

US-CERT Control Systems Security Center Standards Awareness & Capabilities Overview

Kevin D. Robbins

Representing the US-CERT CSSC
Standards Awareness & Capabilities Team

Sandia National Laboratories
Information Operations Red Team and Assessments
Critical Infrastructure Systems

27 October 2005



US-CERT Control Systems Security Center

The US-CERT Control Systems Security Center (CSSC)

- ▶ funded by the Department of Homeland Security
- ▶ is one response to the National Strategy to Secure Cyberspace,
- ▶ and works with industry, universities, national laboratories, and government agencies to develop and deploy technologies that protect critical infrastructures against cyber-attacks.

The CSSC Cyber-Security Protection Framework

- ▶ will provide owners, operators, and vendors a tool
- ▶ to assess security of control systems against a database of cyber-security requirements, initially developed from the Common Criteria.

Standards Awareness & Capabilities Overview

goals and team members

Goals of this cyber-security task include

- ▶ supporting development of CSSC Framework by identifying
 - ▶ operational requirements, guidelines, standards, and regulations
 - ▶ that drive industry practice in control systems (CS) security in critical infrastructures (CI), and
- ▶ comparing CS security standards with the CSSC Framework.

The standards awareness & capabilities team is

- ▶ a multilaboratory effort involving
- ▶ Argonne National Laboratory, Idaho National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratories.

Comparing CS Security Standards with CSSC Framework

to understand the state of standards and to validate the CSSC Framework cyber-requirements

The team compared CS security standards with the CSSC Framework

- ▶ to identify requirements common to both,
- ▶ to identify requirements found in one but not the other, and
- ▶ to identify families of requirements not found in the CSSC Framework.

The CSSC Framework provided an objective basis for the comparison.

But, matching requirements needed judgment, because

- ▶ control systems security standards are often written at a higher level than CSSC Framework cyber-requirements, and
- ▶ the CSSC Framework cyber-requirements, based on Common Criteria components, often purposely require further specification.

Example CSSC Framework Cyber-Requirements

- FAU_SAR.1.1 The TSF shall provide [assignment: authorized users] with the capability to read [assignment: list of audit information] from the audit records.
- FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
- FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards].

Classes of CSSC Framework Cyber-Requirements

At the time of comparison, the CSSC Framework Cyber-Requirements were organized into eleven classes:

- ▶ Security Audit
- ▶ Event Definition
- ▶ Cryptographic Support
- ▶ Resource Utilization
- ▶ Configuration Management
- ▶ Target Access
- ▶ Trusted Channel and Path
- ▶ User Data Protection
- ▶ Identification and Authentication
- ▶ Security Management
- ▶ Protection of Trusted Security Functions

Additional Cyber-Requirements Identified

by standards organizations but not identified in CSSC Framework

Additional Families

	Software Management Control Plan	Product Safety Plan	Operations & Maintenance Manual	Records Retention	Verification & Validation	Risk Assessment	Hazards Analysis	Human Factors Analysis	Failure Analysis	Testing	Training & Security Awareness	Compliance
Chemical	●	◐	○	●	●	●	●	◐	◐	●	●	●
Natural Gas	○	○	○	○	●	●	◐	○	◐	●	◐	○
Petroleum & Oil	●	◐	○	●	○	●	○	◐	◐	●	◐	●
Transportation - Rail	●	●	●	●	●	●	●	●	●		●	○
Cross-sector ISA SP99 TR99	◐	○	○	○	○	●	○	○	○	●	●	●
Electrical Power											●	●
Telecommunications	●	○	○	○	●	●	●	○	○	●	●	○
Water	○	○	○	○	○	○	○	○	○	○	●	○

The comparison identified other families of cyber-requirements not found in the CSSC Framework; those included in the table above were those most commonly addressed in the reviewed standards.

Benefits of the Comparison

of CS Security Standards with CSSC Framework cyber-requirements

The standards awareness & capabilities team expects this work to

- ▶ build awareness and understanding of existing and emerging CS security standards in CI sectors,
- ▶ provide opportunities for standards organizations to collaborate and to leverage each other's work,
- ▶ identify areas of security concern needing further attention, and
- ▶ assist the CSSC Framework team in delivering results that meet industry needs.

Discussion Questions

What other CS security standards should be included in the comparison?

How can the standards organizations use the comparison results and summary tables?

How can the comparison results and summary tables support collaboration among interested standards organizations?

Can the comparison results and summary tables help identify a *meta-standard* that addresses all CSSC Framework cyber-requirements by referencing existing standards that collectively cover the cyber-requirements?