PROJECT PLAN - TWG #1
CYBER SECURITY

1. BACKGROUND:

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 (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," 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 primary objective of this effort will be to provide a coherent set of guidance for future Combined License Applications, or existing licensees who may be developing plant-specific Digital Instrumentation and Control (DI&C) system upgrades. Specific problem statements (see Section 3) were developed based on the October meeting and subsequent input from industry for consideration by the Cyber Security Task Working Group (TWG).

2. SCOPE:

This TWG will be focusing its efforts in addressing inconsistencies within existing NRC and industry cyber security guidance documents. Specifically, the working group will be evaluating the differences between Regulatory Guide 1.152, and NEI 04-04. Chapter 7 of the SRP (e.g., SRP Appendix 7.1-D) will be reviewed at a later date to assure consistent cyber security guidance. The resulting deliverable will be used to modify these documents to build a coherent set of guidance. These documents will potentially be consolidated to provide consistent guidance based on existing requirements.

The development of guidance documents in support of the final cyber security rule, 10CFR73.55(m), is beyond the scope of this working group. The evaluation of specific cyber security technologies, such as firewalls and IDS, is also not within the scope of this task.

3. PROBLEM STATEMENT:

Regulatory Positions 2.1 - 2.9 of RG 1.152 and NEI 04-04 provide conflicting guidance for implementing cyber security requirements for safety systems at nuclear power plants.

4. DELIVERABLES:

Develop one or more interim guides to document the regulatory and design guidance developed by the Cyber Security TWG relative to cyber security for digital systems used at nuclear power plants and fuel facilities.

5. Milestones, Assignments, and Deliverables:

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due date**	**Fsct/Actual**	**Lead**	**Support**
Complete gap analysis of RG1.152R2 and NEI 04-04	✓		F	NRC	NEI
CRGR interaction (as needed)			F	NRC	n/a
Issue draft interim guidance for public comment	✓		F	NRC	NEI
Receive public comments			F	NRC	n/a
CRGR interaction (as needed)			F	NRC	n/a
ACRS interaction (as needed)			F	NRC	n/a
Issue final interim guidance if appropriate	✓		F	NRC	n/a
LONG-TERM					
Revise RG 1.152 and SRP	✓		F	NRC	n/a
Complete Rulemaking on 10CFR73.55(m)			F	NRC	n/a
Develop consensus standard that addresses acceptable cyber security practices			F	NEI	n/a
Issue regulatory guidance related to final rule 10CFR73.55(m), including endorsement of industry standard(s)	✓		F	NRC	n/a