

# **CS<sup>2</sup>SAT**

## **Control Systems Cyber Security Self Assessment Tool**

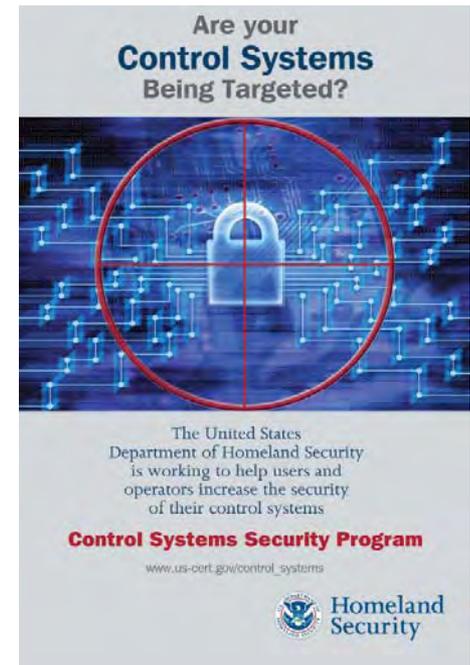
# **CS<sup>2</sup>SAT Training**

**Jeffrey S. Tebbe, PE, Idaho National Laboratory  
Control System Security Program  
PCSF March 6-8, 2007**

# DHS Control Systems Security Program

- ◆ The sponsor for this effort is the Department of Homeland Security (DHS) Control Systems Security Program (CSSSP)
- ◆ The goal of the CSSSP is to

***“Reduce Cyber Risk to Critical Infrastructure Control Systems by providing guidance and building partnerships”***



# CS<sup>2</sup>SAT Training Agenda

- ◆ **What is the basis for the CS<sup>2</sup>SAT**
- ◆ **CS<sup>2</sup>SAT Capabilities**
- ◆ **What is needed to make using the CS<sup>2</sup>SAT successful**
- ◆ **How does the CS<sup>2</sup>SAT work**
- ◆ **Handout / Installing / Launching the tool**
- ◆ **Sample Assessment**
- ◆ **Interpreting the results**

# DHS Control System Security Program

- ◆ **The CS<sup>2</sup>SAT was developed under the CSSP**
- ◆ **Major CSSP objective is cyber risk identification & mitigation for control systems**
- ◆ **CSSP is also involved in:**
  - supporting US-CERT response to incidents
  - partnering with vendors and industry
  - standards development
  - overall awareness activities

# Basis of the CS<sup>2</sup>SAT

## Requirements derived from widely accepted standards

- NIST SPP-CIPCS 1.07
- NIST SPP-PCS 1.0
- ISO/IEC 15408
- ISO 17799
- NIST 800-53, 800-82
- ISA SP-99
- NERC CIP-002 – CIP-009
- and others

# CS<sup>2</sup>SAT Capabilities

## What the CS<sup>2</sup>SAT CAN do:

- ◆ Stand alone interactive assessment tool
- ◆ Assist in evaluating a control system network
- ◆ Provide recommendations for weaknesses
- ◆ Provide standards specific information & reports
- ◆ Provide a baseline of security posture
- ◆ Use as a requirements generator for new purchases

## Limitations:

- ◆ Recommendations only as good as interviewees responses
- ◆ Final implementation / evaluation of recommendations

# Successfully using the CS<sup>2</sup>SAT

What is needed:

**TEAM of participants**

- ◆ **Controls Engineer (knowledge of control system)**
- ◆ **Configuration Manager (knowledge of systems management)**
- ◆ **Operations Manager (knowledge of operations)**
- ◆ **IT Network Specialist (knowledge of IT infrastructure)**
- ◆ **IT Security Officer (knowledge of Policy and Procedures)**

# How does the CS<sup>2</sup>SAT work

Database of Solutions

*to Mitigate Vulnerabilities*

Knowledge Base of Cyber  
Security Requirements

*to Secure a Control System*

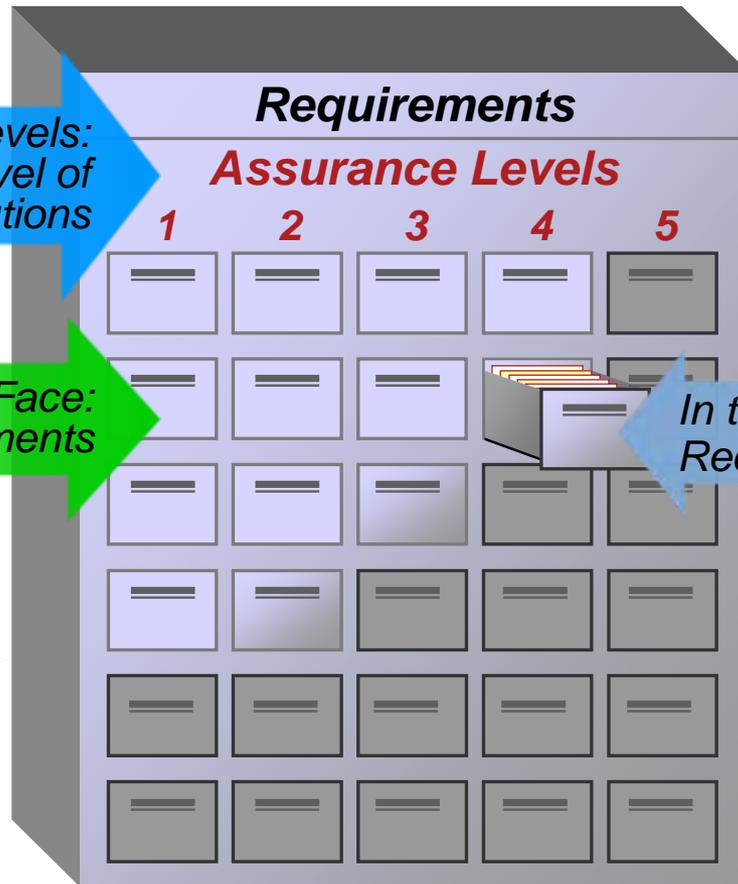
Analysis, Discovery &  
User Interface Tools

*to Assist in the Evaluation  
of a Control System*

# How does the CS<sup>2</sup>SAT work

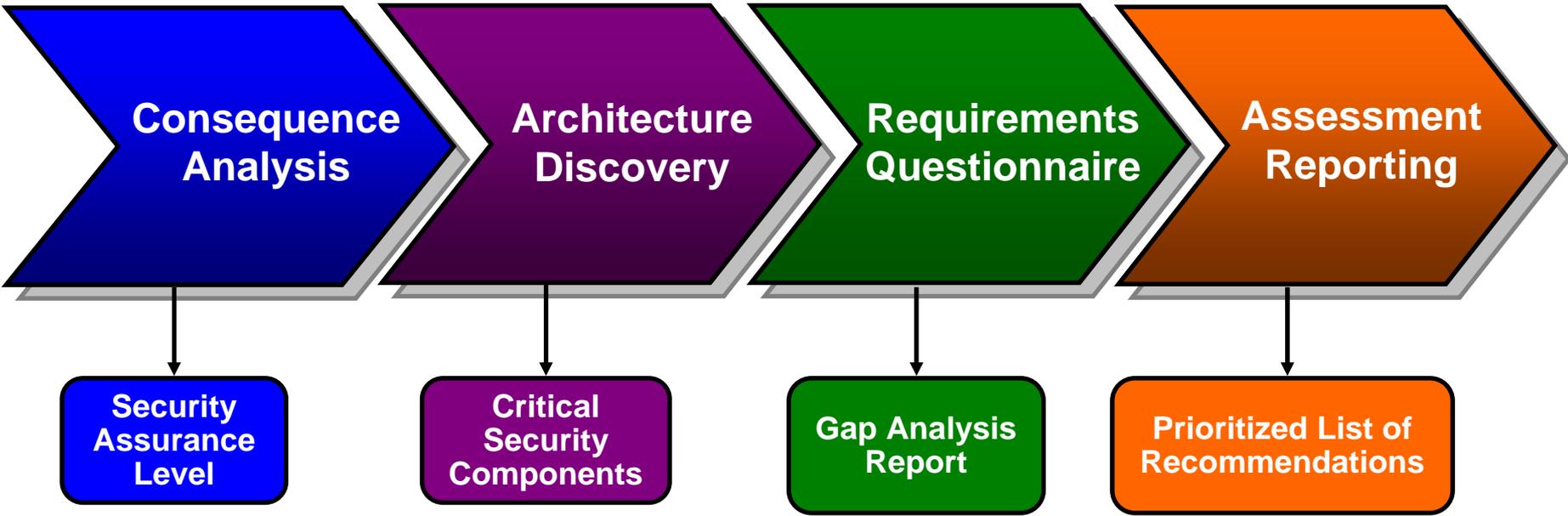
*Assurance Levels:  
Increasing Level of  
Rigor for Solutions*

*On the Face:  
Requirements*



# CS<sup>2</sup>SAT Flow Process

*Four Independent Elements*



# CS<sup>2</sup>SAT Demonstration

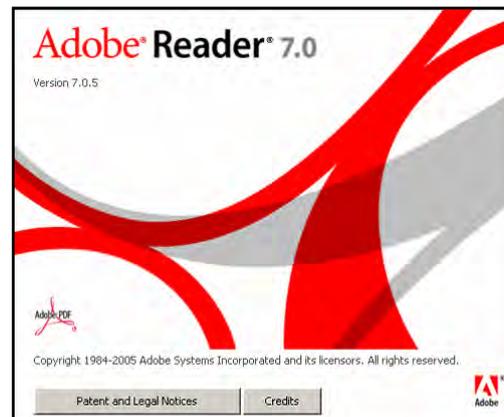
## System Requirements:

**JAVA Version 1.5.6**



**Adobe Reader 5.0**

**Win 2000, XP  
100mb storage  
CD/DVD drive**



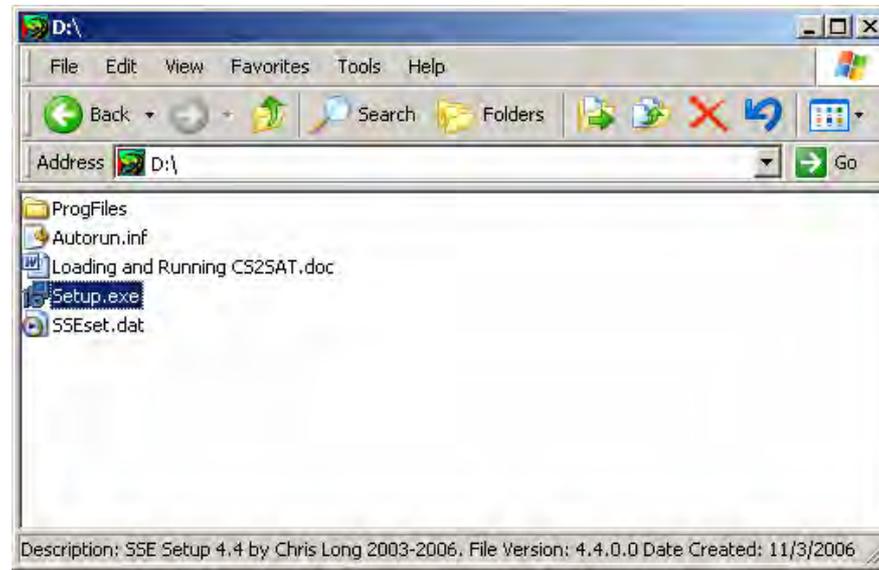
# Installation of CS<sup>2</sup>SAT

Place the CD into the CD-Rom Drive.

If AutoRun is disabled, navigate to the CD-Rom drive and run setup.exe

The installation program will install the software and desktop icon. Follow the on screen instructions to select the directory to place the program.

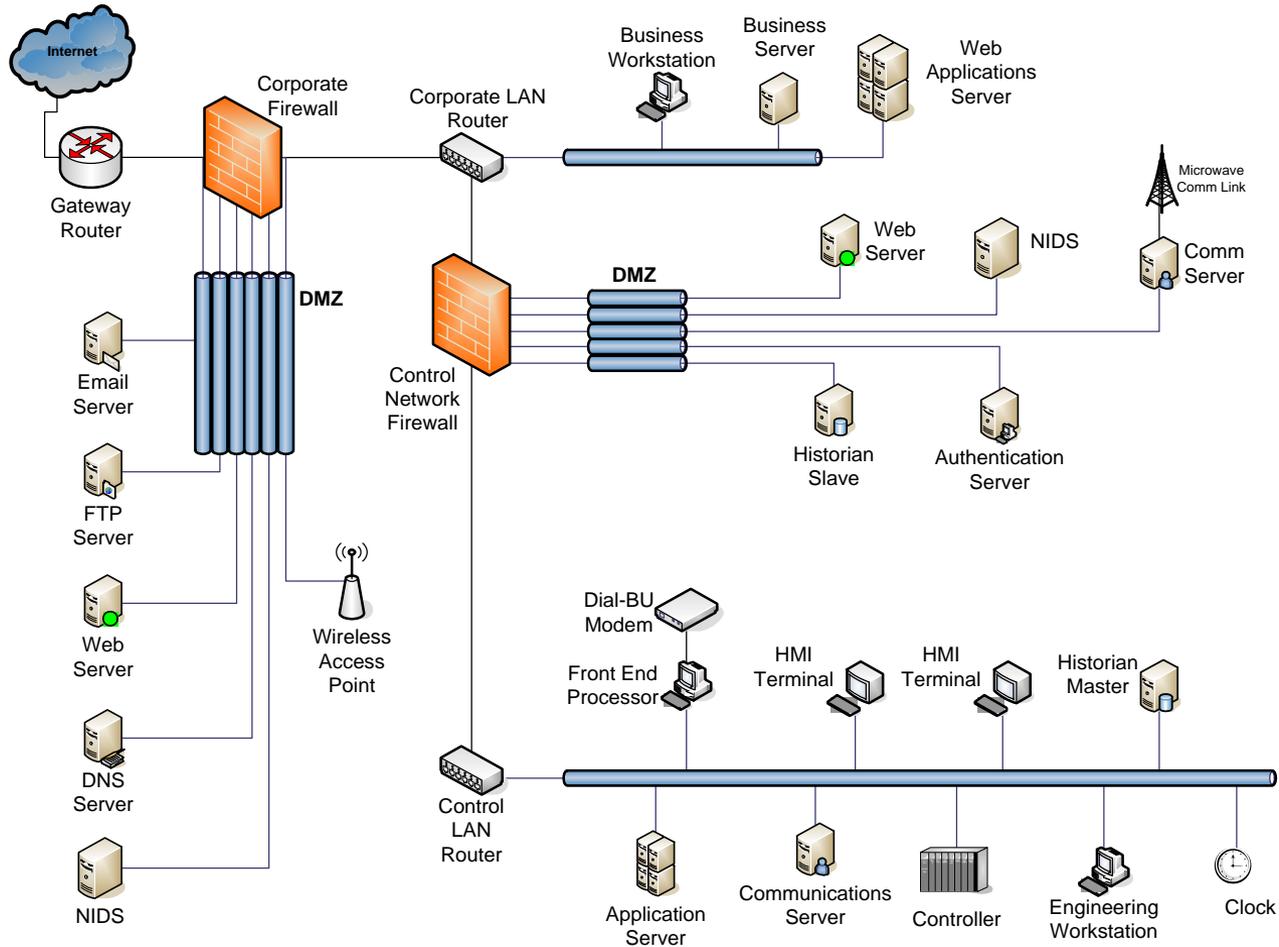
**C:/ProgramFiles/CS2SAT**  
is the default directory  
for installation.



# Splash Screen



# Performing an Assessment



# Interpreting the Results

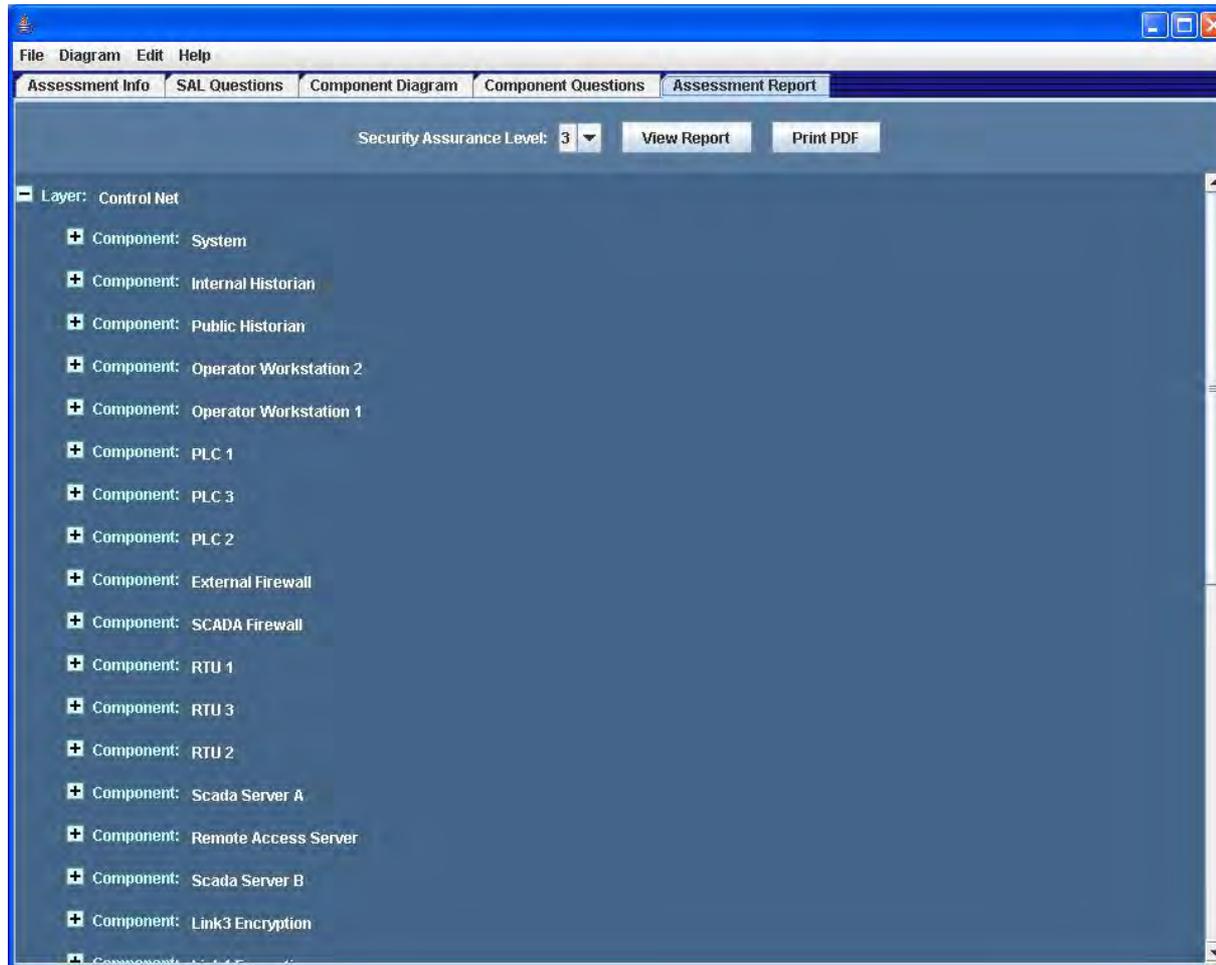
## ◆ On Screen Report

- Gap Analysis
- Recommendations
- Requirement Source Information / Tracking

## ◆ Hard Copy Report

- Executive Summary
- Pie Chart Summary
- Gap Analysis
- Sorted Gap Analysis (Prioritized list)
- Standard Specific Report (NERC CIP comparison)
- Response Summary

# On Screen Report - Summary



# On Screen Report - Detail

CS2SAT - IEIA CIP forum

File Diagram Edit Help

Assessment Info SAL Questions Component Diagram Component Questions Assessment Report

Security Assurance Level: 3 Update Report Print PDF

Average SAL = 4 +/- 2

Component: System

Question: 8. Has a cyber security policy been published that represents management's commitment and ability to security cyber assets?

Question: 12. Is a senior manager assigned overall responsibility for implementation, adherence and maintenance of the CIP standards?

GAP Requirement (System-CIP-003 R2): The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.

Your answers, highlighted in yellow in the table below, place this requirement at SAL 1. To reach your specified SAL of 3, you must be able to select all the answers for a row in the table below that has a level equal to or greater than the SAL shown in green.

SAL	Required Answer(s)
0	Unknown.
1	A senior manager has not been identified for implementation and compliance to CIP.
2	A senior manager is assigned the responsibility for leading and managing the organization's implementation and compliance with the CIP standards.
3	A senior manager is assigned the responsibility for leading and managing the organization's implementation and compliance with the CIP standards.
4	A senior manager is assigned the responsibility for leading and managing the organization's implementation and compliance with the CIP standards.
5	A senior manager is assigned the responsibility for leading and managing the organization's implementation and compliance with the CIP standards.

■ SAL calculated from questionnaire answer  
■ Minimum SAL needed to meet requested :  
■ Answers selected in questionnaire

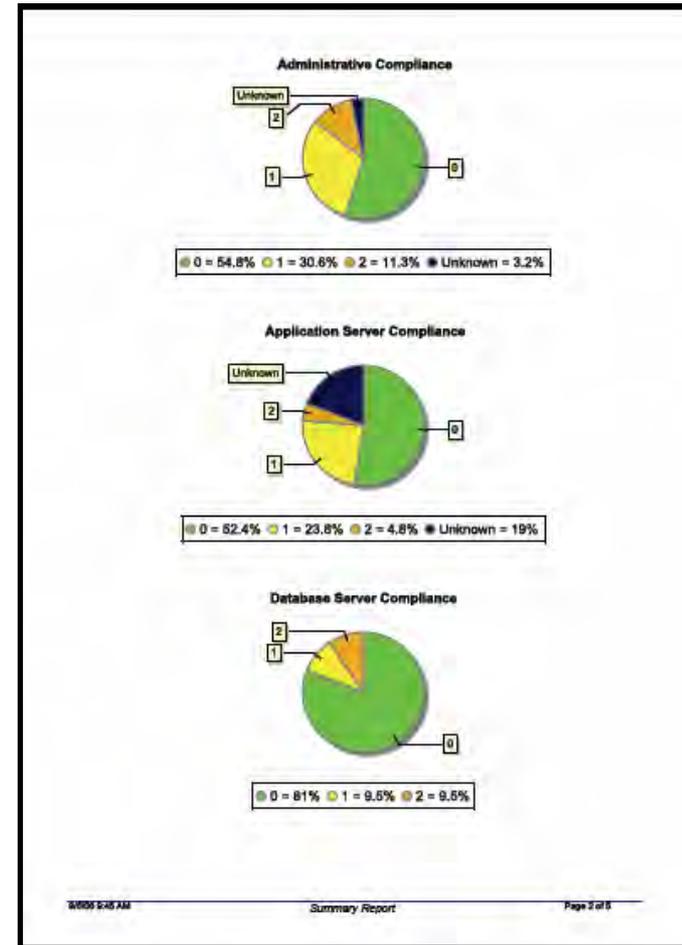
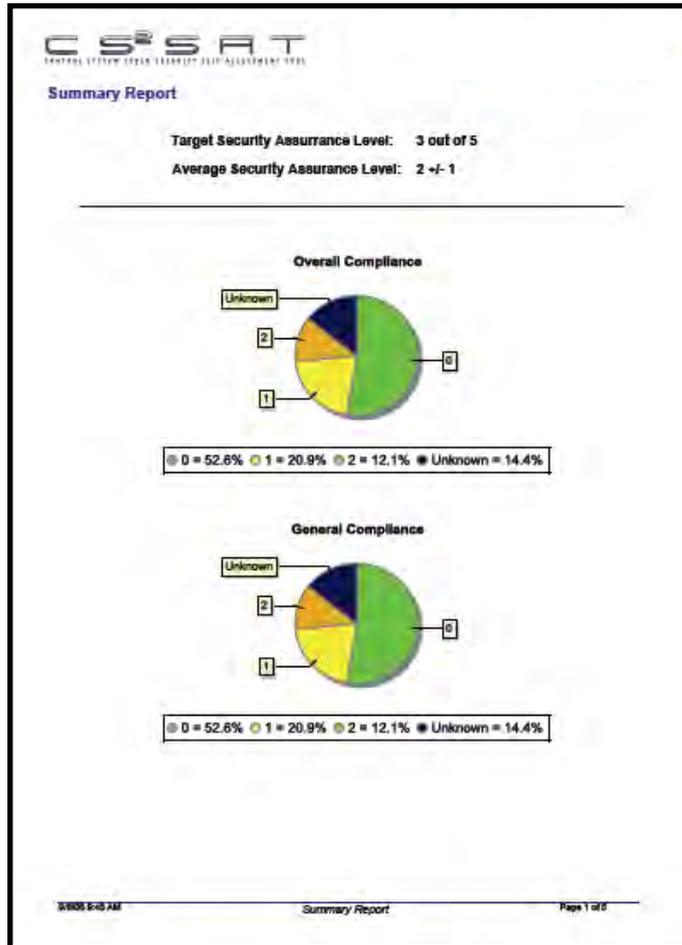
**Level Specific Requirement**  
 A senior manager shall be given the overall responsibility for leading and managing the organizations implementation, adherence and maintenance of the CIP standards.

Show Detail Jump To Question

Question: 16. Have conformance issues with the cyber security policy been documented and authorized by senior management?

Question: 22. Has information to be protected been classified as to sensitivity of the critical cyber asset information?

# Hardcopy Report - Summary



# Hardcopy Report - Detail

**CSSAT**  
CONTROL SYSTEMS SECURITY SELF-ASSESSMENT TOOL

Sorted Gap Analysis Report

**Legend**

- SAL calculated from questionnaire answers
- Minimum SAL needed to meet requested SAL
- Answers selected in questionnaire

Component: External Firewall    Asset: Firewall    Layer: Control Net    Compliance(N): 0

**Question:** Are cryptographic keys destroyed according to recognized standards?

**Requirement:** The firewall security functionality shall destroy cryptographic keys in accordance with a specified key destruction method that is based on an assigned standard.

SAL	Answers
0	Unknown.
1	Keys are not destroyed.
2	Destruction involves zeroization of all private keys.
3	Destruction involves zeroization of all private keys, plaintext keys and key data.
4	Destruction involves zeroization of all private keys, plaintext keys and key data and all other cryptographic security parameters.

**Level Specific Requirement:**  
Cryptographic key destruction should involve the zeroization of all private cryptographic keys, plaintext cryptographic keys and key data.

Component: External Firewall    Asset: Firewall    Layer: Control Net    Compliance(N): 0

**Question:** Is the responsibility for accessing and changing firewall component security-related data limited to authorized security personnel?

**Requirement:** The firewall security functions shall allow only authorized users to manage security data.

SAL	Answers
0	Unknown.
1	No, anyone can change security-related data.
2	Yes, only authorized security personnel can access and modify the values of firewall component security data.

**Level Specific Requirement:**  
The firewall components shall restrict the ability to query, modify, delete, clear, and create the security relevant security related data except for audit records, user security attributes, and critical security parameters to authorized security personnel.

10:00:54 AM    Sorted Gap Analysis Report    Page 1 of 7

Component: SCADA Firewall    Asset: Firewall    Layer: Control Net    Compliance(N): 0

**Question:** Are cryptographic keys destroyed according to recognized standards?

**Requirement:** The firewall security functionality shall destroy cryptographic keys in accordance with a specified key destruction method that is based on an assigned standard.

SAL	Answers
0	Unknown.
1	Keys are not destroyed.
2	Destruction involves zeroization of all private keys.
3	Destruction involves zeroization of all private keys, plaintext keys and key data.
4	Destruction involves zeroization of all private keys, plaintext keys and key data and all other cryptographic security parameters.

**Level Specific Requirement:**  
Cryptographic key destruction should involve the zeroization of all private cryptographic keys, plaintext cryptographic keys and key data.

Component: SCADA Firewall    Asset: Firewall    Layer: Control Net    Compliance(N): 0

**Question:** Is the responsibility for accessing and changing firewall component security-related data limited to authorized security personnel?

**Requirement:** The firewall security functions shall allow only authorized users to manage security data.

SAL	Answers
0	Unknown.
1	No, anyone can change security-related data.
2	Yes, only authorized security personnel can access and modify the values of firewall component security data.

**Level Specific Requirement:**  
The firewall components shall restrict the ability to query, modify, delete, clear, and create the security relevant security related data except for audit records, user security attributes, and critical security parameters to authorized security personnel.

Component: External Firewall    Asset: Firewall    Layer: Control Net    Compliance(N): 0

**Question:** Are monitored firewall component available events compared against a fixed rule set regularly for potential violations?

**Requirement:** The firewall component security functionality shall define (and enforce) a fixed rule set indicating potential violations of the system.

SAL	Answers
0	Unknown.
1	No monitoring of the firewall component.
2	The firewall component available events identified are monitored against rule sets periodically commensurate with need.
3	The firewall component available events identified are monitored against rule sets when configuration changes are made.
4	The firewall component available events identified are monitored against rule sets continuously.

**Level Specific Requirement:**  
The firewall component performs daily monitoring of available events.

10:00:54 AM    Sorted Gap Analysis Report    Page 2 of 7

# Hardcopy Report – Prioritized

**CS2SAT**  
CONTROL SYSTEMS SECURITY SELF-ASSESSMENT TOOL

Sorted Gap Analysis Report

Legend:   
■ SAL calculated from questionnaire answers   
■ Minimum SAL needed to meet requested SAL   
■ Answers selected in questionnaire

Consistent: External Firewall    Asset: Firewall    Layer: Control Net    **Compliance (%) 0**

Question: Are cryptographic keys destroyed according to recognized standards?  
 Requirement: The firewall security functionality shall destroy cryptographic keys in accordance with a specified destruction method that is based on an approved standard.

SAL	Answers
0	Unknown
1	Keys are not destroyed.
2	Destruction involves zeroization of all private keys.
3	Destruction involves zeroization of all private keys, plaintext keys and key data.
4	Destruction involves zeroization of all private keys, plaintext keys and key data and all other cryptographic security parameters.

Level Specific Requirement:  
 Cryptographic key destruction should involve the zeroization of all private cryptographic keys, plaintext cryptographic keys and key data.

Consistent: External Firewall    Asset: Firewall    Layer: Control Net    **Compliance (%) 0**

Question: Is there responsibility for accessing and changing firewall component security-related data limited to authorized security personnel?  
 Requirement: The firewall security functions shall allow only authorized users to manage security data.

SAL	Answers
0	Unknown
1	No, anyone can change security-related data.
2	Yes, only authorized security personnel can access and modify the values of firewall component security data.

Level Specific Requirement:  
 The firewall components shall restrict the ability to query, modify, delete, clear, and create the security-relevant security-related data stored for audit records, user security attributes, and critical security parameters to authorized security personnel.

WIKO 2016-01-01    Sorted Gap Analysis Report    Page 1 of 7

*Prioritized Gap Analysis based on % Target met*

# Hardcopy Report – NERC CIP



## CIP Report

### System-CIP-002

- R1 - The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1 - The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2 - The risk-based assessment shall consider the following assets: R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard. R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System. R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System. R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System. R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

<b>Component: System</b>	<b>Asset: System</b>	<b>Requirement: System-CIP-002 R1</b>	<b>Target(%) 100</b>
--------------------------	----------------------	---------------------------------------	----------------------

- |   |  |   |
|---|--|---|
| ● | Has a risk-based assessment methodology been documented to identify Critical Assets? | A risk-based assessment methodology for identification of critical assets has been developed. |
|---|--|---|

<b>Component: System</b>	<b>Asset: System</b>	<b>Requirement: System-CIP-002 R1.1</b>	<b>Target(%) 100</b>
--------------------------	----------------------	---	----------------------

- |   |   |   |
|---|---|---|
| ● | Is the risk-based assessment documentation, procedures, and evaluation criteria maintained as required? | Yes, the risk-based assessment documentation to include procedures and evaluation criteria is maintained. |
|---|---|---|

<b>Component: System</b>	<b>Asset: System</b>	<b>Requirement: System-CIP-002 R1.2</b>	<b>Target(%) 100</b>
--------------------------	----------------------	---	----------------------

- |   |   |  |
|---|---|--|
| ● | Does the risk-based assessment consider the required assets (see HELP for required assets)? | Yes, the risk-based assessment considers all of the required assets. |
|---|---|--|

# Hardcopy Report – Answer Key



## Framework Report

### System - System

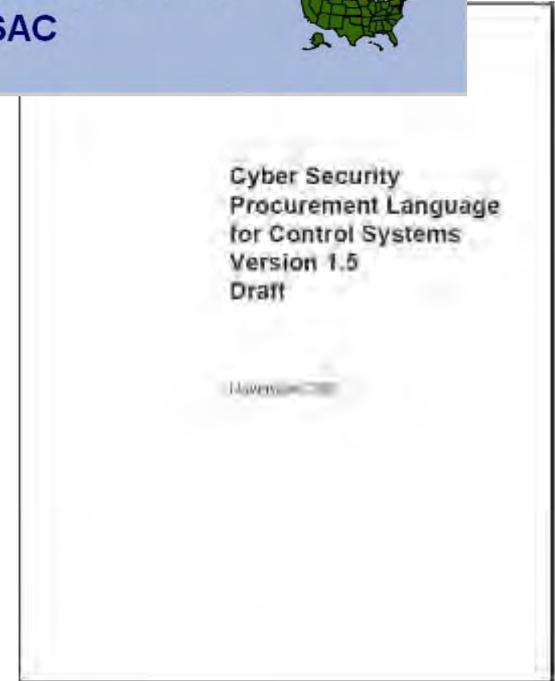
Question	Answer
<input checked="" type="radio"/> Branching Question - Select the Standards to be included in this assessment.	NERC CIP-002 through CIP-009  NIST SP800-53  ISO/IEC 15408 v3,1 Assurance Rqmts.
<input checked="" type="radio"/> Has a risk-based assessment methodology been documented to identify Critical Assets?	A risk-based assessment methodology for identification of critical assets has been developed.
<input checked="" type="radio"/> Is the risk-based assessment documentation, procedures, and evaluation criteria maintained as required?	Yes, the risk-based assessment documentation to include procedures and evaluation criteria is maintained.
<input checked="" type="radio"/> Does the risk-based assessment consider the required assets (see HELP for required assets)?	Yes, the risk-based assessment considers all of the required assets.
<input checked="" type="radio"/> Have the critical assets been identified using the risk-based assessment approach and reviewed and updated as necessary at least annually?	The risk-based assessment methodology is used on an annual basis to determine critical assets.
<input checked="" type="radio"/> Have critical cyber assets been identified with a similar risk-based assessment approach?	Critical Cyber assets are developed using a similar risk-based assessment approach used for identification of other assets.

# Procurement Language



## Current Status:

- Collaborated with Industry in releasing Procurement Language guide, which provides sample or recommended language for control systems security requirements



## Project Website:

<http://www.msisac.org/scada/>

# Questions?

Are your  
**Control Systems**  
Being Targeted?



The United States  
Department of Homeland Security  
is working to help users and  
operators increase the security  
of their control systems

**Control Systems Security Program**

[www.us-cert.gov/control\\_systems](http://www.us-cert.gov/control_systems)



**Homeland  
Security**

For additional information on the  
Control Systems Security Program

[www.us-cert.gov/control\\_systems](http://www.us-cert.gov/control_systems)

Or email us at [cssp@dhs.gov](mailto:cssp@dhs.gov)