nuclear power plants."

In October 2006, NRC, NEI, and industry representatives met and discussed, among other things, how to resolve differences between the various regulatory guidance documents pertaining to cyber security of power reactors. The following problem statements were developed based on the October meeting and subsequent input from NEI for consideration by the Cyber Security Task Working Group (TWG):

a) The cyber security requirements in Regulatory Guide 1.152 and NEI 04-04 are not consistent and can provide conflicting guidance for implementing cyber security plans.

Deliverables:

1. Complete gap analysis of Regulatory Guide 1.152 and NEI 04-04

2. Facilitate revision of either Regulatory Guide 1.152 or NEI 04-04 to reconcile any differences between the two documents.

b) Existing cyber security requirements and guidance documents may lack coherence. Various regulatory guidance documents, such as Revision 2 to Regulatory Guide 1.152, Chapter 7 of the Standard Review Plan (e.g., SRP Appendix 7.1-D, and NEI 04-04) may need revision to provide consistent cyber security guidance.

Deliverables:

1. Establish/develop clear guidance for assuring effective implementation of current cyber security requirements at power reactors as well as acceptable cyber security practices in the design of digital safety systems.
2. Analysis of existing and proposed cyber security regulations and requirements to develop recommendations to ensure a consistent and coherent regulatory framework for cyber security of power reactors.
3. Publish document(s) describing the regulatory guidance needed to implement the criteria developed in previous two deliverables
4. Prepare one or more Regulatory Information Summaries (RIS) (or other vehicle as designated by the Digital I&C Steering Committee) to disseminate and facilitate the implementation of the TWG recommendations.

8. Milestones, Assignments, and Deliverables

Milestones and Deliverables	deliverable	Due Date	**F**cast/**A**ctual
Initial TWG meeting		Feb 21	A
Develop draft Cyber Security Project Plan		Mar	F
TWG meeting/teleconference to review/finalize draft Cyber Security Project Plan		Mar	F
DI&C-SC endorsement of Cyber Security Project Plan		Mar	F
Describe existing regulatory requirements and regulatory guidance, perform gap analysis of RG1.152R2 and NEI 04-04		Apr	F
Provide recommendations on addressing gaps		May	F
Identify consensus standards and other relevant cyber security recommended best practices		May	F
Develop one or more RIS to document the regulatory and design guidance developed by the Cyber Security TWG.		June	F
Revise guidance appropriately			
RG1.152R2		July	F

NEI 04-04		July	F
Update SRP(s) with guidance		Sep	F
Complete rulemaking on 10 CFR 73.55			F
Develop nuclear industry consensus standard that addresses acceptable cyber security practices for power reactors.			F
Update SRP(s) with guidance			F
Issue regulatory guidance related to final rule 10 CFR 73.55(m), including possible endorsement of industry standard(s)			F