ENCLOSURE 4

Westinghouse Non-Proprietary

WCAP-16791-NP, Rev. 0

"AP1000 Cyber Security Implementation"

May 2007

Public Version

Redacted version of Enclosure 1 with sensitive unclassified non-safeguards information related to the physical protection of an AP1000 Nuclear Plant withheld from public disclosure pursuant to 10 CFR 2.390(d)

AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____ APY: _____

RFS#: _____ RFS ITEM #: _____

AP1000 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
APP-GW-GLR-104	0	Page 1 of 30	W-MCGINNIS

ALTERNATE DOCUMENT NUMBER: WCAP-16791-NP WORK BREAKDOWN #:

ORIGINATING ORGANIZATION: Westinghouse Electric Co., LLC

TITLE: **AP1000 CYBER SECURITY IMPLEMENTATION**

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
APP-GW-GLR-104	PDF	See EDMS

(C) WESTINGHOUSE ELECTRIC COMPANY LLC – 2007

☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

Class 3 Documents being transmitted to the NRC require the following two review signatures in lieu of a Form 36.

LEGAL REVIEW	SIGNATURE/DATE
PATENT REVIEW	SIGNATURE/DATE

☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

ORIGINATOR	SIGNATURE/DATE	
M. A. Gasparovic	** Electronically Approved	
REVIEWERS	SIGNATURE/DATE	
L. L. Santoline	** Electronically Approved	
VERIFIER	SIGNATURE/DATE	VERIFICATION METHOD
A. W. Crew	** Electronically Approved	
AP1000 RESPONSIBLE MANAGER	SIGNATURE*	APPROVAL DATE
C. A. McGinnis	** Electronically Approved	

* Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

** Electronically approved records are authenticated in the electronic document management system.

Westinghouse Non-Proprietary Class 3

WCAP-16791-NP
APP-GW-GLR-104
Revision 0

May 2007

AP1000 Cyber Security Implementation

Westinghouse

WCAP-16791-NP
APP-GW-GLR-104
Revision 0

May 2007

AP1000 Cyber Security Implementation

WESTINGHOUSE NON-PROPRIETARY CLASS 3

WCAP-16791-NP
APP-GW-GLR-104
Revision 0

AP1000 Cyber Security Implementation

Michael A. Gasparovic*, I&C Lead / Cyber Security Coordinator
AP1000 Projects, NPP

May 2007

Verifier: Linda L. Santoline*, Technical Advisor, I&C Systems
Repair, Replacement and Automation Services

Reviewer: Albert W. Crew*, Consulting Engineer, I&C Development
Repair, Replacement and Automation Services

Approved: Cynthia A. McGinnis*, Manager, Nuclear Systems
New Plants Engineering

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2007 Westinghouse Electric Company LLC
All Rights Reserved

TABLE OF CONTENTS

LIST OF TABLES

None

LIST OF FIGURES

REFERENCES

1. 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage

2. 10 CFR 73.56, Personnel access authorization requirements for nuclear power plants

3. IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", Institute of Electrical and Electronics Engineers, Inc., 1991

4. IEEE Standard 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations", Institute of Electrical and Electronics Engineers, Inc., 2003

5. NEI 04-04, "Cyber Security Program for Power Reactors", Nuclear Energy Institute, Revision 1, November 18, 2005

6. NUREG-0696, "Functional Criteria for Emergency Response Facilities"

7. NUREG-0737, "Clarification of TMI Action Plan Requirements"

8. WNA-DS-01150-GEN, Rev. 0 (Proprietary) "Standard General Requirements for Cyber Security", Westinghouse Electric Company, LLC

9. WNA-PD-00029-GEN, Rev. 0 (Proprietary) "RRAS I&C Cyber Security Strategy and Plan", Westinghouse Electric Company, LLC

SRI

DEFINITIONS

Demilitarized Zone: In computer security, a demilitarized zone (DMZ) or perimeter network is a network area (a sub-network) that sits between an organization's internal network and an external network. The point of a DMZ is that connections from the internal and the external network to the DMZ are permitted, whereas connections from the DMZ are only permitted to the external network — hosts in the DMZ may not connect to the internal network. This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. For someone on the external network who wants to illegally connect to the internal network, the DMZ is a dead end.

Intrusion Detection System: An intrusion detection system is used to detect many types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

Intrusion Prevention System: An intrusion prevention system is a computer security device that exercises access control to protect computers from exploitation. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS) technology but it is actually another form of access control, like an application layer firewall. The latest Next Generation Firewalls leverage their existing deep packet inspection engine by sharing this functionality with an Intrusion-prevention system. Intrusion prevention systems (IPS) were invented to resolve ambiguities in passive network monitoring by placing detection systems in-line. IPS make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done.

DEFINITIONS (Continued)

Private Branch eXchange (PBX): A Private Branch eXchange (PBX) is a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public.

SRI

[ ]

ABBREVIATIONS

AA	Access Authorization
ARP	Address Resolution Protocol
CDA	Critical Digital Asset
CWG	Cut-Wire Gateway
DAS	Diverse Actuation System
DDS	Data Display and Processing System
DMZ	De-militarized Zone
ER	Emergency Response
ERDS	Emergency Response Data System
EOF	Emergency Operations Facility
FW	Firewall
HMI	Human Machine Interface
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input / Output
I&C	Instrumentation and Control
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
LAN	Local Area Network
NEI	Nuclear Energy Institute
NUREG	US Nuclear Regulatory Commission Regulation
OSC	Operational Support Center
PBX	Private Branch Exchange
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
POTS	Plain Old Telephone Service
SQA	Software Quality Assurance
TSC	Technical Support Center
USB	Universal Serial Bus
V&V	Verification and Validation
VPN	Virtual Private Network
WAN	Wide Area Network

1 INTRODUCTION

SRI a,c

The general structure of this technical report will be as follows:

- Section 2 will provide a brief overview of the documents that guide cyber security for US Nuclear Power Reactors and shall be used for AP1000.
- Section 3 will address the NEI 04-04 requirements including the defensive strategy for AP1000.
- Section 4 will provide a summary / conclusion.

Submittal of this information allows for early NRC review of the cyber security strategy for AP1000 and its' compliance with applicable regulatory guidance and criteria prior to completion of the detailed design.

2 OVERVIEW OF REGULATORY GUIDANCE

For the purpose of establishing a cyber security strategy for AP1000, a joint decision was made by Westinghouse and NuStart to use the following documents / guides as the basis for this technical report:

- NEI 04-04, "Cyber Security Program for Power Reactors"
- 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage
- 10 CFR 73.56, Personnel access authorization requirements for nuclear power plants

2.1 NEI 04-04

SRI

[ ]

2.2 10 CFR 73.55 AND 10 CFR 73.56

10 CFR 73.55 and 10 CFR 73.56 address requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage, and personnel access authorization requirements for nuclear power plants. Design Basis Threat, as it applies to cyber security, was taken into consideration.

3 IMPLEMENTATION

SRI

3.1 DEFENSIVE STRATEGY FOR AP1000

SRI

SRI **3.1.1 AP1000 Cyber Security Defensive Model** a,c

SRI a,c

[ ]

SRI **3.1.2 Level 4** a,c

[ ]

SRI **3.1.2.1 Cyber Security Requirements Level 4** a,c

[ ]

SRI a,c

[ ]

SRI

3.1.2.2 Cyber Security Risk Mitigation Strategy for Level 4

a,c

[ ]

SRI a,c

[ ]

SRI **3.1.2.3 Cyber Security Interface Requirements from Level 4** a,c

[ ]

SRI **3.1.3 Level 3 Root** a,c

[ ]

SRI **3.1.3.1 Cyber Security Requirements Level 3** a,c

[ ]

SRI a,c

[ ]

3.1.3.2 Cyber Security Risk Mitigation Strategy for Level 3

SRI a,c

[ ]

SRI a,c

[ ]

SRI

3.1.3.3 Cyber Security Interface Requirements To / From Level 3

a,c

[ ]

SRI a,c

[ ]

SRI

3.1.4 Level 1 and Level 2

a,c

[ ]

3.1.5 Protection of Level 4 Digital Assets

SRI a,c

[ ]

SRI **3.1.6 Protection of Level 3 Digital Assets** a,c

[ ]

SRI **3.1.7 Password Policy** a,c

[ ]

3.2 TRAINING

In accordance with Section 6.5 of NEI 04-04, Westinghouse will develop a training program for personnel designing and supporting systems and components contained in Level 4 and Level 3. That program will include the following:

3.2.1 Technical Training

Training shall be provided for designers and technicians who have direct roles in the design and implementation of Level 4 and Level 3 AP1000 systems. This training will include technical cyber security fundamentals, assessment methodologies, testing methodologies including vulnerability and penetration, configuration management, and software quality assurance.

3.2.2 Awareness Program and Training

Training shall be provided to AP1000 project personnel to establish an adequate awareness to the AP1000 cyber security requirements and protection of assets during the design and implementation phases.

3.3 PROCEDURES

Westinghouse has developed two procedures that provide details for the implementation of requirements for general cyber awareness. These generic procedures outline how Westinghouse is designing, developing and documenting instrumentation and control systems that comply with both the general power plant industry standards and the specific nuclear plant standards for cyber security, as well as identifying the generic requirements necessary to address cyber security issues for computer-based safety and non-safety systems.

- WNA-PD-00029-GEN, RRAS I&C Cyber Security Strategy and Plan
- WNA-DS-01150-GEN, Standard General Requirements for Cyber Security

Westinghouse will perform a review of its software quality assurance program and make necessary updates to take into consideration cyber security.

Westinghouse design/control procedures will be reviewed for cyber security impact, and changes will be made as required to address cyber security requirements and the performance of tests to validate them.

Procedures will be developed to address 10 CFR 73.55 requirements for non-safety related systems (ER response).

Formal assessments during design reviews will be performed to meet requirements of this technical report and Section B.2 of NEI 04-04.

Items procured that are significant to cyber security will be in accordance with this technical report and the Westinghouse SQA program.

3.4 INCIDENT HANDLING AND RESPONSE

SRI a,c

[ ]

4 SUMMARY

In Summary, this technical report outlines the NEI 04-04 based defensive strategy for implementing cyber security on the AP1000. This technical report identifies the requirements for each level of cyber security, how separation between levels of cyber security will be incorporated to support functional requirements of AP1000, and the approach taken to mitigate risk for each level of cyber security.

Additionally, this technical report identifies how Westinghouse will address software quality assurance integration requirements, incident handling and response, and procedure implementation requirements.

A complete Cyber Security Program in accordance with NEI 04-04 shall be in place prior to first fuel load.

SRI a.c

Figure 2 – Four-Level Network Overview

SRI a,c

Figure 3 – Three-Level Network Overview