Department of Homeland Security: Cyber Security Procurement Language for Control Systems

August 2008

Homeland Security

Control Systems Security Program
National Cyber Security Division

FOREWORD

A key component in protecting a nation’s critical infrastructure and key resources (CIKR) is the security of control systems.

WHAT ARE CONTROL SYSTEMS?

Supervisory Control and Data Acquisition (SCADA), Process Control System (PCS), Distributed Control System (DCS), etc. generally refer to the systems which control, monitor, and manage the nation’s critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, natural gas pipelines, and many others. Simply stated, a control system gathers information and then performs a function based on established parameters and/or information it received.

For example, a control system might gather information pertaining to a leak in a pipeline. The system would then transfer the information back to a central site alerting a control station that the leak has occurred, carrying out necessary analysis and control such as determining if the leak is impacting operations and displaying the information in a logical and organized fashion. In this example, shutting down the pipeline is one of the functions that the control system could perform, if a leak is detected.

Control systems can be relatively simple, such as one that monitors environmental conditions of a small office building, or incredibly complex, such as a system that monitors all the activity in a nuclear power plant or the activity of a municipal water system.

Because the function control systems perform for the continuous and safe operation of the nation’s critical infrastructures, it is essential to recognize and understand the important roles these systems play. In addition, there should be a heightened interest in recognizing the potential vulnerabilities, consequences, and challenges in securing these systems from compromise.

One example of the challenges presented was the recent disclosure of a SCADA system compromise, which was responsible for controlling a local government’s municipal water supply. This example highlights the need to focus cyber security efforts and the importance of critical infrastructure. SCADA security is an emerging issue, which can no longer be ignored. Stakeholder education is also a critical factor for success when addressing the need for control systems cyber security. The U.S. Department of Homeland Security recognizes the importance of control systems security education and awareness and offers the Cyber Security Procurement Language document as a means to help asset owners integrate security into their control systems security lifecycle.

WHY SHOULD WE BE CONCERNED?

Control system technology has evolved over the past 30 years as a method of monitoring and controlling industrial processes. Control systems were first used in the 1960s to control and monitor events that were performed by humans. Industry trends have demonstrated that the life cycle of a control system is now between 15 and 30 years.

Thirty years, or even 15 years ago, security was not generally a priority in the control systems environment. Traditionally, control systems were stand-alone devices, not connected to business networks or the outside world via the Internet.

Over the years, these systems have gone from proprietary, stand-alone systems, to those that use commercial off-the-shelf (COTS) hardware and software components. With the increase of more commonly used hardware and software, comes the potential for information technology (IT) vulnerabilities to be exploited within the control systems environment.

The Symantec Internet Security Threat Report issued in September 2006[a] documented nearly 7,000 new worms and viruses, and more than 2,200 new vulnerabilities in the first half of 2006; this is the highest number ever recorded for a 6-month period. In the past, software fixes were available months before attackers would exploit the vulnerabilities with fast spreading worms such as Slammer or Nimda. The trend has been reversed; software vulnerabilities are routinely exploited before the vulnerabilities are fully understood or protection mechanisms are identified.

Not all SCADA systems are vulnerable or are at risk of attacks. However, these systems manage critical infrastructure assets that are vital to a nation's economy. Whether the threats are real or perceived, it is in a nation's interest to provide guidance on the protection of these assets.

In March 2004, the U.S. Government Accountability Office (GAO) published a report on SCADA security[a] that it produced at the request of the U.S. House Committee on Government Reform Subcommittee on Technology and Information Policy. That report focused, in part, on why the risk to control systems is increasing.

The report listed the four contributing factors to the escalation of risk to SCADA systems:

1. Control systems are adopting standardized technologies with known vulnerabilities
2. Control systems are connected to other networks that are not secure
3. Insecure connections exacerbate vulnerabilities
4. Manuals on how to use SCADA systems are publicly available to the terrorists as well as to legitimate users.

[a] GAO, "Challenges and Efforts to Secure Control Systems," March 2004.

BACKGROUND

The U.S. Department of Homeland Security Control Systems Security Program, Idaho National Laboratory, Chief Information Security Officer (CISO) of New York State, and the SANS Institute have established an initiative to bring public and private sector entities together to improve the security of control systems. The goal is for private and public asset owners and regulators to come together and adopt procurement language that will help ensure security integration in control systems.

The Cyber Security Procurement Language for Control Systems effort was established in March 2006. The results of this endeavor represent the joint effort of the public and private sectors focused on the development of common procurement language for use by all control systems stakeholders. The goal is for federal, state, and local asset owners and regulators to obtain a common control systems security understanding; using these procurement guidelines will help foster this understanding and lead to integration of security into control systems.

The Cyber Security Procurement Language Project Workgroup comprises 242 public and private sector entities from around the world representing asset owners, operators, and regulators. Additionally, over 20 vendors participate in a working group to assist in reviewing and producing the procurement language.

Comments on this document are welcome and should be submitted to cssp@dhs.gov with the subject line of “Procurement Project.”

This document provides information and specific examples of procurement language text to assist the control systems community, both owners and integrators, in establishing sufficient control systems security controls within contract relationships to ensure an acceptable level of risk.

SECURITY OBJECTIVES

A discussion of security objectives is provided as a framework to establishing security controls within the context of control systems procurement. A common understanding of security objectives is required to facilitate comprehensive controls necessary to operate at an acceptable level of risk.

There are three security objective categories as defined in traditional information assurance areas: Availability, Integrity, and Confidentiality.[b] SCADA and control systems must be available continuously when controlling critical infrastructure or life-safety systems. A control systems operator must rely on the integrity of the information in order to take appropriate actions based on the readings or status of the system. Confidentiality is not as important since most of the information used and transmitted is state-based and only valid for that specific time. For example, the set point for a process is only valid until the next set point is sent, which may be as short as a second. Contrast that to the traditional IT world where a credit card number is valid for many years. For traditional IT systems, integrity assumes authentication, authorization, and access control based on the decades of implementation of role-based access control (RBAC). This is not the case for legacy control systems where the use of RBAC is rare. For this reason, Authentication, Authorization, and Access Control will be discussed under the Integrity section. Nonrepudiation is important for selected industry segments that use data from control systems and SCADA for financial markets (see the Confidentiality section for more information).

Availability

Availability is defined as providing the data when needed or "ensuring timely and reliable access to and use of information…."[c] A loss of availability is the disruption of access to or use of information from an information system. Availability is of the highest priority for control systems and SCADA environments due to the near real-time nature of these applications. Simple Denial of Service (DoS) type of IT attacks applied to a control system will have large impacts due to the importance of control and monitoring functions within a control systems environment.

The timeliness of data being sent or received from control systems is paramount. The control system operator needs assurance that the data being sent or received are true. These two requirements inherently require that a high priority be given to meeting the availability and integrity objectives for control systems.

The availability objective has differing importance across large integrated systems that use SCADA or control system data. Enterprise level management systems generally require a medium availability, while control systems require high availability. The outage of a management system will not result in the loss of control, but of situational awareness that may or may not result in a system

[b] FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," Federal Information Processing Standards, December 2003.

[c] 44 United States Code, Section 3542.

failure. Because the failure of a control system could result in significant impact or consequence, over engineering and redundant features are utilized to ensure the high rate of availability.

Basic protections need to be in place to prevent random non-targeted IT-based attacks from impacting the control systems environment. On the other side, security measures implemented cannot impact the availability of a system. For example, an anomaly-based network intrusion detection system (NIDS) is not recommended for a network whose communication method is to report by exception when the system normally has events that cause all devices to report at the same time (e.g., severe weather in the electrical sector). Thus, added security measures should be tested in abnormal conditions to ensure that availability has not been impacted and should be able to be removed quickly, if necessary, to ensure continued operations.

Integrity

Integrity is ensuring that the data presented are the true valid master source of the data or "guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity...."[d] A loss of integrity is the unauthorized modification, insertion, or destruction of information. The underlying mechanisms that normally aid in the integrity of a system are missing or weak in control systems (reference the sections on authentication and authorization). False data displayed on the human-machine interface (HMI) or sent to applications or remote field devices could result in system failure. Also, alterations in the applications (programs and memory) could affect the integrity or availability of the system.

Access control, authentication, and authorization are specifically discussed for integrity, since control systems do not have a 20-year history of applying passwords, accounts, and role-based permissions to these applications such as in the IT community. Due to the lack of role-based permissions, some unique workarounds have been implemented to support the control system environment.

A large part of the access control objective is physical. All of the required cyber security layers will fail if the attacker has physical access to the systems.

Access control is making the data/application/communication available to only those with permission. Loss of access control allows unauthorized entry into a system. If role-based permissions do not exist, the breach in access control may result in a loss of confidentiality, integrity, and system availability. For this reason, access control is included as a security objective. Moreover, when control system assets are located in remote, geographically dispersed areas, access control is particularly challenging.

Authentication is ensuring that entities verify that they are who they claim to be and are not malicious spoofing authorized identities. Authentication is important when an entity first attempts to gain access to a system or application. There are four authentication factors: "what you know" (i.e., username and

[d] 44 United States Code, Section 3542.

password), “what you have” (i.e., key, digital certificates, and smart cards), “what you are” (i.e., biometric scan such as fingerprints and iris recognition), and “what you do” (i.e., dynamic biometrics such as hand writing and voice recognition). The more detailed privileged rights are discussed in the Authorization section. A loss of authentication could lead to a loss of confidentiality, integrity, and system availability. Authentication is normally handled by checks in protocols or by account and password functions, and is included in the integrity security objective in traditional IT-based systems. This is included as a security objective since most control systems and protocols that support those systems have weak, or no authentication.

Authentication is a unique challenge in the control system environment since the initiating sources could be processes, applications, or information on a field device. Hardware authentication can be done via static addressing, or passing keys or certificates. Adhering to static addressing and enforcing hardware authentication for network access is one layer of added security that bypasses all the domain name server-type of exploits. Authorization also has a unique perspective in the control system environment, since the entity could be another process or communication link.

Authorization is granting a user, program, or process the right of limited control once authentication has been determined. This ensures that the entity is permitted to perform the read, write, delete, and update functions, or execution of a task, which is normally managed by role-based permissions. A breakdown of role-based restrictions may result in an entity that has access to the system gaining the ability to run processes and control the system above their permission level. In the traditional IT world, role-based permissions are implemented and normally linked to an account password authentication task and permission tables for applications. However, most legacy control systems are not designed for role-based permissions.

The code resident in memory in the remote field devices is also subject to integrity concerns that include authentication, authorization, and access control. This code controls the remote device’s actions during normal communications to the control system and during times when communication to the larger control system or SCADA is not available. Most of this “code” appears like actual data. There is a trend to include resident memory for nonrepudiation checks to ensure that the code has not been changed since its last installation.

Other solutions to maintain integrity may include one or more of the following: deep packet inspection of data, sequence numbers in proprietary protocols, checksums in protocols, and host-based intrusion detection systems (IDSs) that record changed, stored, or running applications.

Confidentiality

Confidentiality means keeping the data unseen by others, or "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...."[e] A loss of confidentiality is the unauthorized disclosure of information.

Attackers can identify account names and passwords if transmitted in clear text and use this information to gain access to a system. Sophisticated target attacks may be possible through traffic analysis of control systems, allowing the attacker to reverse engineer protocols. This information, along with operational data, may then be used for a targeted attack. Other sophisticated targeted attacks are possible by studying the control system applications to discover and exploit vulnerabilities to gain control of the system.

The basic accounts and passwords in control systems are the primary data that need to be protected. This is commonly achieved by storing these files in an encrypted format.

Other information, such as the application code, also needs to be protected from release. Some system configurations store the human readable code on the same networks as the control system. An attacker on such a network could review the code for possible vulnerabilities (e.g., buffer overflows) and exploit the system. Configuration files should also be protected to prevent an attacker from gaining knowledge of the control system operation.

Due to the state-based nature of control systems, only some network traffic information needs to be kept confidential unless it would provide an advantage to a competitor. Some communications between the field devices or peer entities (endpoints) and these applications are encrypted. There is an initiative to encrypt more of these communication links.[f] The commands sent to the endpoints are normally not understandable (e.g., 670M), but could be studied for a protocol attack. The databases that store input and output points and the applications that display this information in context make command information valuable. Some control system communications may warrant encryption, such as those carrying market sensitive information, encryption of these communication links is often used for the authentication functions rather than for the confidentiality aspects. The reason encryption is being used is due to the lack of robust protocols, which do not authenticate that the sent item is what was received and that it was sent by an authorized entity.

Network encryption limits the ability to use intrusion detection systems. Signatures, stateful packet inspection, malformed packets, and deep packet inspection cannot be done if the network is encrypted. In addition, any encryption scheme will need to be tested to ensure that system performance and availability has not been degraded or compromised.

[e] 44 United States Code, Section 3542.

[f] American Gas Association, Report No. 12, "Cryptographic Protection of SCADA Communications General Recommendations," Draft 3, August 14, 2004, prepared by AGA 12 Task Group.

Nonrepudiation is ensuring that a traceable legal record is kept and has not been changed by a malicious entity. A loss of nonrepudiation would result in the questioning of the transactions that have occurred. Some SCADA and control systems interface with applications for financial contracts (e.g., energy market). Forecasting and financial data do not control a physical device directly, but do impact the systems' perception of capacity, load, and generation. These perceptions are used to optimize the settings on the physical devices of the power grid. Since the SCADA/Energy Management System (EMS) typically provides data to other forecasting and financial systems, those communications have to be managed to obtain the security objectives identified. When control systems are interfaced to corporate applications/networks, regulation-mandated security requirements, such as Sarbanes-Oxley,[g] need to be considered as well.

[g] The Sarbanes Oxley Act of July 30, 2002, SOX.

CONTENTS

ACRONYMS

ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
ARP	Address Resolution Protocol
BERT	Bit Error Test
BIND	Berkeley Internet Name Domain
BIOS	Basic Input/Output System
BSS	Basic Service Set
CB	Citizen Band
CERT	Computer Emergency Response Team
CIKR	Critical Infrastructure and Key Resources
CISO	Chief Information Security Officer
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Video Disc
EAP	Extensible Authentication Protocol
EMS	Energy Management System
ESP	Encapsulating Security Payload
FAT	Factory Acceptance Test
FEP	Front-End Processor
FTP	File Transfer Protocol
GAO	Government Accountability Office
HIDS	Host Intrusion Detection System
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection System

I/O	Input/Output
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
INL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISA	Instrumentation, Systems, and Automation Society
ISAC	Information Sharing and Analysis Center
ISC	Internet Software Consortium
ISM	Industrial, Scientific, and Medical
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
LOS	Line-Of-Sight
LR-WPAN	Low-Rate Wireless Personal Area Networks
MAC	Media Access Control
MCM	Manual Control Mechanism
MISPC	Minimum Interoperability Specification for PKI Components
MITM	Man-in-the-Middle
NAT	Network Address Table
NERC	North American Electric Reliability Corporation
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPC	National Infrastructure Protection Center
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OS	Operating System
OSI	Open Systems Interconnectivity
PBX	Private Branch Exchange
PCS	Process Control System
PLC	Programmable Logic Controller
PROFIBUS	Process Field Bus

PSTN	Public-Switched Telephone Network
RBAC	Role-Based Access Control
RFC	Request for Comments
RFI	Remote File Include
RPC	Remote Procedure Call
RTU	Remote Terminal Unit/Remote Telemetry Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedure
SQL	Structured Query Language
SSH	Secure Shell Terminal Emulation
SSL	Secure Sockets Layer
SSO	Single Sign-On
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual LAN
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WPA	WiFi Protected Access
XSS	Cross-Site Scripting

Department of Homeland Security

Cyber Security Procurement Language for Control Systems

1. INTRODUCTION

The purpose of this document is to summarize security principles that should be considered when designing and procuring control systems products and services (software, systems, maintenance, and networks), and provide example language to incorporate into procurement specifications. The guidance is offered as a resource for informative use—it is not intended as a policy or standard.

This document is a "tool kit" designed to reduce control systems cyber security risk by asking technology providers, through the procurement cycle, to assist in managing known vulnerabilities and weaknesses by delivering more secure systems. It initially targets high-value security risk reduction opportunities achieved through the procurement cycle.

The tool kit includes a collection of security procurement language that map directly to critical vulnerabilities observed in current and legacy control systems and that can be mitigated by technology providers and organizations through effective management of the technology across the systems' operational lifespan. The procurement language document is the result of a process that brought together leading control system security experts, purchasers, integrators, and technology providers and vendors across industry sectors, such as electrical, gas, petroleum and oil, water, transportation, chemical and others, and included members from the U.S. federal and state governments and from other international stakeholders.

The high value target opportunities were derived from a body of knowledge developed jointly by participants, from actual control systems testing results, cyber security related field assessments, and other observations. These topics are not presented in an order of importance nor prioritized based on risk. Topics may be selected at the user's discretion based on their own risk mitigation analyses.

The information provide in the procurement language document does not forego the use of engineering practices. The system's prime requirements, functions, design, and expected behaviors need to be taken into account prior to adding or requesting security requirements. Each topic merits individual consideration. This document is not intended to be a "one-size-fits-all" for all control systems. This is a model that must be converted into a specification for each purchaser's needs.

The Purchaser is encouraged to work with the vendor(s) to identify risk mitigation strategies specific to their system that may include solutions outside of those presented in this document. Many vendors are considered industry experts and are a valuable resource to the Purchaser. It is not the intention of this document to discount the expertise leveraged by the purchaser.

Information produced from activities associated with this document may be considered sensitive in nature for both the Vendor and Purchaser/Operator. Information protection schemes must be established prior to initiating procurement cycle, which could range from non-disclosure agreements for the request of proposal response to encrypting files containing sensitive configuration information.

A note on hyperlinks in the electronic version of this document: Many terms defined in the Terminology section are hyperlinked to Internet definitions sites. In the body of the document, some terms are linked to the terminology section. Therefore, one click on a term within the document body will take you to the local definition. Once there, a second click will bring up a full definition.

1.1 Topical Template

This document is presented as a series of categorized high-level topics, each addressing a particular control system security area of concern. For each topic, the following information is provided:

Basis: A topic’s basis is a summary of the potential exposures and vulnerabilities associated with a particular class of problem (i.e., why the topic is included).

Language Guidance: Additional information on the procurement language and how it intends to meet the needs described in the Basis.

Procurement Language: Example specification language is provided that can be included as part of procurement specifications to mitigate the Basis. References are made to specific timing of deliverable information. All language is agreed upon pre-contract award; proprietary or business sensitive information will be delivered after the contract is signed (post-contract award).

Note the terms “Factory Acceptance Test” and “Site Acceptance Test” are used generically; the testing cycles are described by regulatory agencies and are different for each sector.

Factory Acceptance Test Measures: The Factory Acceptance Test (FAT) is necessary to verify that security features function properly and provide the expected levels of functionality. Each topic includes FAT tasks specific to that topic. In general, prior to initiation of each FAT, the Vendor shall install all operating systems and application patches, service packs, or other updates certified for use with the provided system by the time of test, and documentation of the configuration baseline. Note that FAT is a process, not an event, and could in fact extend over several weeks or months.

Site Acceptance Test Measures: The asset Purchaser’s Site Acceptance Test (SAT) typically repeats a subset of a FAT after system installation with additional integrated functions. Typically, the SAT is performed before the cutover or commissioning, to validate that the site installation is equivalent to the system tested at the factory. Like the FAT, the SAT may extend several weeks or months and may occur at multiple locations.

Maintenance Guidance: This is guidance on how the Vendor will maintain the level of system security based lined during the SAT as the system evolves, is upgraded, and is patched. This subsection may be best included as a security clause in a maintenance contract, rather than in a procurement specification to maintain ongoing support.

References: External supporting information, practices, and standards are included.

Dependencies: Internal topics that should be in concert with the given topic.

2. SYSTEM HARDENING

System Hardening refers to making changes to the default configuration of a Network Device and its operating system (OS), software applications, and required third-party software to reduce system security vulnerabilities.

2.1 Removal of Unnecessary Services and Programs

Unnecessary services and programs are often installed on network devices.

2.1.1 Basis

Unused services in a host operating system that are left enabled are possible entry points for exploits on the network and are generally not monitored since these services are not used. Only the services used for control systems operation and maintenance shall be enabled to limit possible entry points.

2.1.2 Language Guidance

Often, networked devices ship with a variety of services enabled and default operating system programs/utilities pre-installed. These range from system diagnostics to chat programs, several of which have well-known vulnerabilities. Various attacks have been crafted to exploit these services to obtain information leading to compromise the system.

Any program that offers a network service that “listens” on specific addresses for connection requests. On a Transmission Control Protocol (TCP)/Internet Protocol (IP) network, these addresses are a combination of IP address and TCP or User Datagram Protocol (UDP) ports. A recommended hardening activity is simply disabling or removing any services or programs, which are not required for normal system operation, thus removing potential vulnerabilities.

Port scans are the normal method of assuring existence of required services and absence of unneeded services. A port scan shall be run before the FAT with a representative, fully functional system configuration. All input/output (I/O) ports need to be scanned for UDP and TCP. The scan needs to be run before the FAT and again prior to the SAT. *Note that port scans can rarely be used on production systems. In most cases, scanners will disrupt operations.*

2.1.3 Procurement Language

Post-contract award, the Vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the control system.

The Vendor shall provide a listing of services required for any computer system running control system applications or required to interface the control system applications. The listing shall include all ports and services required for normal operation as well as any other ports and services required for emergency operation. The listing shall also include an explanation or cross reference to justify why each service is necessary for operation.

The Vendor shall verify and provide documentation that all services are patched to current status.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the control system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but is not limited to:

1. Games
2. Device drivers for network devices not delivered
3. Messaging services (e.g., MSN,[h] AOL IM, etc.)
4. Servers or clients for unused Internet services
5. Software compilers in all user workstations and servers except for development workstations and servers
6. Software compilers for languages that are not used in the control system
7. Unused networking and communications protocols
8. Unused administrative utilities, diagnostics, network management, and system management functions
9. Backups of files, databases, and programs used only during system development
10. All unused data and configuration files
11. Sample programs and scripts
12. Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).

2.1.4 FAT Measures

The Vendor shall verify that the Purchaser requires the results of cyber security scans (as a minimum a vulnerability and active port scan, with the most current signature files) run on the control system as a primary activity of the FAT. This assessment is then compared with an inventory of the required services, patching status, and documentation, to validate this requirement. Other measures provided include:

1. The Vendor shall provide for each networked device or class of device (e.g., server, workstation, and switch) the following configuration documentation lists:
    a. Network services required for the operation of that device. Indicate the service name, protocol (e.g., TCP and UDP) and port range
    b. Dependencies on underlying operating system services
    c. Dependencies on networked services residing on other network devices
    d. All of the software configuration parameters required for proper system operation
    e. Certified OS, driver, and other software versions installed on the device
    f. Results found by the vulnerability scans with mitigations affected.
2. The Vendor shall install Firmware updates available for the computer or network device certified by the system manufacturer at the time of installation and provide documentation.
3. The Vendor shall provide a summary table indicating each communication path required by the system. Include the following information in this table:

[h] Product Disclaimer

References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, any agency thereof.

a. Source device name and Media Access Control (MAC) and/or IP address

b. Destination device name and MAC and/or IP address

c. Protocol (e.g., TCP and UDP) and port or range of ports.

4. The Vendor shall perform network-based validation and documentation steps on each device:

   a. Full TCP and UDP port scan on Ports 1–65535. This scanning needs to be completed during a simulated “normal system operation.”

2.1.5 SAT Measures

The Vendor shall compare the results of cyber security scans run on the system, as a primary activity of the SAT, with an inventory of the required services, patching status, and required documentation. At the conclusion of the SAT and before cutover or commissioning, the above cyber security scans (with the most current signature files) must be run again.

2.1.6 Maintenance Guidance

Document the system operating system and software patches as the system software evolves to allow traceability and to verify no extra services are reinstalled. Anytime the system is upgraded it is recommended that system Vendors rerun appropriate subsets of the FAT on the baseline system before delivery to Purchaser.

2.1.7 References

North American Electric Reliability Corporation (NERC) CIP-007-1 R2, “Electronic Access Controls,” Cyber Security—Critical Infrastructure Protection, June 1, 2006.[i]

ANSI/ISA-99.00.01, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 5,[j]

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3, B.14, C.3.

National Institute of Standards and Technology (NIST)[k]—Special Publications (SP), 800-42, “Guideline on Network Security Testing.”

2.1.8 Dependencies

None, this topic is stand-alone.

2.2 Host Intrusion Detection System

A host intrusion detection system (HIDS) can be installed to perform a variety of integrity checks to detect attempted unauthorized access.

[i] NERC CIP standards are available at http://www.nerc.com/~filez/standards/Reliability_Standards.html

[j] Instrumentation, Systems, and Automation Society (ISA) standards are available at http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=8997

[k] NIST publications are located at, http://csrc.nist.gov/publications/nistpubs/

2.2.1 Basis

In unmonitored systems, it is difficult to detect unauthorized changes or additions to the operating system or application programs. The vulnerability scans suggested in the prior section only identify what is known. Continuous monitoring is necessary to detect emerging unauthorized changes or additions, or unauthorized escalation of process privileges.

2.2.2 Language Guidance

Typically, the HIDS operates by performing checks on files to detect tampering, escalations of privileges, and unauthorized account access; by intercepting sensitive operating system functions; or by some combination of both. Additional HIDS capabilities may include monitoring attempts to access the system remotely (e.g., “scanning”).

Note that the resources required to configure the HIDS is minor compared to the resources required for ongoing log reviews, as log files generated by the HIDS can be voluminous. Log review and notification software tools may be appropriate. Also, sending log entries in real time over a network can overwhelm the network. Thus, it may be necessary to write logs to a local storage device such as a Universal Serial Bus (USB) or Digital Video Disc (DVD) drive. If possible, storage devices shall be configured as “append-only” to prevent alteration of records.

2.2.3 Procurement Language

Post-contract award:

- The Vendor shall provide a configured HIDS and/or provide the information to configure a HIDS to include, but not be limited to, static file names, dynamic file name patterns, system and user accounts, execution of unauthorized code, host utilization, and process permissions sufficient for configuring the HIDS.
- The Vendor shall configure the HIDS such that all system and user account connections are logged. This log will be configured such that an alarm can be displayed to the operator or security personnel if an abnormal situation occurs.
- The Vendor shall recommend a configuration for the HIDS in a manner that does not negatively impact the operating system functions or business objectives.
- The Vendor shall recommend log review and notification software tools.
- The Vendor shall configure devices as “append only” to prevent alteration of records on local storage devices.

2.2.4 FAT Measures

The Vendor shall verify and provide documentation that for Vendor-supplied HIDS; the Vendor shall run the HIDS during the entire FAT process and periodically interject applicable malware.

The Vendor shall examine log files and validate the expected results. FAT procedures shall include validation and documentation of this requirement.

2.2.5 SAT Measures

The Vendor shall verify and provide documentation that for Vendor-supplied HIDS, the Vendor shall run the HIDS during the entire SAT process and periodically interject applicable malware.

The Vendor shall examine log files and validate the expected results. SAT procedures shall include validation and documentation of this requirement.

The Vendor shall generate a system image at the conclusion of the SAT to be used later as a control baseline.

2.2.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, rules updates and patches to the HIDS as security issues are identified to maintain the established level of system security.

2.2.7 References

NERC CIP-005-1 R3, "Monitoring Electronic Access."

NERC CIP-007-1 R6, "Security Status Monitoring."

ANSI/ISA-99.00.01, "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 3."

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections C.3."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook."

NIST SP 800-82, "Draft Guide to Industrial Control Systems (ICS) Security."

NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)."

2.2.8 Dependencies

Section 3.2, "Network Intrusion Detection Systems."

2.3 Changes to File System and Operating System Permissions

Hardening file system configurations and restricting operating system permissions reduce the vulnerabilities associated with default configurations.

2.3.1 Basis

Configurations for out-of-the-box operating systems and file systems normally are more permissive than necessary allowing exploitation.

2.3.2 Language Guidance

In many cases, the operating system is shipped with the default configurations that allow unneeded access to files, and loose configuration parameters that can be exploited to gain information for further attacks. Common examples include operating system recovery procedures, elevated-permission user or system accounts, diagnostic tools, remote access tools, and direct access to network device addresses. Hardening tasks include changing or disabling access to such files and functions.

2.3.3 Procurement Language

The Vendor shall configure hosts with least privilege file and account access and provide documentation of the configuration.

The Vendor shall configure the necessary system services to execute at the least user privilege level possible for that service and provide documentation of the configuration.

The Vendor shall document that changing or disabling access to such files and functions has been completed.

2.3.4 FAT Measures

The Vendor shall provide, as a part of the FAT procedures, validation and documentation of the permissions assigned.

2.3.5 SAT Measures

The Vendor shall provide, as a part of the SAT procedures, validation and documentation of the permissions assigned.

2.3.6 Maintenance Guidance

The Vendor shall reassess permissions and security settings on the baseline system before delivery of any upgrades.

2.3.7 References

NERC CIP-007-1 R5.2, “Account Management.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3, B.14, C.3.”

2.3.8 Dependencies

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

2.4 Hardware Configuration

Unnecessary hardware can be physically disabled, removed, or its configuration altered through software.

2.4.1 Basis

Most control system network devices have multiple communication and data storage capabilities. These can be utilized to introduce vulnerabilities such as viruses, root kits, malware, bots, key-loggers, etc.

2.4.2 Language Guidance

Hardware configuration activities may include configuring the network devices to limit access from only specific locations (e.g., IP filtering) or requiring additional verification of user credentials (e.g., password, PIN, crypto key, or token). Local hardening can require similar verification for protecting system Basic Input/Output System (BIOS) configuration parameters, and limiting system access through local media (e.g., disabling/removing USB ports, CD/DVD drives, and other removable media devices). It may be desirable to physically lock devices with accessible drives or ports, such that only the human-machine interface (HMI) is accessible.

It is recommended that system administrators be able to re-enable devices if the devices are disabled by software.

2.4.3 Procurement Language

The Vendor shall disable, through software or physical disconnection, all unneeded communication ports and removable media drives, or provide engineered barriers, and provide documentation of the results.

The Vendor shall password protect the BIOS from unauthorized changes unless it is not technically feasible, in which case the Vendor shall document this case and provide mitigation measures.

The Vendor shall provide a written list of all disabled or removed USB ports, CD/DVD drives, and other removable media devices.

The Vendor shall configure the network devices to limit access to/from specific locations, where appropriate, and provide documentation of the configuration.

The Vendor shall configure the system to allow the system administrators the ability to re-enable devices if the devices are disabled by software and provide documentation of the configuration.

2.4.4 FAT Measures

The Vendor shall provide, as a part of the FAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.

2.4.5 SAT Measures

The Vendor shall provide, as a part of the SAT procedures, validation and documentation of the disabled or locked physical access and the removed drivers.

2.4.6 Maintenance Guidance

The Vendor shall verify and provide documentation that any replacement device is configured the same and exhibits the same behaviors as the original.

2.4.7 References

NERC CIP-005-1, “Electronic Security Perimeter(s).”

NERC CIP-006-1, “Physical Security of Critical Assets.”

2.4.8 Dependencies

None, this topic is stand-alone.

2.5 Heartbeat Signals

Heartbeat signals indicate the communication health of the system.

2.5.1 Basis

Heartbeat signals or protocols can be corrupted, spoofed, or possibly used as an entry point for unauthorized access.

2.5.2 Language Guidance

Heartbeat status signals can be sent over serial connections or routed protocols. These are often used in reporting-by-exception schemes, and may be used by third-party add-on applications. Heartbeat signals can be configured in the hardware, software, or firmware.

2.5.3 Procurement Language

The Vendor shall identify heartbeat signals or protocols and recommend whether any should be included in network monitoring.

Post-contract award, the Vendor shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic if the signals are included in the network monitoring.

2.5.4 FAT Measures

The Vendor shall provide, as a part of the FAT procedures, documentation of the requirements.

The Vendor shall create a baseline of the heartbeat communications traffic, to include frequency, packet sizes, and expected packet configurations.

2.5.5 SAT Measures

The Vendor shall provide, as a part of the SAT procedures, documentation of the requirements.

The Vendor shall create a baseline of the heartbeat communications traffic and validate the results against FAT documentation.

2.5.6 Maintenance Guidance

The periodicity of the heartbeat communications is normally configurable. The Vendor shall provide a recommended frequency for monitoring. If changed, the network monitoring shall be modified and documented by the appropriate party.

2.5.7 References

NERC CIP-007-1 R6, “Security Status Monitoring.”

2.5.8 Dependencies

Section 0, “Host Intrusion Detection System.”

Section 3.2, “Network Intrusion Detection System.”

2.6 Installing Operating Systems, Applications, and Third-Party Software Updates

Patches and software updates, including those for anti-virus scanners, are required to reduce attack surface.

2.6.1 Basis

Most successful cyber attacks occur in non-patched systems or applications.

2.6.2 Language Guidance

As control system applications come under increased scrutiny by the hacker community, it can be expected that any vulnerabilities and exploits will become common knowledge among that community quickly, as has been shown within the IT community. Responsible system and product Vendors regularly release updates, patches, service packs, or other fixes to their products to address known and potential vulnerabilities. Of course, to be effective, these must be installed in a timely fashion.

Most common operating systems ship with a number of well-known vulnerabilities; even a new system is likely to be vulnerable based on the services that are active and because patches are not likely to be current. Therefore, an essential system hardening activity is simply installing the latest versions or updates of any necessary software loaded on a system. Of course, testing and validation of the patches and upgrades are necessary prior to performing the updates on a production system.

In many cases, Vendor support is limited to the installation of specific software releases. Therefore, updates can only be reliably applied based on the requirements of that particular software product. Patches have been known to introduce security vulnerabilities or reverse security features making it important to understand all processes (services, ports, permissions, etc.) affected by the patch.[l]

Scanning is an effective tool to identify vulnerabilities. Use caution however, as active scanning of live control system networks has been known to disable the networks during operations. FAT and SAT provide critical opportunities for active scanning tests without an impact to production. Even passive scanning is not recommended on production systems until the impact to operations is fully understood.

2.6.3 Procurement Language

The Vendor shall have a patch management and update process.

Pre-contract award, the Vendor shall provide details on their patch management and update process. Responsibility for installation and update of patches shall be identified.

Post-contract award, the Vendor shall provide notification of known vulnerabilities affecting Vendor-supplied or required OS, application, and third-party software within a prenegotiated period after public disclosure.

Post-contract award, the Vendor shall provide notification of a patch(es) affecting security within a prenegotiated period as identified in the patch management process. The Vendor shall apply, test, and validate the appropriate updates and/or workarounds on a baseline reference system before distribution. Mitigation of these vulnerabilities shall occur within a prenegotiated period.

2.6.4 FAT Measures

The Vendor shall install and update all tested and validated security patches prior to the start of the FAT.

The Vendor shall verify and provide documentation that all updates have been tested and installed.

The Vendor shall perform contractually agreed upon security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase.

The Vendor shall provide documentation of the results of the scans.

[l] http://www.theregister.co.uk/2004/09/02/winxpsp2_security_review/

The Vendor shall document the system after the FAT to support future validation of patches. (In many instances, this is referred to as the system baseline.)

2.6.5 SAT Measures

The Vendor shall install and update all tested and validated security patches at the start of the SAT.

The Vendor shall provide documentation that all the updates have been tested and installed.

The Vendor shall verify system functionality, based upon prenegotiated procedures, at the conclusion of patch updates, and provide documentation of the results.

The Vendor shall perform security scans (with the most current signature files) to verify that the system has not been compromised during the testing phase of the results.

The Vendor shall document the system after the SAT to support future validation of patches. (In many instances, this is referred to as delivered system configuration.)

2.6.6 Maintenance Guidance

The Vendor shall provide a patch management process to include policies and procedures for the system after installation. These policies and procedures shall include the patch management process and mitigation strategies for instances when the Vendor informs the user not to apply released patches.

The Vendor shall provide a level of support for testing patch releases. This shall include the level of revision on a documented system configuration (i.e., Vendor platform, FAT system, SAT system, current production).

Users are encouraged to install received security updates on a non-production system for testing and validation prior to installation on production systems.

2.6.7 References

NERC CIP-007-1 R3, “Security Patch Management.”

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 6.5.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 3.29, 3.43, 5.3, B.14, B.17, B.19, C.3. ”

2.6.8 Dependencies

Section 4.5, “Role-Based Access Control for Control System Applications.”

Section 5.1, “Coding for Security.”

Section 6.1, “Notification and Documentation from Vendor.”

3. PERIMETER PROTECTION

Perimeter Protection refers to providing a clear demarcation between the protected internal network and unprotected and untrusted external networks.

3.1 Firewalls

Firewalls are used to stop unauthorized connections, or to allow limited communications between two networks or from a network to a networked device. Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways, and stateful multilayer inspection firewalls. Firewalls can be implemented in software, hardware or a combination of both.

3.1.1 Basis

Overly permissive, non-existent, or unpatched firewalls create vulnerabilities by allowing unauthorized access.

3.1.2 Language Guidance

Firewalls are network devices, which block selective (filter) traffic between network zones (subnets) or from a network to a device. Historically, firewalls, or simple "screening routers," blocked traffic based on IP address and port combinations.

Although any network device that filters traffic may be referred to as a firewall; modern usage typically assumes some advanced potentials beyond these rudimentary capabilities. These are often described as "application aware," "stateful inspection," or other Vendor variations. These capabilities take into account not only the IP addresses and ports used in a connection, but track the address that originated a connection (allowing control of direction), state of the connection, and any number of other factors. Advanced products also perform verification of the packet payload (which means verifying that higher-level protocols are enforced), and provide protection to specific protocols such as simple mail transfer protocol (SMTP), file transfer protocol (FTP), and others. Although most commercial products provide only limited protection for industrial protocols, such as those commonly used in control system networks, this is changing as manufacturers respond to market demand.

Firewalls produce traffic logs that are vital for network monitoring. All traffic through the firewall needs to be logged, including outbound traffic. These logs, if effectively and efficiently designed to be used with HIDS, NIDS, application logs, etc., are essential for forensic purposes.

Network Appliances or "all in one solutions" can combine antivirus, firewall, and NIDS functionality. The signature file updates for such appliances are large and can rarely be sent over a control system network. Testing signature updates on a non-production system can be done to verify limitations of signature file size. In such instances, alternative methods of updating signature files may be necessary.

3.1.3 Procurement Language

The Vendor shall provide firewalls and firewall rule sets between network zones or provide firewall rule sets if the firewalls are not provided by the Vendor.

The Vendor shall provide firewall rule sets and/or other equivalent documentation. The basis of the rule set shall be "deny all," with exceptions explicitly identified by the Vendor. Note that this information is deemed business sensitive and shall be protected as such.

Post-contract award, the Vendor shall provide detailed information on all communications (including protocols) required through a firewall, whether inbound or outbound, and identify each network device initiating a communication in accordance with the corresponding rule sets.

3.1.4 FAT Measures

The Vendor shall install the firewall(s) or the configuration(s) and run the firewall(s) continuously during the entire FAT process for Vendor-supplied firewall(s), or Vendor provided firewall configuration(s).

The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

3.1.5 SAT Measures

The Purchaser shall run the firewall(s) during the entire SAT process.

The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time.

3.1.6 Maintenance Guidance

There shall be an ongoing patch management and signature update process.

3.1.7 References

NERC CIP-005-1 R1, “Electronic Security Perimeter.”

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 3.5, 5.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections B.1, B.14, C.3, D.4.”

NIST SP 800-41 Rev 1, “Guidelines on Firewalls and Firewall Policy (Draft).”

NIST SP 800-82, “Draft Guide to Industrial Control Systems (ICS) Security.”

3.1.8 Dependencies

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

3.2 Network Intrusion Detection System

A network intrusion detection system (NIDS) is used to identify unauthorized or abnormal network traffic.

3.2.1 Basis

Firewalls or other vulnerabilities may allow unauthorized access, which are detectable by a NIDS.

3.2.2 Language Guidance

A NIDS is not always part of a control system. It can be included as part of the higher-level IT infrastructure, and thus outside the scope of this guide. This section assumes the NIDS is part of the control system network.

There are two basic types of NIDSs: signature and anomaly-based. Signature-based NIDSs are similar to antivirus and vulnerability scanners in that only known signatures are detected. The signatures are essentially strings of code known to be indicative of malicious traffic. Anomaly-based NIDSs function on historically-based network traffic and alarm when traffic is outside of the expectations. Anomaly-based NIDSs require running a network to record known, good traffic to which to compare future traffic. The challenge for anomaly-based detection is defining what is normal. This makes it very difficult to establish a baseline if normal network behavior constantly changes. However, anomaly-based NIDSs work well for deterministic networks with few report-by-exception events.

As with any appliance that can generate voluminous logs, the configuration of the NIDS is a minor effort as compared to the degree of effort required for ongoing log reviews. Log review and notification software tools may be appropriate to semi-automate the review of voluminous data.

3.2.3 Procurement Language

Pre-contract award, the Vendor shall provide a recommended placement of the NIDS within the control system network.

The Vendor shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries, for anomaly-based NIDSs.

The Vendor shall provide appropriate signatures, for signature-based NIDSs.

Post-contract award, the Vendor shall provide a configured NIDS and/or provide the information to configure a NIDS.

3.2.4 FAT Measures

The Vendor shall install the NIDS or the configuration(s) and run the NIDS continuously during the entire FAT process for Vendor-supplied NIDSs, or Vendor-provided NIDS configuration(s).

The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

3.2.5 SAT Measures

The Vendor shall run the NIDS(s) during the entire the SAT process to include exercising this functionality, examining the log files, and validating the results.

The Vendor shall document the results of tuning signatures and adjusting thresholds to reduce false positives and minimize false negatives.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time.

3.2.6 Maintenance Guidance

The Vendor shall tune signatures and adjust thresholds to reduce false positives and minimize false negatives.

The Vendor shall update the NIDS configuration and/or documentation as needed when changes are made.

3.2.7 References

NERC CIP-005-1 R1, "Electronic Security Perimeter."

ANSI/ISA-99.00.01, "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Sections B.10, C.3."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook."

NIST SP 800-82, "Draft Guide to Industrial Control Systems (ISC) Security."

NIST SP 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)."

3.2.8 Dependencies

Section 4.1, "Disabling, Removing, or Modifying Well-Known or Guest Accounts."

3.3 Canaries

Honey pots (which analyze unauthorized connections) and/or Canary(ies) (which flag that a connection attempt has taken place) have been implemented in certain network configurations to provide passive network monitoring.

3.3.1 Basis

Canaries enhance network traffic screening since most signatures created for a NIDS are immature and only detect proper protocol versions limiting network-monitoring capabilities.

3.3.2 Language Guidance

Canaries only work in a static address topology or where dynamic host configuration protocol (DHCP) is not used. It is not recommended that retaliatory devices or actions (poison boxes) be used. Canary(ies) can be a stand-alone computer or an unused network interface card (NIC) in existing hardware.

3.3.3 Procurement Language

Pre-contract award, the Vendor shall provide a recommended placement of the canary(ies) within the control system network.

The canary(ies) shall be configured with alerting software to indicate unauthorized connection attempts.

Post-contract award, the Vendor shall provide a configured canary(ies) or information to configure a canary(ies).

3.3.4 FAT Measures

The Vendor shall install the canary(ies) or the configuration(s) and run the canary(ies) continuously during the entire FAT process for Vendor-supplied canary(ies) or Vendor-provided canary configuration(s).

The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that FAT procedures include written validation and documentation of the requirements.

3.3.5 SAT Measures

The Vendor shall run the canary(ies) during the entire SAT process.

The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that SAT procedures include written validation and documentation of the requirements. Any Vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time.

3.3.6 Maintenance Guidance

The Vendor shall reconfigure canary(ies) as needed when network address topologies change.

3.3.7 References

NERC CIP-005-1 R2, “Electronic Access Controls.”

3.3.8 Dependencies

Section 0, “Host Intrusion Detection Systems.”

Section 3.2, “Network Intrusion Detection System.”

4. ACCOUNT MANAGEMENT

Account Management is essential to properly maintain and secure a control systems network. Account management regulates who has access, limits permission to only those required, and mitigates vulnerabilities in default accounts. It also covers password management.

With careful account management, default accounts and passwords, which typically exist in control systems and pose a substantial risk, can be eliminated or mitigated.

Control of user access can be broken into three major topics:

1. **Authentication**. Is the ability to verify an identity based on the following attributes: “what you have” (i.e., key, digital certificate, or smart card), “what you know” (i.e., username and password), and “what you are” (i.e., biometric iris, fingerprint scan, or fingerprints), and/or “what you do” (i.e. dynamic biometric handwriting scan or voice recognition).
2. **Authorization**. Is the ability to control user permissions within the system to include network access. Authorization capabilities and processes vary widely between products, from none in the case of an “all-or-nothing” access, to a very specific control of user capabilities in more advanced cases.
3. **Accounting**. The ability to provide an audit trail of activities within the system. Accounting is typically accomplished through logging activities of significance, such as a login, changing passwords, or making significant system changes. Accounting is related to auditing.

4.1 Disabling, Removing, or Modifying Well-Known or Guest Accounts

Disabling, removing or modifying well-known or guest accounts and changing default passwords are necessary to reduce system vulnerabilities.

4.1.1 Basis

Default accounts and passwords are available on many control systems and are often publicly available in published materials allowing unauthorized system access.

4.1.2 Language Guidance

Default, guest, or anonymous accounts are commonly used to gain limited access and potentially useful system privileges. These can be used in turn to escalate privileges and gain unauthorized access to additional information. Hardening activities to address these concerns include disabling, removing, or modifying such accounts or changing default passwords.

Remote access and perimeter devices have unique account management requirements. These topics are addressed in other sections (see Sections 9 “End Devices” and Section 10 “Remote Access”).

4.1.3 Procurement Language

The Vendor shall recommend which accounts need to be active and those that can be disabled, removed, or modified. The Purchaser shall approve in writing the Vendor’s recommendation.

The Vendor shall disable, remove, or modify all the accounts pursuant to the approved recommendation.

Post-contract award, the Vendor shall disable or remove all default and guest accounts prior to the FAT. Once changed, new accounts will not be published except that new account information and passwords will be provided by the Vendor via protected media. After the SAT the Vendor shall disable, remove, or modify all Vendor-owned accounts or negotiate account ownership with the Purchaser.

4.1.4 FAT Measures

The Vendor shall verify that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that FAT procedures include written validation and documentation of the requirements.

4.1.5 SAT Measures

The Vendor shall verify that SAT procedures include exercising this functionality, examining the log files, and validating the results.

The Vendor shall verify that SAT procedures include written validation and documentation of the requirements.

4.1.6 Maintenance Guidance

The Vendor shall not introduce any new accounts without explicit requirements to do so by the Purchaser or designated authorized individual.

4.1.7 References

NERC CIP-007 R5, “Account Management.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3.11, B.14.2, B.14.4, C.3.11.”

NIST SP 800-82, “Draft Guide to Industrial Control Systems (ICS) Security.”

4.1.8 Dependencies

Section 4.3, “Password/Authentication Policy and Management.”

Section 9, “End Devices.”

Section 10, “Remote Access.”

4.2 Session Management

Weak session practices and insecure protocols exist on many systems for convenience, backwards compatibility, and on legacy systems.

4.2.1 Basis

Unauthorized access can be achieved through clear-text accounts and passwords along with weak session security practices.

4.2.2 Language Guidance

Many legacy system utilities transport user credentials in clear text, using protocols such as FTP and TELNET—this is not acceptable. Other weak session practices include concurrent session logins, remembered account information between login, auto-filling of fields during logins, and anonymous services such as FTP. In many systems, you are your account, and once the account is compromised, the system has no way of knowing who is actually using the account.

By using access protocols that encrypt or securely transmit user-login credentials (names and passwords), such vulnerabilities can be reduced. Other hardening activities include disabling the use of insecure protocols to access network devices, enabling secure protocols (Secure Sockets Layer [SSL] or tunneling through Secure Shell Terminal Emulation [SSH] for instance), and setting appropriate system parameters to enforce minimum levels of encryption. Note that certain applications such as alarms and HMIs should not time out, black out, or otherwise be blocked.

4.2.3 Procurement Language

The Vendor shall not permit user credentials to be transmitted in clear text.

The Vendor shall provide the strongest encryption method commensurate with the technology platform and response time constraints.

The Vendor shall not allow multiple concurrent logins, applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.

The Vendor shall provide user account-based logout and timeout settings.

4.2.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

4.2.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

4.2.6 Maintenance Guidance

The Vendor shall not introduce any new session algorithms without explicit requirements to do so by the Purchaser or a designated authorized individual.

The Vendor shall change encryption keys at reasonable intervals commensurate with need.

4.2.7 References

NERC CIP-007 R5, “Account Management.”

NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook.”

NIST SP 800-15, “Minimum Interoperability Specification for PKI Components (MISPC), Version 1.”

NIST SP 800-32, “Introduction to Public Key Technology and the Federal PKI Infrastructure.”

NIST SP 800-67, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher.”

4.2.8 Dependencies

Section 4.3, “Password/Authentication Policy and Management.”

4.3 Password/Authentication Policy and Management

Instant availability requirements in control systems often result in a weak password policy.

4.3.1 Basis

Weak passwords introduce vulnerabilities to the control systems network. In addition, sometimes passwords are hard-coded into software to facilitate control system internal communications allowing anyone with access to the code/configuration files knowledge of the password(s).

4.3.2 Language Guidance

This requirement can apply to any of several authentication methods. Users often select poor or easily-guessed passwords even with the best of intentions. Commonly, an automated “brute force” attack can be used to guess user passwords by using common dictionary terms, sequential password patterns, and other means, often revealing the correct password within minutes. By enforcing password complexity limits, restricting user-login attempts, and locking out accounts after repeated failed attempts such attacks can be thwarted.

4.3.3 Procurement Language

The Vendor shall provide a configurable account password management system that allows for selection of password length, frequency of change, setting of required password complexity, number of login attempts, inactive session logout, screen lock by application, and denial of repeated or recycled use of the same password.

The Vendor shall not store passwords electronically or in Vendor-supplied hardcopy documentation in clear text unless the media is physically protected.

The Vendor shall control configuration interface access to the account management system.

The Vendor shall provide a mechanism for rollback of security authentication policies during emergency system recovery or other abnormal operations, where system availability would be negatively impacted by normal security procedures.

4.3.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation of the password and authentication policy and management.

4.3.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation of the password and authentication policy and management.

4.3.6 Maintenance Guidance

The Vendor shall not introduce changes to password or authentication policy and management without explicit requirements to do so by the Purchaser or other designated authorized individual.

4.3.7 References

NERC CIP-007 R5, “Account Management.”

FIPS PUB 112, “Password Usage Standard.”

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Sections 5.7.4, 6.5.3”.

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3.11, B.14.1, B.14.2, B.14.4, C.2, C.3.11.”

NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook.”

NIST SP 800-53 Revision 2, “Recommended Security Controls for Federal Information Systems.”

NIST SP 800-63 Version 1.0.2, “Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology.”

NIST SP 800-82, “Draft Guide to Industrial Control Systems (ICS) Security.”

4.3.8 Dependencies

Section 5, “Coding Practices.”

4.4 Account Auditing and Logging

Account auditing and logging allow the Purchaser/Operator to verify that authorized operations have been maintained. Logging is also necessary for forensic analysis and anomaly detection.

4.4.1 Basis

Logging and auditing of both active and disabled accounts are useful for anomaly and unauthorized access detection. However, cyber attackers commonly modify audit logs to cover activities.

4.4.2 Language Guidance

Account logging must provide an audit trail of user activity that allows specific actions to be traced to a single user/process, location, and time in a verifiable manner.

Advanced cyber security attackers will modify log files to make forensics activities difficult. Monitoring of log access will detect malicious modifications. Writing log files to read-only media also prevents malicious modification.

4.4.3 Procurement Language

The Vendor shall provide a system whereby account activity is logged and is auditable both from a management (policy) and operational (account use activity) perspective.

The Vendor shall time stamp, encrypt, and control access to audit trails and log files.

The Vendor shall ensure audit logging does not adversely impact system performance requirements.

The Vendor shall provide read-only media for log creation.

4.4.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

The Vendor shall record system performance measurements that include the system with and without logging activities.

4.4.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

The Vendor shall record system performance measurements to verify that logging activities do not adversely impact system performance.

4.4.6 Maintenance Guidance

The Vendor shall archive auditing and logging records.

The Vendor shall configure audit policies and review audit data on a regular basis.

4.4.7 References

NERC CIP-007 R5, "Account Management."

ANSI/ISA-99.00.01, "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Section 5.7"

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 4.15, 4.19, 5.3.12, 5.3.15, B.3, B.5, B.15.4, B.19, C.3.3, C.3.8, C.3.13, C.3.15, C.3.17."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook."

NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

NIST SP 800-61, "Computer Security Incident Handling Guide."

NIST SP 800-82, "Draft Guide to Industrial Control Systems (ICS) Security."

NIST SP 800-92, "Guide to Computer Security Log Management."

4.4.8 Dependencies

None, this topic is stand-alone.

4.5 Role-Based Access Control for Control System Applications

Role-based access control (RBAC) refers to the system's ability to make access decisions based on the role(s) of individual users/processes in the control system environment. Using RBAC results in significant improvements in security. The use of roles to control access can be an effective means for developing and enforcing system wide security policies and for streamlining security management processes. RBAC limits the exposure to risk associated with unauthorized actions by assigning the least privileges corresponding to the assigned duty or function. The use of RBAC for administrative functions is not common on legacy systems.

4.5.1 Basis

Legacy control systems typically do not have RBAC, which allows any user full access, control, and administrative privileges. Thus if an unauthorized user achieves login, that user would have full access to the system.

4.5.2 Language Guidance

User credentials consist of account names, passwords/pass phrases and other factors used to authenticate a user to the network or to a network device. Credentials are the most basic form of security control used to protect systems. User accounts and identification required by control system applications, system operator access, database maintenance, display maintenance, and overall system operation and maintenance with access to resources and functionality must be appropriate for the user’s role (i.e., areas of responsibility and authority). Thus, each role may need unique access and permission levels. Note that logging must nevertheless resolve individual users and applications as resources are accessed.

Once the RBAC scheme is established, it shall be protected (e.g., encrypted). Only approved administrators, who are aware of how roles and permissions can affect the security of the control system, shall be allowed to change the RBAC scheme.

4.5.3 Procurement Language

The Vendor shall provide for user accounts with configurable access and permissions associated with the defined user role.

The Vendor shall adhere to least privileged permission schemes for all user accounts, and application-to-application communications.

The Vendor shall configure the system so that initiated communications start with the most privileged application controlling the communication. Upon failed communication, the most privileged side will restart communications.

The Vendor shall verify that the master network device initiates communications. The Vendor shall inform the Purchaser if this condition cannot be met.

The Vendor shall verify that a user cannot escalate privileges, under any circumstances, without logging into a higher-privileged role first.

The Vendor shall provide a mechanism for changing user(s) role (e.g., group) associations.

Post-contract award, the Vendor shall provide documentation defining access and security permissions, user accounts, applications, and communication paths with associated roles.

4.5.4 FAT Measures

The Vendor shall compare the control system assessment during this period with required documentation to validate the requirements.

The Vendor shall baseline user roles and permissions and negotiate agreements on modifications with the system Purchaser/Operators.

4.5.5 SAT Measures

The Vendor shall verify that all additions to the control system, after the completion of the FAT, have the same rigor of documentation that was necessary pre-FAT and appropriate comparisons are required post-SAT to validate the requirement.

4.5.6 Maintenance Guidance

The Vendor shall verify that all additions to the control system during the warranty/maintenance period have the same rigor of documentation, as stated in this requirement.

4.5.7 References

NERC CIP-007 R5, "Account Management."

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3.11, B.14.2, B.14.4, C.3.117."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook."

NIST SP 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."

NIST SP 800-27 Rev A, "Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A."

NSIT SP 800-82 (Draft), "Guide to Industrial Control Systems (ICS) Security."

4.5.8 Dependencies

None, this topic is stand-alone.

4.6 Single Sign-On

Single sign-on (SSO) refers to a means of user authentication such that a single login allows a user to have authorized role-based access across a network or between programs and systems, without requiring re-authentication to each application.

4.6.1 Basis

Single sign-on authentication has been commonly designed for convenience, sometimes at the expense of security, and potentially provides an avenue for the introduction of vulnerabilities. However, careful attention to system design can lead to single sign-on schemes that enhance security.

4.6.2 Language Guidance

To enhance security, single sign-on shall be used with RBAC and a two-factor authentication. For configured users of the system, permissions should be validated and show equivalent results in running validation tests against a direct login and a single sign-on login, on each terminal and for each application. Single sign-on may not prohibit the weak session practice of concurrent logins. SSO can also be between enterprise systems using federated authentication not currently applicable in control systems.

4.6.3 Procurement Language

The Vendor shall provide an SSO such that RBAC enforcement is equivalent to that enforced as a result of direct login.

The Vendor shall provide a means of allowing SSO to a suite of applications via SSH, terminal services, or other authenticated means. This system should be RBAC capable.

The Vendor shall provide documentation on configuring such a system, and documentation showing equivalent results in running validation tests against the direct login and the SSO.

The Vendor shall protect key files and access control lists (ACLs) used by the SSO system from nonadministrative user read, write, and delete access. Note that SSO must resolve individual user's logins to each application.

4.6.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation that the SSO permissions and session management are handled properly.

4.6.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation that the SSO permissions and session management are handled properly.

4.6.6 Maintenance Guidance

The Vendor shall not introduce changes to the SSO process without explicit requirements to do so by a Purchaser’s system administrator or other designated authorized individual.

4.6.7 References

NERC CIP-007 R5, “Account Management.”

4.6.8 Dependencies

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.2, “Session Management.”

Section 4.5, “Role-Based Access Control for Control System Applications.”

4.7 Separation Agreement

The Purchaser needs to have agreements with Vendors to protect their control systems security posture.

4.7.1 Basis

Integrators and companies that support control systems are very dynamic and competitive, resulting in frequent turnover of key support personnel potentially exposing sensitive information.

4.7.2 Language Guidance

Many stakeholders including Purchasers/Operators, Vendors, and contractors hold control systems-related sensitive information. Sensitivity needs to be maintained as individuals move to new positions or leave the organization. In addition, should a Vendor become unable to maintain control of its products (e.g., go out-of-business), the Vendor products used to construct the Purchaser’s control system would need to be accessible.

4.7.3 Procurement Language

Pre-contract award, the Vendor shall provide a separation agreement to delineate how Vendor employees who have sensitive knowledge of the Purchaser’s control systems and who leave their positions or have responsibilities changed will be prohibited from disclosing that knowledge, where disclosure could lead to a reduction in security.

The Vendor shall notify the Purchaser within a prenegotiated period when key personnel leave or change positions, should it possibly impact control system security.

The Vendor shall provide detailed documentation on how the control system security can be maintained and supported in the event the Vendor leaves the business (e.g., security-related procedures and products placed in escrow).

The Vendor shall return to the Purchaser any sensitive data in the Vendor’s possession when the Vendor is no longer able to maintain control of the Purchaser’s products.

4.7.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation of the ability to change key employee/support personnel access and permissions.

4.7.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation of the ability to change key employee/support personnel access and permissions.

4.7.6 Maintenance Guidance

The Vendor shall notify the Purchaser within a prenegotiated period when key personnel leave or change positions, should it possibly impact control system security.

4.7.7 References

NERC CIP-007 R4, “Malicious Software Prevention.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections C.2, C.3.5, C.3.13.”

NIST SP 800-12, “An Introduction to Computer Security: The NIST Handbook.”

4.7.8 Dependencies

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

5. CODING PRACTICES

Secure coding practices refer to techniques for building and validating high levels of security into software, beginning at the requirements phase, implemented during the coding phase, and finally validated during the FAT and SAT.

5.1 Coding for Security

Standard programming texts generally address data processing, but not security ramifications; this may mislead programmers into writing insecure code.

5.1.1 Basis

Software flaws are a primary avenue for gaining system access. Many control system security vulnerabilities are the direct result of writing software with inadequate attention to defense against deliberate and persistent malicious attack. These attacks include, but are not limited to:

- Buffer overflows, in which input fields are populated with long data sequences that overflow program buffers, often yielding program controls to the remote user (providing a useful command prompt in some cases).
- Data insertion and injection, in which input fields are populated with control or command sequences embedded in various ways that are nevertheless accepted by the application, or possibly passed to the OS, and that allow privileged malicious and unauthorized programs to be run on the remote system.

These vulnerabilities are particularly threatening because the control system can be compromised by bypassing normal access control checks, such as firewalls—control system traffic will appear normal as far as the network is concerned. Network protections such as proxies, which provide some defense against these vulnerabilities, are available for well-known protocols such as Web-based (HTTP) or e-mail (SMTP), but not for some lesser-known protocols.

5.1.2 Language Guidance

Software development process standards have been historically used as an indirect measure of the quality, safety, and security of computer source code written according to those process standards. One software process element, the code review, is widely recognized as an effective mechanism for assessing security, among other attributes. Code reviews can be accomplished through numerous means with varying degrees of automation. The Vendor shall provide documentation of code reviews and other software development process steps used to assess software security. Software subject to these reviews shall include both Vendor-developed applications and any other source code the Vendor has control over that forms a necessary part of the control system.

Many critical systems have software reviewed by the Purchaser or third-party prior to acceptance of the system. Third-party software integrated into Vendor products shall be assessed for security vulnerabilities. Experience has shown that system integration often contributes to the overall vulnerability of the system.

Because control system software, with regard to security, is very similar to other real-time distributed software systems, many existing security references apply. Most software security references include the following imperatives:

- Check inputs for reasonable values
- Encrypt data files

- Understand security impacts of OSs and other third-party libraries
- Make sure OSs and other third-party libraries have an update policy
- Forbid buffer overflow
- Verify log files are unalterable
- Use end-to-end authentication and integrity checks on process-to-process data communications
- Verify no clear-text passwords or encryption keys are embedded in the code or communicated
- Use design and code reviews.

5.1.3 Procurement Language

Pre-contract award, the Vendor shall provide documentation of development practices and standards applied to Vendor-written control system software, including firmware, used to ensure a high level of defense against unauthorized access.

The Vendor shall provide the results of Code Reviews.

Post-contract award, the Vendor shall provide documentation of coding practices used in developing the delivered software.

5.1.4 FAT Measures

The Vendor shall verify that FAT procedures include validation and documentation of the software development process and/or code review.

5.1.5 SAT Measures

The Vendor shall verify that SAT procedures include validation and documentation of the software development process and/or code review.

5.1.6 Maintenance Guidance

The Vendor shall verify that software upgrades and patches are validated according to the same software development process or review plan.

5.1.7 References

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Section B.17.4."

NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook."

NIST SP 800-42, "Guideline on Network Security Testing."

5.1.8 Dependencies

Section 4.3, "Password/Authentication Policy and Management."

6. FLAW REMEDIATION

Flaw Remediation refers to the actions to be performed and documentation to be produced when flaws are discovered in control system software, hardware, and system architectures created by or under the control of the Vendor.

6.1 Notification and Documentation from Vendor

Flaw remediation is a process by which flaws are documented and tracked for completion of corrective actions.

6.1.1 Basis

Vulnerabilities exist in control systems when flaws in software and/or hardware configurations are not patched. Many times intended patches are not applied in a timely manner due to operational issues. In many instances, workarounds and temporary fixes may become permanent solutions; however, the vulnerabilities may be reintroduced with future updates, upgrades, patches, and fixes.

6.1.2 Language Guidance

Awareness of application vulnerabilities, particularly security related flaws, is needed in a timely fashion. Guidance about corrective actions, fixes, or monitoring is needed to mitigate all vulnerabilities associated with the flaw. Auditable history of flaws and remediation steps are required to roll back patches. Vulnerabilities and flaws are normally closely held until remediation becomes available. However, some vulnerabilities are made public before a fix has been developed and then it becomes urgent to mitigate these vulnerabilities.

6.1.3 Procurement Language

The Vendor shall have and provide documentation of a written flaw remediation process.

The Vendor shall provide appropriate software updates and/or workarounds to mitigate all vulnerabilities associated with the flaw within a prenegotiated period.

Post-contract award, after the Vendor is made aware of or discovers any flaws, the Vendor shall provide notification of such flaws affecting security of Vendor-supplied software within a prenegotiated period. Notification shall include, but is not limited to detailed documentation describing the flaw with security impact, root cause, corrective actions, etc. (This language is typically found in a quality assurance document, but is included here for completeness.)

6.1.4 FAT Measures

The Vendor shall verify that for flaws known by the Vendor, the Vendor's corrective actions follow their process and the process is effective.

The Vendor shall verify that FAT documentation of the flaws validation and remediation are provided.

The Vendor shall verify that any changes to the core system code, logic, or configuration are analyzed to verify new vulnerabilities are not introduced into the system as a result of the change.

6.1.5 SAT Measures

The Vendor shall verify that for flaws known by the Vendor, the Vendor's corrective actions follow their process and the process is effective.

The Vendor shall verify that SAT documentation of the flaws validation and repair are provided.

The Vendor shall verify that any changes to the core system code, logic, or configuration are analyzed to verify new vulnerabilities are not introduced into the system as a result of the change.

6.1.6 Maintenance Guidance

The Vendor shall maintain for a prenegotiated period a master list of all flaws and corrective actions for auditing purposes.

6.1.7 References

NIST SP 800-40 Version 2.0, "Creating a Patch and Vulnerability Management Program."

6.1.8 Dependencies

Section 2.6, "Installing Operating Systems, Applications, and Third-Party Software Updates."

6.2 Problem Reporting

Vulnerabilities exist in core logic and configuration of control systems. When flaws in software and/or hardware configuration are discovered by users, the Vendor shall have a process in place by which the user can report such flaws. A flaw remediation process should be used to track progress of patches, fixes, and workarounds until completion.

6.2.1 Basis

Zero-day exploits are not defendable and are a primary attack vector.

6.2.2 Language Guidance

Timely notification of flaws is essential to create defenses for zero-day exploits. The Vendor and the Purchaser must communicate flaw information in a secure manner during the mitigations development process.

Public release of problem reports could lead to non-defendable exploits. Consequently, knowledge of open flaws should be closely protected.

6.2.3 Procurement Language

The Vendor shall provide a process for users to submit problem reports and remediation requests to be included in the system security. The process shall include tracking history and corrective action status reporting.

The Vendor shall review and report their initial action plan within 24 hours of submitting the problem reports.

The Vendor shall protect problem reports regarding security vulnerabilities from public discloser, and notify Purchaser of all problems and remediation steps, regardless of origin of discovery of the problem.

The Vendor shall inform the Purchaser in writing of flaws within applications and operating systems in a timely fashion, and provide corrective actions, fixes, or monitoring guidance for vulnerability exploits associated with the flaw.

The Vendor shall provide an auditable history of flaws including the remediation steps taken for each.

6.2.4 FAT Measures

None.

6.2.5 SAT Measures

None.

6.2.6 Maintenance Guidance

The Vendor shall provide prenegotiated updates to the Purchaser.

6.2.7 References

NIST SP 800-40 Version 2.0, "Creating a Patch and Vulnerability Management Program."

6.2.8 Dependencies

None, this topic is stand-alone.

7. MALWARE DETECTION AND PROTECTION

Malware is any unauthorized software. Because many control networks are connected to other networks or updated by media, malware can enter into the network and affect process control and/or communications. Malware consist of many different types of software and may include, but is not limited to bots, Trojans, worms, viruses, backdoors, and zombies. Malware detection can occur on a host or a network-based device.

7.1 Malware Detection and Protection

Updates to malware detection software may adversely impact control system behavior.

7.1.1 Basis

Malicious code—worms, viruses, and Trojans, can propagate through a control system and potentially impact or curtail operations.

7.1.2 Language Guidance

In most systems, network-based malware detection can occur on the outer perimeter of the process control network. Perimeter malware detection is common for legacy components since the impact on these components vary. Traditional malware detection and removal software usage involves updating the signatures that identify the malware frequently (normally once a day on highly exposed systems) and continuously scanning incoming files for infected data.

Both of these acts of updating to the latest detection signatures and scanning the files may affect control system networks, especially those with legacy components. Manual scanning or scanning files for malware on a scheduled basis is known to use up central processing unit (CPU) resources and may impact other process executions on the host. Active scanning is the process of scanning files only when the files are accessed or modified and have been used in control systems. In-memory scans will detect the presence of malware in memory, which may affect performance of the system.[m] Faulty signature files may impact critical control system files requiring the need for quick roll back of the signatures and restoring the suspected files. Quarantining the files provides a mechanism to perform forensics if malicious code is detected. In industry, some Vendors only provide guidance to determine which type of detection should be used, while others provide guidance on how to configure malware scans, and still others bundle malware detectors into the system.

Updates to malware detection software may change control system behavior enough to require retesting to determine the impact to operations.

7.1.3 Procurement Language

The Vendor shall disclose the existence and reasons for any known or identified backdoor codes.

The Vendor shall meet one of two conditions:

1. Provide a host-based malware detection scheme for the control system network. The Vendor shall verify adequate system performance for host-based malware detection, quarantine (instead of automatically deleting) suspected infected files, and provide an updating scheme for the signatures. The Vendor shall also test major updates to malware detection applications and provide performance measurement data on the impact of using the malware detection applications in an active system.

[m] Joe Falco, Steve Hurd, and David Teumin, “Using Host-Based Anti-Virus Software in Industrial Control Systems: Integration Guidance and a Testing Methodology for Accessing Performance Impacts,” Version 1.0 Draft, May 30, 2006.

Measurements shall include, but are not limited to network usage, CPU usage, memory usage, and any other impact to normal communications processing.

2. If the Vendor is not providing the actual host-based malware detection scheme, the Vendor shall suggest malware detection products to be used and provide guidance on malware detection settings that will work with Vendor products.

7.1.4 FAT Measures

The Vendor shall record system performance measurements that include the system with and without malware detection.

The Vendor shall verify all media and equipment is scanned under the most current malware detection versions available prior to onsite transport.

The Vendor shall exercise the malware detection system.

The Vendor shall document any known or identified backdoor codes.

7.1.5 SAT Measures

The Vendor shall record system performance measurements to verify that malware detection does not adversely impact system performance.

The Vendor shall document any known or identified backdoor codes.

7.1.6 Maintenance Guidance

The Vendor shall provide documentation of the malware detection software retest when significant changes are made to determine possible impacts to performance.

The Vendor shall retain malware detection application logs for a prenegotiated period for possible forensics tasks.

The Vendor shall update malware detection software as required to be effective for the most recent malware released since these signatures are reactive. As the malware variants change, new, more precise or tuned signatures need to be applied.

The Vendor shall disclose the existence and reasons for any known or identified backdoor codes.

7.1.7 References

NERC CIP-007 R4, “Malicious Software Prevention.”

NIST SP 800-82, “Draft Guide to Industrial Control Systems (ICS) Security.”

NIST SP 800-83, “Guide to Malware Incident Prevention and Handling.”

7.1.8 Dependencies

None, this topic is stand-alone.

8. HOST NAME RESOLUTION

The Domain Name System (DNS) performs a key function in IP networks by providing name resolution services, translating computer names to IP addresses, and translating IP addresses to computer names. Dynamic host configuration protocol (DHCP) is often used in conjunction with the DNS server to assign IP addresses to client computers. DHCP allows the IP allocation to be completed dynamically with the address expiring after a pre-determined length of time.

8.1 Network Addressing and Name Resolution

Each computer in a network has a unique IP address. Remembering each address for each computer in a network is difficult, so addresses are often mapped to host names, which are easier to remember. DNS servers translate the host name used by people to the IP address used by computers. IP addresses can be assigned statically or can be allocated dynamically from a pool of addresses using DHCP. The most widely used DNS software is Berkeley Internet Name Domain (BIND) produced by Internet Software Consortium (ISC), although other packages exist, including Microsoft DNS.

8.1.1 Basis

DNS servers are susceptible to many types of cyber exploits including spoofing, cache poisoning, and denial of service (DoS) attacks. In a spoofing attack, an attacker who has obtained DNS zone data (the name to IP address mapping) creates packets that appear to come from a valid address. The attacker can then redirect clients by appearing as the legitimate name server. Cache poisoning involves polluting the cache on the DNS server with erroneous data to redirect traffic to a server under the control of the attacker. In a DoS attack, the attacker floods the DNS server with recursive queries. Eventually, the DNS service is no longer available.[n]

8.1.2 Language Guidance

To protect against DNS exploits, DNS servers for the internal control system network should reside inside the firewall and should be separate from the DNS servers on the corporate network. DNS servers for the control system network should be authoritative for the address space of the control system network only. That is, the DNS servers should contain the complete zone information (name to IP address mappings) only for hosts on the control system network. Ideally, the control system network is isolated and hosts will not need to resolve external names. However, if hosts need to resolve names for hosts outside the trusted control system network, queries should go to the control system DNS server, which will forward the queries through the firewall to a DNS server on the corporate network.

DNS servers are typically set up as a minimum configuration in pairs for failover and reliability. A master server and a slave server make up the pair. The master server contains the original zone data, and zone transfers are made to the slave server when changes occur. As mentioned above, IP addresses can be assigned statically or dynamically. If possible, static addressing schemes should be used in control system networks. Dynamic addressing results in frequent IP address changes, and thus, frequent zone updates and transfers. Zone updates and transfers can provide a potential avenue for an attacker to modify DNS records or to gain information about the network. With dynamic addressing, the zone data on the master server are updated automatically with DHCP. With static addressing, zone data changes can be made manually by a system administrator, eliminating potential vulnerabilities associated with automatic updates. Also, the stable IP addresses associated with static addressing results in fewer zone transfers. Regardless of whether static or dynamic addressing is used, restrictions should be placed on both master

[n] Microsoft, “Securing DNS for Windows 2003,” <http://technet2.microsoft.com/WindowsServer/en/Library/fea46d0d-2de7-4da0-9c6f-2bb0ae9ca7e91033.mspx?mfr=true>.

and slave servers to only allow zone transfers to trusted hosts. In addition, Transaction Signatures should be used to authenticate zone transfers by adding cryptographic signatures.[o]

Considerations for securely configuring DNS are summarized by[p]:

- Using dedicated servers for DNS and related services and disable all unneeded services.
- Using the latest software builds with current patches.
- Backing up and reviewing DNS configuration files periodically and running integrity checks to verify the integrity of configuration files, zone data, and other DNS files.
- Running DNS servers as a user other than a root. Enabling access controls to allow only specific individuals to create, delete, or modify DNS data.
- Enabling cache pollution prevention.
- Restricting addresses that can query control system DNS servers to control system hosts.
- Restricting zone transfers to only trusted hosts and authenticating zone transfers.
- Using a static addressing scheme. If dynamic addressing is used, allow dynamic updates from only trusted hosts.
- Configuring the firewall to allow communication between the control system and corporate DNS servers only on UDP and TCP Port 53.
- Allowing special considerations for hosts with multiple IP addresses for redundancy.

8.1.3 Procurement Language

Pre-contract award, the Vendor shall provide recommended network addressing and name resolution methodology.

The Vendor shall provide a means to verify the integrity of configuration files, zone data, and other DNS files (e.g., such integrity checking may be done with a HIDS).

Post-contract award, the Vendor shall provide a configured DNS server(s) or the information to configure a DNS server(s) that meets a prenegotiated standard of security.

The Vendor shall consider addressing information as business sensitive and protect it as such.

8.1.4 FAT Measures

The Vendor shall install and run Vendor-supplied DNS servers continuously during the entire FAT process.

The Vendor shall verify all domain servers and hosts within the domain involved in testing are resolvable by all client and server systems connected to the network.

The Vendor shall document both forward (hostname to IP address) resolution and reverse (IP address to hostname) resolution.

8.1.5 SAT Measures

The Vendor shall run the DNS server during the entire SAT process.

[o] RFC 2845: Secret Key Transaction Authentication for DNS (TSIG).

[p] Allen Householder et al., “Securing an Internet name server,” August 2002, http://www.cert.org/archive/pdf/dns.pdf; Cheng C. Teoh, “Defense in Depth for DNS,” 2003, http://www.sans.org/reading_room/whitepapers/dns/.

The Vendor shall verify all domain servers and hosts within the domain involved in testing are resolvable by all client and server systems connected to the network.

The Vendor shall document both forward (hostname to IP address) resolution and reverse (IP address to hostname) resolution.

8.1.6 Maintenance Guidance

The Vendor shall provide an ongoing patch management process for DNS and related services such as DHCP.

8.1.7 References

NIST SP 800-53 Revision 2, “Recommended Security Controls for Federal Information Systems.”

NIST SP 800-81, “Secure Domain Name System (DNS) Deployment Guide.”

8.1.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 0, “Host Intrusion Detection System.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

9. END DEVICES

End devices refer to components in the control system that gather information or control a process. These could include sensors, controllers, valves, processors, etc. Network and security architectures will change during the long lifespan of end devices, which necessitates detailed end device specifications (e.g., latency, calibrations, protocols, interoperability, and default security settings).

End devices are being delivered with common computer software (e.g., Web, ftp, telnet) for ease of maintenance and configuration. Exploits have been found and published for these applications and are susceptible to new and emerging exploits. Some Vendors are combining security functions (e.g., encryption and authentication) to protect these devices.

End devices are generally located in remote areas raising physical security concerns.

Intelligent end devices, remote terminal units, and programmable logic controllers incorporate microprocessors and are considered “smart” end devices. Sensors, actuators, and meters traditionally incorporate limited processing capabilities and are also known as “dumb” end devices. Communication (serial or Ethernet) to/from “smart” or “dumb” end devices to the control system can be intercepted and modified adversely affecting the controlled process.

9.1 Intelligent Electronic Devices

An intelligent electronic device (IED) is sometimes referred to as an intelligent end device. It incorporates microprocessors within the device, receives information from process sensors or from the power equipment, and issues control commands to process equipment such as breakers, valves, pumps, transformers, etc.

9.1.1 Basis

Intelligent electronic devices can be used as access points to other systems that perform command and control functions. The devices are used to provide system control at the lowest level of a process and are vulnerable to communication interception and modification. Hardware and software (e.g., portable configuration computers) are needed to program IEDs. IEDs and configuration computers need to be secured by physical and cyber means (see Sections 2.4, 2.6, 4.1–4.5, and 7).

9.1.2 Language Guidance

Intelligent electronic devices are a part of the entire system and must be able to communicate with the rest of the system while performing specific control functions. If the communication from the network to the device or from the device to the network is intercepted and modified, the controlled process could be adversely affected. Therefore, it is necessary to verify that both the device itself and the communication to and from the device are secured to achieve integrity of the communication. In addition, modifications to the control function of the device can affect the integrity of the data transmitted and the actions taken by the control system. To avoid this, it is necessary to secure the IED from both cyber and physical modifications.

9.1.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the safety instrumented system (SIS) is certified after incorporating the security devices.

9.1.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput for field communications.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

9.1.5 SAT Measures

The Vendor shall verify and provide documentation of any changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

9.1.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the IED as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the control system during the warranty/maintenance period.

9.1.7 References

IEC61850, “International Standard for Substation Automation Systems.”

EIA-485, “OSI Model Physical Layer Electrical Specification of a Two-wire, Half-duplex, Multipoint Serial Connection.”

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Sections 6.3.2.2, 6.3.6.”

ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems, Section 5.1.”

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-006-1 R1.1, “Physical Security of Critical Cyber Assets.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R3, “Security Patch Management.”

NERC CIP-007-1 R5, “Account Management.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems,” Appendix F: AC-2, AC-3, IA-2, IA-5.

9.1.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 2.4, “Hardware Configuration.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

Section 6, “Flaw Remediation.”

Section 7.1 “Malware Detection and Protection.”

Section 8.1, “Network Addressing and Name Resolution.”

Section 10, “Remote Access.”

Section 11, “Physical Security.”

9.2 Remote Terminal Units

A remote terminal unit (RTU) is a microprocessor-controlled device that is used to provide system control of industrial processes.

9.2.1 Basis

RTUs can be used as access points to other systems that perform command and control functions. The devices are used to provide system control at the lowest level of a process and are vulnerable to communication interception and modification. Hardware and software (e.g., portable configuration computers) are needed to program RTUs. RTUs and configuration computers need to be secured by physical and cyber means (see Sections 2.4, 2.6, 4.1–4.5, and 7).

9.2.2 Language Guidance

The RTU accepts inputs from multiple sources, outputs control signals to control devices, and interfaces with a distributed control system or SCADA network by transmitting data to the system and/or altering the state of connected objects based on control messages received from the system. The RTU is a first-level decision-making device that is a part of the entire system and must be able to communicate with the rest of the system while performing its specific control function. If the communication from the input device (e.g., sensor) to the RTU or from the RTU to the output device (e.g., controller) or the network is intercepted and modified, the controlled process could be adversely affected. In addition, the processing unit within the RTU is susceptible to modification thus affecting the control functions. Therefore, it is necessary to verify that both the RTU itself and the communication to and from the device are secured to achieve integrity of the communication and the processing unit. It is also necessary to secure the RTU from both cyber and physical modifications.

9.2.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

9.2.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

9.2.5 SAT Measures

The Vendor shall verify and provide documentation of changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

9.2.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the RTU as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the control system during the warranty/maintenance period.

9.2.7 References

ISO 11898-3:2006, Road vehicles -- Controller area network (CAN) -- Part 3: Low-speed, fault-tolerant, medium-dependent interface

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Sections 3.2.57, 6.2.1.4, 6.3.2.2, 6.3.6.”

ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems, Sections 5.1.1, 6.2.6, 7.3.4, 8.6.2, 9.2.4.”

ISA-99.00.02 (DRAFT), Security for Industrial Automation and Control Systems: Part 2: Establishing an Industrial Automation and Control Systems Security Program, Sections 5.3, B.14, C.3.”

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-006-1 R1.1, “Physical Security of Critical Cyber Assets.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R3, “Security Patch Management.”

NERC CIP-007-1 R5, “Account Management.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-3, IA-2, IA-5.”

9.2.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 2.3, “Changes to File System and Operating System Permissions.”

Section 2.4, “Hardware Configuration.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

Section 6, “Flaw Remediation.”

Section 7.1 “Malware Detection and Protection.”

Section 8.1, “Network Addressing and Name Resolution.”

Section 10, “Remote Access.”

Section 11, “Physical Security.”

9.3 Programmable Logic Controllers

A programmable logic controller (PLC) is a digital computer used to provide system control of industrial processes. PLCs are designed for multiple inputs and outputs along with a processing unit used to monitor inputs, make decisions, and control outputs.

9.3.1 Basis

Programmable logic controllers can be used as access points to other systems that perform command and control functions. PLCs communicate over open networks that are vulnerable to communication interception and modification. Hardware and software (e.g., portable configuration computers) are needed to program PLCs. PLCs and configuration computers need to be secured by physical and cyber means (see Sections 2.4, 2.6, 4.1–4.5, and 7).

9.3.2 Language Guidance

The PLC is a first-level decision-making device that is a part of the entire system and must be able to communicate with the rest of the system while performing its specific control function. If the communication from the input device (e.g., sensor) to the PLC or from the PLC to the output device (e.g., controller) or the network is intercepted and modified, the controlled process could be adversely affected. In addition, the processing unit within the PLC is susceptible to modification thus affecting the control functions. Therefore, it is necessary to verify that both the PLC itself and the communication to and from the device are secured to achieve integrity of the communication and the processing unit. It is also necessary to secure the PLC from both cyber and physical modifications.

Some newer PLCs are including embedded operating systems that have many common operating system components (e.g., Linux). These embedded operating systems need to be hardened (see Section 2).

Safety instrumented systems (SIS) frequently run on PLC architectures. These systems are the last line of automated protection for critical processes that could result in severe damage or fatalities if compromised. Industry certifications are common for SIS. Legacy SIS/PLCs run on separate architectures from control functions. There is a new trend for SIS to be integrated with traditional control functions (e.g., one PLC runs control and safety functions). The cyber security concerns for integrated SIS are paramount.

9.3.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

9.3.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

9.3.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

9.3.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the PLC as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the control system during the warranty/maintenance period.

9.3.7 References

IEC 61131-3, “Programmable Controllers – Part 3: Programming Languages.”

ANSI/ISA-99.00.01, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models, Sections 3.2.57, 6.2.1.4, 6.3.2.2, 6.3.6.”

ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems, Sections 5.1.1, 6.2.6, 7.3.4, 8.6.2, 9.2.4.”

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-006-1 R1.1, “Physical Security of Critical Cyber Assets.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R3, “Security Patch Management.”

NERC CIP-007-1 R5, “Account Management.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-3, IA-2, IA-5.”

9.3.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 2.3, “Changes to File System and Operating System Permissions.”

Section 2.4, “Hardware Configuration.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

Section 6, “Flaw Remediation.”

Section 7.1 “Malware Detection and Protection.”

Section 8.1, “Network Addressing and Name Resolution.”

Section 10, “Remote Access.”

Section 11, “Physical Security.”

9.4 Sensors, Actuators, and Meters

Sensors, actuators, and meters are traditionally dumb devices that produce outputs or accept inputs from a control system. The trend is toward sensors, actuators, and meters that incorporate microprocessors, also known as “smart devices.” “Smart” sensors are also referred to as “smart transducers.”

9.4.1 Basis

Sensors, actuators, and meters can be used as access points to other systems (e.g., PLCs and IEDs) that perform command and control functions. These devices communicate over networks that are vulnerable to communication interception and modification. Hardware and software (e.g., portable configuration computers) are needed to program smart devices. Smart devices and configuration computers need to be secured by physical and cyber means (see Sections 2.4, 2.6, 4.1–4.5, and 7).

9.4.2 Language Guidance

These devices are a part of the entire system and must be able to communicate with the rest of the system while performing specific control functions. Since the devices do not possess processing capabilities, the only vulnerability is the communication link with the control system. If the communication from the input device (e.g., sensor or meter) to the control system or from the control system to the output device (e.g., actuator) is intercepted and modified, the controlled process could be adversely affected. These communication paths, Ethernet or serial, can be compromised. Security measures such as port security (e.g., one MAC/port) or inline encryption are options. Sensors, actuators, and meters and the communication to and from these devices need to be secured from both cyber and physical modifications.

Sensors and meters are now often network-enabled and contain resident logic. These devices have network and computer components that require security (e.g., updates).

Wireless communications are central in many sensor and meter networks complicating the security profile (e.g., WPA).

9.4.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall provide secure (serial, Ethernet, and wireless) communication paths, including the ability to filter and monitor communications.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

For smart devices:

- The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.
- The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.
- The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

9.4.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

For smart devices:

- The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.
- The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

9.4.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing any changes.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

For smart devices:

- The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.
- The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default usernames, passwords, or other access methods are changed at the start of the SAT.

9.4.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the devices as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the control system during the warranty/maintenance period.

9.4.7 References

ANSI/ISA-99.00.01, "Security for Industrial Automation and Control Systems Part 1: Terminology, Sections 6.2.1.4, 6.3.8."

ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems, Section 9.2.24."

NERC CIP-005-1 R1.1, "Electronic Security Perimeter."

NERC CIP-005-1 R2, "Electronic Access Controls."

NERC CIP-006-1 R1.1, "Physical Security of Critical Cyber Assets."

NERC CIP-007-1 R2, "Ports and Services."

NERC CIP-007-1 R3, "Security Patch Management."

NERC CIP-007-1 R5, "Account Management."

NERC CIP-007-1 R8, "Cyber Vulnerability Assessment."

NIST SP800-53 Revision 1, "Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-3, IA-2, IA-5."

9.4.8 Dependencies

Section 2.1, "Removal of Unnecessary Services and Programs."

Section 2.4, "Hardware Configuration."

Section 6, "Flaw Remediation."

Section 7.1 "Malware Detection and Protection."

Section 8.1, "Network Addressing and Name Resolution."

Section 10, "Remote Access."

Section 11, "Physical Security."

10. REMOTE ACCESS

Remote access refers to the ability to connect to a computer or network from a different location via modem, Ethernet, serial, TCP/IP, VPN, or wireless.

10.1 Dial-Up Modems

Dial-up modems allow remote access to control system equipment.

10.1.1 Basis

Modems, often considered part of the telephone system and not the control network, are vulnerable and easily overlooked. Modem lines connected to the network or control system equipment that are left enabled are possible “back door” entry points for exploits on the network or directly on the control system equipment.

Dial-up modems connected through the public-switched telephone network (PSTN), as opposed to dedicated-line modems, are accessible to anyone in the world with a modem and are easy to discover via war dialing.

10.1.2 Language Guidance

Control system equipment is installed with modems enabled. Properly implementing modem security settings (telephony firewalls and authentication, automated log monitoring, disabling power and phone lines, dial-back modem features, caller ID authentication) mitigates modem vulnerabilities. It is common to find little or no security protection for modem connections. Often, the only protection is provided by the control system devices. These devices may require a password or user ID/password combination, but even this simple protection may not be offered, especially for older legacy equipment. Throughput, latency, and bandwidth must be investigated when considering security methods.

Modem security settings may exist on the company private branch exchange (PBX). Many of these security settings can limit the time of day a phone line is active. Others may provide active logging capabilities that can be used in an IDS for modem connections.

Telephony firewalls can provide voice-level capabilities similar to the data-level capabilities of network firewalls in use today. The devices are normally placed between the PSTN and the modem.

Telephony authentication uses hardware keys on the PSTN side of the modem; when two modems attempt to connect, the master key must validate the slave key before a PSTN connection is allowed. However, if a slave key was compromised and not removed from the valid key list, an unauthorized user could obtain access.

Automated monitoring of modem and control device connection logs can allow the system to alarm on unexpected activities.

One simple approach to modem security is only connecting the modem power or phone line when needed (e.g., power outlet timer). Another option to limit phone line connectivity is using PBX time-window programming.

Configuring modems to dial back instead of auto-answer can provide another layer of authentication security. Unfortunately, hackers have developed “dial-back spoofing” methods where a fake dial tone is fed to the modem allowing the hacker to maintain the connection and ignore the dial-back process.

Caller ID can be combined with modems to allow or deny access based on comparison to a preprogrammed list of valid phone numbers. Caller ID is typically used to block war dialing efforts. Attackers have found ways to spoof a caller ID number to indicate a false number, but a correct number on the list would first need to be discovered.

Using authentication allows both modems to confirm connection to an authorized party. Many of these components, such as RTUs, PLCs, and IEDs may not require any authentication for connection. Modems can be purchased with embedded keys, or hardware keys can be added to existing modems.

Man-in-the-middle (MITM) attacks use clear-text protocols to inject the attacker into the communication stream to read user IDs and passwords and/or change the intercepted data before forwarding it. The MITM attack and could originate within the public telephone system, the internal PBX system, or through a VoIP communication path. In-line encryption (bump-in-the-wire) devices can act as an intermediary between the serial port and the modem, helping mitigate this vulnerability. However, encryption may reduce overall throughput of the connection.

10.1.3 Procurement Language

The Vendor shall verify that modems are enabled only when needed (e.g., time constraint) or limit possible entry points (e.g., access list).

The Vendor shall change or disable configuration settings that could be used for exploitation when not needed.

The Vendor shall provide a telephony firewall to include authorized list, automatic block, and alarm during unauthorized access and automatic log review.

The Vendor shall not permit user credentials to be transmitted in clear text.

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall provide a list including all ports and services required for normal operation and emergency operation and troubleshooting.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the modem and modem security system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but is not limited to:

- Device drivers for network devices not delivered
- Unused networking and communications protocols
- Unused administrative utilities, diagnostics, network management, and system management functions
- All unused data and configuration files.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

Post-contract award, the Vendor shall provide documentation detailing all modem configurations, services, and all software/modem device protection configurations and keys, including revisions and/or patch levels.

10.1.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

The Vendor shall provide a summary table indicating each communication path required by the system. This table should include:

- Source device name and MAC/IP address
- Destination device name and MAC/IP address
- Protocol (e.g., TCP and UDP) and port or range of ports.

The Vendor shall perform network-based validation and documentation steps on each device including full TCP and UDP port scans.

The Vendor shall complete the cyber security scans during a simulated “normal system operation.”

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.1.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall perform war dialing or discovery activities and provide documentation of the results.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.1.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.1.7 References

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-007-1 R5, “Account Management.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-17, IA-2, IA-5.”

Department of Homeland Security, Recommended Practice for Securing Control System Modems, January 2008.[q]

[q] http://csrp.inl.gov/Documents/SecuringModems.pdf

10.1.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 2.4, “Hardware Configuration.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

Section 6, “Flaw Remediation.”

Section 7.1 “Malware Detection and Protection.”

Section 8.1, “Network Addressing and Name Resolution.”

Section 9, “End Devices.”

Section 10, “Remote Access.”

Section 10.2, “Dedicated Line Modems.”

Section 11, “Physical Security.”

10.2 Dedicated Line Modems

Modems allow remote access to control system equipment.

10.2.1 Basis

Modems connected by dedicated lines, also known as nonswitched lines, are often not considered vulnerable since the lines are permanently connected together and do not have phone numbers. While dedicated-line modems are considered more secure than dial-up modems, the devices, like dial-up modems, are not impervious to information discovery and hacking.

10.2.2 Language Guidance

Encryption and authentication are two security methods applicable to both dial-up and dedicated-line modems.

Using authentication allows both modems to confirm connection to an authorized party. Many of these components, such as RTUs, PLCs, and IEDs may not require any authentication for connection. Password authentication can be impractical with dedicated-line modems. Modems can be purchased with embedded keys, or hardware keys can be added to existing modems.

Man-in-the-middle (MITM) attacks use clear-text protocols to inject the attacker into the communication stream to read user IDs and passwords and/or change the intercepted data before forwarding it. The MITM attack and could originate within the public telephone system (even over leased lines), the internal PBX system, or through a VoIP communication path. In-line encryption (bump-in-the-wire) devices can act as an intermediary between the serial port and the modem, helping mitigate this vulnerability. However, encryption may reduce overall throughput of the connection.

10.2.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall not permit user credentials to be transmitted in clear text.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall provide a list including all ports and services required for normal operation and emergency operation and troubleshooting.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

The Vendor shall remove and/or disable all software components that are not required for the operation and maintenance of the modem and modem security system prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled. The software to be removed and/or disabled shall include, but is not limited to:

- Device drivers for network devices not delivered
- Unused networking and communications protocols
- Unused administrative utilities, diagnostics, network management, and system management functions
- All unused data and configuration files.

Post-contract award, the Vendor shall provide documentation detailing all modem configurations, services, and all software/modem device protection configurations and keys, including revisions and/or patch levels.

10.2.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall provide a summary table indicating each communication path required by the system. This table should include:

- Source device name and MAC/IP address
- Destination device name and MAC/IP address
- Protocol (e.g., TCP and UDP) and port or range of ports.

The Vendor shall perform network-based validation and documentation steps on each device, including full TCP and UDP port scans.

The Vendor shall complete the cyber security scans during a simulated “normal system operation.”

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.2.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing any changes.

The Vendor shall perform discovery activities and provide documentation of the results.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.2.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.2.7 References

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-006-1 R1.1, “Physical Security of Critical Cyber Assets.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R3, “Security Patch Management.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-3, IA-2, IA-5.”

Department of Homeland Security, Recommended Practice for Securing Control System Modems , January 2008.[r]

10.2.8 Dependencies

Section 2.1, “Removal of Unnecessary Services and Programs.”

Section 2.4, “Hardware Configuration.”

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

Section 6, “Flaw Remediation.”

Section 7.1, “Malware Detection and Protection.”

Section 8.1, “Network Addressing and Name Resolution.”

Section 9, “End Devices.”

Section 10, “Remote Access.”

Section 10.1, “Dial-up Modems.”

Section 11, “Physical Security.”

[r] http://csrp.inl.gov/Documents/SecuringModems.pdf

10.3 TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack is the foundation of communication on the Internet and most commercial networks. It is named after its two most important protocols: the IP and the TCP. Other important IP protocols include User Datagram Protocol (UDP), Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP). IP operates at the network layer of a network and provides connectionless unreliable communication. IP is responsible for sending and routing packets, but is connectionless and does not guarantee transmission. TCP runs on top of the IP and provides connection-oriented reliable communication.

10.3.1 Basis

Poor TCP/IP implementations and/or implementations that do not fully comply with TCP/IP Requests for Comments (RFCs) can result in protocol stacks that contain vulnerabilities. Buffer overflows, the inability to handle packet fragmentation, or malformed network traffic are common problems. Intentional or accidental exploitation of vulnerabilities can lead to a device/function being compromised/targeted or can produce a DoS.

10.3.2 Language Guidance

The TCP/IP specifications lack basic security mechanisms resulting in fully-compliant implementations remaining vulnerable to attacks (e.g., DoS, IP spoofing, session hijacking, and syn flooding). At this time, within the TCP/IP framework external mitigations are required (e.g. encryption, authentication, proper network partitioning, and correct firewall configuration). A good software security solution is IP Security (IPsec), which provides the ability to authenticate and encrypt IP traffic within the protocol stack.

Intrusion Detection Systems (IDS) will not work with encrypted data. In order to use encryption and IDSs in a control system, it is necessary to place an IDS on a device that can decrypt the traffic, analyze it, and then re-encrypt it before forwarding it.

There are currently two IP standards: IPv4 and IPv6. Most network devices comply with IPv4 specifications; however, many newer devices are compatible with both IPv4 and IPv6. When IPv6 is the main standard, new network devices may not be backwards compatible with IPv4. Control system devices are often operational in excess of 20 years; therefore, it is advisable that the devices be IPv6 compatible.

10.3.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate protocol stack updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

The Vendor shall use a TCP/IP implementation that fully complies with the current TCP/IP RFCs.

The Vendor shall deliver a product that is IPv6 compatible.

The Vendor shall provide the ability to monitor traffic in an encryption scheme.

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the protocol stack as vulnerabilities are identified to maintain the established level of system security.

Post-contract award, the Vendor shall provide an independent third-party security validation of the IPv6 implementations (e.g., using fuzzing techniques).

Post-contract award, the Vendor shall mitigate all vulnerabilities discovered during the testing of the IPv6 implementations and provide documentation of the results.

10.3.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall provide documentation of the results of the independent third-party security validation of the IPv6 implementations.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.3.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.3.6 Maintenance Guidance

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the protocol stack as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.3.7 References

NERC CIP-005-1 R1.1, “Electronic Security Perimeter.”

NERC CIP-005-1 R2, “Electronic Access Controls.”

NERC CIP-006-1 R1.1, “Physical Security of Critical Cyber Assets.”

NERC CIP-007-1 R2, “Ports and Services.”

NERC CIP-007-1 R3, “Security Patch Management.”

NERC CIP-007-1 R5, “Account Management.”

NERC CIP-007-1 R8, “Cyber Vulnerability Assessment.”

NIST SP800-53 Revision 1, “Recommended Security Controls for Federal Information Systems, Appendix F: AC-2, AC-3, IA-2, IA-5.”

RFC 793, Transmission Control Protocol.

RFC 791, Internet Protocol.

RFC 793, Transmission Control Protocol.

RFC 4301, Security Architecture for the Internet Protocol.

10.3.8 Dependencies

Section 0, “Host Intrusion Detection Systems.”

Section 3.1, “Firewalls.”

Section 3.2, “Network Intrusion Detection System.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 12, “Network Partitioning.”

10.4 Web-based Interfaces

Many control systems have Web-based interfaces for performing some tasks.

10.4.1 Basis

Web-based interfaces to control systems are gaining popularity and are often poorly designed and configured making these interfaces vulnerable to exploits.

10.4.2 Language Guidance

Web applications are often vulnerable to injection attacks of several varieties including command injection, Remote File Include (RFI) and Cross-Site Scripting (XSS). Web applications with a database back-end commonly mishandle Structured Query Language (SQL) statements as well, allowing SQL injection. Additionally, the HTTP servers on which these applications are hosted can be vulnerable to buffer overflows or other memory corruption attacks. Another common mistake in Web applications is directory traversal, which allows attackers access to more files than the programmer intended. Web applications in embedded devices are often written in a low-level language like C and are potentially vulnerable to buffer overflows.

Other non-HTTP services are also commonly included (e.g., ftp, telnet) on devices and the combination of these services can lead to greater information disclosure or other attacks.

Authentication. Web interfaces typically contain a large amount of configuration and site-specific information, therefore authentication is essential to prevent an attacker from gaining more knowledge about the system. Poorly implemented interfaces using default passwords can completely undermine the security provided by authentication. Authentication can also be circumvented by SQL injection and XSS flaws, allowing an attacker to gain database access that can lead to database corruption or a full compromise of the host or device.

RFI. Remote File Include (RFI) vulnerabilities are only present, except in rare circumstances, in applications written in the PHP (hypertext preprocessor) scripting language. When an RFI attack is successful, it results in the attacker running arbitrary PHP scripts on the Web server; this is usually equivalent to full-host compromise.

Input Validation. String input validation is needed to prevent command injection, which can lead to complete host compromise. Like SQL injection, command injection can be accomplished by inputting characters that the application treats specially. The specific characters used will depend on the target system, but commonly include those in the following (non-exhaustive) list: $ % ! ` ; ' " \. Flaws of this nature are usually easy to find, are relatively simple, and provide access to an attacker as the user running the HTTP server. When combined, these factors make command injection a dangerous vulnerability that must be addressed.

Cross-Site Scripting (XSS). There are two basic types of XSS: reflected and persistent. In a reflected XSS vulnerability, the attacker must convince a user to visit a malicious Web site or click on a malicious link. The persistent variety, in which the exploit is stored on the target server itself, is less common but more likely to succeed in a control system environment because using the Web application is sufficient to trigger the exploit. Regardless of how XSS is launched, it works by running JavaScript on the user's browser in the context of the target Web page. This allows an attacker to steal the user's cookies, thereby gaining access as that user.

Like other types of software, Web applications need to be designed and developed with security in mind.

10.4.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components and services that are not required for the operation and maintenance of the devices that run an HTTP server prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

The Vendor shall provide documentation of input sanitization for all Web-form inputs, including, but not limited to, measures for prevention of command injection, SQL injection, directory traversal, RFI, XSS, and buffer overflow.

The Vendor shall follow secure coding practices and reporting for all Web-based interface software (see Section 5.1). This requirement includes both Web applications and Web servers.

The Vendor shall provide user configurable and managed passwords (see Section 4.3).

The Vendor shall provide an independent third-party security code validation of all Web-based interface software (see Section 5.1).

10.4.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of all communications to and from any device running an HTTP server and configuration including, but not limited to cyber security features, Web-based interfaces, software, protocols, ports, and services and provide documentation describing the functionality of each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall provide documentation of the results of the independent third-party security code validation for all Web application and Web server software.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.4.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the system from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of all communications to and from any device running an HTTP server and configuration including, but not limited to cyber security features, Web-based interfaces, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.4.6 Maintenance Guidance

The Vendor shall create a new baseline of all Web-based interfaces and provide documentation explaining any changes to the functionality of each interface.

The Vendor shall create a new baseline of all communications to and from any device running an HTTP server and provide documentation explaining any changes to the functionality of each service and protocol.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall provide, within a prenegotiated period, upgrades and patches to the Web applications as security issues are identified to maintain the established level of system security.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.4.7 References

None, this topic is stand-alone.

10.4.8 Dependencies

Section 4.1, “Disabling, Removing, or Modifying Well-Known or Guest Accounts.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 5.1, “Coding for Security.”

10.5 Virtual Private Networks

Virtual Private Networks (VPNs) allow for secure or trusted communications over an unsecured or untrusted infrastructure such as the Internet. The advantages of such systems are confidentiality, integrity, and availability. A poorly configured VPN creates easily exploitable vulnerabilities. The term VPN is a very large category that includes any mechanism that creates a logical division where there is not a physical division of a network, thereby creating a subnetwork that is not accessible by members of the network who are not part of the subnetwork. This large category encroaches on the category of network partitioning. This section will concentrate on the subcategory of VPN limited to the encrypted tunneling of traffic through untrusted networks. Examples of where this type of VPN is useful are:

- Site-to-site control system communication over an unsecured communication line (i.e., Internet).
- Non-local Vendor support of a deployed control system.

10.5.1 Basis

The primary vulnerability of any VPNs is the end-points. If one end-point is compromised, then the entire VPN is potentially compromised.

10.5.2 Language Guidance

The main components that make a VPN secure are encrypted traffic and protected authentication mechanism. The authentication method used can be security token, known key, securely distributed certificate, password, or combination of any of these methods. Once the authentication is complete, the VPN should encrypt all traffic between end-points to ensure no data is leaked, and prevent MITM attacks. Multifactor identification and authentication is strongly advised to neutralize the effectiveness of brute-force attacks. A common multifactor identification is a combination of a security token, known key, or certificate and a password, PIN, or biometrics.

When using any statically assigned authentication value such as password, PIN, certificate, etc., the value must never be communicated in plain text through an untrusted network.

With the addition of encryption comes the reduction in ability to monitor communications. Some installations need to be able to monitor all communications to and from the installation site. When encrypting the VPN communication, the standard firewall and IDS may not be able to inspect the contents of the VPN communication. Most VPNs can have monitoring software installed on the server or an end-point to record the pre-encrypted traffic.

Additional security measures may be necessary when partitioning a network that contains a VPN server. As such, VPN server placement and ownership should be agreed upon for each VPN that is being deployed. A good solution is to place the VPN server in a DMZ separate from the control network and allow a user on it to connect onto the control network using the authentication process required for a user who is accessing the network locally.

VPNs are strongly affected by firewall rules and as such should be considered when requesting firewall solutions. The form of VPN affects the ability to filter traffic on the firewall. VPNs that are created on Layer 3, like IPSec, can only be filter-based on IP addresses, protocol number, and entropy. VPNs that are created on Layer 4, like those based on SSL, can be filter on the aforementioned properties plus port numbers and additional TCP/UDP properties. The actual filtering effectiveness may not improve with additional properties; however, the ability to route traffic through Network Address Table (NAT) firewalls usually improves with additional properties.

10.5.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to multi-factor authentication (e.g., security token, known key, and/or certificate), encryption, access control, event and communication logging, monitoring, and alarming to protect the system and configuration computer from unauthorized modification or use.

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

The Vendor shall provide a DMZ outside of the control network for the VPN server to reside.

The Vendor shall use different authentication methods for establishing control network access and VPN connection.

10.5.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to multi-factor authentication (e.g., security token, known key, and/or certificate), encryption, access control, event and communication logging, monitoring, and alarming to protect the system and configuration computer from unauthorized modification or use.

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall create a baseline of the delivered system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing each item.

Post-FAT, the Vendor shall create a baseline of the delivered system communications and configuration including, but not limited to cyber security features, Web-based interfaces, software, protocols, ports, and services and provide documentation describing the functionality of each item.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.5.5 SAT Measures

The Vendor shall verify and provide documentation of and changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed at the start of the SAT.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

10.5.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.5.7 References

RFC 2341, “Cisco Layer Two Forwarding (Protocol) "L2F".”

RFC 2637, “Point-to-Point Tunneling Protocol.”

RFC 2661, “Layer Two Tunneling Protocol "L2TP".”

RFC 2764, “A Framework for IP Based Virtual Private Networks.”

RFC 4026, “Provider Provisioned Virtual Private Network (VPN) Terminology.”

10.5.8 Dependencies

Section 2.6, “Installing Operating Systems, Applications, and Third-Party Software Updates.”

Section 3.1, “Firewalls.”

Section 4.3, “Password/Authentication Policy and Management.”

Section 12, “Network Partitioning.”

10.6 Serial Communications Security

Many protocols are used for both serial and Ethernet communications.

10.6.1 Basis

Researchers have demonstrated that the protocols used in serial communications can be exploited to gain control of network devices. These devices can then be leveraged by an attacker to gain further control of the network.

10.6.2 Language Guidance

When a vulnerability is found in one of these protocols (usually over Ethernet) it is often overlooked in the serial realm. Mitigation strategies must be employed to prevent exploitations from occurring within the serial domain. These mitigation strategies often involve patching applications supporting the protocol or the protocol itself. Field communication devices (e.g., front-end processor [FEP], data acquisition processor, protocol converter, or data concentrator) are often interconnected, which can provide an attacker with greater access to the control system after a compromise has occurred.

Due to the legacy issues with serial protocols, the protocols are commonly excluded in cyber security standards. Vulnerable end-point protocols create a larger attack surface due to the distribution of serial devices over a large geographic area.

Link encryptors are used to protect field communications (e.g., bump-in-the-wire devices).

10.6.3 Procurement Language

The Vendor shall provide physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the serial communications and communication devices from unauthorized modification or use.

The Vendor shall provide an independent third-party validation of all software running on field communication devices (see Section 5.1).

The Vendor shall clearly identify the physical and cyber security features and provide the methodology(ies) for maintaining the features, including the methods to change settings from the Vendor-configured or manufacturer default conditions.

The Vendor shall verify through security scans of the field communications that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified for serial communications, including during the SAT when connected to existing equipment.

The Vendor shall remove or disable all software components that are not required for the operation and maintenance of the device prior to the FAT. The Vendor shall provide documentation on what is removed and/or disabled.

The Vendor shall provide, within a prenegotiated period, appropriate software and service updates and/or workarounds to mitigate all vulnerabilities associated with the product and to maintain the established level of system security.

The Vendor shall verify and provide documentation that the SIS is certified after incorporating the security devices.

10.6.4 FAT Measures

The Vendor shall verify and provide documentation of physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the serial communications and communication devices from unauthorized modification or use.

The Vendor shall provide documentation of the independent third-party validation of all software running on field communication devices (see Section 5.1).

The Vendor shall verify and provide documentation that all validated security updates and patches are installed and tested at the start of the FAT.

The Vendor shall verify and provide documentation that all unused software and services are removed or disabled.

Post-FAT, the Vendor shall create a baseline of the system communications and configuration including, but not limited to cyber security features, software, protocols, ports and services and provide documentation describing each item.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput.

The Vendor shall verify that FAT procedures include validation and documentation of the requirements.

10.6.5 SAT Measures

The Vendor shall verify and provide documentation of any changes to physical and cyber security features, including but not limited to authentication, encryption, access control, event and communication logging, monitoring, and alarming to protect the device and configuration computer from unauthorized modification or use.

Post-SAT, the Vendor shall create a baseline of all serial communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall verify through cyber security scans of the system and provide documentation that the addition of security features does not adversely affect adequate connectivity, latency, bandwidth, response time, and throughput for field communications when connected during the SAT.

The Vendor shall verify that SAT procedures include validation and documentation of the requirements.

The Vendor shall test and install all validated security updates and patches at the start of the SAT.

10.6.6 Maintenance Guidance

The Vendor shall provide, within a prenegotiated period, upgrades and patches as security issues are identified to maintain the established level of system security.

The Vendor shall create a baseline of the updated system communications and configuration including, but not limited to cyber security features, software, protocols, ports, and services and provide documentation describing any changes.

The Vendor shall verify and provide documentation that any Vendor-configured or manufacturer default accounts, usernames, passwords, security settings, security codes, and other access methods are changed, disabled, or removed.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements to maintain the established level of system security.

The Vendor shall supply maintenance capabilities for delivered system security features.

The Vendor shall document all additions and changes to the remote access equipment during the warranty/maintenance period.

10.6.7 References

None, this topic is stand-alone.

10.6.8 Dependencies

Section 4.3, "Password/Authentication Policy and Management."

Section 5.1, "Coding for Security."

11. PHYSICAL SECURITY

This procurement guide focuses on cyber security language for control systems. Physical security must be taken into account for a total security posture. This section is not intended to be a comprehensive physical security guide. Suggestions made in this section are based on common physical security issues related to cyber security components.

Subsection 11.1 covers the ability of an intruder to gain cyber access (e.g., plugging into a switch). The physical perimeter access section is the traditional "gates, guns, and guards" of physical security. The manual override section is specific to manual override control devices in the field. Subsection 11.4 describes the safeguards needed to protect communications in remote unmanned areas.

11.1 Physical Access of Cyber Components

Control system networks and devices require protection from physical access as well as cyber access.

11.1.1 Basis

Physical access to cyber equipment circumvents all cyber security controls.

11.1.2 Language Guidance

Physical access to systems should have the same level of security as cyber access. Unlocked control cabinets or operator or engineering workstations in unsecured rooms and buildings often only require access by a computer or control system-knowledgeable person to have a significant impact on operations by changing set points, altering code, performing manual overrides, or cycling systems with the intent of burning up motors or disrupting the process.

Commonly, computer components such as CPUs or keyboards are locked in cabinetry while pointing devices, limited keyboards, and monitors for operator functions are available.

Higher security facilities require two-factor authentication for cyber access. These methods can include biometrics, passwords, and security tokens/certificates. Some authentication can be tightly coupled with physical security (e.g., proximity monitors, keycard access to buildings) and control access and logoff to cyber systems.

11.1.3 Procurement Language

The Vendor shall provide a detailed plan for appropriate physical security mechanisms.

The Vendor shall provide lockable or locking enclosures for control system components (e.g., servers, clients, and networking hardware).

The Vendor shall provide locking devices with a minimum of two keys per lock identifiable to each lock, and keyed or not keyed alike depending on Purchaser requirements.

The Vendor shall recommend a room locking device(s) where the equipment and workstations are located, if not already installed by the Purchaser.

The Vendor shall verify and provide documentation that unauthorized logging devices are not installed (e.g., key loggers, cameras, and microphones).

The Vendor shall provide two-factor authentication for physical access control.

11.1.4 FAT Measures

The Vendor shall verify and provide documentation that physical security components (e.g., hardened devices, locks) are tested and the results provided.

The Vendor shall disable by hardware and software means all unused ports and input/output devices (see Section 2).

The Vendor shall verify and provide documentation on the two-factor authentication requiring physical access control.

11.1.5 SAT Measures

The Vendor shall provide, as a part of the SAT procedures, validation and documentation of any electronic or networked room or area access devices.

The Vendor shall disable by hardware and software means all unused ports and input/output devices.

The Vendor shall verify and provide documentation that physical security access schemes are tested and the results provided.

11.1.6 Maintenance Guidance

The Vendor shall maintain the same configuration and standard for all replacements of physical security components.

11.1.7 References

NERC CIP-006-1, “Physical Security of Critical Cyber Assets”.

11.1.8 Dependencies

Section 2.4, “Hardware Configuration.”

11.2 Physical Perimeter Access

Perimeter security includes, but is not limited to fences, walls, fully enclosed buildings, entrance gates or doors, vehicle barriers, lighting, landscaping, surveillance systems, alarm systems, and guards.

Physical security may also include site entry and exit logging as well as room or area logging possibly through a keycard access system.

11.2.1 Basis

Lack of perimeter identification can facilitate physical intrusions. Lack of notification of unauthorized physical access (e.g., monitoring and alarms) can allow unknown breached perimeters. The ability to detect perimeter intrusions is key to prevent physical attacks.

Individuals with access to critical components could compromise the entire system, whether due from a skillful attack or blind luck.

11.2.2 Language Guidance

A physical intrusion is defined as human-initiated bodily access or physical influence to an area where action may negatively affect the reliability of the system in question. If risk or consequence of physical intrusion is deemed high by the Purchaser, greater perimeter security shall be considered. A control area’s physical perimeter is defined as the external barrier to any type of physical intrusion, whether it be pedestrian, vehicular, or projectile. The Purchaser shall define his or her perimeter such that all components critical to system operation are physically secured to all types of physical access.

Only personnel needing access to a location should be given the access permission. Secured areas with critical equipment should not have equipment or functions associated with it that require access by many people, including contractors.

Overly restricted access measures can hamper operations. During emergency events, previously unauthorized individuals commonly need access to controlled areas. Highly-secured physical perimeters (e.g., access-controlled cabinets) require special environmental conditions to ensure cyber components do not fail (e.g., over-heat). Security is often bypassed if operations are hampered.

Physical security monitoring (e.g., cameras, card access) often alarm to a manned control center. For cyber security concerns these alarms should not be on the same network as control functions.

11.2.3 Procurement Language

The Vendor shall provide a site security assessment, making special note of parameters or events that may influence physical intrusions. The results of this assessment shall be a documented site physical security plan.

The Vendor shall verify and provide documentation that enclosures such as walls, buildings, or fences adequately secure the perimeter against pedestrian, vehicular, and projectile intrusion.

The Vendor shall allow access within the perimeter only to those employees, contractors, or guests cleared by both Vendor and Purchaser.

The Vendor shall verify and provide documentation that that all employed guards have completed background checks.

The Vendor shall coordinate with local authorities when installing and using remote alarm systems.

The Vendor shall provide non-reproducible keys or keycards for all locks.

The Vendor shall verify and provide documentation that security features do not hamper operations.

The Vendor shall verify and provide documentation that monitoring and alarm of physical access can be separated from the control network.

11.2.4 FAT Measures

The Vendor shall test and provide documentation that all alarm systems pick up all instances of intrusion with minimal false alarms.

11.2.5 SAT Measures

The Vendor shall provide access control mechanisms to the Purchaser.

The Vendor shall provide a walk-through of expected physical security functionality to the Purchaser.

The Vendor shall provide adequate onsite training to operators and guards prior to site start up.

The Vendor shall verify and provide documentation on all remote alarm, surveillance, and locking functionality prior to start up.

11.2.6 Maintenance Guidance

The Vendor shall maintain access control mechanisms in a secure configuration.

The Vendor shall validate perimeter security performance on a prenegotiated basis.

The Vendor shall change all locks, locking codes, keycards, and any other keyed entrances on a prenegotiated basis.

The Vendor shall coordinate access control changes with the Purchaser to include, but not be limited to, an update of the site physical security.

11.2.7 References

IEEE Standard 1402-2000, "IEEE Guide for Electric Power Substation Physical and Electronic Security," IEEE, New York, New York, April 4, 2000.

NERC, Critical Infrastructure Protection Reliability Standards, CIP-002-1—CIP-009-1

11.2.8 Dependencies

None, this topic is stand-alone.

11.3 Manual Override Control

Manual override controls include mechanisms such as circuit breaker hand switches, valve levers, and end-device panels.

11.3.1 Basis

Physical security of manual override controls are commonly overlooked with the potential for exploit and system damage.

11.3.2 Language Guidance

Physical access to manual override controls should be heavily restricted to authorized personnel only. Unauthorized access to manual override controls poses the risk for system damage or intrusion, and therefore must be secured.

Detrimental system effects due to physical control or damage to one remote manual control mechanism (MCM) have been demonstrated in interconnected nodal systems. Therefore, although the local node may be unimportant, manual override control of a device within the local node may provide access or influence to other, more critical nodes.

The system importance of a particular MCM is a function of the type and amount of control it performs. In the power system for example, manual control of a transmission circuit breaker may affect operation of a large area of the system, and could result in massive blackouts, whereas control of distribution switchgear may affect a much smaller region, with fewer consequences. If the mal-operation of a MCM results in the loss of the node, plant, substation, or of a significant area outside that which it controls, it should be subject to increased security measures. If it is apparent that control of one MCM may result in the control of an entire system, as may be the case with local SCADA or cyber-related control mechanisms, then security of all such mechanisms shall be deemed of utmost importance.

The Purchaser shall be aware of the system importance of the MCM he or she wishes to protect. For MCMs requiring a locking device, the device shall be appropriate for the environment in which it is deployed.

11.3.3 Procurement Language

The Vendor shall provide the means to physically secure the MCM, whether through a lockable enclosure or locking functionality built into the MCM itself.

The Vendor shall provide two non-reproducible keys to all locking MCMs, as requested by the Purchaser.

The Vendor shall change all locks, locking codes, keycards, and any other keyed entrances according to a prenegotiated period.

11.3.4 FAT Measures

The Vendor shall verify and provide documentation that the MCM meets the requirements appropriate for the environment in which it is deployed.

11.3.5 SAT Measures

The Vendor shall verify and provide documentation that the implemented security does not compromise the required functionality of the MCM.

The Vendor shall provide results of security measure assessments identifying any potential bypass vulnerabilities.

11.3.6 Maintenance Guidance

The Vendor shall verify the implemented security and the functionality of the MCM according to a prenegotiated interval.

11.3.7 References

IEEE Standard 1402-2000, “IEEE Guide for Electric Power Substation Physical and Electronic Security,” IEEE, New York, New York, April 4, 2000.

NERC, Critical Infrastructure Protection Reliability Standards, CIP-002-1—CIP-009-1

11.3.8 Dependencies

Section 11.4, “Intra-perimeter Communications.”

11.4 Intra-perimeter Communications

Mechanisms within the perimeter may rely on intra-perimeter communication to ensure secure operation. The communication medium may consist of a physical, electrical (fly-by-wire), or wireless connection.

11.4.1 Basis

Intra-perimeter communications are commonly overlooked for security concerns. Access to the intra-perimeter communication medium constitutes access to the function or device itself with the potential for exploit and damage. The communication path must be physically secured to the same level as the components.

11.4.2 Language Guidance

The length and complexity of the communication channel to be protected should be minimized. The communication channel and access ports should also be hidden from view, out of reach, and/or behind layers of perimeter security if possible. A conduit may be placed around the communication medium to provide additional resistance to tampering. Wireless communication should not be detectable or accessible outside the perimeter.

11.4.3 Procurement Language

The Vendor shall verify and provide documentation that physical communication channels are secured from physical intrusion.

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter.

The Vendor shall verify and provide documentation that communication channels are as direct as possible.

11.4.4 FAT Measures

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to the required area.

The Vendor shall verify and provide documentation that the physical intrusion of communication channels is detectable.

11.4.5 SAT Measures

The Vendor shall verify and provide documentation that the range of the wireless communications is limited to within the perimeter.

The Vendor shall verify and provide documentation that the physical intrusion of communication channels is detectable.

The Vendor shall document the communication channels’ locations and access points.

11.4.6 Maintenance Guidance

The Vendor shall provide documentation that the implemented security measures are verified according to a prenegotiated interval.

11.4.7 References

IEEE Standard 1402-2000, “IEEE Guide for Electric Power Substation Physical and Electronic Security,” IEEE, New York, New York, April 4, 2000.

NERC, Critical Infrastructure Protection Reliability Standards, CIP-002-1—CIP-009-1

11.4.8 Dependencies

Section 12, “Network Partitioning.”

12. NETWORK PARTITIONING

Network partitioning refers to dividing a networked system in to multiple segments to facilitate better security controls.

12.1 Network Devices

Network devices are used to allow communication between other networked devices and networks.

12.1.1 Basis

The devices used to create, interconnect, segregate, protect, and isolate networks have operating systems (e.g., embedded operating system) and applications (e.g., port security, address blocking) that are susceptible to the same vulnerabilities and exploits found in most computer-based devices. Once deployed and functioning, if patch management for these devices is not rigorous, the devices will be left vulnerable to new exploits.

12.1.2 Language Guidance

Routers are network devices designed to direct network traffic between devices on separate networks. These devices have two or more routing interfaces and may connect to separate dedicated telecommunication equipment. Routers may implement additional capabilities such as ACL, port mirroring (e.g., span port), and some firewall functions. Advanced routers are able to operate in a failover or redundant configuration with another router to prevent communication failure. Routers include a method of interface configuration via a connected network or separate console port. These devices also contain an embedded operating system, which is held in nonvolatile firmware. Upgrades to the firmware may be performed over a network or a directly connected port. Vulnerabilities have been found in the embedded operating systems for routers requiring the need for updates. Exploits on the operating systems (e.g., resetting routers) have also been performed. ACLs are commonly used with routers for a layer of security. For a high-security network, a whitelist ACL is recommended.

Hubs or network concentrators are network devices that direct network traffic to all other devices connected within a network. These devices duplicate each received network packet and repeat it to every device connected to the hub. Hubs allow one connected device to communicate at a time. Multiple transmissions from several hosts can cause collisions that are detected by the hub. Most small hubs do not contain configuration information or firmware that can be upgraded by the end user. Advanced hubs allow management and firmware upgrades through a connected network or console port. Hubs are commonly used for multiple taps into a network (e.g., running two IDSs).

Switches are network devices that direct network traffic to other connected devices within a network. Switches have different switching speeds including 10, 100, 1000, or 10000 megabits per second (Mbps). Switches can have multiple media connections such as copper for lower bandwidth connections and fiber for high bandwidth connections. Switches can be managed or unmanaged. Unmanaged or “dumb” switches inspect received data packets, determine the destination device of that packet, and forward it to the appropriate port (i.e., L2 switches). Managed switches offer features such as virtual LAN (VLAN) segments, link aggregation, port mirroring, and other advanced networking capabilities (i.e., L3 switches). VLAN network segments implement the IEEE 802.1Q protocol for moving data between layer two networks. This allows hosts to be connected to different switches, but communicate as if the hosts share a common switch. Link aggregation or “trunking” refers to a method of moving multiple VLAN segments between switches or routers. This allows a single physical connection to carry multiple virtual network segments between devices. Port mirroring is a method by which data from one or many different switch ports is “mirrored” onto another port for monitoring and debugging. Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and network analyzers are normally connected to these ports. Managed switches can be controlled from a connected network port, separate console port, or an embedded Web-based interface. Managed switches contain an embedded operating system that is upgradeable via the configuration vectors. The embedded operating systems on switches are vulnerable to exploits that may allow access to a connected system or resetting of the switch. Port security can be enabled on switches when one MAC address is uniquely configured to one network port. This provides a layer of security for rogue devices being plugged into the switch.

Network security devices include firewalls, IDS, IPS, and VPN concentrators. These devices are used to segment and protect networks.

Firewalls are network security devices used to separate and control traffic between two or more networks or devices. These devices include features such as packet filtering, stateful packet inspection, and traffic flooding protection. Firewalls differ from routers in that firewalls are optimized to look inside packets for specific content, whereas router ACLs only look at packet headers to determine if a packet is filtered or not. A high security network firewall would have a “deny all” rule set. Firewall rule sets are frequently over complicated. Keeping network segments small, simple, and current aids in the firewall rule complexity issues. Firewalls generate logs that need to be reviewed to verify the firewall is working properly and no new unfiltered traffic exists (see Section 3.1).

Network intrusion detection systems (NIDS) are security devices that monitor traffic on a network segment or multiple segments. IDS appliances use signatures and anomaly-based intelligence to determine unauthorized or abnormal traffic activities on a network segment to generate alerts. NIDS are commonly used in conjunction with a firewall to verify the proper function of the firewall. NIDS produce logs of packet traffic that need to be reviewed for identifying unexpected packets (see Section 3.2).

Network intrusion prevention systems (NIPS) are security devices that monitor traffic on a network segment or multiple segments and use signatures and anomaly-based intelligence to block unauthorized or abnormal traffic. IPS appliances are usually configured inline with a network connection to actively block traffic in contrast to an IDS that passively monitors and alerts on traffic. Reporting by exception communication method is common for many control systems. Anomaly-based NIPS are rarely used since these would block traffic during a time when all end devices need to make a status report.

Virtual Private Network (VPN) concentrators are network devices designed to securely allow local network access to remote users. These systems build an encrypted tunnel between a local network and a remote host after a secure authentication or secure key exchange process. VPN concentrators are the preferred secure method for allowing remote users access to local network resources. Since firewalls and

IDS cannot inspect encrypted packets, exploit code can be sent through an encrypted tunnel without detection. ACL routers can verify IP header information only on encrypted packets (see Section 10.6).

12.1.3 Procurement Language

The Vendor shall provide a method for managing the network devices and changing addressing schemes.

The Vendor shall verify and provide documentation that the network configuration management interface is secured.

The Vendor shall provide ACLs, port security address lists, and enhanced security for the port mirroring.

The Vendor shall remove or disable unused network configuration and management functions on the network devices.

The Vendor shall provide firewall rules for inbound and outbound traffic based on deny-all rule sets.

The Vendor shall provide NIDS rules and log review tools that verify the function of the firewall and detect anomalous traffic.

The Vendor shall provide a NIPS architecture that will work with the communication method.

The Vendor shall provide VPN concentrators configured with filters and port security.

Post-contract award, the Vendor shall provide documentation on the network devices installed with security settings.

12.1.4 FAT Measures

The Vendor shall validate the method for managing the network devices and changing network addresses.

The Vendor shall verify security levels and provide documentation of the network configuration management interface.

The Vendor shall verify the ACLs, port security address lists, and describe the enhanced security for the port mirroring.

The Vendor shall scan the network ports and document traffic origination and functions for each port.

The Vendor shall provide documentation of firewall rules and IDS rules.

The Vendor shall verify and provide documentation of the log review tools validating IDS and firewall functions.

The Vendor shall verify and provide documentation of the NIPS architecture validating operations with normal and emergency control system communications.

The Vendor shall verify and provide documentation of the VPN architecture filters and port security.

The Vendor shall provide upgrades and patches to maintain the established level of system security.

12.1.5 SAT Measures

The Vendor shall validate the method for managing the network devices and changing network addresses.

The Vendor shall verify security levels and provide documentation of the network configuration management interface.

The Vendor shall verify and provide documentation of the ACLs, port security address lists, and describe the enhanced security for the port mirroring.

The Vendor shall scan the network ports and document traffic origination and functions for each port.

The Vendor shall verify and provide documentation of firewall rules and IDS rules.

The Vendor shall verify and provide documentation of the log review tools validating IDS and firewall functions.

The Vendor shall verify and provide documentation of the NIPS architecture validating operations with normal and emergency control system communications.

The Vendor shall verify and provide documentation of the VPN architecture verifying filters and port security.

The Vendor shall provide upgrades and patches to maintain the established level of system security.

12.1.6 Maintenance Guidance

The Vendor shall provide upgrades and patches to maintain the established level of system security.

The Vendor shall validate permissions and security settings on the baseline system before delivery of any upgrades or replacements.

12.1.7 References

NIST SP 800-53 Revision 2, “Recommended Security Controls for Federal Information Systems.”

Department of Homeland Security, Recommended Practice Control Systems Cyber Security Defense in Depth Strategies, May 2006.[s]

12.1.8 Dependencies

Section 3.1, “Firewall.”

Section 3.2, “Network Intrusion Detection System.”

Section 3.3, “Canaries.”

Section 10.5, “Virtual Private Networks.”

12.2 Network Architecture

Network architecture is how a network is designed and segmented into logical smaller functional subnetworks (subnets).

[s] http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

12.2.1 Basis

Poorly designed network architectures are vulnerable to exploits.

12.2.2 Language Guidance

Subnets are small functional groupings of network-attached devices usually connected to the same switch or group of switches. Subnets can contain any number of devices up to 16,777,214. Subnets are classified as Class A, B, or C depending on the size of the IP address space and netmask. Private, non-Internet routable addresses are usually assigned to devices without direct accessibility from the Internet. Private nonroutable addresses are defined as 10.X.X.X, 172.16.X.X, and 192.168.X.X by the Internet Assigned Number Authority (IANA).

A demilitarized zone (DMZ) is a separate network subnet designed to expose specific services to a larger, untrusted network. The subnets are used in large corporations to safely expose functions to the Internet, such as Web or database applications. DMZs are also used internal to networks to facilitate secure data transfer from a high security network zone to a zone with lower security. A DMZ uses explicit access control and contains computer hosts that provide network services to both low and high-security network zones. DMZ networks are usually implemented with a firewall or other traffic routing network device. It can be split into several sub-DMZ networks with specific functional groupings for the computers such Web servers, timeservers, or ftp repositories.

Secure network architectures contain a combination of network segmentation, traffic control, and traffic monitoring. Segmentation is used to separate functional sets of network hosts into groupings. Traffic control is implemented with routers and firewalls to prevent unauthorized access between different subnets. Traffic monitoring validates what traffic is allowed, and alerts when unauthorized traffic is detected.

When segmenting a network, devices associated with a heightened security profile should be grouped together and separated from devices with a lower security profile. An example would be a corporate network with tens or hundreds of normal users separated from a server cluster or network that needs maximum uptime. Data that needs to be moved between zones with different security levels should pass through a third network segment known as a DMZ. The DMZ should be considered to have the lowest security profile. Network devices hosted in a DMZ should replicate data between the higher security networks. The DMZ network collectively should consist of several functional DMZ networks with groupings of network hosts providing similar services. Segmentation is accomplished with firewalls and routers. Segments requiring heightened security should be segmented using a firewall to prevent unauthorized traffic between segments.

Traffic control between security zones should be employed with a firewall and use a “default deny” access policy. This requires all traffic to be dropped unless explicitly allowed with firewall rules. Network traffic should be specified by source and destination IP address and network port at a minimum. Data from a DMZ should be replicated over a minimum number of secure protocols.

Traffic monitoring of security zones should be performed inside each logical network segment at the minimum. For a more robust monitoring solution, both sides of a firewall or router can be monitored as a way to verify ACLs or firewall filtering rules. DMZ network segments should have an IDS dedicated to the segment. DMZ IDS logs should be checked often and validated against traffic in and out of the network. Traffic monitoring inside a static network environment should use whitelisting, port security, and canaries to enhance security (e.g., DMZ).

Secure control system segmentation should be implemented from the inside out. The control network is the highest security profile and requires the maximum uptime. A firewall should separate the control system from all other networks. If data from the control system is needed by another network, data should be replicated to DMZ in a secure manner such as secure ftp or secure copy. Data allowed though the firewall should be heavily restricted and only allow the minimum number of open ports and hosts to be available.

Network simplification should be a priority when designing initial architecture or firewall rules. The variety of protocols open for data should be kept to a minimum. Data that is modified multiple times and retransmitted such as database, Web, and ftp, should be moved to the DMZ first, modified in the DMZ, and transmitted from the DMZ to other networks.

12.2.3 Procurement Language

The Vendor shall provide and document secure network architecture where the higher-security zones originate communication to less-secure zones.

The Vendor shall provide and document the design for all communication paths between networks of different security zones through a DMZ.

The Vendor shall verify and document that disconnection points are established between the network partitions and provide the methods to isolate subnets to continue limited operations.

The Vendor shall provide and document tailored filtering and monitoring rules for all security zones and alarm for unexpected traffic.

The Vendor shall provide and document a DMZ that is restricted to communications where all traffic is monitored, alarmed, and filtered.

The Vendor shall provide and document outbound filtering and alarms for unexpected traffic through security zones.

The Vendor shall define all sources and destinations with enforced communication origination even during restart conditions between security zones.

The Vendor shall provide and document duel DMZ architectures using different products performing the same functionality running in parallel.

The Vendor shall provide and document a mechanism for patching a single DMZ architecture running in a parallel configuration without disruption to the other DMZ running in parallel.

Post-contract award, the Vendor shall provide network architecture documentation.

12.2.4 FAT Measures

The Vendor shall validate and provide documentation that the higher-security zones originate communication to less-secure zones.

The Vendor shall document all communication paths, including filtering, monitoring, and staging zones.

The Vendor shall verify and provide documentation of disconnection points between the network partitions and validate the continuity of limited operations.

The Vendor shall verify and provide documentation of tailored filtering and monitoring rules for all security zones and validate alarms for unexpected traffic.

The Vendor shall verify and provide documentation of restricted communications through the DMZ and verify that all traffic is monitored, alarmed, and filtered.

The Vendor shall verify and provide documentation of outbound filtering and alarms for unexpected traffic through security zones.

The Vendor shall verify and provide documentation of all sources and destinations with enforced communication origination even during restart conditions between security zones.

The Vendor shall verify and provide documentation of duel DMZ architectures using different products performing the same functionality running in parallel.

The Vendor shall verify and provide documentation of a mechanism for patching a single DMZ architecture running in a parallel configuration without disruption to the other DMZ running in parallel.

12.2.5 SAT Measures

The Vendor shall validate and provide documentation that the higher-security zones originate communication to less-secure zones.

The Vendor shall document all communication paths, including filtering, monitoring, and staging zones.

The Vendor shall verify and provide documentation of test disconnection points between the network partitions and validate the continuity of limited operations.

The Vendor shall test and provide documentation of tailored filtering and monitoring rules for all security zones and validate alarms for unexpected traffic.

The Vendor shall validate and provide documentation of restricted communications through the DMZ and verify that all traffic is monitored, alarmed, and filtered.

The Vendor shall validate and provide documentation of outbound filtering and alarms for unexpected traffic through security zones.

The Vendor shall validate and provide documentation of all sources and destinations with enforced communication origination even during restart conditions between security zones.

The Vendor shall validate and provide documentation of duel DMZ architectures using different products performing the same functionality running in parallel.

The Vendor shall validate and provide documentation of a mechanism for patching a single DMZ architecture running in a parallel configuration without disruption to the other DMZ running in parallel.

12.2.6 Maintenance Guidance

The Vendor shall provide upgrades and patches as vulnerabilities are identified in to maintain the established level of system security.

The Vendor shall reassess permissions and security settings on the baseline configuration before delivery of any upgrades or replacement components.

The Vendor shall verify and provide documentation that the network security architecture’s security profile is maintained.

12.2.7 References

NERC CIP-007-1, “Cyber Security — Systems Security Management.”

NIST SP 800-53 Revision 2, “Recommended Security Controls for Federal Information Systems.”

Department of Homeland Security, Recommended Practice Control Systems Cyber Security Defense in Depth Strategies, May 2006.

12.2.8 Dependencies

Section 3.1, “Firewall.”

Section 3.2, “Network Intrusion Detection System.”

13. TERMINOLOGY

Appliance—Used here to mean “all in one security solutions,” that can combine antivirus, firewall, and NIDS functionality.

Authentication—The process of verifying an identity claimed by or for a system entity. Also, any security measure designed to establish the validity of a transmission, message, originator, or a means of verifying and individual’s eligibility to receive specific categories of information (http://www.its.bldrdoc.gov/fs-1037/). Authentication is generally associated with a password and/or token(s) entered into a host system for gaining access to computer application(s) by a computer user. For example, the authentication is described as “what you have” (i.e., key), “what you know” (i.e., username and password), and “what you are” (i.e., biometric scan).

Authorization—A right or a permission that is granted to a system entity to access a system resource.

Auto Answer—A modem configuration where the modem automatically answers the phone when it rings.

Backdoor—A hidden method for bypassing normal computer authentication.

BIOS—Basic Input/Output System or Basic Integrated Operating System. BIOS refers to the software code run by a computer when first powered on. The primary function of BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer. This process is known as booting up.

Canary—In computing, canary or canaries are dummy devices or unused Ethernet ports used in conjunction with detection software to warn of unauthorized network probing or surveillance. The name is an allusion to the use of canaries as warning devices in coal-mines.

Control System (CS)—An interconnection of components (computers, sensors, actuators, communication pathways, etc.) connected or related in such a manner to command, direct, or regulate itself or another system, such as chemical process plant equipment/system, oil refinery equipment/systems, electric generation/distribution equipment/systems, water/waste water systems, manufacturing control systems, etc.

Cross-Site Scripting (XSS) flaws—Programming errors commonly found on commercial Web sites that phishers and online scam artists can use to trick users into giving away personal and financial data.

Data Acquisition—Sampling of the real world to acquire data that can be recorded and/or manipulated by a computer. Sometimes abbreviated DAQ, data acquisition typically involves acquisition of signals and waveforms and processing the signals to obtain desired information.

Dial Back—Also called call-back; it is a modem security feature and configuration used to authenticate users over dial-up connections where the modem automatically answers the phone when it rings, hangs up, and dials back the preprogrammed number in the modem. Some modems can be configured for multiple numbers/users with usernames and passwords.

Dynamic Host Configuration Protocol (DHCP)—A protocol for assigning IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device’s IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address. Many ISPs use dynamic IP addressing for dial-up access.

Extensible Authentication Protocol (EAP)—Pronounced *"eep,"* it is a universal authentication mechanism frequently used in wireless networks and Point-to-Point connections. Although the EAP protocol is not limited to wireless local area networks (LANs) and can be used for wired LAN authentication, it is most often used in wireless LAN networks. The WPA and WPA2 standard has officially adopted five EAP types as its official authentication mechanisms.

Encryption—In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge.

Factory Acceptance Test (FAT)**—**A test conducted at the Vendor's premise usually by a third-party to verify operability of a system according to specifications.

Firewall—Hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy. It has the basic task of controlling traffic between different zones of trust. Typical zones of trust include the Internet (a zone with no trust) and an internal network (a zone with higher trust).

Firmware—Software that is embedded in a hardware device. It is often provided on flash ROMs or as a binary image file that can be uploaded onto existing hardware by a user.

Heartbeat Signals—Also known as watchdog timer, keep-alive, health status. The signals indicate the communications health of the system.

Human-Machine Interface (HMI) Refers to the layer that separates a human that is operating a machine from the machine itself. One example of a HMI is the computer hardware and software that enables a single operator to monitor and control large machinery remotely.

Host-based Intrusion Detection System (HIDS)—An application that detects possible malicious activity on a host from characteristics such as change of files (file system integrity checker), operating system call profiles, etc.

Hyper-Text Transfer Protocol (HTTP)—A request/response protocol between clients and servers. The originating client, such as a Web browser, spider, or other end-user tool, is referred to as the user agent. The destination server, which stores or creates resources such as HTML files and images, is called the origin server.

Intrusion Detection System (IDS)—Software or an appliance used to detect unauthorized access or malicious or abnormal operation to a computer system or network. IDS systems that operate on a host to detect malicious activity are called host-based IDS systems or HIDS. IDS systems that operate on network data flows are called network-based IDS systems or NIDS.

Internet Protocol (IP)—A data-oriented protocol used by source and destination hosts for communicating data across a packet-switched inter-network. Data in an IP inter-network are sent in blocks referred to as packets or datagrams (these terms are basically synonymous in IP).

Intrusion Prevention System (IPS)—Any hardware and/or software system that proactively 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, that uses knowledge of malicious behavior.

Internet Protocol Security (IPSec)—A set of cryptographic protocols for securing packet flows and key exchange. Of the former, there are two: Encapsulating Security Payload (ESP) provides authentication, data confidentiality, and message integrity; Authentication Header (AH) provides authentication and message integrity, but does not offer confidentiality. Originally AH was only used for integrity and ESP was used only for encryption; authentication functionality was added subsequently to ESP.

Leased Lines—A reserved open circuit between two points rented most often by businesses to guarantee bandwidth for network traffic. A subset of dedicated lines.

Local Area Network (LAN)—A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings (campus).

Malware—Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, Root kits, spyware and adware.

Network Device—A computer connected to a network providing services to and/or using services from other network devices. Also called a network node.

Network Intrusion Detection System (NIDS)—A hardware tool which monitors IP traffic on a network segment (or segments) to detect unauthorized access to a computer system or network.

Nonrepudiation—The sender cannot deny that he/she sent the data in question to ensure that a traceable legal record is kept and has not been changed by a malicious entity.

Packet—A structured and defined part of a message transmitted over a network.

Patch—A fix for a software program where the actual binary executable and related files are modified.

Post-Contract Award—A term meaning a point in time in which all terms of the contract have been agreed. Some business sensitive information need not be shared during the bidding process but does when the contract is awarded. The term would be used in a procurement specification to indicate expectations upon the Vendor by the Purchaser for information of products necessary after the contract is awarded.

Programmable Logic Controller (PLC)—A programmable microprocessor-based device designed to control and monitor various inputs and outputs used to automate industrial processes.

Port—Hardware Port: An outlet on a piece of equipment into which a plug or cable connects. Network port: An interface for communicating with a computer program over a network. I/O or machine port - port-mapped I/O: Nearly all processor families use the same assembly instructions for memory access and hardware I/O. Software port: Software is sometimes written for specific processors, operating systems, or programming interfaces. A software port is software that has been changed to work on another system.

Private Branch Exchange (PBX)—A privately owned electronic switching system used to make connections between the PSTN and the internal telephones of a private organization, building, or site.

Process Control—An engineering discipline that deals with architectures, mechanisms, and algorithms for controlling the output of a specific process. For example, heating up the temperature in a room is a process that has the specific, desired outcome to reach and maintain a defined temperature (e.g., 20°C), kept constant over time. Here, the temperature is the *controlled variable*. At the same time, it is the *input variable* since it is measured by a thermometer and used to decide whether to heat or not to heat. The desired temperature (20°C) is the *set point*. The state of the heater (e.g., the setting of the valve allowing hot water to circulate through it) is called the *manipulated variable* since it is subject to control actions.

Process Field Bus (PROFIBUS)—A popular type of fieldbus for factory and industrial automation with worldwide more than 10 million nodes (2004) in use.

Public-Switched Telephone Network (PSTN)— the worldwide collection of public interconnected telephone networks primarily designed for voice traffic. Sometimes referred to as POTS (plain old telephone system).

Role-Based Access Control (RBAC)—An approach to restricting system access to authorized users. It is a newer and alternative approach to Media Access Control (MAC) and Discretionary Access Control.

Root kits—Sets of programs that are introduced into a computer system without permission of the computer operator to obtain privileged access, which would allow control of the computer, usually with capabilities to avoid detection.

Router— A computer networking device that forwards data packets between disparate networks through a process known as routing. Routing occurs at Layer 3 of the OSI seven-layer model.

Scanning—Can refer to any of the following:

- Active Port Scanning—Actively sending out network packets to enumerate all of the open ports of a device, including both TCP and UDP Port ranges 0–65535.
- Passive Traffic Mapping/Scanning—Passively recording network traffic, usually through the use of span/monitor ports on the networking hardware. This discovers the ports that are normally used, but will not detect open ports that are not actively used by the system. As such this method will provide an incomplete view of what services/ports are available.
- Security Scanning—A nebulous term that could refer to any type of scanning.
- Version Scanning—Actively attempts to discover the protocol and the protocol version by connecting to the open ports and performing a sequence of fingerprinting actions.
- Vulnerability Scanning—Actively connects to the remote device and attempts to exploit known vulnerabilities. Often includes active port scanning and version scanning to first discover the vulnerabilities.

Supervisory Control and Data Acquisition (SCADA)—A SCADA computer system is developed for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining and transportation.

Server—A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files, a Web server for access to Web content, a DNS server for domain name services, a database server for access to relational tables, an e-mail server for access to e-mail, etc.

Services—Software application that facilitates communications to other applications or devices either local or distributed. Services are typically associated to a port. Sometimes services are referred to as software ports.

Single Sign-on—A specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems normally enabled by role-based access control.

Site Acceptance Test (SAT)—A test conducted at the customer location, often by a third-party, to verify operability of a system according to specifications immediately prior to commissioning.

Stateful Firewall—A firewall that keeps track of the state of network connections (such as TCP streams) traveling across it. Source packets are entered into the state table. Response packets are checked against the state table and only those packets constituting a proper response are allowed through the firewall.

Transmission Control Protocol (TCP)—One of the main protocols in TCP/IP networks. Whereas, the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data over many packets. TCP includes mechanisms and protocols to ensure delivery of the data in the correct sequence from source to destination.

User Datagram Protocol (UDP)—A connection-less transport layer protocol that is currently documented in IETF RFC 768. In the TCP/IP model, UDP provides a very simple interface between a network layer below and an application layer above. UDP has no mechanism to ensure delivery of the data in the packets, nor can it ensure that delivery of the packets is in the proper sequence. If desired, this must be performed by the application layer.

Upgrade—Generally an upgrade is a new release of software, hardware and/or firmware replacing the original components to fix errors and/or vulnerabilities in software and/or provide additional functionality and/or improve performance.

Universal Serial Bus (USB)—Provides a serial bus standard for connecting devices, usually to a computer, but it also is in use on other devices.

Validate—To give evidence for or establish the soundness of. Validation is a process of checking documents or testing against a formal standard.

Virus—Software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs. See Malware.

Virtual Private Network (VPN)—A private, encrypted communications network usually used within a company, or by several different companies or organizations, used for communicating in a software tunnel over a public network.

War Dialing—The practice of dialing all the phone numbers in a given range to find those numbers connected to devices that will answer a modem.

Wireless Fidelity (WiFi)—Meant to be used generically when referring of any type of 802.11 network, whether 802.11b/a/g dual-band, etc.

Worm—A computer worm is a self-replicating computer program similar to a computer virus. In general, worms harm the network and consume bandwidth.

WiFi Protected Access (WPA)—WPA and WPA2 are wireless standards providing higher levels of security than WEP. WPA2 is based on IEEE 802.11i and provides government grade security based on NIST standards and AES encryption.