Building Insecurity

Lisa Kaiser

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
Insecurity

How do I
- Specify it
- Buy it
- Test it
- Deploy it
- Regret it
- Apologize for it
Specifying Insecurity

- Ignore security entirely
- Specify inappropriate standards
- Use vagueness
- Demand particular technology solutions
Buying Insecurity

- Never mention security
- Don’t put it in writing
- Listen when they say “We’ll secure it later”
- Cheaper is always more secure
- New is more secure
Testing Insecurity

- Never test
- Check only “sunny day” scenarios
- Rely on vendor assurances
- Use only cheap security “experts”
- Use your firewalls
Deploying Insecurity

- Don’t plan
- Use default passwords
- Bypass all the security
- Never do SAT
- Ignore security alarms and alerts

*Photo courtesy of Kristian Ovaska, 2003*
Regretting Insecurity

- Begin with RFQ
- Ignore any breaches
- Shoot the Messenger
- Apply quick-fixes
- Use the “Blame-game”

“Instead of red-light cameras to raise money, we just put toll booths at every intersection!”
Apologizing for Insecurity

- Leave the organization
- Distract customers
- Avoid responsibility
- Attack the messengers
- Use the press
- Blame us
However…

» If you’re NOT trying to Building Insecurity, but instead which to Build In Security…

» Try this to achieve your goal:
Cyber Security Evaluation Tool (CSET®)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy

CSET Download:
http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET
## CSET® Standards

**Requirements Derived from Widely Recognized Standards**

<table>
<thead>
<tr>
<th>Standard/Guideline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Special Publication 800-53</td>
<td>Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls</td>
</tr>
<tr>
<td>NERC Critical Infrastructure Protection (CIP)</td>
<td>Reliability Standards CIP-002 through CIP-009, <strong>Revisions 3 and 4</strong></td>
</tr>
<tr>
<td>DoD Instruction 8500.2</td>
<td>Information Assurance Implementation, February 6, 2003</td>
</tr>
<tr>
<td>NRC Reg. Guide 5.71</td>
<td>Cyber Security Programs for Nuclear Facilities, January 2010</td>
</tr>
<tr>
<td>CFATS RBPS 8- Cyber</td>
<td>Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27</td>
</tr>
<tr>
<td>Transportation Security Agency Pipeline Guidelines</td>
<td>DHS TSA guidance for the pipeline industry</td>
</tr>
</tbody>
</table>
CSET® Capabilities

What the CSET CAN do:

- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cybersecurity recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

What the CSET CAN’T do:

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policy & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities
**Assessment Team**

A TEAM of participants is required to perform a successful assessment

<table>
<thead>
<tr>
<th>Type of Participant</th>
<th>Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Systems Engineer</td>
<td>Control systems</td>
</tr>
<tr>
<td>Configuration Manager</td>
<td>Systems management</td>
</tr>
<tr>
<td>Operations Manager</td>
<td>Business operations</td>
</tr>
<tr>
<td>IT Network Specialist</td>
<td>IT infrastructure</td>
</tr>
<tr>
<td>IT Security Officer</td>
<td>Policy &amp; procedures</td>
</tr>
<tr>
<td>Risk Analyst or Insurance Specialist</td>
<td>Risk</td>
</tr>
</tbody>
</table>
Assessment Process

1. Organize the Team
2. Add Assessment Information
3. Select the Mode and Standards
4. Determine the Security Level
5. Build the Network Diagram
6. Answer Questions
7. Analyze Results
Diagram Screen Layout

CSET includes a drawing tool that is valuable in several ways. First, it provides a place to graphically capture a picture of the control system or information technology network. Second, it incorporates simple network analysis features to identify areas of vulnerability and recommendations for protection. Third, it is used to create the foundation for the question set that is incorporated into the overall assessment and analysis.

When you start a new assessment and click on the Diagram button on the top row of the CSET Main Window, the system will open the screen shown in Figure 1.
Starting Screen

What would you like to do?

- Create a New Assessment
- Open South Creek Plant.cset
- Open an Existing Assessment
- View the User Guide
- Exit the CSET Application
Assessment Info – Main Window

ASSESSMENT:
Assessment Name: Summer Creek Plant Assessment
Facility Name: Summer Creek Plant
Assessment Date: 1/7/2013
City or Site Name: Idaho Falls
State, Province, or Region: Idaho

PRINCIPAL ASSessor:
Name: John Jackson Doe
Email: JJD@acme.com
Telephone: (123) 456-7890

DESCRIPTION OF ASSESSMENT:
This is the baseline assessment of the control systems at the Summer Creek Plant. This will be the first assessment for the company and will review all the cyber and control systems at the plant. A full team will be organized and will include the plant manager, the control systems engineer, the network administrator, the on-site information technology specialist and senior plant operators.

COMMENTS:
After completing the assessment, we found a number of areas that need attention and others that we will plan to address over the next 8 months. We require longer-term policy changes; however, we are going to start the process to make the changes as soon as the immediate issues have been resolved.

ADDITIONAL CONTACTS:
Taranna Smith-Wilkinson (Network Administrator)
(123) 456-8888
tsk@acme.com
Standards Screen – Assessment Modes

**STEP 1 - Assessment Mode**

Most users should select the 'Questions Based' option for a comprehensive evaluation based on questions rather than requirements.

To see the exact requirements for a specific standard, choose the 'Standard Requirements Based' option. This would be common for regulated sectors where the precise wording is important.

What approach would you like to take to perform a cyber security evaluation?
- Questions Based
- Standard Requirements Based

**STEP 2 - Questions and Standards**

**STEP 3 - Security Assurance Level (SAL)**
# Questions and Standards

## STEP 1 - Assessment Mode

## STEP 2 - Questions and Standards

<table>
<thead>
<tr>
<th>Select Standard(s):</th>
<th>Information Technology (IT) Specific Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Control System Standards:</td>
<td>NIST Special Publication 800-53 Rev 3</td>
</tr>
<tr>
<td>- Catalog Of Recommendations Rev 7</td>
<td></td>
</tr>
<tr>
<td>- Universal Questions</td>
<td></td>
</tr>
<tr>
<td>- Key Questions</td>
<td></td>
</tr>
<tr>
<td>- NIST Special Publication 800-82</td>
<td></td>
</tr>
<tr>
<td>- NIST Special Publication 800-53 Rev 3 App I</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sector Specific Standards:</th>
<th>Requirements Mode Only Standards:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- CFATS Risk-Based Performance Standards Guide 8 - Cyber</td>
<td>Consensus Audit Guidelines (CAG)</td>
</tr>
<tr>
<td>- NERC CIP-002 through CIP-009 Rev 3</td>
<td>DOD Instruction 8500.2</td>
</tr>
<tr>
<td>- NERC CIP-002 through CIP-009 Rev 4</td>
<td>Confidentiality Level:</td>
</tr>
<tr>
<td>- NRC Regulatory Guide 5.71</td>
<td>- Classified</td>
</tr>
<tr>
<td>- TSA Pipeline Security Guidelines April 2011</td>
<td>- Sensitive</td>
</tr>
</tbody>
</table>

## STEP 3 - Security Assurance Level (SAL)

Confidentiality Level:
- Classified
- Sensitive
- Public

MAC Level:
- MAC III
- MAC II
- MAC I
Questions and Standards

Select your cyber Security Assurance Level (SAL):

- SAL: High

- General SAL Determination
- NIST SAL Determination

INFORMATION  PREVIOUS  NEXT  DIAGRAM
General SAL Determination

Injury:
If control systems were maliciously accessed and manipulated to cause harm, how many people could sustain injuries not requiring hospital stay in a worst-case scenario? (Consider injuries caused due to any reason.)

Hospital:
If control systems were maliciously accessed and manipulated to cause harm, how many people could sustain injuries requiring hospital stay in a worst-case scenario? (Consider injuries caused due to any reason.)

Death:
If control systems were maliciously accessed and manipulated to cause harm, how many people could be killed in a worst-case scenario? (Consider injuries caused due to any reason.)

Capital Assets:
For a worst-case scenario, estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)

Economic Impact:
For a worst-case scenario, estimate the potential cost in terms of economic impact to both the organization and the community. Consider any losses to community structures and economic impact associated with other losses.
NIST SAL Determination
Diagramming Tool
Diagram – Maximized Screen Space
Questions Screen

Access Control

1. Are appropriate agreements finalized before access is granted, including for third parties and contractors?
2. Are access agreements periodically reviewed and updated?
3. Does the system enforce assigned authorizations for controlling logical access to the system?
4. Are specific user actions that can be performed on the system without identification or authentication identified and documented?
5. Are actions to be performed without identification and authentication permitted only to the extent necessary to accomplish mission objectives?
6. Do the authentication mechanisms obscure feedback of authentication information during the authentication process?
7. Does the system employ authentication methods that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module?
8. Does the failure of cryptographic module authentication NOT create a denial of service or adversely impact the operational performance of the system?
Question Information

![Question Information Image]

Access Control

1. Are appropriate agreements finalized before access is granted, including for third parties and contractors?
2. Are access agreements periodically reviewed and updated?
3. Does the system enforce assigned authorizations for controlling logical access to the system?
4. Are specific user actions that can be performed on the system without identification or authentication identified and documented?
5. Are actions to be performed without identification and authentication permitted only to the extent necessary to accomplish mission objectives?
6. Do the authentication mechanisms obscure feedback of authentication information during the authentication process?
7. Does the system employ authentication methods that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module?
8. Does the failure of cryptographic module authentication NOT create a denial of service or adversely impact the operational performance of the system?
9. Is a defined list of devices uniquely identified and authenticated before a connection is established?
10. Does the system uniquely identify and authenticate organizational users?
11. Does the system employ multifactor authentication for remote access and for access to privileged accounts?
12. Does the system employ multifactor authentication for network access and for access to privileged accounts?
13. Are security measures in place to restrict information input to the system to authorized personnel only?
14. Are there policies and procedures concerning the generation and use of passwords?

Supplemental

The organization may allow limited user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible systems). Organizations should also identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be via a physical switch that is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and authentication have not yet occurred.

Level Specific Requirement

The organization identifies and documents specific user actions, if any, that can be performed on the system without identification or authentication. Requirement Enhancement – The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

Source Documents

- Catalog of Control Systems
  - 2.15.11

Help Documents
Comments, Marked and Alternates
Component Questions

Boundary Protection

1. Are public facing servers placed in a DMZ. In other words, behind a firewall with an additional firewall between that and any systems on the internal network? (Yes, No, N/A, Alt)

2. Have rulesets been reviewed for appropriate order?

3. Have state tables been reviewed?

4. Is all incoming and outgoing ICMP traffic denied except where specifically permitted by your organization.

5. Are loose and strict source routing blocked and logged?

6. Is outbound traffic with an invalid source address blocked? In other words, is egress filtering implemented?

7. Is traffic to your e-mail server only allowed via a specific protocol and port?

8. Is direct external traffic, traffic from the Internet, to critical servers blocked by default?

Components

- Application Server: Override
- Database Server: Override
- Firewall: Override
- Web Server: Override

Level Specific Requirement:

Are public facing servers placed in a DMZ. In other words, behind a firewall with an additional firewall between that and any systems on the internal network?
Component Overrides

Use this window to change the default answers for the displayed component type.

Component Type: Database Server

Question: Are public facing servers placed in a DMZ. In other words, behind a firewall with an additional firewall between that and any systems on the internal network?

Select an option to override all answers for the component types below.

Yes No N/A

<table>
<thead>
<tr>
<th>Component Name</th>
<th>Yes</th>
<th>No</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Historian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Historian</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DBS-6868</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Analysis Screen
Analysis Detail Screens
Analysis Detail - Example

<table>
<thead>
<tr>
<th>Subject Area</th>
<th>Passed</th>
<th>Total</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>11</td>
<td>24</td>
<td>46</td>
</tr>
<tr>
<td>Account Management</td>
<td>16</td>
<td>43</td>
<td>37</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>10</td>
<td>38</td>
<td>28</td>
</tr>
<tr>
<td>Communication Protection</td>
<td>14</td>
<td>21</td>
<td>67</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>11</td>
<td>23</td>
<td>48</td>
</tr>
<tr>
<td>Continuity</td>
<td>12</td>
<td>19</td>
<td>63</td>
</tr>
<tr>
<td>Environmental Security</td>
<td>10</td>
<td>12</td>
<td>83</td>
</tr>
<tr>
<td>Incident Response</td>
<td>3</td>
<td>13</td>
<td>23</td>
</tr>
<tr>
<td>Info Protection</td>
<td>9</td>
<td>18</td>
<td>50</td>
</tr>
<tr>
<td>Information and Document Management</td>
<td>6</td>
<td>11</td>
<td>55</td>
</tr>
<tr>
<td>Maintenance</td>
<td>5</td>
<td>19</td>
<td>26</td>
</tr>
<tr>
<td>Monitoring &amp; Malware</td>
<td>10</td>
<td>30</td>
<td>33</td>
</tr>
<tr>
<td>Organizational</td>
<td>13</td>
<td>28</td>
<td>46</td>
</tr>
<tr>
<td>Personnel</td>
<td>11</td>
<td>18</td>
<td>60</td>
</tr>
<tr>
<td>Physical Security</td>
<td>19</td>
<td>28</td>
<td>68</td>
</tr>
<tr>
<td>Plans</td>
<td>11</td>
<td>50</td>
<td>22</td>
</tr>
<tr>
<td>Policies</td>
<td>5</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>Policies &amp; Procedures General</td>
<td>8</td>
<td>24</td>
<td>33</td>
</tr>
<tr>
<td>Portable/Mobile/Wireless</td>
<td>10</td>
<td>17</td>
<td>59</td>
</tr>
<tr>
<td>Procedures</td>
<td>10</td>
<td>21</td>
<td>48</td>
</tr>
<tr>
<td>Remote Access Control</td>
<td>13</td>
<td>16</td>
<td>81</td>
</tr>
<tr>
<td>Risk Management and Assessment</td>
<td>6</td>
<td>17</td>
<td>35</td>
</tr>
<tr>
<td>System and Services Acquisition</td>
<td>7</td>
<td>18</td>
<td>39</td>
</tr>
<tr>
<td>System Integrity</td>
<td>8</td>
<td>16</td>
<td>50</td>
</tr>
<tr>
<td>System Protection</td>
<td>9</td>
<td>23</td>
<td>39</td>
</tr>
<tr>
<td>Training</td>
<td>6</td>
<td>8</td>
<td>75</td>
</tr>
</tbody>
</table>

This chart shows the degree of compliance in each category for all questions. Click 'Results Per Standard By Subject Area' to view more details by standard.
Question Filters
Hardcopy Reports

SITE SUMMARY REPORT
CONTROL SYSTEMS CYBER SECURITY EVALUATION

South Creek Plant Assessment
1/10/2013
Assessor: Thomas K. Jefferson

Homeland Security

SUMMARY OF RANKED QUESTIONS
CYBER SECURITY EVALUATION

Each Question that did not meet the required security assurance level is shown in ranking order below.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Question</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Does the system enforce assigned authorizations for controlling logical access to the system?</td>
<td>L</td>
</tr>
<tr>
<td>2</td>
<td>Does the system enforce assigned authorizations for controlling physical access to the system?</td>
<td>L</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

COMPONENT COMPLIANCE BY SUBJECT AREA

<table>
<thead>
<tr>
<th>Components</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securing the System</td>
<td>35.00</td>
</tr>
<tr>
<td>Management</td>
<td>100.00</td>
</tr>
<tr>
<td>Securing the Router</td>
<td>80.00</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>50.00</td>
</tr>
<tr>
<td>Securing Content</td>
<td>26.00</td>
</tr>
<tr>
<td>Logging</td>
<td>50.00</td>
</tr>
<tr>
<td>Boundary Protection</td>
<td>26.00</td>
</tr>
<tr>
<td>Firewall</td>
<td>26.00</td>
</tr>
<tr>
<td>Password</td>
<td>18.00</td>
</tr>
<tr>
<td>User Authentication</td>
<td></td>
</tr>
<tr>
<td>Host Intrusion Detection</td>
<td></td>
</tr>
<tr>
<td>Management Practices</td>
<td></td>
</tr>
<tr>
<td>Securing the Component</td>
<td></td>
</tr>
<tr>
<td>Physical Access</td>
<td></td>
</tr>
</tbody>
</table>

2004 The Department of Homeland Security

34
Resource Library

This library of cyber security standards, reports, and templates are provided for your convenience. Additionally, there are several cyber security guides and white papers to assist you in gaining background in cyber security, determining priorities, or specific helps. Specific helps include...
Resource Library - Search

Developing an Industrial Control Systems Cybersecurity Incident Response Capability

Recommended Practice:
Developing an Industrial Control Systems Cybersecurity Incident Response Capability

October 2009

Homeland Security
CSET 6.0 Enhancements

New/Updated Standards

- NEI 08-09 Rev 6
- NISTIR 7628 Ver 1 (August 2010)
- INGAA Ver 1 (January 31, 2011)
- NIST SP800-53 Appendix J Rev 4
- NIST SP800-82 Rev 1 (May 2013)
- CNSSI ICS Overlay Update

New Evaluation Capabilities

- Merging
- Comparison
- Aggregation
- Trending
Aggregation Sample Screen

### Site A
- Total Questions Answered: 560
- Yes: 300
- No: 260
- Components: 76
- Standards: 75
- Overall: 71
- SAL Level: Site C

### Site B
- Total Questions Answered: 342
- Yes: 300
- No: 42
- Components: 66
- Standards: 70
- Overall: 70

### Site C
- Total Questions Answered: 268
- Yes: 152
- No: 116
- Components: 66
- Standards: 70
- Overall: 75

### Graphs

### Sorting
- Option to sort by best and worst.
CSET 6.0 Enhancements (cont.)

New/Updated Functionality

- Inventory Lists
- Security Plans
- YouTube Tutorials
- Updated Diagramming Tool
Key Contact Information

Lisa Kaiser
Lisa.Kaiser@dhs.gov

Download CSET
http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET