ENTERPRISE ENERGY DATA REPORTING SYSTEM SECURITY FUNCTIONAL ARCHITECTURE

1.0 Introduction

This Security Functional Architecture provides details on the security design concepts to be implemented as part of the Enterprise Energy Data Reporting System (EEDRS) TYPE accreditation. The security design addresses the perimeter, enclave, network, and application security.

The EEDRS is integrated and connects to the Department of Defense (DOD) Global Information Grid (GIG). The EEDRS network interfaces or connects to control system networks on the installation. Access control lists (ACL's) applied to the Installation Campus Area Network (ICAN) routers are used to isolate the EEDRS from the rest of the installation; this isolation inherently provides further security to the EEDRS.

This document is aimed at conveying the concepts for identifying mitigating controls to aid in securing and protecting the EEDRS computing environment and achieving the objectives as identified in the Department of Defense Instruction, Information Assurance (IA) Implementation 8500.2 for a Mission Assurance Capability (MAC) II Sensitive system. Throughout the document there are **BOLD** acronyms (e.g., **PECS-1**) that refer to the Department of Defense Directive 8500.2, Information Assurance (IA) controls. These references make it easier to locate IA controls used for tracking compliance.

1.1 Purpose

This document will provide the security design concepts used to protect the EEDRS.

1.2 Authority

Federal and DOD policy requires that information assurance requirements be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, and Appendix III of DOD Directive 5000.1. The EEDRS environment will achieve an appropriate level of confidentiality, integrity, and availability that meets and/or exceeds the security requirements of a DOD system operating at the MAC II Sensitive level, containing unclassified but sensitive information. Information Assurance requirements will be derived from the following regulatory sources.

1.2.1 DODD 8500.1

DODD 8500.1 establishes policy and assigns responsibilities regarding Information Assurance (IA) in DOD information systems. It categorizes all DOD information systems as automated information system applications, enclaves (which include

networks), outsourced IT-based processes, or platform IT interconnections; introduces the concepts of MAC, confidentiality level, and IA controls; provides general guidance regarding DOD minimum standards for availability, integrity, confidentiality, and certification; and assigns IA responsibilities to various individuals and organizations.

1.2.2 DODI 8500.2

DODI 8500.2 provides implementation guidance for the policy established in DODD 8500.1, and assigns further IA responsibilities at lower levels than those covered in DODD 8500.1. DODI 8500.2 also provides detail regarding the IA process; explains the four AIS categories in detail; discusses robustness requirements; and requires Information Systems Security Engineering (ISSE) as part of the acquisition process.

1.2.3 AR 25-2

Army Regulation (AR) 25-2, Information Assurance, establishes policies and assigns responsibilities for achieving minimum acceptable levels of IA in engineering, implementation, operation, and maintenance for all information systems connecting to or crossing any U. S. Army managed network as well as providing administrative and systems security requirements, including those for interconnected systems. AR 25-2 also introduces the concept of Information Assurance Best Business Practices to define and enforce mandatory and specific measures, practices, or procedures to meet changing technology or IA requirements.

1.2.4 Defense Information Systems Agency (DISA) STIGS and NSA SCG

The system is configured using the principles and guidelines from each DISA Security Technical Implementation Guides (STIGs) and National Security Agency Security Configuration Guides (SCGs). These guides will assist in the development of a secure system baseline that can be managed by either the Directorate of Public Works (DPW) or the Network Enterprise Center (NEC). The followings STIGS will be applied to EEDRS during its procurement and lifecycle: **(DCCS-1)**

a. Operating System
b. Network
c. Database
d. Web
e. Wireless (to be complete in Phase 2 or Phase 3)

The intent of the STIGs/SCGs are to include security considerations at the network and component level needed to provide an acceptable level of risk for information transmitted across the EEDRS enclave and Network Enterprise Center (NEC) backbone network. STIGs/SCGs also provide suggestions for redundancy, survivability, and guidelines for best technical practices. DODD 8500.1 requires that “all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines.” These STIGs/SCGs serve as the security configuration guidelines required by DODD 8500.1.

1.2.5 Approved Products

Department of Defense Directives and Instructions (DODD 8500.1 and DODI 8500.2) and Army Regulations (AR 25-2) mandate NIAP approved IA and IA-enabled products be procured for use in DOD and Army systems. DODD 8500.1 requires that "All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11". The Committee on National Security Systems (CNSS), formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC) issued NSTISSP #11 on 1 July 2002. NSTISSP #11 mandates that only products validated by the National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) or by the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Crypto module Validation Program (CMVP) be permitted for use in national security systems for all departments and agencies in the Executive Branch of the government.

The international standard, ISO/IEC 15408 Common Criteria (CC) for Information Technology Security Evaluation provides a uniform mechanism for the evaluation, measurement, testing and recognition of security products. The Common Criteria was adopted when a need for a standardized methodology for discussing and measuring Information Assurance products became evident, not just in the United States, but across the world. The Common Criteria has two parts. First, it provides for the creation of a document called a Protection Profile. The Protection Profile is the document wherein a user community specifies the security functionality and evaluation requirements for a desired system, application or function. The second aspect of the Common Criteria is the Security Target. The Security Target is the document written by a developer to describe how its system or application meets a particular Protection Profile. The process described by the Common Criteria has the developer submit the product, the Security Target and accompanying documentation to an accredited independent NIAP Testing Laboratory for evaluation. The Testing Lab then performs an evaluation and submits the results to an evaluation authority that can validate the findings. Once validated, the product is Common Criteria Evaluated.

The Unified Communications Approved Products List (UC-APL) consists of network devices, operating systems, and IA, IA enabled products that have met the NIAP and FIPS requirements and evaluated by a DOD laboratory. For Army organizations, it is mandated that all IA, IA enabled equipment purchases are on the UC-APL.

The Common Criteria is available at http://www.commoncriteria.org/.

Information on validated products and the NIAP is available at http://www.niap.nist.org/.

The Unified Communications Approved Products list is available at https://aplits.disa.mil/processAPList.do .

1.3 Scope

This document applies to the design, engineering, installation, and sustainment of the EEDRS enclave. The security design requirements set forth in this document are designed to assist the NEC Information Assurance Managers (IAMs), DPW Information Assurance Security Officers (IASO), and System Administrators (SA) in support of implementing, properly configuring, and sustaining the EEDRS security. As a part of this document's scope, it is important to mention that the security design and IA readiness will be monitored, reported, and evaluated as a distinguishable element of the EEDRS mission readiness.

1.4 Writing Convention

- Hyperlinks are in blue.
- Bulleted items are directives from applicable security document and guides.
- The use of the word "will" denotes a mandatory requirement
- The use of the word "should" denotes an optional requirement

1.5 **Terminology:**

a. The term Front-end server refers to application software that runs on either a Microsoft Windows OS or a LINUX OS, such as: Foreseer, Tridium Webstation R2, Echelon Lonmaker 3.2, ADX Server, LCS Server, Niagara AX web Server
b. The term Building Point of Connection refers to all intermediary devices or controllers that are translating meter data into IP and routing it to the Front-end server such as: Echelon Smart Server, Loytec L-IP LON Configuration Server, Loytec L-INX 101, JACE Devices, etc.
c. Meters refer to actual metering devices such as: Square D Power Logic, Shark 200, Wattnode LON FT-10, iTRON, etc.

2.0 Security Guidance

This section provides a description of security services provided, methodology for ensuring secure access to services, and the components used to ensure this secure access.

2.1 Mission Assurance Category

The mission assurance category reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the Warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. DODI 8500.2 defines a Mission Assurance Category (MAC) II system as follows:

Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

2.2 System Description

The Enterprise Energy Data Reporting System is designed to monitor the buildings electrical usage for an installation from a centralized workstation at DPW. The EEDRS is designed to reduce manpower at each site and meet the Energy Act of 2005/2007. Automated alarms will display problems on the screen in near real-time. The EEDRS is the reporting mechanism where the Utility Monitoring and Control Systems/ Energy Monitoring and Control Systems (UMCS/EMCS) can send their power and energy consumption information to be included in the rollup. There are several integrators/vendors solutions for the EEDRS.

2.3 System Architecture

The EEDRS monitors hundreds of buildings on an installation using smart meters. The EEDRS consists mainly of a front-end server with the vendor's enterprise solution installed. The front-end server has a structured query language (SQL) database and a web server interface into the database. The EEDRS also includes an engineering workstation and/or laptop with the vendor's utility tools to configure smart servers/configuration servers (includes IP routers, gateways, Java Application Control Engine (JACE) type boxes) and meters. These laptops are used for configuration purposes only and are not a part of the accreditation. The EEDRS also includes smart servers/configuration servers and meters located at each building which connect to the installations infrastructure using either wired or wireless connectivity on an isolated/restricted virtual local area network (VLAN). Wireless connectivity may be used in a future phase (Phase 2 or 3) of the project if approved for use.

2.3.1 The Architecture will be implemented in phases:

<u>Phase 1a</u>: will be based on a properly engineered secure baseline with the accompanying secure architecture fully documented, tested, and staffed per the DIACAP process, but lacking some of the important lifecycle support and other Information Assurance areas that will be required to maintain this secure baseline over time. As soon as possible after phase 1a is completed, the project will enter phase 1b.

<u>Phase 1b:</u> will be the Functional Type Accreditation. This means after properly security engineering the Front-end servers and the functional architecture to provide Information Assurance (IA) defense in depth with all mitigating strategies in place, the proposed Functional Type Accreditation will follow the normal C&A evaluation process. The only

deviation from a normal architecture will be the use of standardized configuration guidelines for all the EEDRS components except the Front-end servers instead of actual configurations of specific components.

Phase 2: All components of the architecture will be identified, and full configurations of all components will be documented and implemented.

2.3.2 Description of IA Architecture

a. All EEDRS components (Front–end Servers, Building Point of Connection devices, and Meters) will be attached to the network on an isolated/restricted VLAN using non-routable IP addresses to the Main Communications Node (MCN).
b. Once Meters are provisioned and configured, IP functionality will be disabled and they will use only LonTalk or ModBus Protocols using RS 485 or TP/FT-10. All further administration will be via a console cable at the device or using the LonTalk protocol
c. Once Building Point of Connection devices are provisioned and configured, all web, FTP, TFTP, Telnet, SMTP and SNMP functionality will be disable, if the device is capable of these functions. All further administration will be done via a console cable at the device or via the LonTalk protocol, unless properly assessed by the overseeing IA authority and presented to the DAA for acceptance.
d. All devices in the EEDRS will comply with the US Army Password BBP to the extent possible.
e. The MCN will provide Network Address Translation (NAT) for the non-routable devices in the isolated/restricted VLAN. The MCN will contain Access Control Lists (ACLs) that limit communication such that the only communication allowed will be between the Front-end servers to Building Point of Connection using LonTalk, and the Front-end servers to MDMS Gateway server using SSL (port 443).
f. The Front-end servers will be properly configured per DoD and Army Guidance using all applicable STIGs or other IA related guidance. This means they will be made as secure as possible while remaining mission capable. A formal risk assessment, taking into account the Defense in Depth Architecture, will be conducted that will clearly delineate any residual risk.
g. If implemented at a later time (not in Phase 1A), the MDMS gateway will be located in a DMZ off of the TLA firewall.
h. Should MDMS be connected to the EEDRS beyond Phase 1A, communication between the Front-end servers and MDMS will be mediated by both the Main Communications Node (MCN) and the Top Level Architecture (TLA) firewall such that data exchange is limited to communication between MDMS and the Front-end servers only via SSL (Port 443).
i. Since the Front-end servers, along with the rest of the EEDRS will be in an isolated/restricted VLAN(s), care must be taken on the part of the local NEC in terms

of security scanning and patching. Indiscriminate scanning of other than the Front-end servers will likely cause EEDRS components to fail. Also, patching and pushing of Active Directory Group Policy Objects will likely cause the Front-end servers to stop functioning.

j. All wireless implementations must be compliant with the US Army Wireless Best Business Practice and all applicable STIG's. The wireless solution can be either a part of the local NEC accreditation or included as part of the EEDRS implementation.

k. Host-based Intrusion Prevention System and Anti-Virus software will be installed.

Figures 1 and 2 illustrate a typical EEDRS architecture.

Figure 1 EEDRS Physical Diagram

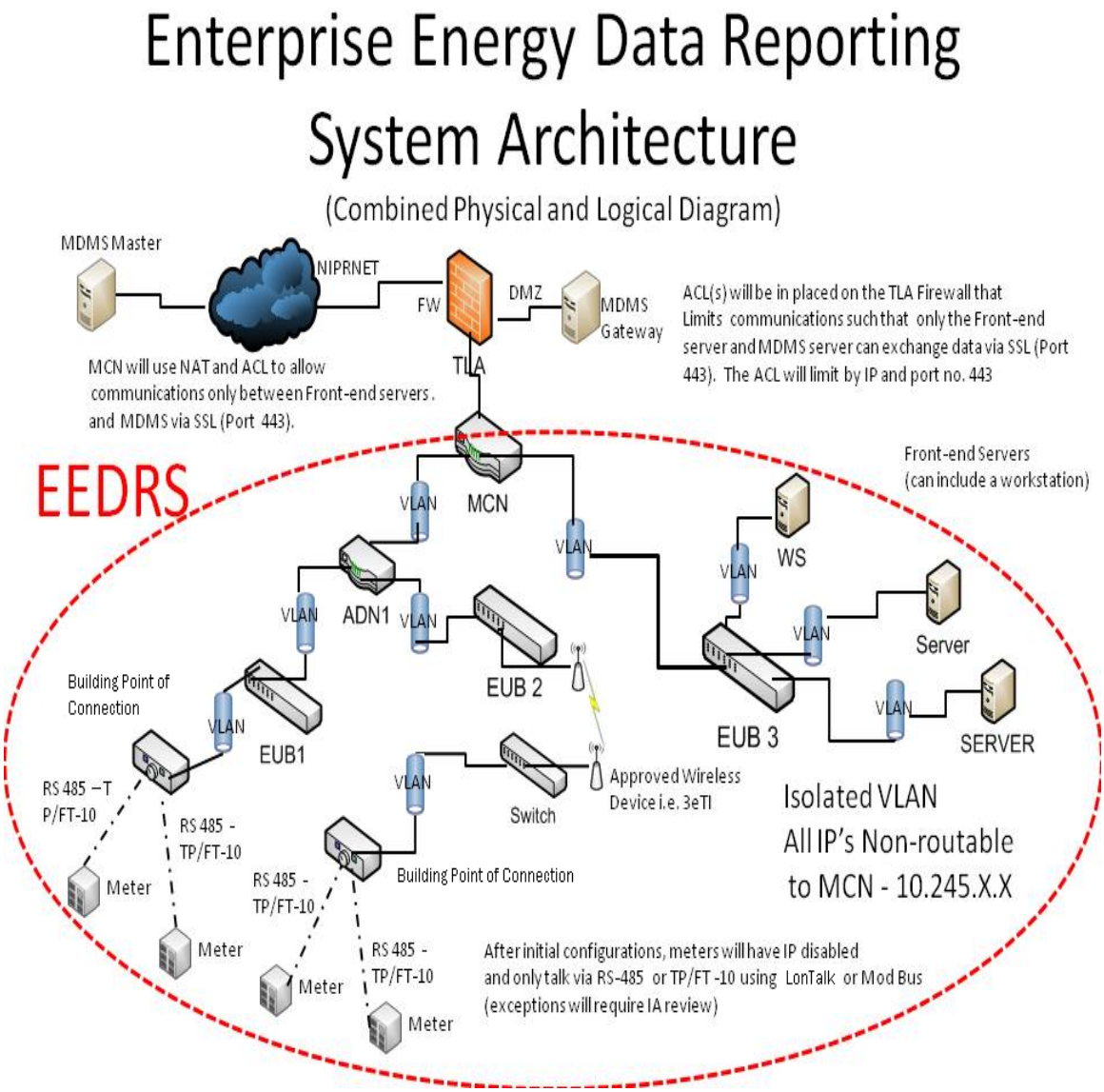
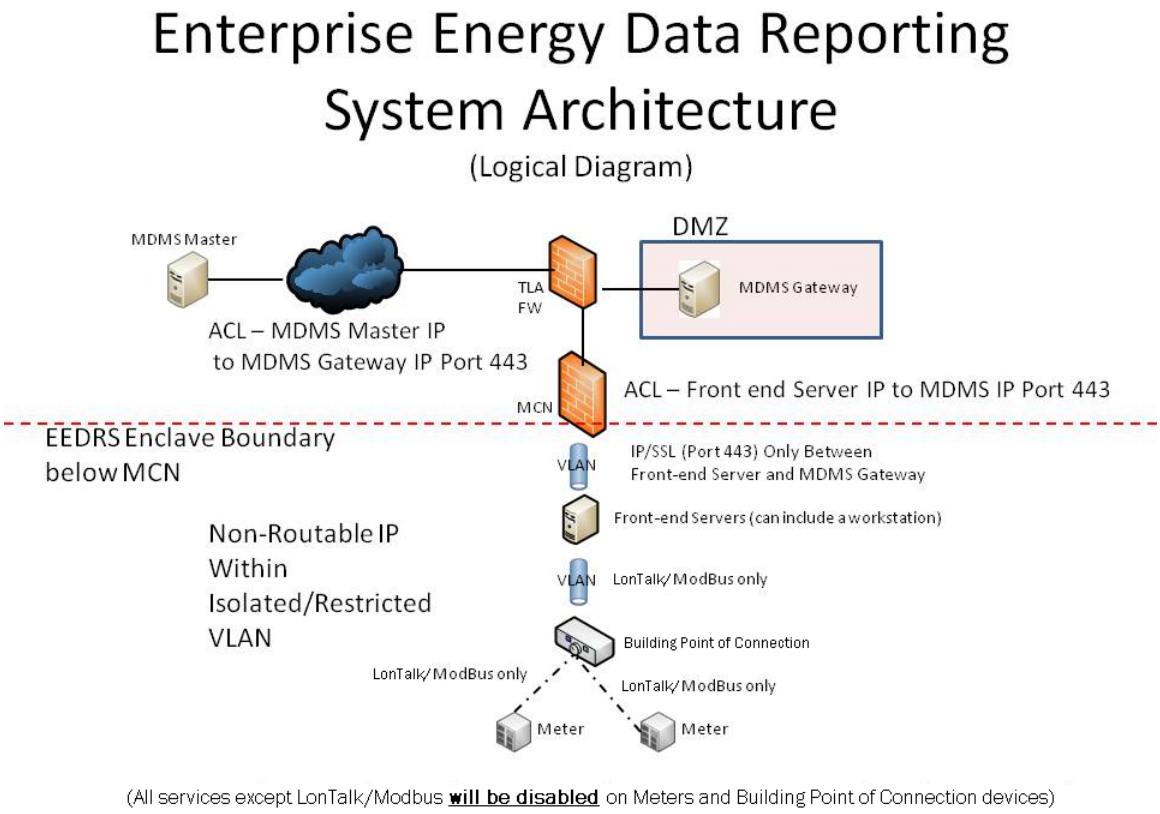


Figure 2 EEDRS Logical Diagram



2.4 Accreditation Boundary

The accreditation for EEDRS is a TYPE accreditation and considered a Mission Assurance Category II system with a Sensitive confidentiality rating. The following system components are inclusive to the accredited system boundary:

a. The front-end server located at the NEC server farm or DPW.

b. The Workstation located at the DPW EEDRS office.

c. The Laptop used for onsite configuration.

d. Various Building Point of Connection devices and meters.

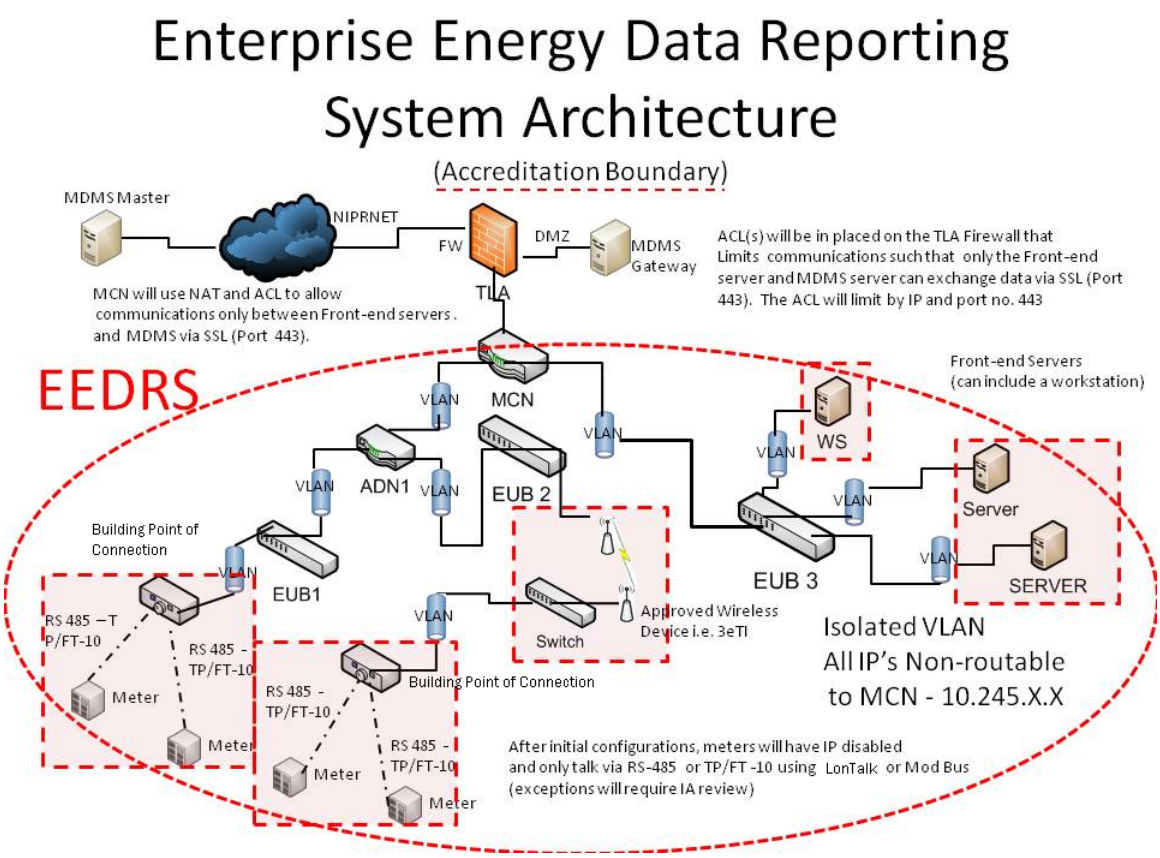
The various Building Point of Connection devices and meters will be identified and added to the accreditation package at a later time. However, these devices will be a part of the Functional Type Accreditation. The Functional Type Accreditation package will contain general IA configuration guidelines that must be implemented to include these devices into the Functional Type Accreditation. In phase two of EEDRS, each component will be identified and specific IA configuration will be documented (see Para 2.2.1). Accreditation of any EEDRS configuration deviations/changes outside of the components listed above is the responsibility of the NEC. Examples of such

configuration changes that would require a NEC to update documentation/accreditation include, but are not limited to:

- Interconnections with installation data networks (e.g., Global Information Grid), except as already noted in this document.
- Access Control Lists applied to the routers or firewalls to isolate the EEDRS. Typically, NEC's will already have a local configuration management process to account for changes to the ACL's on their routers and firewalls. If this is the case, normal NEC processes should be followed.

Figure 3 illustrates the system boundaries for the accreditation of the EEDRS using red broken lines. The MCN and Firewall components are not specifically included in the physical boundary. However, the ACL's required for the EEDRS Architecture are considered part of EEDRS logical accreditation boundary and are required to provide sufficient defense in depth.

Figure 3 EEDRS Accreditation Boundary



2.5 Operational Environment

The EEDRS monitors energy consumption on the installation. The EEDRS assets consist of Commercial-Off-the-Shelf (COTS) hardware and software available to standard Army and DOD contracts. In addition to COTS operating systems, vendor unique applications are incorporated for special purpose functions. The use of freeware and shareware is highly discouraged unless there is an operational need, if an operational need is determined, then approval to use this software must be granted by the DAA. At this time, there is no freeware nor shareware on the system **(DCPD-1).**

2.5.1 EEDRS Subsystems

The EEDRS consists of seven subsystems: front-end Server, Workstation, laptop, Smart Server/Configuration Server, and meters.

2.5.2 Front-end Server

Depending on the vendors software solution, the front-end Server is installed on a Windows 2008 or 2003 (W2K8, W2K3) standard or member server operating system. Additionally, Microsoft SQL 2005 and IIS web server applications are installed to support the monitoring of the energy consumption. The database is used to maintain building information, settings, and logs. Trend analysis reports are derived from this information. The SQL uses a web front end for the workstations to input information and generate reports. The operating system, SQL, and Web servers are hardened IAW the DISA STIGs. Separate administrator accounts are required for each administrator.

2.5.3 Workstation and Laptop

The Workstation is installed on a Windows 7 or Vista operating system. Depending on the vendors, the vendor could use a web browser to access the server or use a standalone application. Additionally, Visio is installed. Visio is used to graphically display the buildings metering system and controls. An operator can go to the drawing and quickly change settings. These settings are maintained on the server. The application on the server controls the various Building Point of Connection devices and meters. The operating system is hardened IAW the DISA STIG. The laptop is configured the same as the workstation for localized installation of a new system and trouble shooting at the building. Additional software could be required depending on the vendor's solution. They will only operate in the EEDRS isolated VLAN environment.

2.5.4 Building Point of Connection

a. As noted in paragraph 1.5 Terminology, the generic term "Building Point of Connection" refers to multiple devices. Essentially, the BPOC establishes a demarcation between field level control protocol and IP. It will receive inputs from non-network meters and move that data onto the IP network and will also receive data from the field level control system and move that to the IP.

b. As subsets of the BPOC definition, the Echelon SmartServer, the Loytec L-IP LON Configuration Server, the Loytec L-INX, the Java Application Control Engines (JACE), and others, convert the digital or analog from the meter and sends a digital signal to the server. They also convert digital signals from the

vendor's application into analog or digital electrical signals for the HVAC controls, sensors, or solenoids. The controller has an RJ-45/RS-232B console interface for configuration. The controller has RS-485 connectors to connect other devices. There is IP capability in the controller. The controller can also use the Modbus protocol to control other devices. These components will not be joined to an AD domain at the installation. They will only operate in the EEDRS isolated VLAN environment. In phase 1, they will be configured, based on the general configuration standards delineated in Para 2.3.2 of this document. In phase 2, they will be configured per specific configuration guides.

2.6 Hardware and Software

Appendix B lists the hardware and software used in the EEDRS. Due to the fact that there are various as yet unknown hardware components used by different vendors, the complete hardware list will be added at a later date. Table 1 is an example only. These lists will be periodically updated as new hardware/software becomes available. Changes to the hardware/software will be tracked by the local CCB after commissioning.

2.7 External Interfaces (DCFA-1)

The EEDRS is an isolated/restricted system utilizing a private IP address VLAN of 10.xxx.xxx.xxx. The buildings are interconnected to the server and workstations using the installation's infrastructure. Although the MDMS is currently not used, the MDMS gateway is programmable to communicate with the Front-end servers which reside in the VLAN. With the exception Front-end servers, no other component in the EEDRS are allowed to communicate outside the isolated VLAN installations infrastructure.

2.8 System Connection Approval Process (DCID)

The Designated Approving Authority grants the authority to operate. A network must receive accreditation before it may operate. The Designated Approving Authority must approve all network changes that could affect network security before implementation. Connected devices, local area networks (LANs), and enclaves, regardless of the command affiliation of their owner(s), must adhere to a single connection policy. The NEC is mandated to verify compliance with this policy and impose restrictions on connected systems for non-compliance.

Network connection rules must be consistent with network accreditation criteria. Network accreditation is the culmination of strict procedures that organize and configure the network to achieve an acceptable level of risk. Network connection security ensures that the EEDRS employs proper security controls to prevent unauthorized access by remote users and prevent denial of service conditions.

3.0 Perimeter Security (EBBD-2)

The main purpose of the EEDRS enclave security is to limit the access to the hosted application only to authorized users. This is accomplished by segregating the traffic into separate VLANS. Access to each VLAN will be controlled by a specific ACL. Separating the EEDRS enclave from the rest of the NEC network is critical to the protection of the EEDRS.

This architecture is predicated on the assumption that the perimeter security for the EEDRS is provided by the NEC as an inherited feature. The firewall and IDS that are incorporated into the NEC infrastructure protect the EEDRS from outside observation or attack by denying all traffic to the EEDRS VLAN except as noted in that architecture document. The defense in depth strategy used to mitigate security issues specific to EEDRS is also predicated on the assumption that the NEC IA architecture complies with the DoDI 8500.2 requirements and has an approved and current Authority to Connect (ATO) from the DAA.

3.1 ACL

Access Control Lists on the router interfaces for the VLAN to the building meters are applied to prevent unauthorized access. The EEDRS, which uses router and switches to interconnect within an installation uses an access control list (ACL) to isolate and restrict the network traffic from the rest of the installations traffic, which mitigates a significant portion of risk to the network to the EEDRS enclave.

3.2 DOD Ports, Protocols, and Services

In accordance with DOD policy, a Deny-by-Default posture will be implemented on every device protecting the EEDRS System's boundaries. The only protocols traversing through the core network are those required for operation by the corresponding enclave. See Appendix B for a list of Ports and Protocols that are being utilized on the EEDRS. After installation and verification of proper communications using the LonTalk or Modbus protocols and networks, all of the functionalities for Telnet, FTP, SNMP, TFTP, SMTP, and WEB have to be disabled.

4.0 Computing Environment

The computing environment security mechanisms provide the innermost layer of defense in depth for enclaves. These security mechanisms are implemented on the end system workstations, servers, and network devices. The computing environment security mechanisms are described in the following sections.

4.1 Operating System Security

The security mechanisms of discretionary access control of using individual accounts and passwords are applied to the workstations and servers. The passwords follow the requirements stipulated in AR 25-2 and the Password BBP to the extent possible.

4.1.1 Security Configuration Guides

The EEDRS will be secured and hardened using security configuration guides. The main guidance that will be used are Security Technical Implementation Guides (STIG) from DISA. Included as part of the STIGs are check lists and Security Requirements Guides (SRG). The National Security Agency Security Configuration Guides for operating systems will also be used. In situations where there is no published government security guide, industry best business practices (BBP) can be used. If BBP's are used, the system owner will write a SRG and provide the guide to DISA. Any IA controls not implemented from any guide will be justified, mitigated, and documented.

4.1.2 Application and Data Security

Application level software that will be supporting EEDRS include: a range of software, such as SQL, IIS and vendor specific applications. These applications introduce both capabilities and vulnerabilities. The applications will be configured to restrict access permissions.

4.1.3 Antivirus Protection and Detection

Approved antivirus protection and detection software is installed on each Front-end server, engineering workstation and laptop IAW AR 25-2 and DoDI 8500.2. Because of the nature of all of the other devices in the EEDRS (smart server/configuration server), they will not have antivirus protection and detection software installed. This is one reason it is critical to maintain the proper defense in depth posture and ensure all of these devices remain in a protected enclave. The only component of the EEDRS that will be allowed communications outside the protected enclave (EEDRS VLAN) will be the Front-end server components that will have properly installed configured and updated antivirus protection.

4.1.4 Mobile Code

Mobile Code can be characterized as software modules obtained from remote systems, transferred across a network, then downloaded and executed on a local system. Examples of Mobile Code include JavaScript and ActiveX. Mobile Code is used by developers to run mini-applications or scripts, and they are somewhat easily altered when not properly validated and coming from a trusted source. Reference the DOD Mobile Code Policy http://www.defenselink.mil/nii/org/cio/doc/mobile-code11-7-00.html.

- **Category 1 (ActiveX and Postscript)** Exhibit a broad functionality allowing unmediated access to host and remote system services. Category 1 technologies have known security exploits with few or no countermeasures once access is gained.
- **Category 2 (Java, MS Officer VBA, Lotus, PerfectScript).** Category 2 technologies have partial functionality allowing mediated access and environment-controlled access to host system services. Category 2 technologies may have known security exploits, but also have known fine-grained, periodic, or continuous countermeasures/safeguards.
- **Category 3 (JavaScript and PDF)** Technologies in Category 3 support limited functionality, with no capability for direct access to host system services. Category 3 technologies may have a history of known exploits, but also support fine-grained, periodic, or continuous security safeguards. Category 3 technologies may be used in DOD ISs.
- **Non-Categorized Mobile Code Technologies.** Given the amount of uncertain risk, Non Categorized Mobile Code Technologies are prohibited unless explicitly authorized by the DOD CIO Control Board.

Only Category 3 mobile code will be used in EEDRS. The integrator/vendor will declare the type of mobile code used for their applications. For any mobile code other than Category 2, a waiver will be required from the CIO.

4.1.5 Database Application

EEDRS uses databases to define, store, and manipulate data. These databases support distributed applications with security integrated into the database. Security controls such as password policies, auditing, access control, and role-based access will be configured into each database consistent with system security policies as defined by the regulations. All sample data and scripts must be removed to further protect the databases since most sample data and scripts can execute with administrative privileges.