
Smart Grid Interchange Requirements Analysis and Standards Conformance Project

White Paper

Automating Smart Grid Security

Applications of the Security Content Automation Protocol to the Smart
Grid for Risk Management Activities

Date: December 7, 2011

Version: 1.4

Prepared for
National Institute of Standards and Technology
Under Contract Number: SB13110CN0101

Prepared By:
Scott Shorter and Greg Hollenbaugh
Electrosoft Services
11417 Sunset Hills Road, Suite 228
Reston, VA - 20190
Tel: (703)-437-9451 Fax: (703)-437-9452
<http://www.electrosoft-inc.com>

Table of Contents

1	Executive Summary	3
2	Smart Grid Risk Management Activities	4
2.1	Overview of Smart Grid Security Requirements	4
2.2	Asset Identification, Security Planning, System Assessment and Continuous Monitoring	6
2.2.1	Asset Identification	6
2.2.2	Security Planning.....	7
2.2.3	Security Assessment	7
2.2.4	Continuous Monitoring	8
2.3	Smart Grid Risk Management Requirements	8
2.3.1	NERC's Critical Infrastructure Protection.....	8
2.3.2	ISA99.....	9
2.3.3	NISTIR 7628.....	10
3	Security Content Automation Protocol (SCAP)	13
3.1	SCAP Languages	13
3.2	SCAP Reporting Formats	15
3.3	SCAP Enumerations and Data Feeds	15
3.4	Event Management Automation Protocol (EMAP).....	16
3.5	SCAP Products	17
4	Applying SCAP to the Smart Grid	18
4.1	Adopt the Asset Identification Format for Smart Grid Component Inventories	18
4.2	Enhance ICS-CERT Security Advisories with Vulnerability Scoring.....	18
4.3	Use of Asset Reporting Format for Interoperable Compliance Reporting	19
4.4	Utilize Common Platform Enumeration	19
4.5	Utilize Common Vulnerability Enumeration	20
4.6	Extend OVAL Support to Smart Grid Systems	20
4.7	Automate Smart Grid Continuous Monitoring	20
4.8	Develop Security Checklists for Smart Grid Systems.....	21
5	Conclusions	22
6	Background	23
6.1	Acronyms	23
6.2	References	24
6.2.1	Documents.....	24
6.2.2	Web Resources.....	26

Table of Tables

Table 1 - NERC CIP Requirements Pertaining to Asset Identification	9
Table 2 - NERC CIP Requirements Pertaining to Continuous Monitoring.....	9
Table 3 - ISA99 System Requirements Pertaining to Asset Identification	10
Table 4 - ISA99 System Requirements Pertaining to System Assessment	10
Table 5 - ISA99 System Requirements Pertaining to Continuous Monitoring	10
Table 6 - NISTIR 7628 High Level Requirements Pertaining to Asset Identification	11
Table 7 - NISTIR 7628 High Level Requirements Pertaining to Security Planning	11
Table 8 - NISTIR 7628 High Level Requirements Pertaining to System Assessment	11
Table 9 - NISTIR 7628 High Level Requirements Pertaining to Continuous Monitoring.....	11
Table 10 - SCAP Protocols.....	13
Table 11 - SCAP Product Capabilities	17

1 Executive Summary

The purpose of this paper is to describe the developing field of security automation technology, particularly the Security Content Automation Protocol, and applications of those technologies to improving the cyber security of the Smart Grid. The audience for this document includes individuals responsible for maintaining or verifying the security of Smart Grid systems. This includes asset owners, system integrators, security consultants and vendor product managers.

The Smart Grid is a rapidly developing technological domain containing both Information Technology (IT) systems and Industrial Control Systems (ICS), and while these domains are known to require different technical security controls to protect their assets, the overall process of risk management for IT and ICS systems is similar.

First, we describe security frameworks applicable to the Smart Grid and demonstrate that they all require broadly similar activities, described here as Asset Identification, Security Planning, System Assessment and Continuous Monitoring. This paper reflects current research in the field of Smart Grid security, and we discuss security requirements such as the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection requirements, the International Society of Automation's ISA99 standard for cyber security of automation and Industrial Control Systems and the National Institute of Standards and Technology's Interagency Report (NISTIR) 7628 Guidelines for Smart Grid Cyber Security and demonstrates the ways in which these documents contain activities that map to the processes in the Department of Energy's draft Electricity Sector Cybersecurity Risk Management Process Guidelines, with additional references to documents developed by the National Institute of Standards and Technologies (NIST) pursuant to the Federal Information Management Security Act of 2002 (FISMA).

Next, the paper describes the Security Content Automation Protocol (SCAP) at a high level, discussing the different languages, reporting formats, enumerations and data feeds that comprise the protocol, and provides an overview of currently validated SCAP products.

Then we provide a number of specific technical recommendations that could be undertaken to promote the use of SCAP to automate security processes in the Smart Grid and Industrial Control Systems more broadly. These recommendations include:

- Adopt the Asset Identification Format for Smart Grid Component Inventories
- Enhance ICS-CERT Security Advisories with Vulnerability Scoring
- Use of Asset Reporting Format for Interoperable Compliance Reporting
- Utilize Common Platform Enumeration
- Utilize Common Vulnerability Enumeration
- Extend OVAL Support to Smart Grid Systems
- Automate Smart Grid Continuous Monitoring
- Develop Security Checklists for Smart Grid Systems

The document then offers some conclusions and provides a list of references and web resources for additional information.

2 Smart Grid Risk Management Activities

2.1 Overview of Smart Grid Security Requirements

The Smart Grid is a general term for the technological changes that are occurring in the bulk electricity supply systems world-wide. It has often been observed that Alexander Graham Bell would not be able recognize the telephone systems of today, whereas Thomas Alva Edison would immediately comprehend the engineering principles of today's electrical grid. The current systems for delivering energy from suppliers to consumers are being enhanced to support new technologies such as distributed generation, demand response, electric vehicles and dynamic pricing. The Smart Grid is a term for a wide variety of technologies that are being used to modernize electricity networks to support more flexible generation, distribution, transmission and metering of electric power. The Smart Grid requires greater interoperability and cyber security of system components than has ever existed in this industry and the challenges to achieving this are myriad.

Section 1301 of the Energy Independence and Security Act of 2007 (P.L. 110-140) defines the Smart Grid in the following manner:

“It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

- Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.
- Dynamic optimization of grid operations and resources, with full cyber-security.”

As with many large systems of critical infrastructure, Smart Grid systems comprise both Industrial Control Systems (ICS) and Information Technology (IT) systems. The ICS systems include the equipment that performs the bulk electricity delivery from generator to consumer, but those systems interface with IT systems at many points, including customer management and billing systems, electronic power markets, and others. There are well-developed principles of security engineering that have been developed for IT systems that are directly applicable to the IT portions of the Smart Grid and can be modified for ICS. NIST Special Publication 800-53 is a catalog of security controls for Federal information management systems which includes an appendix on applying those security controls to Industrial Control Systems. Also, NIST Special Publication 800-82, Guide to Industrial Control Systems Security provides information specific to ICS security. That document defines the characteristics of Industrial Control Systems as they differ from general IT systems.

Historically, ICS were developed as isolated systems running proprietary protocols, and were characterized by more rigorous performance, safety and reliability/availability requirements than most IT systems are subject to. Downtime in an IT system can mean an

interruption of revenue or business service, whereas downtime in the Smart Grid can mean power blackouts and the consequent disruption of productivity and services. ICS hardware systems are also deployed for very long time periods compared to the components of IT systems. Because equipment is replaced infrequently, enhancements to the security of the protocols will take place at a slow rate and piecemeal. Compensating security controls must be developed and deployed to make up for the limitations and particular requirements of the ICS domain.

In August of 2010 NIST released NIST Interagency Report (NISTIR) 7628, titled Guidelines for Smart Grid Cyber Security, including Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, Vol. 2, Privacy and the Smart Grid and Vol. 3, Supportive Analyses and References. These guidelines provide extensive background information and best practices for cyber security, but they are not mandatory requirements. The document refers to the development of Security Planning documents and performing security assessments, but does not provide specific guidance for those activities. However, in 2011, the National Rural Electric Cooperative Association released a Guide to Developing a Cyber Security and Risk Management Plan, and the Smart Grid Interoperability Panel is in the process of finalizing an assessment guide for NISTIR 7628 requirements.

The bulk power generation, distribution and transmission facilities of Smart Grid systems are operated by electric utilities and independent system operators that in North America are private businesses, which are owned either by investors or by their customers. These businesses are subject to a number of regulations on safety and environmental impact, reliability, pricing, standard of service and other areas. The North American Electric Reliability Corporation (NERC) was established to ensure the reliability of the electric grid, and they have been certified by the Federal Energy Regulatory Commission (FERC) as an electric reliability organization (ERO) to establish and enforce reliability standards for the bulk-power system. NERC's reliability standards include a number of requirements for Critical Infrastructure Protection (CIP), including cyber security requirements, and FERC has issued regulation making compliance with CIP and other NERC standards mandatory.

In September 2011, the Department of Energy released a draft of Electricity Sector Cybersecurity Risk Management Process Guidelines (DOE RMPG) that follow the general approach from NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. This document divides responsibilities for cyber security into three tiers, Tier 1 being the organizational level at which policies are developed, Tier 2 being the business or mission level and Tier 3 being the operational level of systems. A critical Tier 3 activity in the DOE RMPG is performing cybersecurity assessments to feed into the overall organizational risk management process, and performing ongoing monitoring of the system's cyber security state afterwards.

2.2 Asset Identification, Security Planning, System Assessment and Continuous Monitoring

Best practices in security risk management call for obtaining an accurate inventory of assets, developing a detailed plan for protecting those assets and performing security assessments and continuous monitoring of system status to obtain assurance that the Security Plan has been implemented correctly. The subsections below discuss these activities in more detail.

2.2.1 Asset Identification

The assets of an organization are those items of value possessed or controlled by that organization, and the overall security objective of the organization is to protect those assets. Comprehensive Security Planning is not possible without an awareness of the organization's assets, and asset identification provides key initial information required to apply risk management processes to improve security. The Risk Assessment phase of the DOE RMPG process calls for identification of assets, describing in section 5.1.2.1 the activity of Information Technology and Industrial Control Systems Inventory as:

“The IT and ICS inventory process begins by identifying the systems, resources, and relationships between IT and ICS; the mission and business processes; and the applications they support. The organization that owns, manages, and/or controls the resources is derived from the relationship between the mission and business process, the application owner, and any contractual arrangements with internal or external organizations. This establishes authority and accountability for cybersecurity of the systems and resources.”

For entities subject to NERC's regulations, CIP-002-4 is a mandatory requirement for identification of critical cyber assets. The standards provide criteria for determining whether assets are needed to support reliable operation of the bulk electric system and thus deemed critical. NERC defines assets as “facilities, systems, and equipment¹” but the concept can be extended to include personnel and organizations. NERC requires annual reporting of critical cyber assets.

Asset identification of system equipment can be used to describe networks, devices, software, data or services, and includes information either intrinsic to the asset such as a hardcoded MAC address, or assigned to the asset from another system such as an assigned network address. Asset identification includes an organization specified identifier, whether a hostname, device id, employee id, or other, and will often include additional properties such as physical location or logical location, for example, network parameters. Once assets are identified, relationships among the different types of assets can be defined that describe physical interconnections between equipment, software installed on a device, or even an employee's administrative privilege to a device or system.

¹ NERC Glossary of Terms, August 4, 2011, p. 12

2.2.2 Security Planning

Security Planning consists of determining what security controls should be implemented to protect the organization's assets. The process results in a system Security Plan, as per NIST 800-38 RMF, or a cyberSecurity Plan in the DOE RMPG. In 2011, the National Rural Electric Cooperative Association (NRECA) released a Guide to Developing a Cyber Security and Risk Management Plan that provides additional information on developing a similar sort of document.

The method of Security Planning is outside the scope of this document, but the Security Plan that results will include identification of the organization's assets and a selection of security controls. The Security Plan will form the basis for security assessments and continuous monitoring activities.

2.2.3 Security Assessment

The security assessment consists of the following steps:

- Developing, reviewing, and approving a Security Assessment Plan to assess the security controls in the Security Plan,
- Assessing the security controls in accordance with that Security Assessment Plan,
- Preparing a security assessment report, and
- Conducting initial remediation actions based on the findings of the security assessment report.

In NIST Special Publication 800-53A, the section titled, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans" provides an excellent methodology for performing security assessments of information systems. It provides potential assessment methods for the security controls in NIST Special Publication 800-53 and describes the development of a Security Assessment Plan. A Security Assessment Plan will typically include a full description of the scope of the assessment. The scope description is based on the organization's Security Plan, and includes security controls and control enhancements under assessment, assessment procedures to be used to determine security control effectiveness, and assessment environment, assessment team, and assessment roles and responsibilities.

The Smart Grid Interoperability Panel is in the process of finalizing a Guide for Assessing the High Level Security Requirements in the NISTIR 7628 Guidelines for Smart Grid Cyber Security. This document follows the approach of SP 800-53A but operates against the security requirements of NISTIR 7628, as opposed to SP 800-53's security control.

The Department of Homeland Security's Control Systems Security Program published a guide to Cyber Security Assessments of Industrial Control Systems that provides additional guidance on general and ICS specific security assessment activities. It is worth noting that this document references the Common Vulnerability Enumeration (CVE) and Common Vulnerability Scoring System (CVSS) which are key components of SCAP.

2.2.4 Continuous Monitoring

NIST Special Publication 800-137 provides a framework for continuous monitoring of information systems in support of organizational risk management processes. The publication defines continuous monitoring as “maintaining ongoing awareness to support organizational risk decisions.” Continuous monitoring includes information security continuous monitoring, risk monitoring and status monitoring. Information security continuous monitoring is a high level activity, defined as “Ongoing monitoring sufficient to ensure and assure effectiveness of security controls related to systems, networks, and cyberspace, by assessing security control implementation and organizational security status in accordance with organizational risk tolerance – and within a reporting structure designed to make real-time, data driven risk management decisions.” Risk monitoring involves “Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions,” while status monitoring is a lower level activity, “monitoring information security metrics defined by the organization in their information security continuous monitoring strategy.”

Implementation of organization-wide continuous monitoring involves collection and analysis of large amounts of system status and configuration data and enables a real-time view of aggregate system risk. SP 800-137 defines a hierarchy of tiers within the organization, the Organization/Governance level (Tier 1) that addresses high level security governance policies and overall organizational risk tolerance, the Mission/Business level (Tier 2) that applies Tier 1 risk management policies to organizational business processes and monitors the output from Tier 3, and the Information Systems level (Tier 3) where the bulk of the security status information is collected and summarized for higher levels. Tier 3 continuous monitoring activities include configuration management and change control processes, security impact analyses, ongoing assessment of security controls and security status reporting. Implementation of a well-designed and managed continuous monitoring program will result in the ongoing maintenance of up-to-date copies of required system information and data such as the System Security Plan, Risk Assessment Report, Security Assessment Report and the Plan of Action and Milestones (POA&M) documents.

2.3 Smart Grid Risk Management Requirements

Given the importance of asset identification, security planning, security assessment and continuous monitoring to assuring the ongoing security of Smart Grid systems, it is not surprising that numerous sources identify requirements for these activities. The subsections below identify relevant requirements from NERC CIP, ISA99 and NISTIR 7628.

2.3.1 NERC’s Critical Infrastructure Protection

The North American Electric Reliability Corporation’s Functional Model is a set of mandatory functional requirements for the bulk electric system. A subset of those requirements categorized as Critical Infrastructure Protection requirements include a number of sets of cyber security requirements. The following tables identify CIP requirements that pertain to asset identification and continuous monitoring.

Table 1 - NERC CIP Requirements Pertaining to Asset Identification

CIP Req #	Requirement Name	Description
CIP-002-4	Identifying Critical Cyber Assets	Requires identification and documentation of critical cyber assets.
CIP-003-2 R6	Change Control and Configuration Management	Requires organizations to follow an ongoing configuration management process.

Table 2 - NERC CIP Requirements Pertaining to Continuous Monitoring

CIP Req #	Requirement Name	Description
CIP-002-4	Identifying Critical Cyber Assets	Requires identification and documentation of critical cyber assets.
CIP-003-2 R6	Change Control and Configuration Management	Requires organizations to follow an ongoing configuration management process.
CIP-005-2a R3	Monitoring Electronic Access	Requires organizations to log remote access 24/7.
CIP-006-4 R5	Monitoring Physical Access	Requires organizations to monitor and log physical access 24/7.
CIP-007-4 R3	Security Patch Management	Requires organizations to manage and monitor patch status.
CIP-007-4 R6	Security Status Monitoring	Requires implementation automated tools or organizational process controls to monitor system events.
CIP-007-4 R8	Cyber Vulnerability Assessment	Requires annual vulnerability assessment.

2.3.2 ISA99

ISA99, otherwise known as IEC 62443 is a set of standards for industrial network and system security, ranging from low level technical requirements to operational and organizational requirements. The standards that comprise ISA99 are aimed at the following interest groups:

- General: Terminology, concepts and models; master glossary and system security compliance metrics
- Asset Owner: Establishes and operates an IACS security program, patch management and certification of supplier security practices.
- System Integrator: Security technologies, security assurance levels for zones and conduits and system security requirements and security assurance levels
- Component Provider: Product development requirements, technical security requirements for components

ANSI/ISA-99.03.03, otherwise known as IEC 62443-3-3, describes system security requirements and security assurance levels for industrial automation and control systems. It expands the Foundational Requirements (FRs) defined in ISA-99.01.01 into series of System Requirements (SRs), each of which consists of a baseline requirement and one or

more Requirements Enhancements (REs). The document defines Security Assurance Levels (SALs) 1 through 4 which defines increasing levels of security requirements developed to counter increasing levels of attacker sophistication and consequences of threat.

There is no explicit requirement for Security Planning in ISA99-3-3 but the following SRs pertain to the topics of asset identification, security assessment and continuous monitoring:

Table 3 – ISA99 System Requirements Pertaining to Asset Identification

Req #	Name	Requirement
SR 7.8	ICS Component Inventory	Requires the capability to report on the installed components of the ICS and their properties.

Table 4 – ISA99 System Requirements Pertaining to Security Assessment

Req #	Name	Requirement
SR3.3	Security Functionality Verification	Requires verification of intended operation of security functions, during factory acceptance testing, site acceptance testing and scheduled maintenance.

Table 5 – ISA99 System Requirements Pertaining to Continuous Monitoring

Req #	Name	Requirement
SR6.2	ICS Monitoring Tools and Techniques	Requires continuous monitoring of ICS activities to detect attacks or unauthorized activities.
SR7.6(1)	Network and Security Configuration Settings	The requirement enhancement for SAL3 and above requires the capability to generate a machine-readable report of the currently deployed security settings.

2.3.3 NISTIR 7628

In August 2010, NIST released NIST Interagency Report 7628: Guidelines for Smart Grid Cyber Security. Volume one of NISTIR 7628 provides a number of high-level requirements that may be followed to secure Smart Grid systems. The requirements were compiled from the security controls in NIST Special Publication 800-53, the Department of Homeland Security’s security control catalog (also based on SP 800-53), and the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. The high level requirements in NISTIR 7628 can be selected by an organization to address their particular security objectives. The system Security Plan that results can then be the basis for system assessments as well as continuous monitoring activity.

Because of the guidance nature of NISTIR 7628, the high-level requirements are not mandatory. Instead, organizations are advised to determine the requirements that will be met and express those in a system Security Plan. The system Security Plan forms the basis

of a system assessment, and a document is being developed by the Cyber Security Working Group of the Smart Grid Interoperability Panel to provide specific guidance on how perform system security assessments.

Table 6 - NISTIR 7628 High Level Requirements Pertaining to Asset Identification

Req #	Name	Requirement
SG.CM-8	Component Inventory	Requires development of an inventory of the components of a Smart Grid system

Table 7 - NISTIR 7628 High Level Requirements Pertaining to Security Planning

Req #	Name	Requirement
SG.PL-2	Smart Grid Information System Security Plan	Requires development of Security Plans to describe the security objectives for the system and what security requirements shall be implemented to achieve them.

Table 8 - NISTIR 7628 High Level Requirements Pertaining to Security Assessment

Req #	Name	Requirement
SG.PM-6	Security Authorization to Operate Process	Organizations are required to implement a process of security authorization.
SG.CA-1	Security Assessment and Authorization Policy and Procedures	Organizations are required perform security assessments.
SG.CA-2	Security Assessments	Organizations are required to develop system Security Plans and assess the requirements on a regular basis.
SG.CA-5	Security Authorization to Operate	Organizations are required to authorize systems to operate based on the results of security assessments.

Table 9 - NISTIR 7628 High Level Requirements Pertaining to Continuous Monitoring

Req #	Name	Requirement
SG.AC-15	Remote Access	Organizations are required to monitor remote access methods.
SG.AU-6	Audit Monitoring, Access and Reporting	Organizations are required to regularly analyze audit records for indications of unauthorized activity.
SG.CA-2	Security Assessments	Organizations are required to regularly assess security requirements in the Smart Grid information system

SG.CA-6	Continuous Monitoring	Organizations are required to establish a continuous monitoring strategy and program that includes ongoing security requirements assessment and regularly reporting the security state of the Smart Grid information system.
SG.CM-4	Monitoring Configuration Changes	Requires the implementation of processes to monitoring changes to Smart Grid information systems
SG.IR-6	Incident Monitoring	Requires the organization to track security incidents.
SG.MA-6	Remote Maintenance	Requires the monitoring of remote maintenance and diagnostic activity
SG.PE-4	Monitoring Physical Access	Requires monitoring of physical access logs
SG.PM-6	Security Authorization to Operate Process	Requires monitoring the security state of Smart Grid information systems
SG.SC-7	Boundary Protection	Requires monitoring of communications at the external boundaries of Smart Grid information systems
SG.SC-16	Mobile Code	Requires monitoring the use of mobile code.
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	Requires monitoring of events to detect attacks, unauthorized activities and errors.
SG.SI-7	Software and Information Integrity	Requires monitoring of unauthorized changes to software.

3 Security Content Automation Protocol (SCAP)

According to NIST SP 800-117, Guide to Adopting and Using SCAP, the Security Content Automation Protocol was developed with the goal of providing:

“an automated, standardized approach to maintaining the security of enterprise systems, such as implementing security configuration baselines, verifying the presence of patches, performing continuous monitoring of system security configuration settings, examining systems for signs of compromise, and having situational awareness—being able to determine the security posture of systems and the organization at any given time.”

The SCAP standard consists of a suite of subsidiary standards defined by of NIST SP 800-126. At the time of publication, the final version of SCAP version 1.2 was specified in NIST SP 800-126 Rev 2, published in September 2011.

The following table indicates the additional specifications referenced in SCAP versions 1.1 and 1.2, and the subsections below describe the subsidiary standards in more detail.

Table 10 - SCAP Protocols

Protocol	Name	Type	SCAP 1.1	SCAP 1.2
XCCDF	Extensible Configuration Checklist Description Format	Language	1.1.4	1.2
OVAL	Open Vulnerability Assessment Language	Language	5.8	5.10
OCIL	Open Checklist Interactive Language	Language	2.0	2.0
CPE	Common Platform Enumeration	Enumeration	2.2	2.3
CCE	Common Configuration Enumeration	Enumeration	5	5
CVE	Common Vulnerability Enumeration	Enumeration	n/a	n/a
CVSS	Common Vulnerability Scoring System	Data Feed	2.0	2.0
CCSS	Common Configuration Scoring System	Data Feed		1.0
ARF	Asset Reporting Format	Reporting Format		1.1
AI	Asset Identification	Reporting Format		1.1
TMSAD	Trust Model for Security Automation Data	Integrity Model		1.0

3.1 SCAP Languages

A critical component of SCAP is the ability to express security benchmarks and checklists in a machine readable fashion. Extensible Configuration Checklist Description Format (XCCDF) is the language that provides this ability. It provides a data model for representing sets of security requirements as a collection of security configuration rules to be applied to the applicable target systems. Important benchmarks, such as the Federal Desktop Core Configuration and the United States Government Configuration Baseline, provide security configuration baselines for widely deployed IT systems within the United States Federal government and are expressed in XCCDF format. The specification supports the exchange of information, generation of reports and policy documents, tailoring for organizational and system-specific sets of security controls, and working with OVAL (see below) to support automated compliance testing and reporting of target systems. The results of benchmark compliance testing can be stored in a test results benchmark format that can feed results back into the risk management framework. XCCDF is specified in NISTIR 7275 and while it is mature for many purposes it is still developing. Revision 4 of XCCDF version 1.2 of XCCDF was released in September 2011.

XCCDF is used to express the rules, but it requires something called a check system to actually perform the low level testing. There are currently two defined check systems, OVAL and OCIL. OVAL is used for automated checks of IT systems and OCIL is used for human-driven checklists.

The Open Vulnerability and Assessment Language (OVAL) is used to test and report on the state of computer systems. This protocol enables a standardized approach for collecting automated reports of configuration information from systems; testing systems for the presence of vulnerabilities, misconfigurations, security patches; and standardizing the results of those reports and tests. The language has been in development since 2005. Currently, it supports such operating systems as Windows, Mac OS and many versions of UNIX and Linux as well as Cisco platforms, Apache and VMWare. Services using OVAL can provide organizations with automatically collected, consistently reported and standardized information about the state of machines in their system. OVAL is maintained by MITRE, who frequently adds new features.

The Open Checklist Interactive Language (OCIL) is a way to handle the security content that cannot be automated by providing a consistent framework for expressing and collecting answers to a set of questions from a human user. The language defines a framework to represent questions to be presented to the user and the ways to interpret and store the answers. OCIL can be used to allow a system operator or field technician (for example) to answer a security checklist and have the results then stored and utilized as SCAP content, and thus fed into the overall organizational risk management data stream. OCIL version 2.0 is specified in NISTIR 7692, published April 2011. As that publication explains:

“OVAL and OCIL complement each other and they can be considered peers. OVAL is used to collect specified pieces of information from systems directly and automatically, without

human interaction; OCIL is used to collect specified pieces of information by harvesting existing sources of collected data or by asking a human to supply it. Both OVAL and OCIL produce XML-based reports, which support aggregation of OVAL and OCIL results.”

3.2 SCAP Reporting Formats

Defined in NISTIR 7693, Asset Identification 1.1 is a format for uniquely identifying and gathering information about assets based on known identifiers and properties of those assets. It provides for associating assets with Common Platform Enumeration identifiers (see below) to aid in vulnerability analysis, and defining relationships between assets to further define networks and systems of assets.

The Asset Reporting Format is defined in NISTIR 7694 and provides a standard format for reporting the results of automated or non-automated assessment activities. The report contains information about: the identity of the assessed asset; the requirements that asset was assessed against; any other inputs to the assessment process; and the assessment results. For example, in the case of an XCCDF-expressed automated benchmark assessment of a computer host, the report would include the results of the XCCDF benchmark evaluation against that host, the OVAL and OCIL results of the low level assessment activities (testing, configuration checks, interviews, etc), and the contents of any other SCAP data input during the assessment. ARF can be thus used for tracking the results of the myriad individual assessments that will be created during system assessment and continuous monitoring activities, and provides technical mechanisms to support aggregation, correlation and management of those reports.

3.3 SCAP Enumerations and Data Feeds

Through the National Vulnerability Database (NVD), NIST maintains a repository of security relevant sources of SCAP content, providing an up-to-date common baseline for SCAP systems to refer to vulnerabilities, misconfigurations, platforms and scoring systems. The enumerations consist of lists of unique identifiers of those elements with additional information attached to some kinds. All of the data streams are openly available.

Related to the NVD is the National Checklist Program (NCP), a repository of security configuration checklists with detailed guidance on how to securely configuring specific operating systems, devices and applications. Checklists are allocated to one of multiple tiers according to how readily the checklist can be automated. Tier I is a fully manual checklist in prose form, while Tier IV consists of validated SCAP content ready for use with SCAP validated products, including mappings from low level content such as configuration settings up to the high level security controls that mandate them. A Tier IV checklist will include XCCDF and OVAL/OCIL content. It should be noted that the NCP accepts checklists from numerous sources, including government and industry.

The Common Platform Enumeration (CPE) is a naming scheme for IT systems, platforms, and packages. Its syntax is based on that for Uniform Resource Identifiers (URI), providing a formalized naming format, a means for describing complex platforms, and rules for checking names.

The Common Configuration Enumeration (CCE) is a list of unique identifiers of system configuration issues. It can be used for correlation of configuration data across multiple data streams and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice documents.

The Common Vulnerability Enumeration (CVE) is a global dictionary of publicly known security vulnerabilities. The CVE identifiers provide a means of exchanging data between security tools, and include a description of the vulnerability and references to more information, including background information and relevant OVAL identifiers. CVE entries are created when a potential security vulnerability is discovered and reported to a CVE Candidate Numbering Authority (CNA). The entry is initially posted to the enumeration as a 'candidate' entry, and after approval by the CVE Editorial Board the entry is upgraded to 'entry' status.

The Common Vulnerability Scoring System (CVSS) is a framework for communicating the nature and impact of security vulnerabilities. It measures exploitability, such as attack complexity and whether authentication is required to exploit; impact on confidentiality, availability and integrity; and temporal scores, such as the availability and verification of the exploit and the availability of remediation. These metrics can be combined for an overall impact level of the vulnerability of a particular system. CVSS is used to calculate the severity of vulnerabilities discovered in a system and prioritize vulnerability remediation activities. The Common Configuration Scoring System (CCSS) is defined in NIST Interagency Report 7502, and consists of similar metrics for assessing software misconfiguration issues.

Finally, the Trust Model for Security Automation Data (TMSAD) is a trust model that can be applied within a security automation domain such as SCAP. It provides the foundation for authentication of source material via XML digital signatures and identity information. This can be used to establish trusted publishers of SCAP data streams.

3.4 Event Management Automation Protocol (EMAP)

The Event Management Automation Protocol (EMAP) is a protocol suite being developed that is intended to stand alongside SCAP. While still in the early stages of development, it is intended to provide a common language designed to enable a common method for communicating event management data. The goal of EMAP is to enable standardized content, representation, exchange, correlation, searching, storing, prioritization, and auditing of event records within an organizational IT environment. EMAP consists of a number of components, including the Common Event Expression (CEE), Open Event Expression Language (OEEL), Common Event Rule Expression (CERE), Common Event Scoring System (CESS) and the Cyber Observable Expression (CyBOX).

The Common Event Expression (CEE) provides a common language and syntax for standardizing how information system events are described, logged, and exchanged. The purpose is to provide an interoperable mechanism for logging events so that disparate

products can have their logs correlated and aggregated, enabling organization-wide log management and analysis.

3.5 SCAP Products

NIST operates the SCAP Validation Program to validate the ability of products to use the features and functionality of SCAP correctly. At this time, the focus of the SCAP program in the Federal government is to secure Windows and Red Hat Linux operating systems. The U.S. Government Configuration Baseline (USGCB) is a set of SCAP content developed to provide a list of security settings for Windows computers, so the category of FDCC Scanner is one of the most validated product capabilities. NIST maintains an up to date list of SCAP validated products on its SCAP web portal. The table below shows the number of validated products listed on the SCAP web portal, by SCAP capability. Note that revision 3 of NISTIR 7511 defines a smaller set of capabilities, namely Authenticated Configuration Scanner and Authenticated Vulnerability and Patch Scanner.

Table 11 - SCAP Product Capabilities

SCAP Capability	Description	Validations ²
FDCC Scanner (deprecated)	The capability to audit and assess a target system to determine its compliance with the FDCC requirements.	37
Authenticated Configuration Scanner	The capability to audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges.	31
Authenticated Vulnerability and Patch Scanner	The capability to scan a target system to locate and identify the presence of known vulnerabilities and evaluate the software patch status to determine compliance with a defined patch policy using target system logon privileges.	30
Unauthenticated Vulnerability Scanner (deprecated)	The capability of determining the presence of known vulnerabilities by evaluating the target system over the network.	9
Patch Remediation (deprecated)	The capability to install patches on a target system in compliance with a defined patching policy.	0
Misconfiguration Remediation (deprecated)	The capability to alter the configuration of a target system to bring it into compliance with a defined set of configuration recommendations.	5

² As of September 2011.

4 Applying SCAP to the Smart Grid

NIST SP 800-117, Guide to Adopting and Using the Security Automation Content Protocol (SCAP), provides extensive discussion of the applications of SCAP technology for such purposes as security configuration verification, requirements traceability, standardized security enumerations, vulnerability management and security data analytics. SCAP has been developed in the IT domain, but all of these activities are equally necessary in the Smart Grid domain. The subsections below discuss specific technical steps that could be taken to use SCAP in the Smart Grid domain.

4.1 Adopt the Asset Identification Format for Smart Grid Component Inventories

Many requirements and guidance documents specify that organizations are to develop inventories of system components and the relationships and connections between them, to be used for system Security Planning. SCAP's Asset Identification format provides a framework for this information that can be useful for many types of tools that can consume Asset Identification content. NISTIR 7693 identifies the following use cases that an interoperable Asset Identification specification enables:

- Correlation of gathered data
- Federation of asset databases
- Directly targeted remediation actions
- Management of asset data

Asset Identification provides a standard for output from asset management tools (the AI producers) which provide a standard input format that can be used by security automation tools with a need to identify assets (the AI consumers).

As a note to the maintainers of the Asset Identification specification, the document is currently targeted at IT systems, with options specified for Internet Protocol (IP) address and similar IT network-centric values. An update to the document to reflect common identifying parameters in ICS communications systems, for example, the BACnet device id, could make specification more widely applicable. Identifying a Smart Grid related organization to collaborate with the developers of the Asset Identification standard (and other SCAP standards) would be a useful step in this process.

4.2 Enhance ICS-CERT Security Advisories with Vulnerability Scoring

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is a source of information about control system related computer vulnerabilities and security advisories, provided by the Department of Homeland Security's US Computer Emergency Readiness Team. ICS-CERT disseminates information about vulnerabilities in their advisories, which provide an overview of the vulnerabilities, identify the affected products and the impact of the vulnerability. The security advisories also provide an analysis of the vulnerability that occasionally includes references to any CVE entries that have been

issued. ICS-CERT security advisories provide important information for control systems owners to perform their risk analysis.

ICS-CERT security advisories do not provide vulnerability scoring information, although in many cases sufficient information is present in the advisory for a Base CVSS version 2 score to be expressed. Vulnerability scoring information enables system owners to understand the risk imposed by vulnerabilities, and provides a valuable stream of information that assist system owners in prioritizing their mitigation activities.

Awareness of vulnerability scoring is growing in the ICS and Smart Grid industry. The Department of Homeland Security's 2010 document on Cyber Security Assessments of Industrial Control Systems contains information about using CVSS for vulnerability scoring, and the September 2011 publication by the Department of Energy of a Vulnerability Analysis of Energy Delivery Control Systems provides CVSS scoring for ten common types of vulnerabilities identified in cybersecurity assessments by the National SCADA Test Bed (NSTB).

4.3 Use of Asset Reporting Format for Interoperable Compliance Reporting

The ARF specification's initial purpose was to encapsulate the results of XCCDF Benchmark assessments and related data. However, the ARF specification suggests an additional use of the data format for tracking an asset's compliance with various compliance schemes such as: FISMA reporting to the Payment Card Industry (PCI); Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules; and Sarbanes-Oxley (SOX) compliance. In addition to these schemes, the ARF format could be used to track conformance with Smart Grid relevant requirements such the NERC reliability standards and ISA99.

4.4 Utilize Common Platform Enumeration

The Common Platform Enumeration (CPE) provides a naming scheme for hardware, operating systems and applications. It supports application of vulnerability and configuration guidance, patching and remediation, asset management, and other security related tasks. Currently, the CPE is focused on IT system components such as general purpose computers and network appliances; Windows, Mac and Linux operating systems; and applications of various sorts that operate on those platforms.

However, Industrial Control System components do not run on Windows desktops. SCADA systems consist of Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), supervisory computer systems and Human Machine Interfaces (HMI). Supervisory computer systems are often old-school mainframes such as the VAX/VMS system cited in the Bellingham WA Control System Cyber Security Case Study. Many HMI systems do run Windows operating systems, but PLCs and RTUs are specialized platforms with requirements for real-time performance and high availability and run on specialized firmware. Although Common Platform Enumeration primarily covers IT

system computers and applications, there is no technical impediment to allocating names for control system equipment and applications as well. To extend the usefulness of the CPE to Smart Grid domains, the hardware, operating systems and applications that are used in Industrial Control Systems and Smart Grid deployments should also be assigned CPE names. Once these are available, asset inventories for Smart Grid systems can include CPE names of the components that make up those assets, enabling organizations to assess their exposure to vulnerabilities more readily. Again, this is work that can be done by a Smart Grid organization in collaboration with the maintainers of the CPE.

4.5 Utilize Common Vulnerability Enumeration

The Common Vulnerability Enumeration (CVE) provides a naming scheme for publicly known information security vulnerabilities, enabling organizations to determine the current vulnerability exposure of their assets. Names are assigned by a Candidate Numbering Authority (CAN), organizations whose members include MITRE (the primary CAN), software vendors who assign CVE identifiers for their own products, third parties such as CERT/CC, and vulnerability research labs. To enable automated vulnerability monitoring of Smart Grid systems, CVEs should be issued for vulnerabilities pertaining to Smart Grid and Industrial Control System hardware and software components, whether by the manufacturers of those components or by a third-party organization that serves as a Candidate Numbering Authority for the industry.

4.6 Extend OVAL Support to Smart Grid Systems

The SCAP check system is the component that performs actual tests, whether through direct technical means such as communicating with an asset to obtain configuration information (using OVAL) or through human-mediated checklists (using OCIL). As the OVAL specification states, the language permits the definition of testable system assertions such as:

- Is the system in a vulnerable state?
- Is a specific patch installed or missing from the system?
- Is a certain piece of software installed on the system?
- Is the system in compliance with a particular set of configuration guidance?

At this time, the technical content of the OVAL language is geared toward IT systems and it is not clear to what extent OVAL will be usable in its current form for Smart Grid Systems, and evaluation of the changes required to OVAL to support Smart Grid and Industrial Control Systems is beyond the scope of this document. However, this is a recommended area of further research.

4.7 Automate Smart Grid Continuous Monitoring

Continuous monitoring of system security requires gathering a great deal of data. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems, describes an example:

“a metric that an organization might use to monitor status of authorized and unauthorized components on a network could rely on related metrics such as physical asset locations, logical asset locations (subnets/Internet protocol (IP) addresses), media access control (MAC) addresses, system association, and policies/procedures for network connectivity. The metrics would be refreshed at various frequencies in accordance with the ISCM strategy. The metrics might be computed hourly, daily, or weekly. Though logical asset information might change daily, it is likely that policies and procedures for network connectivity will be reviewed or revised no more than annually.”

Gathering the vast amount of information required for proper continuous monitoring practices using manual methods would be costly and prone to error, and this is an area that lends itself to automation. If all the various tools that comprise a continuous monitoring system report their information in a common format, that information can be more easily aggregated and used for risk management.

4.8 Develop Security Checklists for Smart Grid Systems

The National Checklist Program Repository of the National Vulnerability Database houses security checklists of many sorts that range from manual checklists to highly automatable SCAP-expressed benchmarks. These checklists include security configurations produced by Government Authorities such as the Federal Desktop Core Configuration (FDCC), the United States Government Configuration Baseline (USGCB) and Security Technical Implementation Guides (STIGs) as well as vendors and third parties.

At this time, the repository houses security checklists of relevance to the IT domain. Similar security checklists should be developed for Industrial Control Systems and other Smart Grid components that are not traditional IT systems.

5 Conclusions

The SCAP protocol was developed with the purpose of helping organizations maintain secure configurations, managing the technical aspects of assessing system compliance with security requirements, measuring security, automating security operations and communicating about vulnerabilities. These issues were identified in the IT security domain, but there is a considerable need to address these challenges in the Smart Grid and ICS domains as well. Security automation can help asset owners obtain a clear understanding of the security status of their systems, and SCAP provides a technical framework for doing this.

Including ICS related vulnerabilities in the CVE and ICS related platforms in the CPE is a simple first step towards utilization of SCAP in the Smart Grid and ICS domains. The use of CVSS for vulnerability scoring appears to be catching on. Additional applications such as development of XCCDF-expressed checklists and automated OVAL-based check systems are more challenging, but as the state of security awareness in the industry grows, it is hoped that the field of Smart Grid and ICS security can follow recent developments in the IT security domain to realize the benefits of security automation.

6 Background

6.1 Acronyms

Acronym	Definition
AI	Asset Identification
ARF	Asset Reporting Format
ASAP-SG	Advanced Security Acceleration Project
C&A	Certification and Accreditation
CAN	CVE Candidate Numbering Authority
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CEE	Common Event Expression
CERE	Common Event Rule Expression
CESS	Common Event Scoring System
CIP	Critical Infrastructure Protection
CPE	Common Platform Enumeration
CSWG	Cyber Security Working Group
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
CyBOX	Cyber Observable Expression
EMAP	Event Management Automation Protocol
ERO	Electric Reliability Organization
FDCC	Federal Desktop Core Configuration
FERC	Federal Energy Regulatory Commission
FISMA	Federal Information Security Management Act
ICS	Industrial Control System
IT	Information Technology
NCP	National Checklist Program
NERC	North American Electric Reliability Corporation
NESCO	National Electric Sector Cybersecurity Organization
NIST	National Institute of Standards and Technology
NSTB	National SCADA Test Bed
NVD	National Vulnerability Database
OCIL	Open Checklist Interactive Language
OEEL	Open Event Expression Language
OVAL	Open Vulnerability and Assessment Language
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SGIP	Smart Grid Interoperability Panel
TMSAD	Trust Model for Security Automation Data
URI	Uniform Resource Identifier
XCCDF	Extensible Configuration Checklist Description Format

XML	Extensible Markup Language
-----	----------------------------

6.2 References

6.2.1 Documents

Short Name	Title	Date
AMI-SEC	Security Profile for Advanced Metering Infrastructure	December 2009
Bellingham Case Study	Bellingham, Washington, Control System Cyber Security Case Study	September 2007
CIP-002-4	Cyber Security - Critical Cyber Asset Identification	January 2011
CIP-003-4	Cyber Security - Security Management Controls	January 2011
CIP-005-4a	Cyber Security - Electronic Security Perimeter(s)	January 2011
CIP-006-4c	Cyber Security - Physical Security of Critical Cyber Assets	January 2011
CIP-007-4	Cyber Security - Systems Security Management	January 2011
CIP-008-4	Cyber Security - Incident Reporting and Response Planning	January 2011
CIP-009-4	Cyber Security - Recovery Plans for Critical Cyber Assets	January 2011
CSWG-TCC-001 V0.3	NISTIR 7628 Assessment Guide (and companion spreadsheet)	Under Development
	DoE Report on Common Cybersecurity Vulnerabilities in Industrial Control Systems	May 2011
	DoE Report on Cyber Security Assessments of Industrial Control Systems	November 2010
	Department of Energy Electricity Sector Cybersecurity Risk Management Process Guidelines	Public Draft September 2011
	NIST's Enterprise Continuous Monitoring Technical Reference Architecture	December 2010
NIST IR 7275 Rev. 4 DRAFT	Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2	July 2011
NIST IR 7511 Rev. 2 DRAFT	Security Content Automation Protocol (SCAP) Version 1.0 Validation Program Test Requirements	February 2011
NIST IR 7511 Rev. 3 DRAFT	Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements	November 2011
NIST IR 7692	Specification for the Open Checklist Interactive Language (OCIL) Version 2.0	April 2011
NIST IR 7756	CAESARS Framework Extension: An Enterprise	February 2011

DRAFT	Continuous Monitoring Technical Reference Architecture (Draft)	
NIST Special Publication 800-117	Guide to Adopting and Using the Security Content Automation Protocol (SCAP)	July 2010
NIST Special Publication 800-126 Rev. 4 DRAFT	The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2	September 2011
NIST Special Publication 800-128	Guide for Security-Focused Configuration Management of Information Systems	August 2011
NIST Special Publication 800-137 Initial Public Draft	Information Security Continuous Monitoring for Federal Information Systems and Organizations	December 2010
NIST Special Publication 800-37 Revision 1	Guide for Applying the Risk Management Framework to Federal Information Systems	February 2010
NIST Special Publication 800-51 Revision 1	Guide to Using Vulnerability Naming Schemes	February 2011
NIST Special Publication 800-53 Revision 3	Recommended Security Controls for Federal Information Systems and Organizations	May 2010
NIST Special Publication 800-53A Revision 1	Guide for Assessing the Security Controls in Federal Information Systems and Organizations	June 2010
NIST Special Publication 800-70 Revision 2	National Checklist Program for IT Products— Guidelines for Checklist Users and Developers	February 2011
NIST Special Publication 800-82	Guide to Industrial Control Security	June 2011
NISTIR 7275 Rev 3	Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4	January 2008
NISTIR 7275 Rev 4 DRAFT	Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2	July 2011
NISTIR 7435	The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems	August 2007
NISTIR 7502	The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities	December 2010
NISTIR 7628	Guidelines for Smart Grid Cyber Security	August 2010
NISTIR 7692	Specification for the Open Checklist Interactive Language (OCIL) Version 2.0	April 2011

6.2.2 Web Resources

Topic	Title	URL
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	http://www.us-cert.gov/control_systems/
NCP	National Checklist Program Repository	http://web.nvd.nist.gov/view/ncp/repository
NERC Reliability Standards	North American Electric Reliability Corporation Reliability Standards	http://www.nerc.com/page.php?cid=2 20
NIST Documents	NIST Computer Security Division Computer Security Resource Center	http://csrc.nist.gov/publications/index.html
NVD	National Vulnerability Database, automating vulnerability management, security measurement, and compliance checking	http://nvd.nist.gov/
OVAL	Open Vulnerability Assessment Language, the standard for determining vulnerability and configuration issues on computer systems	http://oval.mitre.org/
SCAP	The Security Content Automation Protocol (SCAP)	http://scap.nist.gov/
SCAP Products	SCAP Validated Products	http://nvd.nist.gov/scaproducts.cfm