

Cyber Security: Critical Infrastructure Controls Assessment Framework

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

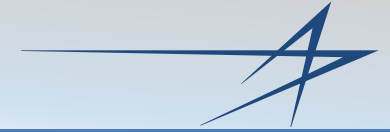
Bharat Shah
Lockheed Martin IS&GS
bharat.shah@lmco.com

Report Documentation Page

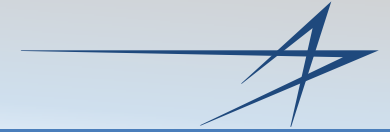
Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

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	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
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:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



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.



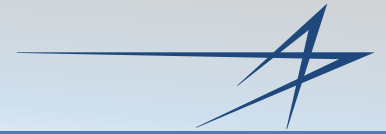
Understand what “Critical Infrastructure” and “Cyber (Physical) System” are

Understand the challenges and issues related to the cyber security

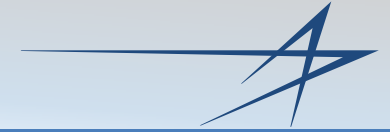
Understand applicable cyber security standards

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

http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

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

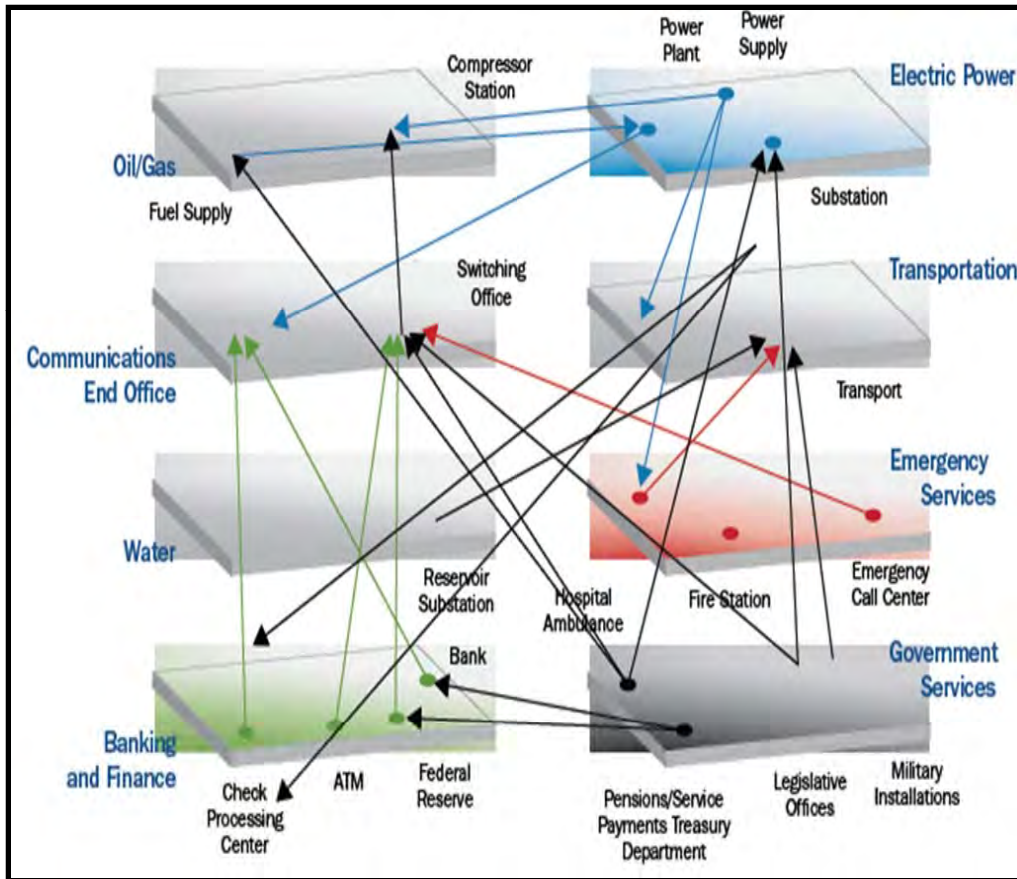
-- USA Patriot Act (P.L. 107-56)



Critical Infrastructures are public and private institutions



Geographical, Physical, Cyber and Logical



Disruption in interdependencies can cause

Electricity Outage

Oil & Gas Outage

Water Outage

Communications Outage

Civil Services Interruptions

Business Interruptions

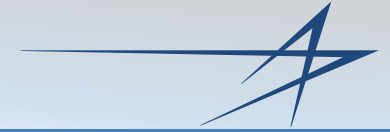
Emergency Services Interruptions

And Many

More.....

<http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf>

Huge interdependencies across economy that we do not understand.....



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>

Cyber System

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

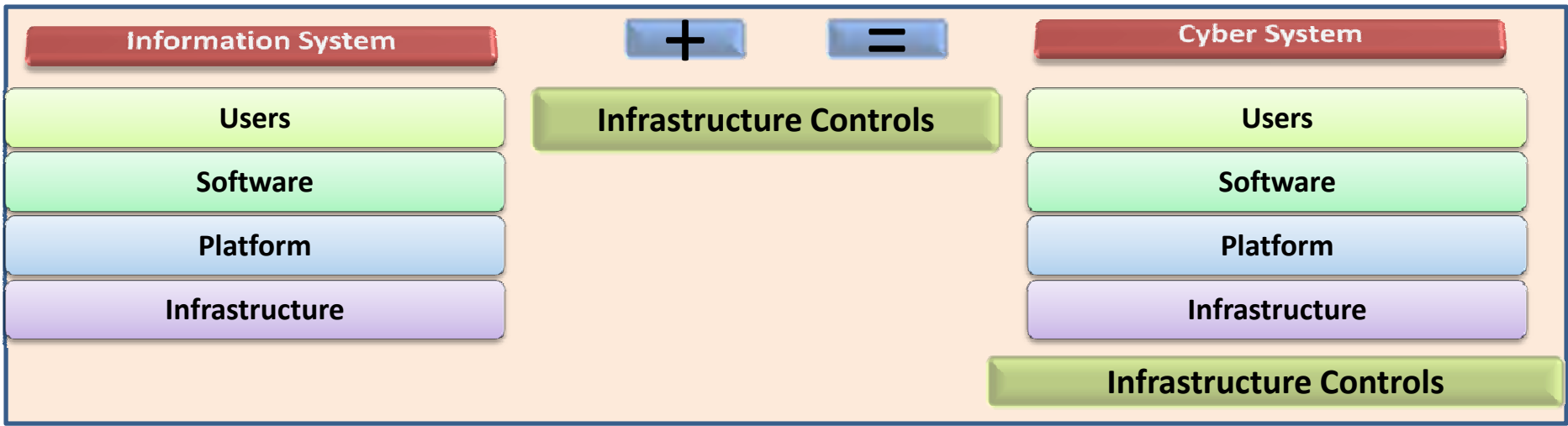
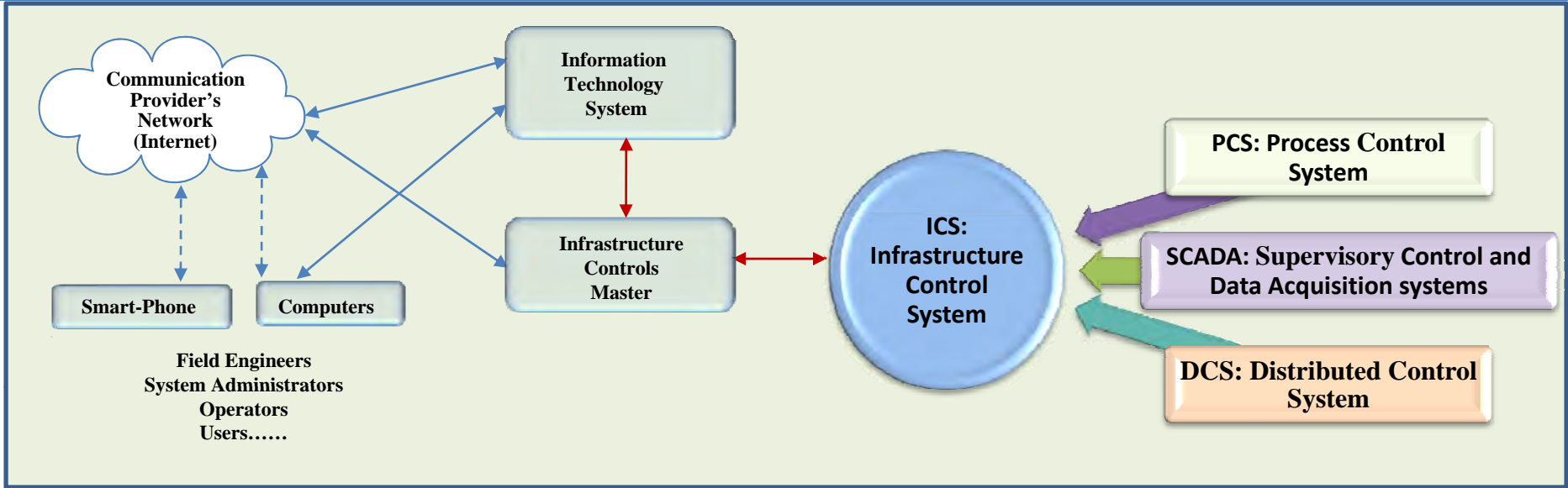
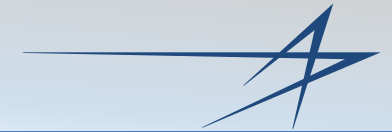
Cyber Physical System

is typically designed as a network of interacting elements with physical input and output instead of as standalone devices

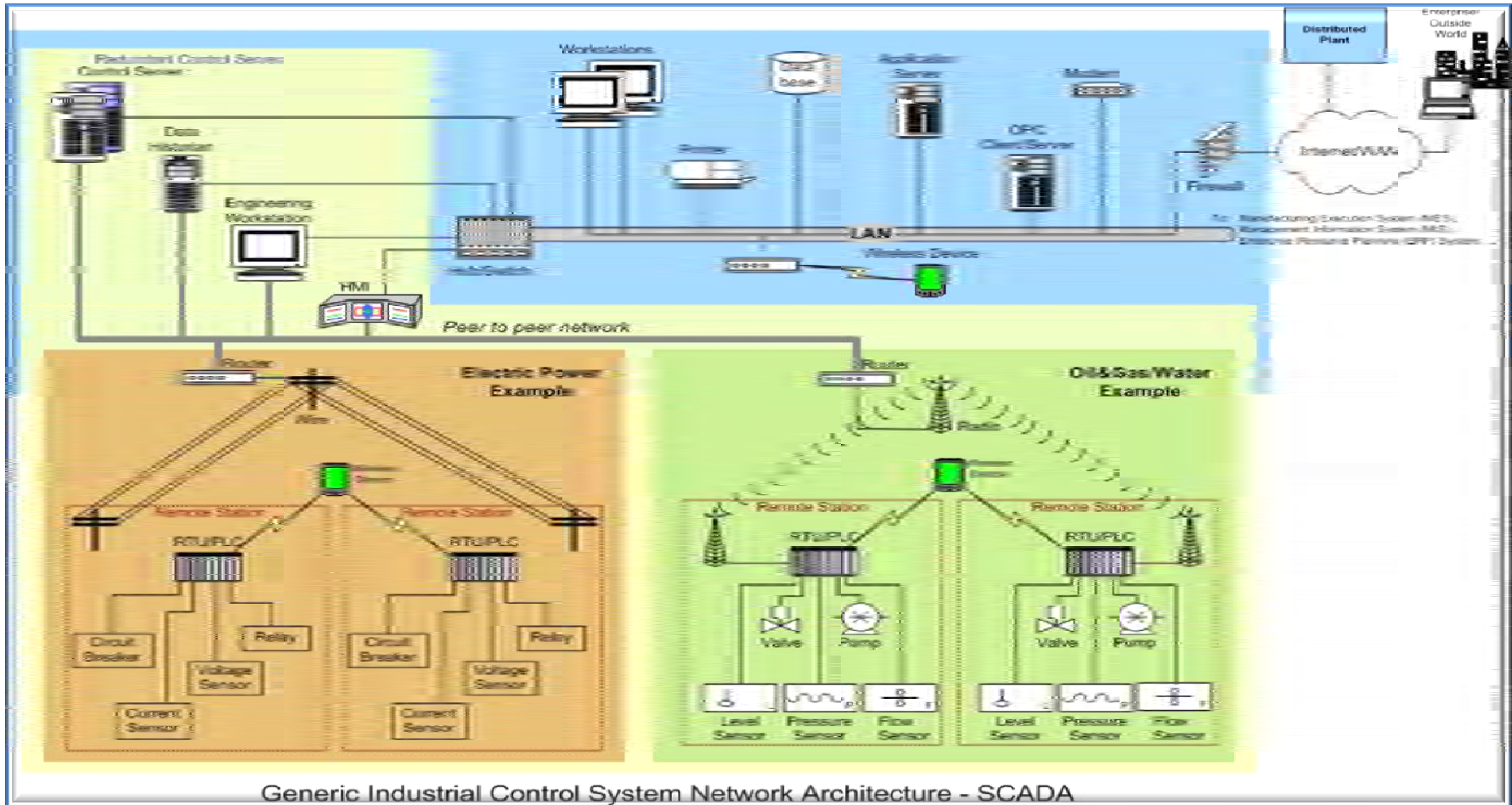
http://en.wikipedia.org/wiki/Cyber-physical_system

Cyber = Enabling of Internet technologies

What is Cyber System?

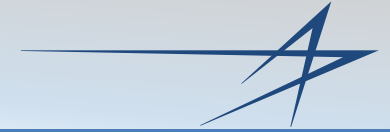


Critical infrastructures rely upon physical and cyber-based systems for their daily operations



<http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf>

Critical Infrastructure using Industrial Controls



SYNCHING-UP WITH TECHNOLOGIES: CYBER SECURITY ISSUES AND CHALLENGES



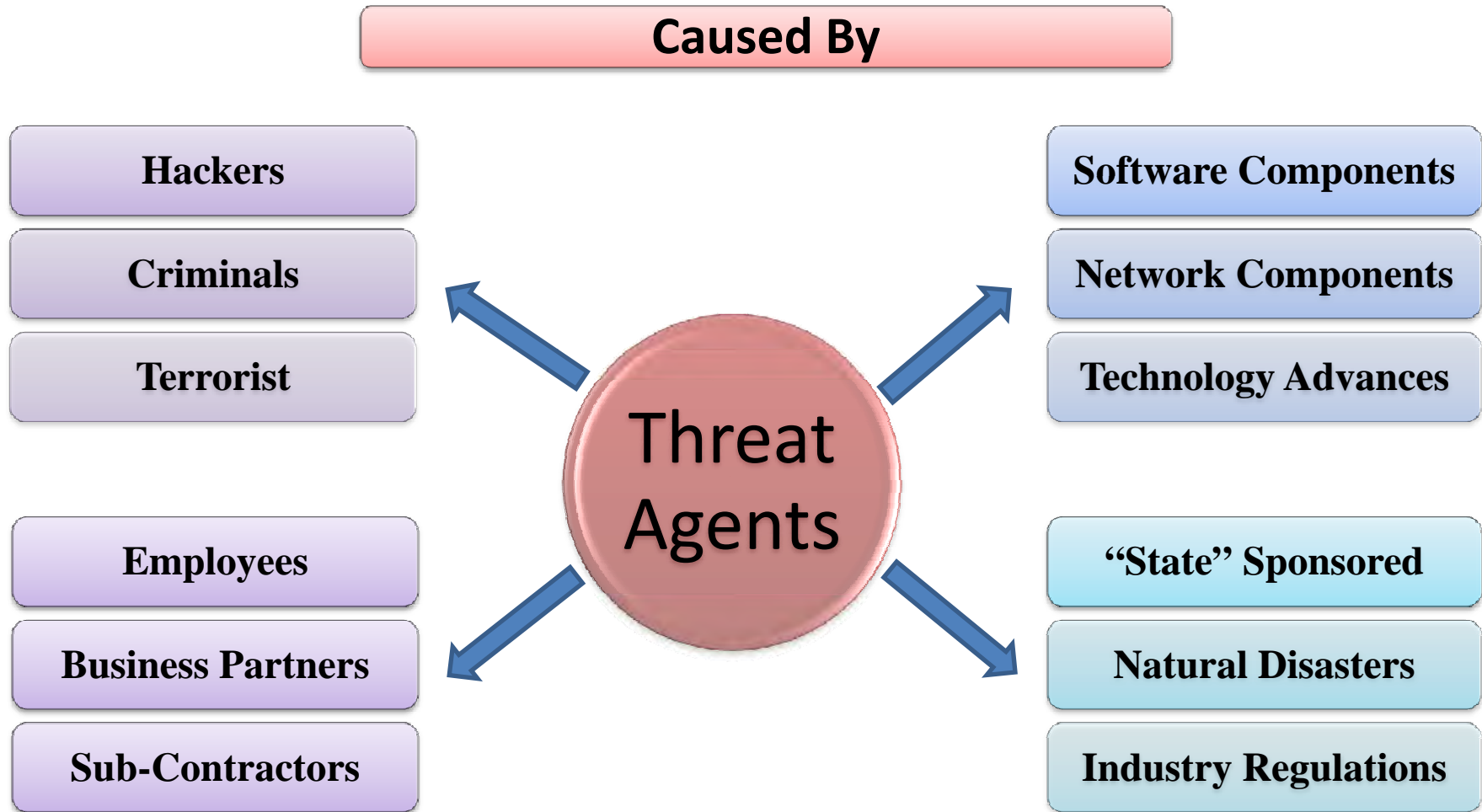
Emerging Trends

- 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

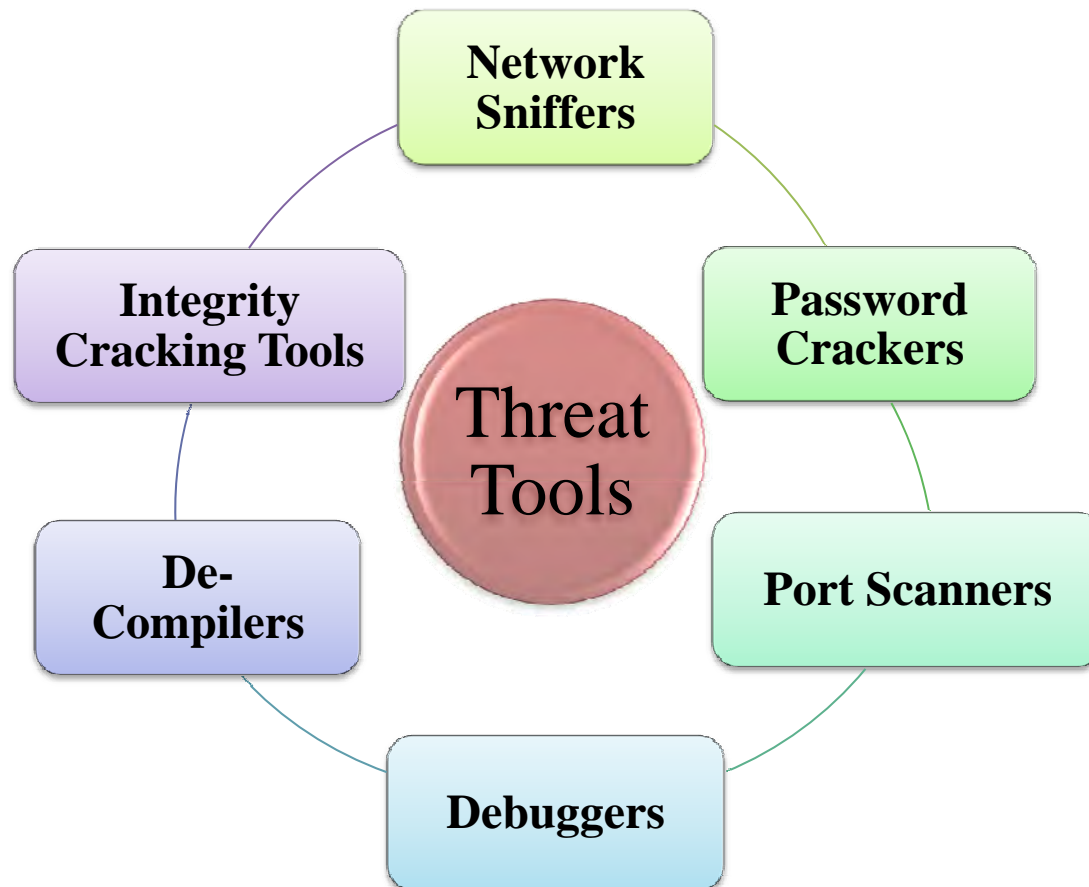
And Increasing



There are many different agents and with varying motivations in the cybersecurity domain.



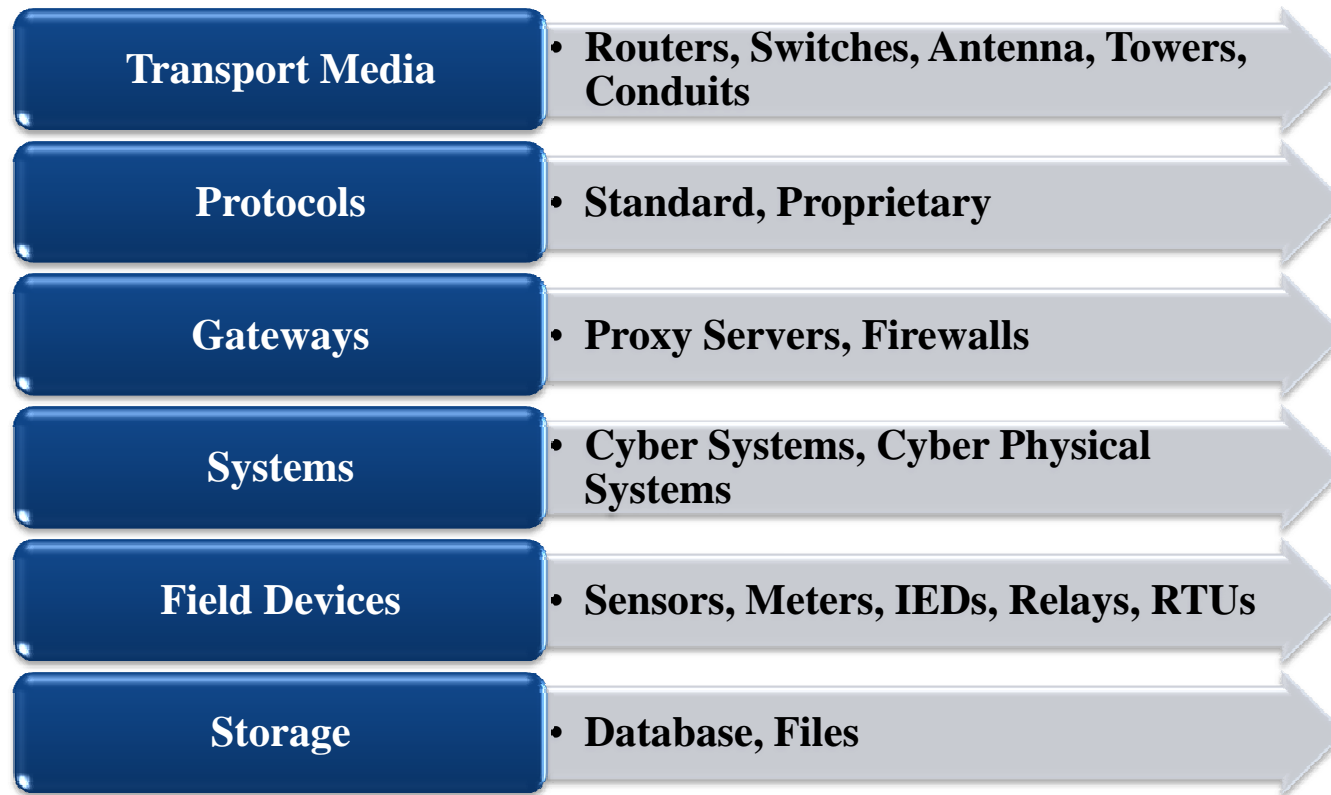
Using



Growth of network threat tools have changed threat environment forever....



Causing loss of control and communications in



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**

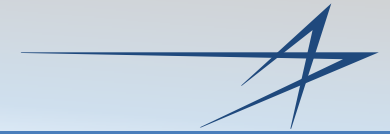
**Legal
Liabilities**



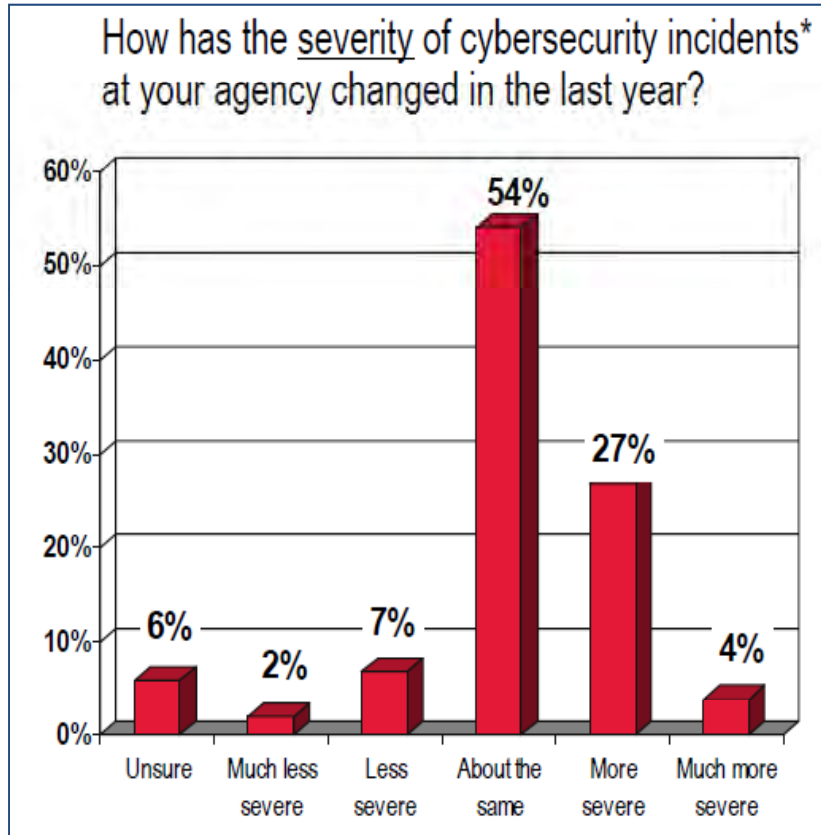
CAUTION

**Delays and
Denial of Service**

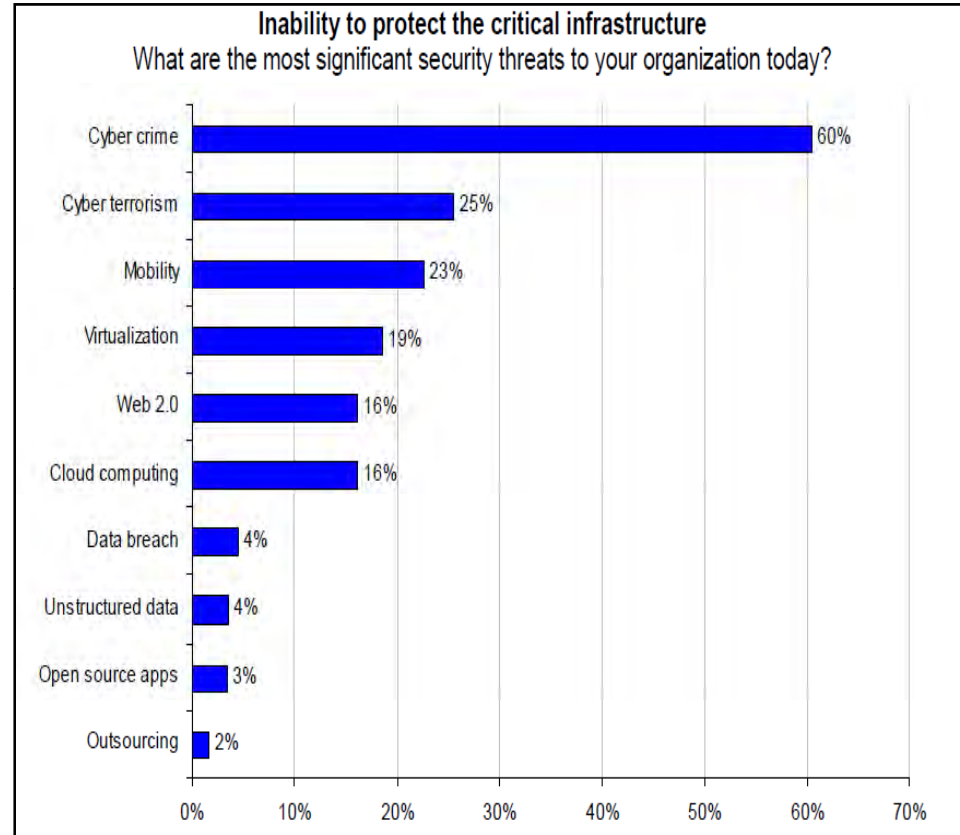
And Numerous Cascading Effect because of Domain Interdependencies



Having Statistics



<http://webobjects.cdw.com/webobjects/media/pdf/Newsroom/2009-CDWG-Federal-Cybersecurity-Report-1109.pdf>



<http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/CA%20Security%20Mega%20Trends%20White%20Paper%20FINAL%20%20%282%29.pdf>



Because of Gaps in Technology Assessment

**Knowledge of attack
vectors used by
attackers**

**Security controls
assessment guidelines**

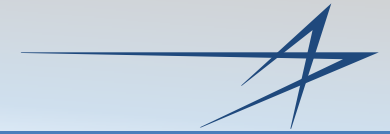
**Ability to identify the
actual perpetrator**

**Measurement guidelines
for security assessment**

**Skills to perform
security controls
assessments**

**Organizational
uniformity in security
assessment planning**

Investing in Security Assessment is NOT an Option BUT a Necessity



CYBER SECURITY REQUIREMENTS AND CONTROLS



Security

- Confidentiality
- Integrity
- Availability

Safety

- People
- Assets
- Nature

Survivability

- Reliable
- Responsive
- Resilient

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...>

Industry

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

Critical Infrastructure

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

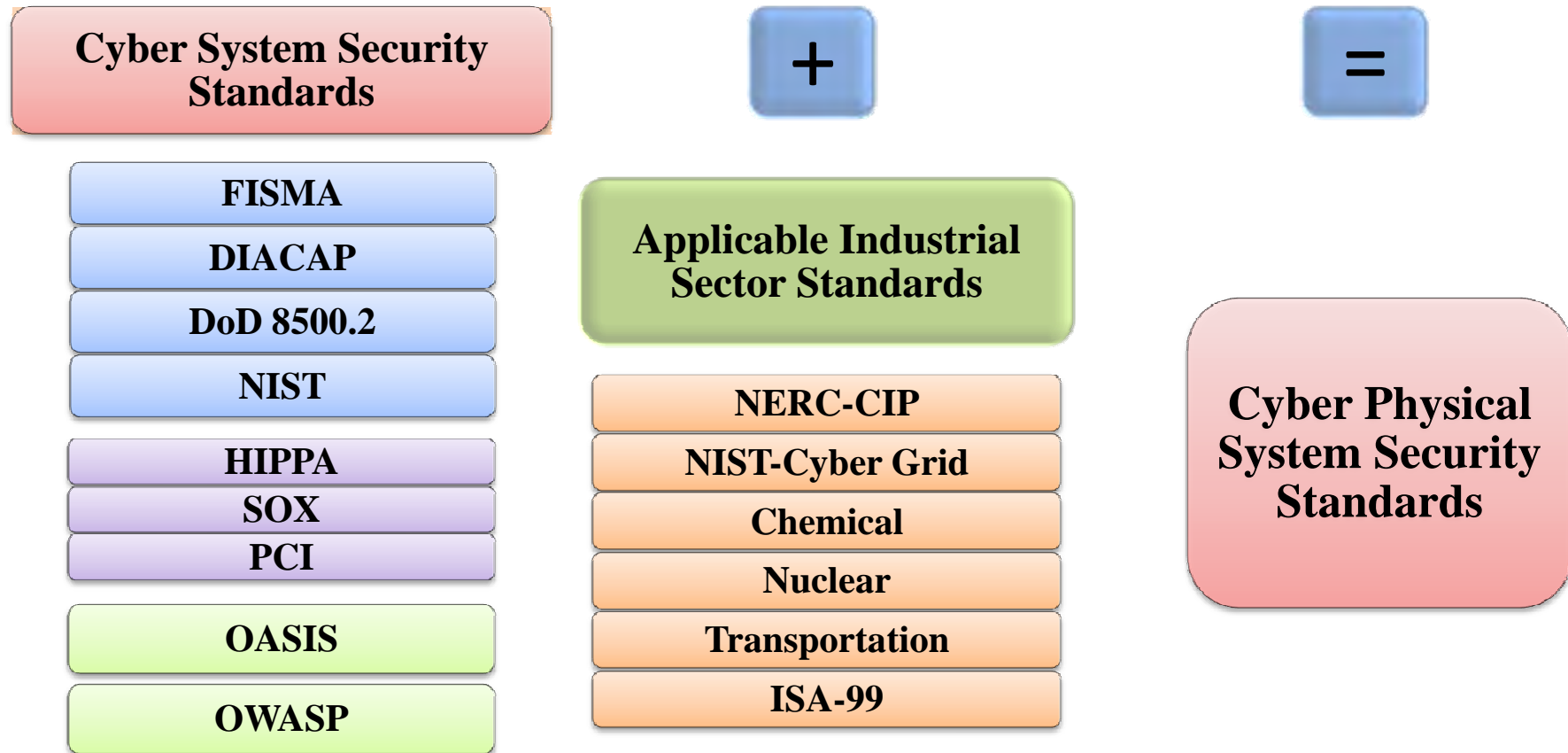
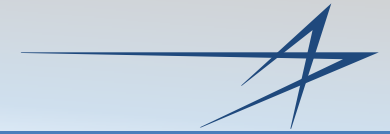
International

- ISO
- ITU
- <more...>

Private

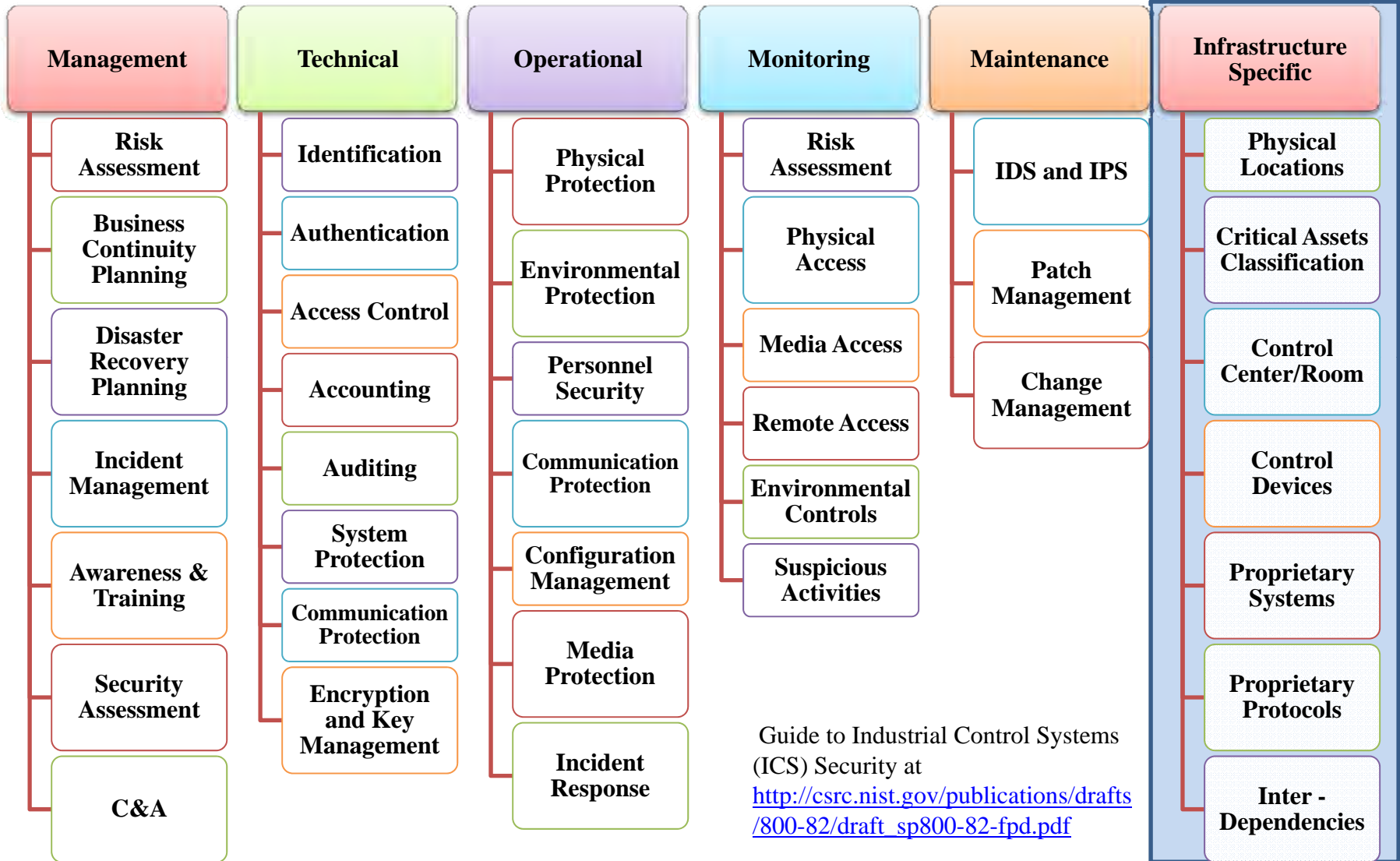
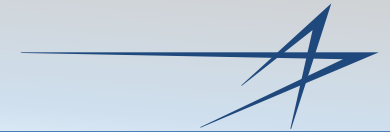
- SANS - CAG
- OASIS
- OWASP
- <more...>

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



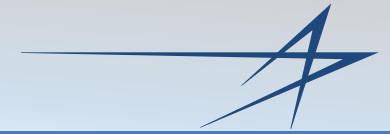
To build Trust and Confidence in system environment



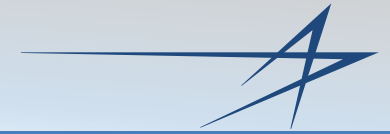
	ISO 17799	API 1164	IEEE 1402	AGA Report No. 12 ^f	NERC Security Guideline	NERC 1200	NERC 1300 ^g	ISA TR99-01	ISA TR99-02	PCSRF	IEC 62210	IEC 62351
Availability		✓			✓		✓			✓	✓	✓
ACCESS CONTROL												
Business requirements for access control.	✓	✓			✓			✓		✓		
User access management.	✓	✓		✓	✓	✓	✓	✓	✓	✓		
User responsibilities.	✓	✓	✓	✓	✓		✓		✓	✓		
Network access control.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Operating system access control.	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Application access control.	✓								✓			
Monitoring system access and use.	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Mobile computing and teleworking considerations.	✓	✓			✓			✓	✓			
Field Device Access		✓			✓			✓	✓		✓	

http://www.oe.energy.gov/DocumentsandMedia/Summary_of_CS_Standards_Activities_in_Energy_Sector.pdf

A summary of controls for Energy sector



CYBER SECURITY ASSESSMENT FRAMEWORK

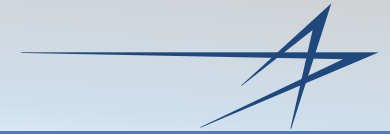


Cyber Security Assessment

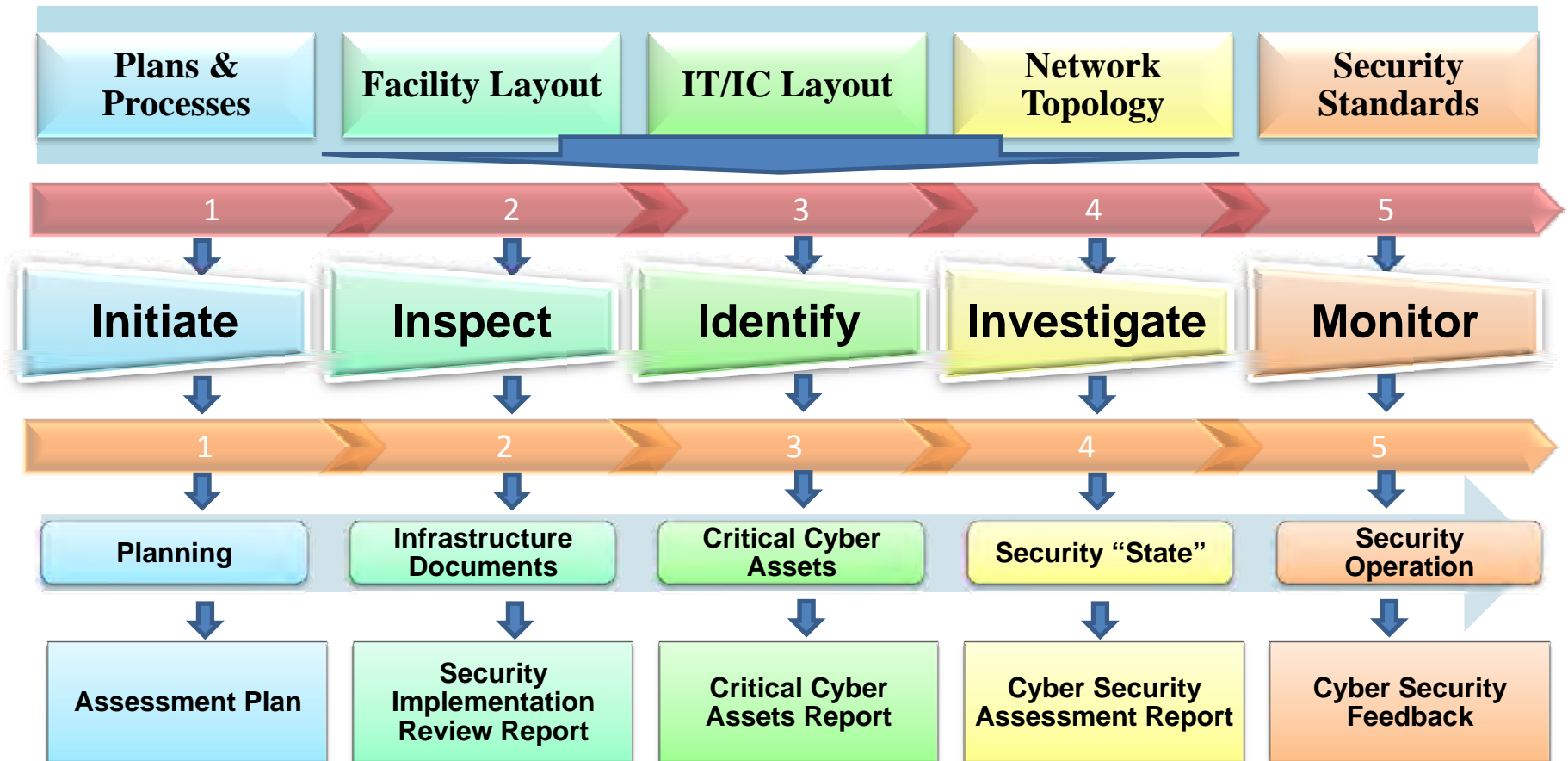
The test and evaluation of the cyber system security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system

- 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
- 5 • Ensure cyber infrastructure is reliable, recoverable and resilient

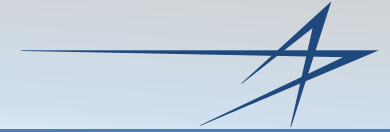
Develop the business case for cyber security assessment that will enhance infrastructure security.



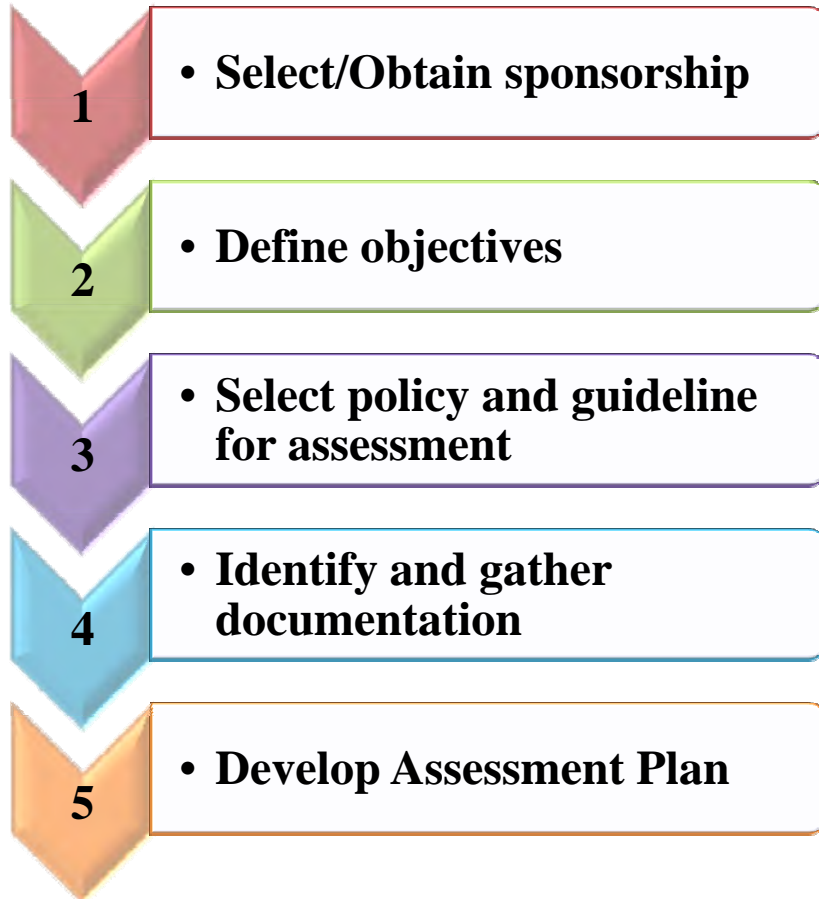
Cyber Security Controls Assessment Life Cycle – I⁴M



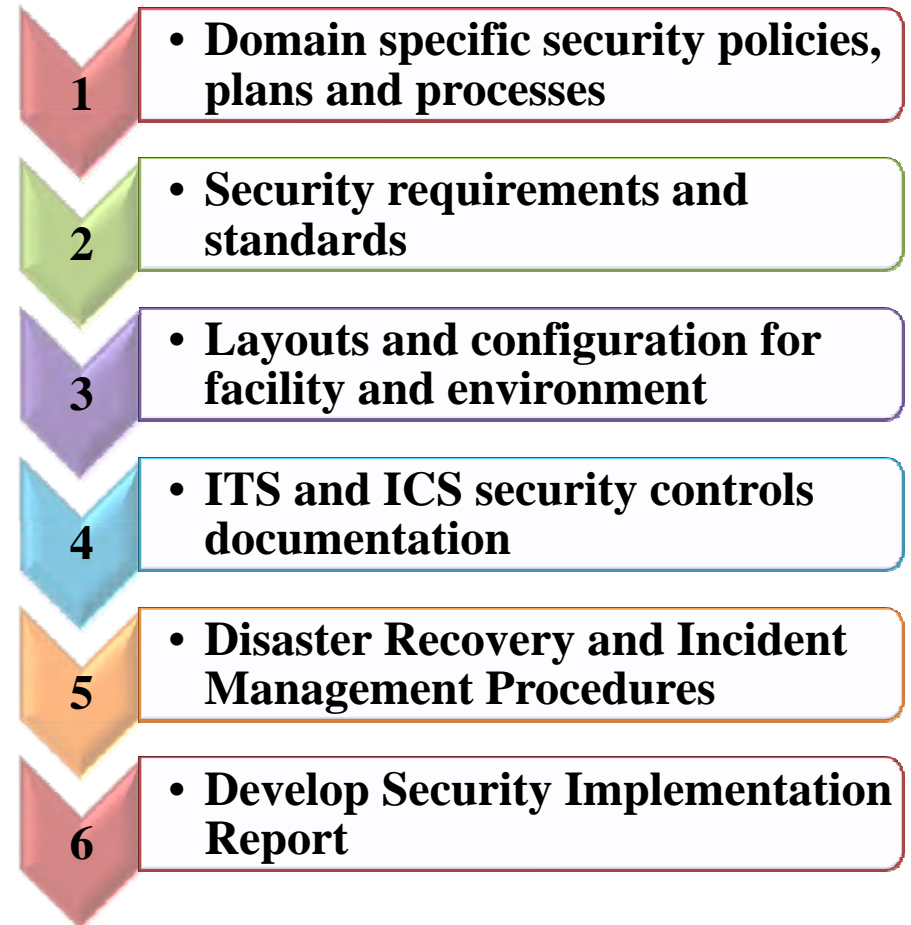
Assess readiness of system and related infrastructure in accordance with security standards/controls



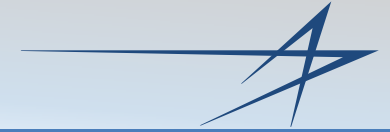
Initiate



Inspect



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

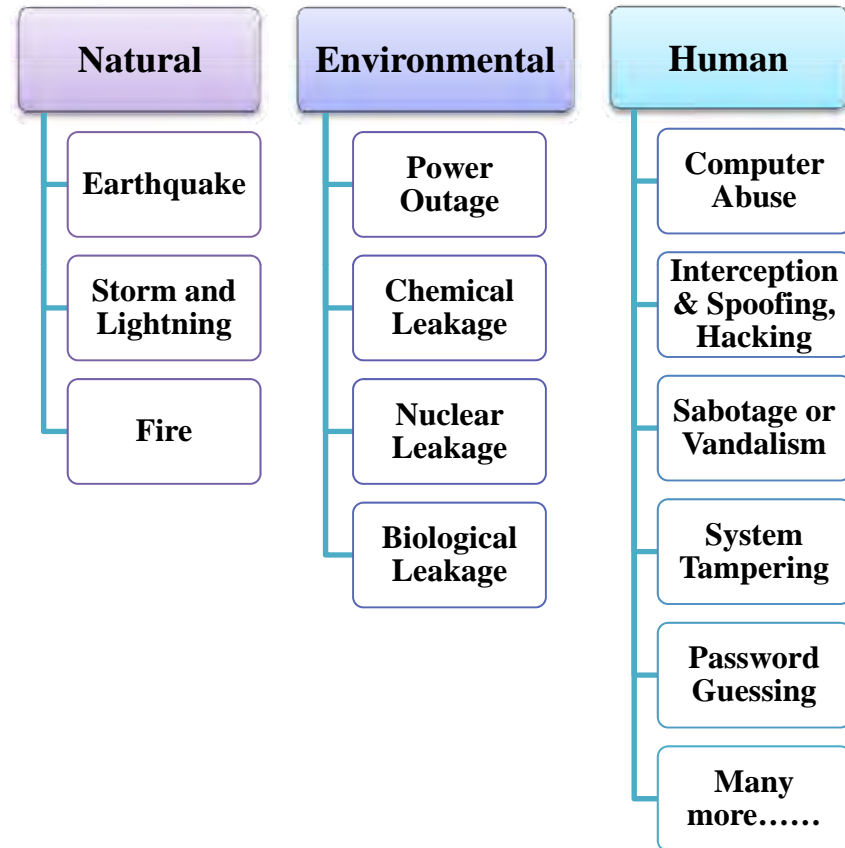
Identify and rank all critical cyber assets from a security perspective



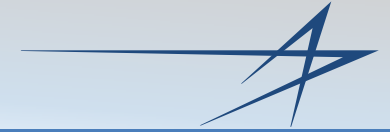
Investigate



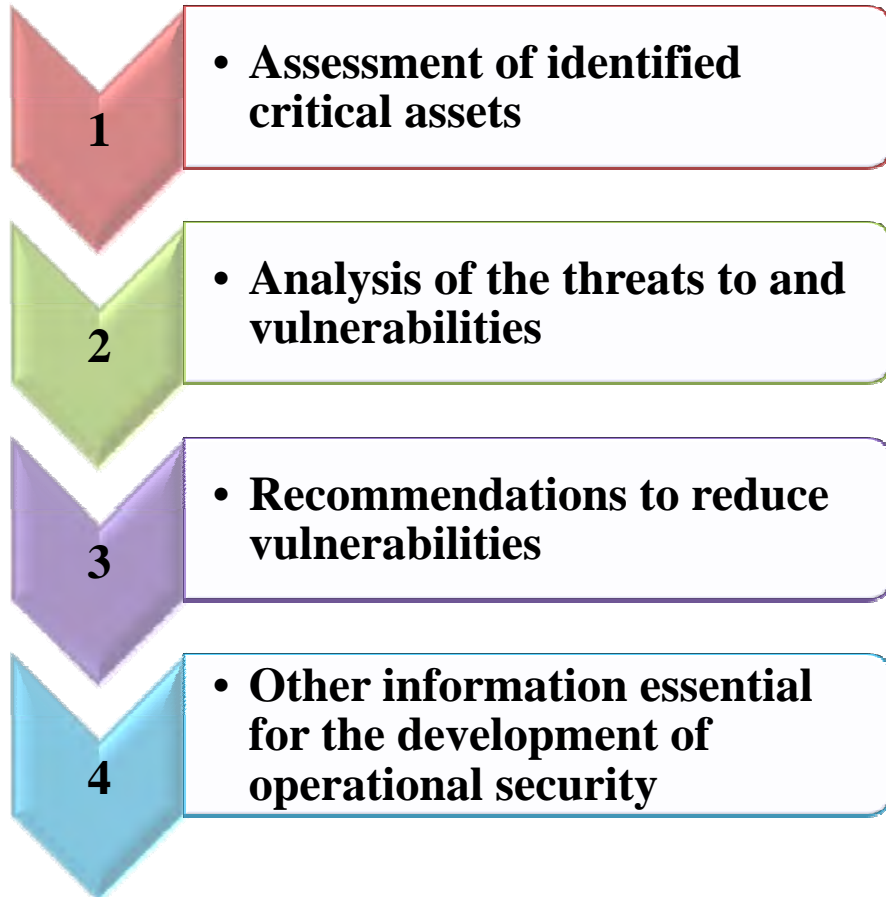
For Threats



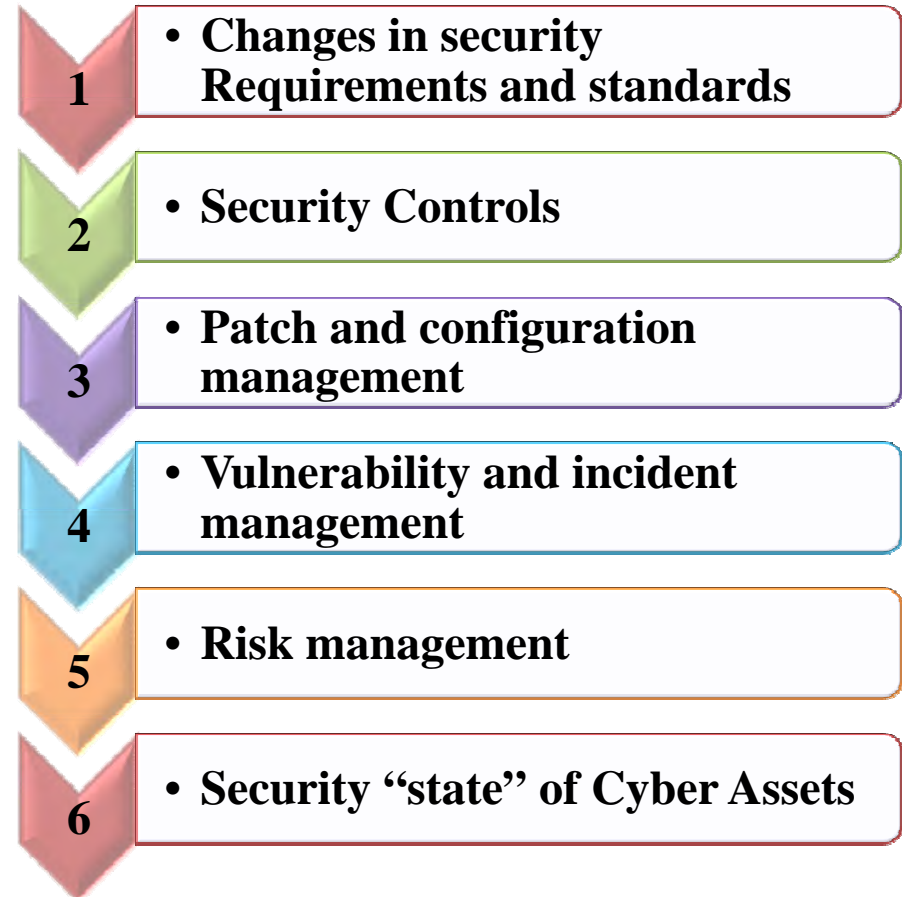
Understand and capture system security view of critical operation



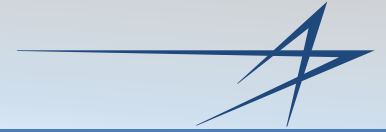
Report



Monitor



Continuously monitor and report



VULNERABILITY ASSESSMENT



Objectives

Using

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

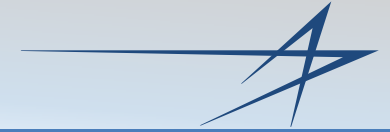
- Enable management to make informed decisions regarding implementation of security controls and remediation measures

Sources

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

Methods

- Automated vulnerability scan
- Network mapping
- Penetration testing



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

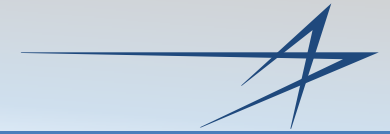
- Logic Flow Check
- Memory Allocation Check
- Data Type Check
- Data Variables Usage Check
- Buffer Overflow Check
- Error Handling Check

Vulnerability Test

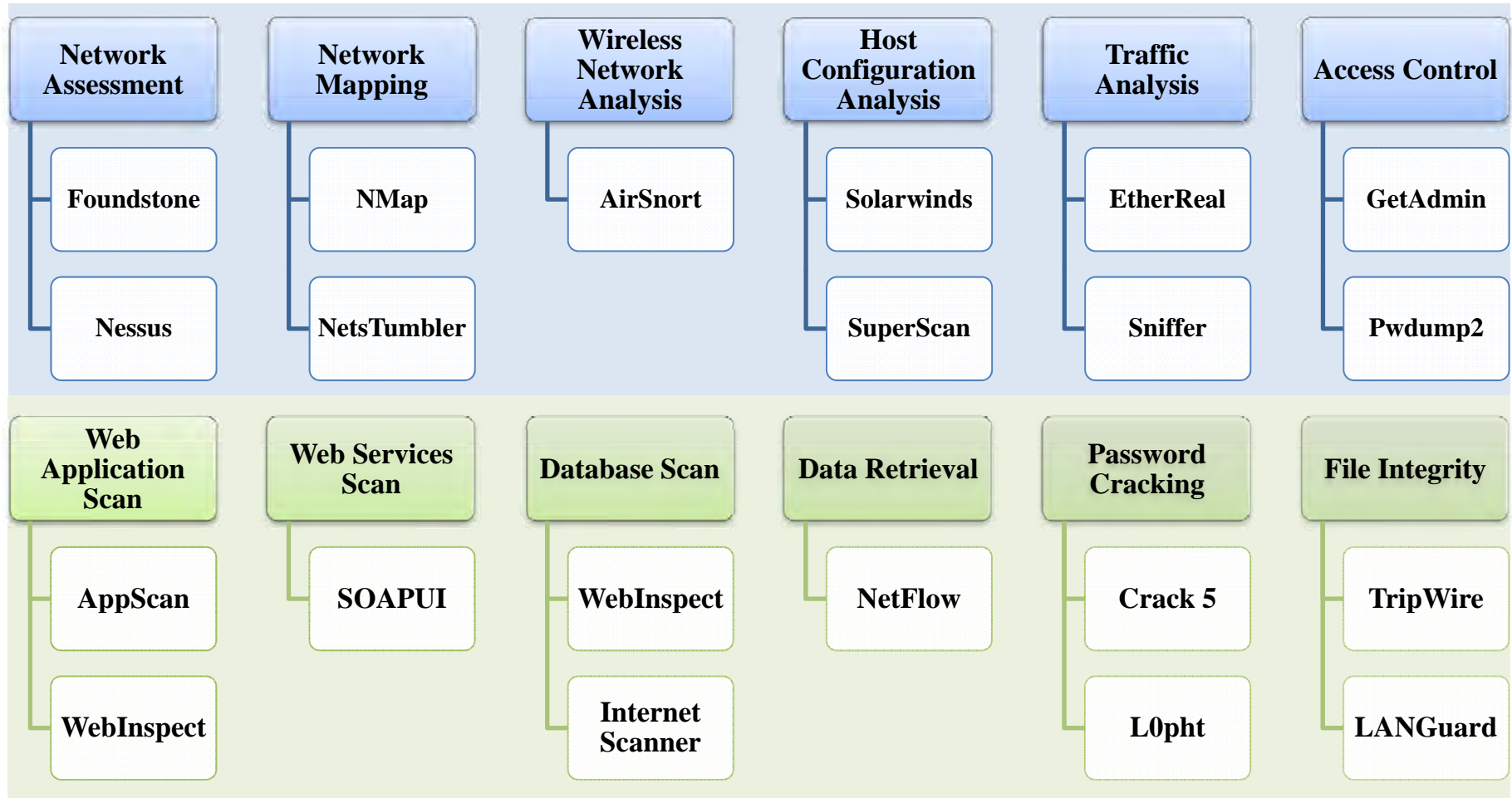
- Operating Systems
- Network Drivers
- Software Libraries
- Software Applications
- Database
- Data Corruption
- Virus Detectors

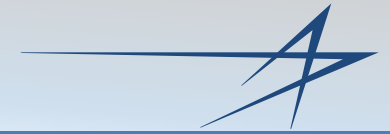
Penetration Test

- Network Servers
- Network Devices
- Network Protocols
- Denial-of-Services

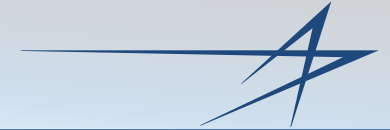


And Test Tools





CONCLUSION

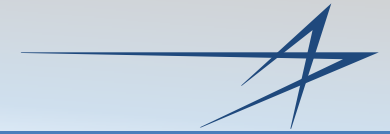


Cyber based critical infrastructure assets are vulnerable to cyber attacks because of the increasing interdependence and automation of cyber systems.

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.

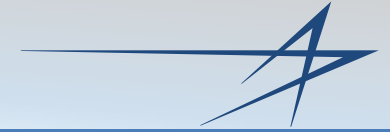
Lockheed Martin is developing innovative approaches to test, evaluate and assess the security posture of organizations' information system and cyber system environment.



REFERENCES & ACRONYMS



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>
2. 2009 CDW-G Federal Cybersecurity Report: Danger on the Front Lines, November 2009 at <http://webobjects.cdw.com/webobjects/media/pdf/Newsroom/2009-CDWG-Federal-Cybersecurity-Report-1109.pdf>
3. Cyber Security Market Update <http://www.prweb.com/releases/2009/06/prweb2513744.htm>
4. Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance at http://csis.org/files/media/csis/pubs/090223_cag_1_0_draft4.1.pdf
5. Control Systems Cyber Security for Managers and Operators at http://www.inl.gov/scada/training/d/4hr_introduutory_scada_security.pdf
6. Cyber Security Mega Trends - Study of IT leaders in the U.S. federal government at <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/CA%20Security%20Mega%20Trends%20White%20Paper%20FINAL%20%20%282%29.pdf>
7. 21 Steps to Improve Cyber Security of SCADA Networks, at <http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf>
8. A Summary of Control System Security Standards Activities in the Energy Sector at http://www.oe.energy.gov/DocumentsandMedia/Summary_of_CS_Standards_Activities_in_Energy_Sector.pdf
9. NIST SP 800-82, Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security - <http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf>
10. NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf
11. NIST SP 800-82, DRAFT *Guide to Industrial Control Systems Security*, September 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf
12. NERC Critical Infrastructure Protection Standards 002-009, at <http://www.nerc.com/page.php?cid=2|20>
13. IT Security for Industrial Control Systems at <http://www.isd.mel.nist.gov/documents/falco/ITSecurityProcess.pdf>
14. Interim Voluntary Security Guidance for Water Utilities, Section 5; http://www.awwa.org/science/wise/#P7_623



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