

Cyber Security Procurement Language for Control Systems Version 1.6

Gary Finco, Kathleen Lee, Greg Miller,
Jeffrey Tebbe, Rita Wells

June 2007

Cyber Security Procurement Language for Control Systems Version 1.6

**Authors: Gary Finco, Kathleen Lee, Greg Miller, Jeffrey Tebbe, Rita Wells
Contributors: Dirck Copeland, Edward Gorski, David Kuipers, Jerry Litterer,
Will Pelgrin, May Permann, Heather Rohrbaugh**

June 2007

**INL Critical Infrastructure Protection/Resilience Center
Idaho Falls, Idaho 83415**

**Prepared by
Idaho National Laboratory
for the
U.S. Department of Homeland Security, National Cyber Security Division
Under DOE Idaho Operations Office Contract DE-AC07-051D14517**

FORWARD

A key component in protecting our nation's most important critical infrastructure 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 the 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 information it received.

For example, a control system gathers information such as where a leak in a pipeline has occurred, transfers the information back to a central site alerting the home station that the leak has occurred, carrying out necessary analysis and control such as determining if the leak is critical and displaying the information in a logical and organized fashion. In this example, one of the functions that the control system could perform if a leak is detected is to shut down the pipeline.

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 of the critical infrastructure involved with control systems, there needs to be a general recognition of the important role that these systems perform, the associated potential vulnerability and challenges and consequences if these systems are compromised.

The recent disclosure of a SCADA system compromise responsible for controlling a local government's municipal water supply is just one example, which highlights the need to focus cyber security efforts in this important and critical area. SCADA security is an emerging issue, which can no longer be ignored. Education is a critical factor for success. A concerted educational and awareness campaign has to be implemented.

WHY SHOULD WE BE CONCERNED?

Control system technology has evolved over the past 30 years as a method of monitoring and controlling large processes. Control systems were first used in the 1960s. The life cycle of a control system is between 15 and 30 years.

30 years or even 15 years ago, security was not generally on anyone's priority agenda. With regard to control systems, it just was not an issue for systems like these. Traditionally, these control systems were stand alones, not connected to the outside world via the Internet.

Over the years, these systems have gone from proprietary, stand-alone systems, to those that use off-the-shelf hardware and software components. With

more commonly used hardware and software, comes the potential for increased concern of vulnerabilities and attacks.

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

This is not to say that all SCADA systems are vulnerable or are at risk of attack. The fact is that these systems control some of the nation's most critical assets. These systems are so important that whether the threat is real or an urban legend does not matter, they must be protected.

In March 2004, the Government Accountability Office (GAO) published a report on SCADA security¹ that it produced at the request of the 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 factors contributing 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.

THE CYBER SECURITY PROCUREMENT LANGUAGE FOR CONTROL SYSTEMS

Idaho National Laboratory, Department of Homeland Security, the CISO of New York State, and SANS Institute have developed an initiative to bring public and private sector entities together to improve our security posture around control systems. The goal is for private and public asset owners and regulators to come together and adopt procurement language that will help ensure that security is integrated into control systems.

The Cyber Security Procurement Language for Control Systems project, established in March 2006, is a joint effort among public and private sectors focused on development of common procurement language that can be used by

1. [GAO "Challenges and Efforts to Secure Control Systems," March 2004.](#)

everyone. The goal is for federal, state, and local asset owners and regulators to come together using these procurement requirements and to maximize the collective buying power to help ensure that security is integrated into control systems.

The Procurement Project Workgroup comprises 172 public and private sector entities from around the world representing asset owners, operators, and regulators. In addition, over 20 vendors participate in a working group to assist in reviewing and producing the procurement language. The Procurement Project is undertaking a number of initiatives to meet its goals.

Visit www.msisac.org/scada for the most up to date information and the latest release of the document. The document was downloaded 4,947 times from just October through December of 2006.

ACKNOWLEDGMENTS

Michael Assante and the author team of Idaho National Laboratory (INL), Will Pelgrin of the State of New York, and Alan Paller of SANS wish to thank their colleagues and industry participants who reviewed drafts of the document and contributed to its technical contents. Although no longer considered a draft, comments on this document continue to be welcome and encouraged. Submit comments to scadasummit@inl.gov with the subject line of “Procurement Project.” The authors would also like to acknowledge the Department of Homeland Security National Cyber Security Division, which funded this effort.

TRADEMARK INFORMATION

All product names are registered trademarks or trademarks of their respective companies.

SECURITY OBJECTIVES

Security objectives are divided into seven categories, as defined in traditional information assurance areas: Confidentiality, Integrity, Availability, Access Control, Authentication, Authorization, and Nonrepudiation.² For information technology (IT) systems, this has evolved into Confidentiality, Integrity, and Availability. For the control system configurations the importance of these objectives is reversed with Availability being the most important followed by Integrity and Confidentiality. The Supervisory Control and Data Acquisition (SCADA) and control systems must be available continuously when controlling critical infrastructure or life safety systems. Integrity of the information is important for the operators to act on the readings of the sensors or status of the system being operated. 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....”³ 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 their control and monitoring functions.

The timeliness of data being sent to or received from control systems is paramount. The control system also has to know that the data being sent or received are true. These two requirements inherently require that a high priority be given for 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 result in failure. Because the

2. FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems,” Federal Information Processing Standards, December 2003.

3. 44 United States Code, Section 3542.

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

Basic protections need to be in place to prevent any random non-targeted IT-based DoS from impacting the control system. 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 master source of the data or “guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity...”⁴ 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 (see 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 themselves (programs and memory) could affect the integrity of the system.

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

A large part of the access control objective is physical. All the cyber security layers required 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 (see Authorization), the breach in access control may result in a loss of confidentiality, integrity, and system availability. Access control is a particularly difficult situation for assets located in remote geographically dispersed areas. For this reason, access control is included.

Authentication is ensuring that entities verify who they say they are and that a malicious entity is not spoofing an authorized identity. Authentication is important when the entity first gains access to a system or applications. There are three types of authentication that is described as “what you have” (i.e., key), “what you know” (i.e., username and password), and “what you are” (i.e.,

4. 44 United States Code, Section 3542.

biometric scan). The more detailed privileged rights will be 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 issue when the entities are not human, but processes and information on an end-field device. Hardware authentication can be done via static addressing, or the passing of 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. In the traditional IT world, role-based permissions are implemented and normally linked to an account password authentication task, and permission tables for applications. 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 behavior 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" really looks like data. There is a trend to include this as nonrepudiation to ensure the code has not been changed since its last installation.

Other unique solutions for integrity include a deep packet inspection of data, sequence numbers in proprietary protocols, checksums in protocols, and host-based intrusion detection systems (IDSs) that records 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..."⁵ A loss of confidentiality is the unauthorized disclosure of information.

Attackers can identify account names and passwords if sent in clear text and use this to gain access to a system. Sophisticated target attacks can be done

5. 44 United States Code, Section 3542.

by studying network traffic on control systems allowing the attacker to reverse engineer protocols. This information, along with operational data, is used for a targeted attack. Sophisticated targeted attacks can be done by studying the applications to discover vulnerabilities and exploiting to gain control of the system.

The primary data that needs to be kept unseen are the most basic accounts and passwords in control systems commonly achieved by storing these files encrypted.

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

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.⁶ The commands sent to the endpoints are normally not understandable (i.e., 670M), but could be studied for a protocol attack. The databases that store the input and output points and the applications that display this information in context make this information valuable. Encryption of these communication links is often used for the authentication functions rather than the confidentiality aspects. The reason encryption is being used is due to the lack of robust protocols that do not ensure the sent item is what was received and that it was sent by an authorized entity.

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

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 they 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) provides the data for the forecasting and financial systems, those communications have to be managed to obtain the security objectives identified. Mandated security requirements, such as Sarbanes-Oxley,⁷ that govern financial data, need to be considered when control systems are interfaced to corporate applications.

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

7. The Sarbanes Oxley Act of July 30, 2002, SOX.

FUTURE TOPICS

Procurement language planned for a future release is specific to the following topics:

- Configuration Management
- Backup and Recovery
- Disaster Recovery
- Wireless Networks and Communications
- End Network Devices
- Lifecycle Issues
- System Integration
- Logging and Auditing
- Training
- Least Privilege
- Enumeration
- Physical Access
- Contract Services
- Redundancy
- Policies and Procedures
- Network Partitioning
- Remote Access.

CONTENTS

FORWARD	iii
ACKNOWLEDGMENTS	vii
TRADEMARK INFORMATION	vii
SECURITY OBJECTIVES	ix
FUTURE TOPICS	xiii
ACRONYMS	xxi
1. INTRODUCTION	1
1.1 Topical Template	2
2. SYSTEM HARDENING	3
2.1 Removal of Unnecessary Services and Programs	3
2.1.1 Basis	3
2.1.2 Language Guidance	3
2.1.3 Procurement Language	3
2.1.4 FAT Measures	4
2.1.5 SAT Measures	5
2.1.6 Maintenance Guidance	5
2.1.7 References	5
2.1.8 Dependencies	5
2.2 Host Intrusion Detection Systems	5
2.2.1 Basis	5
2.2.2 Language Guidance	6
2.2.3 Procurement Language	6
2.2.4 FAT Measures	6
2.2.5 SAT Measures	6
2.2.6 Maintenance Guidance	7
2.2.7 References	7
2.2.8 Dependencies	7
2.3 Changes to File System and Operating System Permission	7
2.3.1 Basis	7
2.3.2 Language Guidance	7
2.3.3 Procurement Language	7
2.3.4 FAT Measures	8
2.3.5 SAT Measures	8
2.3.6 Maintenance Guidance	8
2.3.7 References	8

2.3.8	Dependencies	8
2.4	Hardware Configuration	8
2.4.1	Basis	8
2.4.2	Language Guidance.....	8
2.4.3	Procurement Language.....	9
2.4.4	FAT Measures	9
2.4.5	SAT Measures	9
2.4.6	Maintenance Guidance.....	9
2.4.7	References	9
2.4.8	Dependencies	9
2.5	Heartbeat Signals.....	10
2.5.1	Basis	10
2.5.2	Language Guidance.....	10
2.5.3	Procurement Language.....	10
2.5.4	FAT Measures	10
2.5.5	SAT Measures	10
2.5.6	Maintenance Guidance.....	10
2.5.7	References	10
2.5.8	Dependencies	10
2.6	Installing Operating Systems, Application, and Third Party Software Updates	11
2.6.1	Basis	11
2.6.2	Language Guidance.....	11
2.6.3	Procurement Language.....	11
2.6.4	FAT Measures	12
2.6.5	SAT Measures	12
2.6.6	Maintenance Guidance.....	12
2.6.7	References	12
2.6.8	Dependencies	13
3.	PERIMETER PROTECTION.....	14
3.1	Firewalls	14
3.1.1	Basis	14
3.1.2	Language Guidance.....	14
3.1.3	Procurement Language.....	14
3.1.4	FAT Measures	15
3.1.5	SAT Measures	15
3.1.6	Maintenance Guidance.....	15
3.1.7	References	15
3.1.8	Dependencies	15
3.2	Network Intrusion Detection System	15
3.2.1	Basis	15

3.2.2	Language Guidance.....	16
3.2.3	Procurement Language.....	16
3.2.4	FAT Measures.....	16
3.2.5	SAT Measures.....	16
3.2.6	Maintenance Guidance.....	16
3.2.7	References.....	17
3.2.8	Dependencies.....	17
3.3	Canaries.....	17
3.3.1	Basis.....	17
3.3.2	Language Guidance.....	17
3.3.3	Procurement Language.....	17
3.3.4	FAT Measures.....	17
3.3.5	SAT Measures.....	18
3.3.6	Maintenance Guidance.....	18
3.3.7	References.....	18
3.3.8	Dependencies.....	18
4.	ACCOUNT MANAGEMENT.....	19
4.1	Disabling, Removing or Modifying Well-Known or Guest Accounts.....	19
4.1.1	Basis.....	19
4.1.2	Language Guidance.....	19
4.1.3	Procurement Language.....	19
4.1.4	FAT Measures.....	20
4.1.5	SAT Measures.....	20
4.1.6	Maintenance Guidance.....	20
4.1.7	References.....	20
4.1.8	Dependencies.....	20
4.2	Session Management.....	20
4.2.1	Basis.....	20
4.2.2	Language Guidance.....	20
4.2.3	Procurement Language.....	21
4.2.4	FAT Measures.....	21
4.2.5	SAT Measures.....	21
4.2.6	Maintenance Guidance.....	21
4.2.7	References.....	21
4.2.8	Dependencies.....	21
4.3	Password/Authentication Policy and Management.....	22
4.3.1	Basis.....	22
4.3.2	Language Guidance.....	22
4.3.3	Procurement Language.....	22
4.3.4	FAT Measures.....	22
4.3.5	SAT Measures.....	22
4.3.6	Maintenance Guidance.....	22

4.3.7	References	22
4.3.8	Dependencies	23
4.4	Account Audit and Logging	23
4.4.1	Basis	23
4.4.2	Language Guidance.....	23
4.4.3	Procurement Language.....	23
4.4.4	FAT Measures	23
4.4.5	SAT Measures	23
4.4.6	Maintenance Guidance.....	23
4.4.7	References	23
4.4.8	Dependencies	24
4.5	Role-Based Access Control for Control System Applications.....	24
4.5.1	Basis	24
4.5.2	Language Guidance.....	24
4.5.3	Procurement Language.....	24
4.5.4	FAT Measures	25
4.5.5	SAT Measures	25
4.5.6	Maintenance Guidance.....	25
4.5.7	References	25
4.5.8	Dependencies	25
4.6	Single Sign-On	25
4.6.1	Basis	25
4.6.2	Language Guidance.....	25
4.6.3	Procurement Language.....	26
4.6.4	FAT Measures	26
4.6.5	SAT Measures	26
4.6.6	Maintenance Guidance.....	26
4.6.7	References	26
4.6.8	Dependencies	26
4.7	Separation Agreement	26
4.7.1	Basis	26
4.7.2	Language Guidance.....	27
4.7.3	Procurement Language.....	27
4.7.4	FAT Measures	27
4.7.5	SAT Measures	27
4.7.6	Maintenance Guidance.....	27
4.7.7	References	27
4.7.8	Dependencies	27
5.	CODING PRACTICES	28
5.1	Coding for Security	28

5.1.1	Basis	28
5.1.2	Language Guidance.....	28
5.1.3	Procurement Language.....	29
5.1.4	FAT Measures	29
5.1.5	SAT Measures	29
5.1.6	Maintenance Guidance.....	29
5.1.7	References	29
5.1.8	Dependencies	30
6.	FLAW REMEDIATION	31
6.1	Notification & Documentation from Vendor	31
6.1.1	Basis	31
6.1.2	Language Guidance.....	31
6.1.3	Procurement Language.....	31
6.1.4	FAT Measures	31
6.1.5	SAT Measures	32
6.1.6	Maintenance Guidance.....	32
6.1.7	References	32
6.1.8	Dependencies	32
6.2	Problem Reporting.....	32
6.2.1	Basis	32
6.2.2	Language Guidance.....	32
6.2.3	Procurement Language.....	33
6.2.4	FAT Measures	33
6.2.5	SAT Measures	33
6.2.6	Maintenance Guidance.....	33
6.2.7	References	33
6.2.8	Dependencies	33
7.	MALWARE DETECTION AND PROTECTION.....	34
7.1	Malware Detection and Protection	34
7.1.1	Basis	34
7.1.2	Language Guidance.....	34
7.1.3	Procurement Language.....	34
7.1.4	FAT Measures	35
7.1.5	SAT Measures	35
7.1.6	Maintenance Guidance.....	35
7.1.7	References	35
7.1.8	Dependencies	35
8.	HOST NAME RESOLUTION.....	36
8.1	Network Addressing and Name Resolution	36
8.1.1	Basis	36

8.1.2	Language Guidance.....	36
8.1.3	Procurement Language.....	37
8.1.4	FAT Measures.....	37
8.1.5	SAT Measures.....	38
8.1.6	Maintenance Guidance.....	38
8.1.7	References.....	38
8.1.8	Dependencies.....	38
9.	TERMINOLOGY.....	39

ACRONYMS

BIOS	Basic Input/Output System
BIND	Berkeley Internet Name Domain
CERT	Computer Emergency Response Team
CPU	Central Processing Unit
CS	Control System
DCS	Distributed Control System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Video Disc
EAP	Extensible Authentication Protocol
EMS	Energy Management System
FAT	Factory Acceptance Test
FTP	File Transfer Protocol
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
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
ISA	Instrumentation, Systems, and Automation Society

ISAC	Information Sharing and Analysis Center
ISC	Internet Software Consortium
ISO	International Standards Organization
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
NERC	North American Electric Reliability Corporation
NIDS	Network Intrusion Detection System
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
OLE	Object Linking and Embedding
OPC	OLE for process control
OS	Operating System
OSI	Open Systems Interconnectivity
PCS	Process Control System
PLC	Programmable Logic Controller
PROFIBUS	Process Field Bus
RBAC	Role-Based Access Control
RPC	Remote Procedure Call
RTU	Remote Terminal Unit/Remote Telemetry Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedure
SSH	Secure Shell Terminal Emulation
SSL	Secure Sockets Layer

SSO	Single Sign-On
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WiFi	Wireless Fidelity
WPA	WiFi Protected Access

Cyber Security Procurement Language for Control Systems Version 1.0

1. INTRODUCTION

The purpose of this document is to summarize security principles that should be considered when designing and procuring control systems products (software, systems, and networks) and provide example language to incorporate into specifications, which addresses these concerns. 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 cyber security risk in control systems 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 requirements that map directly to critical vulnerabilities that have been observed in current and legacy control systems and that can be mitigated by technology providers and organizations through effective management of the technology across its operational lifespan. It is the result of a process that brought together leading control system security experts, purchasers, integrators, and technology providers or 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 countries around the world.

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 existence of this specification does not forego engineering practices. The prime requirements, functions, design, and expected system behaviors need to be taken into account prior to adding or requesting security requirements. Each topic should be considered individually. 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 customer’s needs.

The user should be 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. The vendor could be a valuable resource to the purchaser as many are considered industry experts. It is not the intention of this document to discount the expertise of the system vendors.

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. This would range from non-disclosure agreements for the request of proposal response to encrypting files containing sensitive configuration information.

This will be a living document, due to the rapidly changing security environment and on-going vulnerability and exploit discovery. The procurement and maintenance language will be updated to add new topics as vulnerabilities that are critical are identified, as technology changes, and as more current methods of mitigating security risk are identified. A list of proposed future topics is found on page xiii.

A note on hyperlinks in the electronic version of this document: Many terms defined in the [Terminology](#) section are [hyperlinked](#) to Internet definitions sites (mainly wikipedia.org/wiki). 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, that is, 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).

Factory Acceptance Test Measures: The [Factory Acceptance Test](#) (FAT) is necessary to ensure security features function properly and provide the expected levels of functionality. Each topic includes FAT tasks specific to that topic. However, in general, prior to initiation of each FAT, the vendor shall install all operating systems (OS) 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, but before cutover or commissioning, to demonstrate 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 in addition occur at multiple locations.

Maintenance Guidance: This is guidance on how the Vendor will maintain the level of system security established during the SAT as the system evolves, is upgraded, and patched. This subsection may be best included as a security clause in a maintenance contract, rather than in a procurement specification to maintain on-going 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 systems (OS), software applications, and required third party software to limit security vulnerabilities.

2.1 Removal of Unnecessary Services and Programs

2.1.1 Basis

Unused services in a host OS that are left enabled are possible entry points for exploits on the network and are generally not monitored since they are not used. Only the services used for control systems (CS) 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 OS 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 “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 Purchaser-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 they 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 their 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 Vendor shall ensure all services are patched to current status.

The Vendor shall provide, within a prenegotiated period, an updated list as upgrades or patches are made available to any of the items mentioned above.

The Vendor shall remove or disable all software artifacts similar to those listed above that are not required for the operation and maintenance of the CS prior to FAT. The software to be removed or disabled shall specifically include, but not be limited to:

1. Games
2. Device drivers for network devices not delivered
3. Messaging services (e.g., MSN,⁸ 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 CS
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, for example, Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.

2.1.4 FAT Measures

The Vendor shall ensure that the Purchaser requires the results of assessment 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, their 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 operation of that device. Indicate the service name, protocol (e.g., TCP and UDP) and port range
 - b. Dependencies on underlying OS 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 effected.

8. Product Disclaimer.

2. The Vendor shall install Firmware updates available for the computer or network device certified by the system manufacturer at the time of installation.
3. The Vendor shall provide a summary table indicating each communication path required by the system. Include the following information in this table:
 - a. Source device name and Media Access Control (MAC)/IP address
 - b. Destination device name and MAC/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 assessment scans run on the system, as a primary activity of the SAT, with an inventory of the required services, their patching status, and their required documentation. At the conclusion of the SAT and before cutover or commissioning the above assessment scans (with the most current signature files) must be run again.

2.1.6 Maintenance Guidance

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

2.1.7 References

Instrumentation, Systems, and Automation Society (ISA), ISA-99.01: 4.2, 4.7; ISA-99.02: 5.3, B.14, C.3

North American Electric Reliability Corporation (NERC), Cyber Security – Critical Infrastructure Protection, CIP-007-1 R2, June 1, 2006

National Institute of Standards and Technology (NIST) – Special Publications, 800-42

2.1.8 Dependencies

None, this topic is stand-alone.

2.2 Host Intrusion Detection Systems

2.2.1 Basis

In unmonitored systems it is difficult to detect unauthorized changes or additions to the OS 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

Host intrusion detection system (HIDS) can be installed to perform a variety of integrity checks to detect attempted unauthorized access. Typically, the HIDS operates by performing checks on files to detect tampering, escalations of privileges, and account access; by intercepting sensitive OS functions; or by some combination of both. Additional HIDS capabilities may include monitoring attempts to access the system remotely (e.g., “scanning”).

Note that configuration of the HIDS is minor compared to required 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 shall be logged by the HIDS. 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 OS functions.

The Vendor shall recommend log review and notification software tools.

If local storage devices are used, the Vendor shall configure devices as “append only” to prevent alteration of records.

2.2.4 FAT Measures

The Vendor shall ensure 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 ensure 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 SAT to be used later as a control baseline.

2.2.6 Maintenance Guidance

The Vendor shall develop an on-going patch management and a rules and filters update process for the specified HIDS configuration agreed upon in the Procurement Language.

2.2.7 References

CIP-005-1 R3

CIP-007-1 R6

ISA-99.01: 3.1; ISA-99.02: C.3.

NIST SP 800-12, 800-31, 800-82 (Draft), 800-94

See Section 3.2 for Network Intrusion Detection Systems (NIDS)

2.2.8 Dependencies

None, this topic is stand-alone.

2.3 Changes to File System and Operating System Permission

2.3.1 Basis

Configurations for out-of-the-box operating systems (OS) and file systems normally are more permissive than necessary.

2.3.2 Language Guidance

In many cases, OSs ship with default configurations that allow unneeded access to files, and loose configuration parameters that can be exploited in order to gain information for further attacks. Common examples include OS 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.

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

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 of the permissions assigned.

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

2.3.5 SAT Measures

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

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

2.3.6 Maintenance Guidance

Anytime the system is upgraded, it is recommended that system vendors reassess permissions and security settings on their baseline system before delivery.

2.3.7 References

CIP-0071-1 R5.2

ISA-99.02: 5.3, B.14, C.3.

2.3.8 Dependencies

Section 4.1

2.4 Hardware Configuration

2.4.1 Basis

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

2.4.2 Language Guidance

Additional 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 drives or ports, such that only the monitor and pointing device and perhaps function panels are accessible.

It is recommended that system administrators be able to re-enable devices if they 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.

If technically feasible, the Vendor shall password protect the BIOS from unauthorized changes.

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

Where appropriate, the Vendor shall configure the network devices to limit access to/from specific locations.

The Vendor shall configure the system to allow the system administrators the ability to re-enable devices if they are disabled by software.

2.4.4 FAT Measures

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

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

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

2.4.6 Maintenance Guidance

If the Vendor supplies a replacement network device, the Vendor shall warrant that the replacement meets the same configuration.

2.4.7 References

CIP-005-1

CIP-006-1

2.4.8 Dependencies

None, this topic is stand-alone.

2.5 Heartbeat Signals

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. They indicate the communications health of the system. 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 they should be included in network monitoring.

If they are to be included in the network monitoring, post-contract award, the Vendor shall provide packet definitions of the heartbeat signals and examples of the heartbeat traffic.

2.5.4 FAT Measures

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

The Vendor shall create a baseline of the heartbeat communications traffic.

2.5.5 SAT Measures

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

The Vendor shall create a baseline of the heartbeat communications traffic and validate 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 by the appropriate party.

2.5.7 References

CIP-007-1 R6

2.5.8 Dependencies

Sections 2.2 and/or 3.2

2.6 Installing Operating Systems, Application, and Third Party Software Updates

2.6.1 Basis

Most successful cyber attacks occur in non-patched systems or applications. Patches and software updates, including anti-virus scanners, are required to lessen the possibility of cyber attack upon known vulnerabilities and exploits.

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, and even a new system is likely to be vulnerable based on the services that are active and because patches are not likely to be up-to-date. Therefore, an essential hardening activity is simply installing the latest versions or updates of any necessary software loaded on a system. Of course, testing and validation are necessary prior to running 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.

Scanning is an effective tool to identify vulnerabilities. Use caution however, as active scanning of control system networks have 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 a known vulnerability 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

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

The Vendor shall document in writing that all the updates have been tested and installed.

As part of the FAT, the Vendor shall perform security scans (with the most current signature files) to ensure that the system has not been compromised during the testing phase.

The Vendor shall document and provide the results of the scans.

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

2.6.5 SAT Measures

At the start of SAT, the Vendor shall install and update all tested and validated security patches.

The Vendor shall document in writing 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.

As a part of SAT, the Vendor shall perform security scans (with the most current signature files) to ensure that the system has not been compromised during the testing phase.

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 Purchaser shall negotiate a patch management process with the Vendor 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 to not apply released patches.

The Purchaser shall negotiate with the Vendor 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

CIP-007-1 R3

ISA-99.01: 5.3; ISA-99.02: 3.29, 3.43, 5.3, B.14, B.17, B.19, C.3

2.6.8 Dependencies

Section 4.5, 5.1, and 6.1

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

3.1.1 Basis

Firewalls are used to stop unauthorized connections between two networks or from a network to a networked device.

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,” simply blocked traffic based on IP address and port combinations.

Although any network device, which 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 which address 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 providing 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 to industrial protocols such as those commonly used in control 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, used in conjunction with HIDS, network intrusion detection systems (NIDS), application logs, etc., can be used for forensic purposes.

The Vendor shall provide exceptions to “deny all” rule sets to allow connections necessary for operation.

Network Appliances or “all in one solutions,” can combine antivirus, firewall, and NIDS functionality. The signature updates for such appliances are large and rarely can be sent over a control network. Testing signature updates on a nonproduction 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.

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.

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

3.1.4 FAT Measures

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

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

The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

3.1.5 SAT Measures

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

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

The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement. 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

CIP-005-1 R1

ISA-99.01: 3.1, 4.2, 4.4, 4.6, 4.7; ISA-99.02: B.1, B.14, C.3, D.4

NIST SP 800-41, 800-82 (Draft)

3.1.8 Dependencies

Section 4.1

3.2 Network Intrusion Detection System

3.2.1 Basis

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

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. Thus, this section assumes the NIDS is part of the control system.

There are two basic types of NIDSs: signature and anomaly based. Signature based NIDSs are similar to antivirus and vulnerability scanners in that they only detect known signatures. 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. This works well for deterministic networks with few report-by-exception events.

As with any appliance which can generate voluminous logs the configuration of the NIDS is a minor effort compared to the required 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 network.

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

Also, after the contract is awarded, for anomaly based NIDS, the Vendor shall provide traffic profiles with expected communication paths, network traffic, and expected utilization boundaries. For signature based NIDSs, the Vendor shall provide appropriate signatures.

3.2.4 FAT Measures

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

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

The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

3.2.5 SAT Measures

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

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

3.2.6 Maintenance Guidance

Changes may require an update to the NIDS configuration and/or documentation.

3.2.7 References

CIP-005-1 R1

ISA-99.02: B.10, C.3

NIST SP 800-12, 800-31, 800-82 (Draft), 800-94

3.2.8 Dependencies

Section 4.1

3.3 Canaries

3.3.1 Basis

Because many control networks contain proprietary protocols, traffic signatures that would allow the use of a commercial NIDS do not exist. A honey pot (which analyzes unauthorized connections) or a Canary (to flag a connection attempt has taken place) has been implemented in certain configurations to provide passive network monitoring.

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 network.

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

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

3.3.4 FAT Measures

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

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

The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

3.3.5 SAT Measures

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

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

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

3.3.6 Maintenance Guidance

Changing network address topologies can require canary(ies) to be reconfigured.

3.3.7 References

CIP-005-1 R2

3.3.8 Dependencies

Section 2.2

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 which pose a substantial risk, can be eliminated or mitigated.

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

1. **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).
2. **Authorization.** Is the ability to control a user’s permissions within the system. Authorization capabilities 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 a user’s 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

4.1.1 Basis

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

4.1.2 Language Guidance

Default, guest, or anonymous accounts are commonly used to gain limited access, but still gain potentially useful system privileges. These can be used in turn to gain access to additional information to launch further attacks. 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. This will be addressed in the Remote Access future topic.

4.1.3 Procurement Language

Post-contract award, the Vendor shall disable or remove all default and guest accounts prior to 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 SAT the Vendor shall disable, remove, or modify all Vendor owned accounts or negotiate account ownership with the Purchaser.

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.

4.1.4 FAT Measures

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

The Vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

4.1.5 SAT Measures

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

The Vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

4.1.6 Maintenance Guidance

No new accounts shall be introduced without explicit requirements to do so by the Purchaser or defined authorized individual.

4.1.7 References

CIP-007 R5

ISA-99.02: 5.3.11, B.14.2, B.14.4, C.3.11

NIST SP 800-82 (Draft)

4.1.8 Dependencies

None, this topic is stand-alone.

4.2 Session Management

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 which encrypt or otherwise 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.

In addition, the Vendor shall not allow multiple concurrent logins, nor for applications to retain login information between sessions, nor provide any auto-fill functionality during login, nor allow anonymous logins.

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

4.2.4 FAT Measures

The Vendor shall ensure that FAT procedures include validation and documentation of this requirement.

4.2.5 SAT Measures

The Vendor shall ensure that SAT procedures include validation and documentation of this requirement.

4.2.6 Maintenance Guidance

No new session algorithms shall be introduced without explicit requirements to do so by the Purchaser or a defined authorized individual. Encryption keys where used shall be changed at reasonable intervals commensurate with need.

4.2.7 References

CIP-007 R5

NIST SP 800-12, 800-15, 800-32, 800-67

4.2.8 Dependencies

None, this topic is stand-alone.

4.3 Password/Authentication Policy and Management

4.3.1 Basis

Instant availability requirements in control systems often result in a weak password policy. 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. Passwords shall not be stored electronically or in Vendor supplied hardcopy documentation in clear text unless the media is physically protected. The configuration interface to the account management system must have controlled access.

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 ensure that FAT procedures include validation and documentation of the password and authentication policy and management.

4.3.5 SAT Measures

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

4.3.6 Maintenance Guidance

No changes to password or authentication policy and management shall be introduced without explicit requirements to do so by the Purchaser or other defined authorized individual.

4.3.7 References

CIP-007 R5

ISA-99.01: 4.7.3, 5.3.3

ISA-99.02: 5.3.11, B.14.1, B.14.2, B.14.4, C.2, C.3.11

NIST SP 800-12, 800-53 rev 1, 800-63, 800-82 Draft

4.3.8 Dependencies

Section 5

4.4 Account Audit and Logging

4.4.1 Basis

Without account auditing and logging, the purchaser/operator cannot demonstrate that authorized operations have been maintained. Logging is also necessary for forensic analysis and anomaly detection.

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, location, and time in a verifiable manner.

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 audit trails and logging files must be time stamped, encrypted, and access controlled.

4.4.4 FAT Measures

The Vendor shall ensure that FAT procedures include validation and documentation of this requirement.

4.4.5 SAT Measures

The Vendor shall ensure that SAT procedures include validation and documentation of this requirement.

4.4.6 Maintenance Guidance

Auditing and logging records shall be archived. The future topic of Backup and Recovery will address the maintenance guidance.

4.4.7 References

CIP-007 R5

ISA-99.01: 4.7, 4.7.2, 4.7.3

ISA-99.02: 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, 800-14, 800-61, 800-82 (Draft), 800-92

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 capability to make access decisions based on the role(s) that individual users have as part of control system environment resulting in significant improvements in security effectiveness. 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. This is done to limit the exposure to risk associated with unauthorized actions. 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 administration privilege. 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 to their 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) and 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 shall start with the most privileged application controlling the communication. Upon failed communication, the most privileged side will restart communications.

The Vendor shall ensure that the master network device will initiate communications. The Vendor shall inform the Purchaser if this condition can not be met.

The Vendor shall ensure that under no circumstances shall a user escalate privileges 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 their associated roles.

4.5.4 FAT Measures

The Vendor shall compare the control system assessment during this period with required documentation to validate this requirement. Vendors shall baseline user roles and permissions, and negotiate agreements on modifications with the system Purchaser/operators.

4.5.5 SAT Measures

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

4.5.6 Maintenance Guidance

The Vendor shall ensure that all additions to the control system during the warranty/maintenance period must have the same detailed documentation as stated in this requirement.

4.5.7 References

CIP-007 R5

ISA-99.02: 5.3.11, B.14.2, B.14.4, C.3.117

NIST SP 800-12, 800-14, 800-27, 800-82 (Draft)

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 normal access across a network, or between programs and systems, without requiring reauthenticating to each application (e.g., terminal server, secure shell, etc.).

4.6.1 Basis

SSO 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 do not degrade security.

4.6.2 Language Guidance

To enhance security, single sign on shall be used with role-based access control (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.

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 also provide documentation on configuring such a system, and documentation showing equivalent results in running validation tests against the direct login and the SSO. Key files and access control lists used by the SSO system shall be protected 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 ensure 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 ensure that SAT procedures include validation and documentation that the SSO permissions and session management are handled properly.

4.6.6 Maintenance Guidance

No changes to the SSO process shall be introduced without explicit requirements to do so by a Purchaser's system administrator or other defined authorized individual.

4.6.7 References

CIP-007 R5

4.6.8 Dependencies

Section 4.1 and 4.5

4.7 Separation Agreement

4.7.1 Basis

Control system-related sensitive information is held by many people such as purchasers/operators, vendors, and contractors. 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.

4.7.2 Language Guidance

Integrators and companies that support control systems are very dynamic and competitive, resulting in frequent turnover of key support personnel. Asset purchasers need to have agreements with these vendors to protect their control systems security posture.

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 pre-negotiated period when this occurs.

The Vendor shall describe in detail 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 Purchaser any sensitive data in their possession when Vendor is no longer able to maintain control of their products.

4.7.4 FAT Measures

The Vendor shall ensure 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 ensure 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 pre-negotiated period when key personnel leave or change positions, should it possibly impact control system security.

4.7.7 References

CIP-007 R4

ISA-99.02: C.2, C.3.5, C.3.13

NIST SP 800-12

4.7.8 Dependencies

Section 4.1 and 4.3

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

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:

1. 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).
2. 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 less well-known protocols.

Standard programming texts generally do not address security ramifications and may mislead programmers into writing insecure code.

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 customer 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:

1. Check inputs for reasonable values
2. Encrypt data files
3. Understand security impacts of OSs and other third party libraries
4. Make sure OSs and other third party libraries have an update policy
5. Forbid buffer overflow
6. Ensure log files are unalterable
7. Use end-to-end authentication and integrity checks on process-to-process data communications
8. Ensure no clear text passwords nor encryption keys are embedded in the code or communicated
9. 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 high level of defense against unauthorized access.

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

The Vendor shall provide the results of [Code Reviews](#).

5.1.4 FAT Measures

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

5.1.5 SAT Measures

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

5.1.6 Maintenance Guidance

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

5.1.7 References

ISA-99.02: B.17.4

NIST SP 800-12, 800-42

5.1.8 Dependencies

None, this topic is stand-alone.

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 & Documentation from Vendor

6.1.1 Basis

Vulnerabilities exist in control systems when flaws in software and/or hardware configuration are not patched. Many times intended patches are not applied in a timely manner due to operational issues. Flaw remediation is a process by which flaws are documented and tracked for completion of corrective actions. 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

The Vendor shall be required to inform Purchaser of flaws within their applications and other software they control in a timely fashion, particularly security related flaws as they are the scope of this document. The Vendor shall also provide guidance to the Purchaser about corrective actions, fixes, or monitoring that should be performed to mitigate all vulnerabilities associated with the flaw. The Vendor shall be required to provide an auditable history of flaws and remediation steps taken for each. Vulnerabilities and flaws are normally closely held until remediation becomes available. However, some vulnerabilities are made public before a fix has been developed and thus it becomes urgent to mitigate vulnerabilities.

6.1.3 Procurement Language

The Vendor shall have a written flaw remediation process.

Post-contract award, the Vendor shall provide notification of any flaws affecting security of Vendor-supplied software within a pre-negotiated period after the Vendor is made aware of or discovers such flaw. 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.)

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

6.1.4 FAT Measures

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

The Vendor shall ensure that FAT documentation of the flaws validation and repair are provided.

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

6.1.5 SAT Measures

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

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

The Vendor shall ensure that any changes to the core system code, logic, or configuration are analyzed to ensure 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 pre-negotiated period a master list of all flaws and corrective actions for auditing purposes.

6.1.7 References

NERC CIP: No references found.

NIST SP 800-40 Ver 2

6.1.8 Dependencies

Section 2.6

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 defensible and are a primary attack vector.

6.2.2 Language Guidance

The Vendor shall be required to keep the Purchaser informed in writing of flaws within their applications and operating systems in a timely fashion, and provide guidance to the Purchaser about corrective actions, fixes, or monitoring to mitigate all vulnerabilities associated with the flaw.

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

Public release of problem reports could lead to non-defensible exploits, and so knowledge of open flaws should be closely held.

6.2.3 Procurement Language

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

Submitted problem reports must be reviewed by the Vendor and the Vendor shall report their initial action plan within twenty four hours.

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

6.2.4 FAT Measures

Not applicable.

6.2.5 SAT Measures

Not applicable.

6.2.6 Maintenance Guidance

The Vendor shall provide pre-negotiated updates to the Purchaser.

6.2.7 References

NERC CIP: No references found.

NIST SP 800-40 Ver 2

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

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. 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 files coming into the system for infected data.

Both these acts of updating to the latest detection signatures and scanning the files may affect a control system network. Manual scanning or scanning files on a scheduled basis is known to use up central processing unit (CPU) resources and may impact other process execution on the host. Active scanning is the process of scanning files only when they 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.⁹ Faulty signature files may impact critical control system files requiring the need for quick roll back of the signatures and a restoring of 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 software may change control system behavior enough to require retesting to determine the impact to operations.

7.1.3 Procurement Language

The Vendor shall meet one of two conditions:

1. Provide a host based malware detection scheme for the control system network. The Vendor shall ensure adequate system performance for host-based malware detection, quarantine suspected infected files instead of automatically deleting them, 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. Measurements shall include but not be limited to network usage, CPU usage, memory usage, and any other impact to normal communications processing.

9. 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.

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 they shall provide guidance on malware detection settings that will work with their products.

7.1.4 FAT Measures

As part of the FAT, the Vendor shall record system performance measurements that include the system with and without malware detection. The Vendor shall ensure all media and equipment is scanned under the most current malware detection versions available prior to onsite transport. The malware detection system should be exercised during the FAT.

7.1.5 SAT Measures

As part of the SAT, the Vendor shall record system performance measurements while malware detection is enabled.

7.1.6 Maintenance Guidance

Significant changes to the malware detection software will require vendor retesting to determine possible impact to performance. Malware detection application logs need to be retained for a pre-negotiated period for possible forensics tasks. Malware detection software requires frequent updates to be effective for the most recent malware released. These signatures are reactive since, as the malware variants change, new, more precise or tuned signatures need to be applied.

7.1.7 References

CIP-007 R4

NIST SP 800-82 (Draft), 800-83

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

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.¹⁰

8.1.2 Language Guidance

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.

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, they 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 and slave server makes 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 with automatic updates. Also,

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

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 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.¹¹

Considerations for securely configuring DNS are summarized by:¹²

- Using dedicated servers for DNS and related services and disable all unneeded services.
- Using the latest software builds with current patches.
- Backing up DNS configuration files, reviewing them 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, restrict 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.

8.1.3 Procurement Language

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

Post-contract award, the Vendor shall provide a configured DNS server(s) or the information to configure a DNS server(s) that meets a pre-negotiated standard of security. The addressing information shall be considered business sensitive and the Vendor shall protect it as such.

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).

8.1.4 FAT Measures

For Vendor-supplied DNS servers, the Vendor shall install and run the server continuously during the entire FAT process. The domain and hosts within the domain involved in testing shall be resolvable by all client and server systems connected to the network. The tests shall include a query to a start of

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

12. 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/.

authority (SOA) record as well as both forward (hostname to IP address) resolution and reverse (IP address to hostname) resolution.

8.1.5 SAT Measures

The Purchaser shall run the DNS server during the entire SAT process. The domain and hosts within the domain involved in testing shall be resolvable by all client and server systems connected to the network. The tests shall include a query to an SOA record as well as 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

NERC CIP: No references found.

NIST SP 800-53, 800-81

8.1.8 Dependencies

Sections 2.1, 2.2, 2.6

9. 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.

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](#), canaries or canary words are dummy data fields used in the implementation of [stack-smashing protection](#). 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.

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.

Dynamic Host Configuration Protocol (DHCP)—A [protocol](#) for assigning [dynamic 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 users](#).

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 premise usually by a third-party to ensure 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. They 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.

[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.

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 buyer for information of products necessary after the contract is awarded.

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.

[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.

[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 toward their destinations between disparate networks through a process known as routing. Routing occurs at layer 3 of the OSI seven-layer model.

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 email, 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.

Site Acceptance Test (SAT)—A test conducted at the customer location, often by a third-party, to ensure 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.

Virus—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.

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.