Cyber Security: Critical Infrastructure Controls Assessment Framework

Systems and Software Technology Conference, Utah
May 16-19, 2011

Bharat Shah
Lockheed Martin IS&GS
bharat.shah@lmco.com
1. REPORT DATE
MAY 2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
Cyber Security: Critical Infrastructure Controls Assessment Framework

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lockheed Martin ,Information Systems & Global Solutions (IS&GS) ,700 N. Frederick Rd,Gaithersburg,MD,20879

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

<table>
<thead>
<tr>
<th>a. REPORT</th>
<th>b. ABSTRACT</th>
<th>c. THIS PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
40

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
Provide an overview on assessment approach for Cyber based critical infrastructure security controls to protect against threats to the security, safety and survivability of critical infrastructure cyber assets, related services and processes.
Session Learning Objectives

Understand what “Critical Infrastructure” and “Cyber (Physical) System” are

Understand the challenges and issues related to the cyber security

Understand applicable cyber security standards

Explore the cyber security assessment approach

Review the test techniques and tools for vulnerability assessment
INTRODUCTION
“The revolution in communications and information technologies have given birth to a virtual world… Cyberspace is real and so are the risks that come with it. It’s the great irony of our Information Age – the very technologies that empower us to create and build also empower those who would disrupt and destroy.”

President Obama

*Remarks by the President on Securing our Nation’s Cyber Infrastructure*

*May 29, 2009*

What is Critical Infrastructure?

---

Critical Infrastructure / Assets

...Those facilities, systems, and equipments if destroyed, would have a debilitating impact on security, health and safety essential for functioning of a society and economy

-- USA Patriot Act (P.L. 107-56)

Critical Infrastructures are public and private institutions

---

CIP Security Controls Assessment -- Bharat Shah
Disruption in interdependencies can cause

- Electricity Outage
- Oil & Gas Outage
- Water Outage
- Communications Outage
- Civil Services Interruptions
- Business Interruptions
- Emergency Services Interruptions
- And Many More

Huge interdependencies across economy that we do not understand……

What is Cyber?

Cyberspace: is the non-physical terrain created by computer systems. Anything related to the Internet also falls under the cyber category. [http://www.webopedia.com/TERM/C/cyber.html](http://www.webopedia.com/TERM/C/cyber.html)

Cyber System: Is composed of interconnected computers, servers, routers, switches and fiber optic cables in which online communications takes place using Internet technologies.

Cyber Physical System: is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. [http://en.wikipedia.org/wiki/Cyber-physical_system](http://en.wikipedia.org/wiki/Cyber-physical_system)

Cyber = Enabling of Internet technologies
What is Cyber System?

Critical infrastructures rely upon physical and cyber-based systems for their daily operations.
Cyber Physical System Example


Critical Infrastructure using Industrial Controls
SYNCHING-UP WITH TECHNOLOGIES:
CYBER SECURITY ISSUES AND CHALLENGES
Emerging Trends

1. Transforming from paper-based to digital
2. Isolated control devices to real-time intelligent processors
3. Rapid integration of COTS and IT products and systems
4. Increasing connectivity among infrastructure control systems and information management system
5. Increasing access to infrastructure assets via Internet based technologies
6. Increasing concerns to Privacy

Emerging Threats

- Increase in malicious physical attack
- Increase in Spyware, Key loggers, Trojans
- Decrease in Time to Exploit Vulnerabilities
- Increase in well organized Cyber Crime Professionals
- Increase in use of unauthorized exploitation of standardized asset
- Increase in Network Threat Tools

And Increasing ...................
There are many different agents and with varying motivations in the cybersecurity domain.
Growth of network threat tools have changed threat environment forever.....
Causing loss of control and communications in

- Transport Media
  - Routers, Switches, Antenna, Towers, Conduits
- Protocols
  - Standard, Proprietary
- Gateways
  - Proxy Servers, Firewalls
- Systems
  - Cyber Systems, Cyber Physical Systems
- Field Devices
  - Sensors, Meters, IEDs, Relays, RTUs
- Storage
  - Database, Files

Growth of cyber technologies have changed threat environment forever.....
Creating Impacts on

National Security
Public Health and Safety
Preservation of Life
Economic Uncertainty

System Destruction
Accurate Data Management
Customer Confidence
Legal Liabilities

Delays and Denial of Service

And Numerous Cascading Effect because of Domain Interdependencies
Synching-up with Technologies-6

Having Statistics


CIP Security Controls Assessment -- Bharat Shah
Because of Gaps in Technology Assessment

- Knowledge of attack vectors used by attackers
- Ability to identify the actual perpetrator
- Skills to perform security controls assessments
- Security controls assessment guidelines
- Measurement guidelines for security assessment
- Organizational uniformity in security assessment planning

Investing in Security Assessment is NOT an Option BUT a Necessity
CYBER SECURITY REQUIREMENTS AND CONTROLS
Cyber Security Principles

To Support Infrastructure Protection

- National Security
- Individual Security
- Societal Stability and Security
- Economic Stability and Security
- Critical Infrastructure Security/Continuity and
- The Preservation of Natural Resources and the Environment.

To build Trust and Confidence in system environment
Following Applicable Security Standards

Federal
- FISMA
- DIACAP
- NIST
- <more...>

International
- ISO
- ITU
- <more...>

Industry
- HIPAA
- PCI
- SOX
- <more...>

Critical Infrastructure
- NERC
- FERC
- CFATS
- NIST Cyber-Grid
- ISA-99
- <more...>

Private
- SANS - CAG
- OASIS
- OWASP
- <more...>

And Growing Day by Day....................
Cyber security standards can be used to help identify problems and reduce the vulnerabilities in a control system.
Cyber Security Controls

To build Trust and Confidence in system environment

## Cyber Security Controls Example

### ACCESS CONTROL

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Business requirements for access control.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User access management.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User responsibilities.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network access control.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating system access control.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application access control.</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring system access and use.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile computing and teleworking considerations.</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field Device Access</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CYBER SECURITY ASSESSMENT FRAMEWORK
Assessment Objectives

The test and evaluation of the cyber system security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

1. Ensure the confidentiality, integrity and availability of the data
2. Ensure safety of people, assets and natural resources
3. Ensure compliance to legislative and regulatory Standards
4. Ensure protection against security vulnerabilities and threats
5. Identify problem areas and provide reasonable options
6. Ensure cyber infrastructure is reliable, recoverable and resilient

Develop the business case for cyber security assessment that will enhance infrastructure security.
Cyber Security Controls Assessment Life Cycle – I⁴M

1. Initiate
   - Planning
     - Assessment Plan
2. Inspect
   - Infrastructure Documents
     - Security Implementation Review Report
3. Identify
   - Critical Cyber Assets
     - Critical Cyber Assets Report
4. Investigate
   - Security “State”
     - Cyber Security Assessment Report
5. Monitor
   - Security Operation
     - Cyber Security Feedback

Assess readiness of system and related infrastructure in accordance with security standards/controls
**Initiate**

1. Select/Obtain sponsorship
2. Define objectives
3. Select policy and guideline for assessment
4. Identify and gather documentation
5. Develop Assessment Plan

**Inspect**

1. Domain specific security policies, plans and processes
2. Security requirements and standards
3. Layouts and configuration for facility and environment
4. ITS and ICS security controls documentation
5. Disaster Recovery and Incident Management Procedures

*Plan and Gain an understanding of security needs*
Identify

1. Criticality Level
2. Critical Functions
3. Critical Assets
4. Critical Asset Location
5. Critical Cyber Assets
6. Infrastructure Interdependencies
7. Develop Critical Cyber Asset Report

Susceptibility to Cyber attacks leading to

- Local Impacts
- Cascading Impacts
- Interdependency Impacts
- Environmental Impacts
- Social Impacts
- Economic Stability Impacts
- National Security Impacts

Identify and rank all critical cyber assets from a security perspective
Investigate

1. Input, output and expected behavior of critical Cyber assets
2. Security controls (implemented, inherited, legacy, hybrid)
3. Risk management based compensating controls
4. Redundancy and recoverability capability
5. Resources and time to repair
6. Develop Cyber Security Assessment Report

For Threats

- Natural: Earthquake, Storm and Lightning, Fire
- Environmental: Power Outage, Chemical Leakage, Nuclear Leakage, Biological Leakage
- Human: Computer Abuse, Interception & Spoofing, Hacking, Sabotage or Vandalism, System Tampering, Password Guessing, Many more

Understand and capture system security view of critical operation
Cyber Security Assessment-5

**Report**

1. Assessment of identified critical assets
2. Analysis of the threats to and vulnerabilities
3. Recommendations to reduce vulnerabilities
4. Other information essential for the development of operational security

**Monitor**

1. Changes in security Requirements and standards
2. Security Controls
3. Patch and configuration management
4. Vulnerability and incident management
5. Risk management
6. Security “state” of Cyber Assets

Continuously monitor and report
VULNERABILITY ASSESSMENT
Vulnerability Assessment-1

Objectives

1. Build awareness - of vulnerabilities for Cyber assets and interdependencies between them

2. Ensure that security vulnerabilities (internal and external) are identified and resolved in a timely manner.

3. Enable management to make informed decisions regarding implementation of security controls and remediation measures

Using

Sources
- Risk assessments
- Vendor advisories
- System test results
- System audit logs

Methods
- Automated vulnerability scan
- Network mapping
- Penetration testing

CIP Security Controls Assessment -- Bharat Shah 33
Vulnerability Assessment-2

Following Applicable Test Techniques

User Interface Test
- Simulate Web Browser
- URL Validation
- Form Validation
- Field Validation
- Workflow Validation
- SQL Injection
- Cross Site Scripting

Static Analysis Test
- Logic Flow Check
- Memory Allocation Check
- Data Type Check
- Data Variables Usage Check
- Buffer Overflow Check
- Error Handling Check

Vulnerability Test
- Operating Systems
- Network Drivers
- Software Libraries
- Software Applications
- Database
- Data Corruption
- Virus Detectors

Penetration Test
- Network Servers
- Network Devices
- Network Protocols
- Denial-of-Services
Vulnerability Assessment-3

And Test Tools

- Network Assessment: Foundstone, Nessus
- Network Mapping: NMap, NetsTumbler
- Wireless Network Analysis: AirSnort
- Host Configuration Analysis: Solarwinds, SuperScan
- Traffic Analysis: EtherReal, Sniffer, Pwdump2
- Access Control: GetAdmin

- Web Application Scan: AppScan, WebInspect
- Web Services Scan: SOAPUI
- Database Scan: WebInspect, Internet Scanner
- Data Retrieval: NetFlow
- Password Cracking: Crack 5, L0pht
- File Integrity: TripWire, LANGuard

---

CIP Security Controls Assessment -- Bharat Shah
CONCLUSION
Cyber based critical infrastructure assets are vulnerable to cyber attacks because of the increasing interdependence and automation of cyber systems.

A diverse range of measures are required to bridge gap between technology advancement and technology assessment.

This presentation has provided an overview on cyber systems, and assessment framework for the required security controls to protect critical cyber assets.

Lockheed Martin is developing innovative approaches to test, evaluate and assess the security posture of organizations’ information system and cyber system environment.
REFERENCES & ACRONYMS
References

1. Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted) at http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf
1. CAG – Consensus Audit Guidelines (SANS 20 security controls)
2. CFATS – Chemical facility Anti-terrorism Standards
3. CIP – Critical Infrastructure Protection
4. COTS – Commercial Off The Shelf
5. DIACAP - DoD Information Assurance Certification and Accreditation Process
6. DCS – Distributed Control System
7. FERC – Federal Energy regulatory Commission
8. FISMA – Federal Information Security Management Act
9. HIPAA - Health Insurance Portability and Accountability Action
10. ICS – Infrastructure Control System
11. IEC – International Electrochemical Commission
12. IED – Intelligent Electronic Devices
13. IEEE – Institute of Electrical and Electronics Engineers
14. ISA – Industrial Society for Automation
15. ISO – International Standards Organization
16. IS&GS – Information Systems and Global Solutions
17. IT – Information Technology
18. ITU – International Telecommunication Union
19. NERC - North American Electric Reliability Corporation
20. NIST – National Institute of Science and Technology
21. OASIS - Organization for the Advancement of Structured Information Standards
22. OWASP - Open Web Application Security Project
23. PCI – Payment Card Industry
24. PCS – Process Control System
25. RTU – Remote Terminal Unit
26. SANS - SysAdmin, Audit, Network, Security
27. SCADA – Supervisory Control and Data Acquisition System
28. SOX - Sarbanes-Oxley Act