Cyber Security Controls Assessment : A Critical Discipline of Systems Engineering

14th Annual NDIA Systems Engineering Conference
San Diego, CA
October 24-28, 2011

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

Purpose

Provide an overview on integrating Security Controls Assessment (SCA) phases with Systems Engineering Life Cycle (SELC) phases to protect against threats to the security principles of enterprise infrastructure assets, information, related services and processes

Session Learning Objectives

- Introduction to “Cyber”
- Understand the challenges and issues related to the cyber security
- Understand applicable cyber security standards
- Explore cyber security assessment integrated with systems engineering life cycle
- Review the assessment process, and tools for vulnerability assessment

INTRODUCTION

Securing Cyber Infrastructure

"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/

For Enterprise Domains

Oil & Gas	Chemical	Electric	Nuclear
Healthcare	Retail	Agriculture	Food & Water
Shipping	Transportation	Defense	Communications Services
Civil Services	Manufacturing	Emergency Management	Financial Services

With facilities, systems, and equipments if destroyed, would have a debilitating impact on security, safety and survivability essential for functioning of enterprise information systems

What is Cyber?

Cyber Space

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 Security

Determines that the security features of the cyber system infrastructure components are designed, implemented and adequate for proposed system environment.

Cyber Security Eng.

A discipline that uses a systems engineering approach to determine the total protection for a system including physical, technical, operational, environmental, administrative, and personnel controls

Cyber = Enabling of Internet Technologies

CYBER SECURITY ISSUES AND CHALLENGES

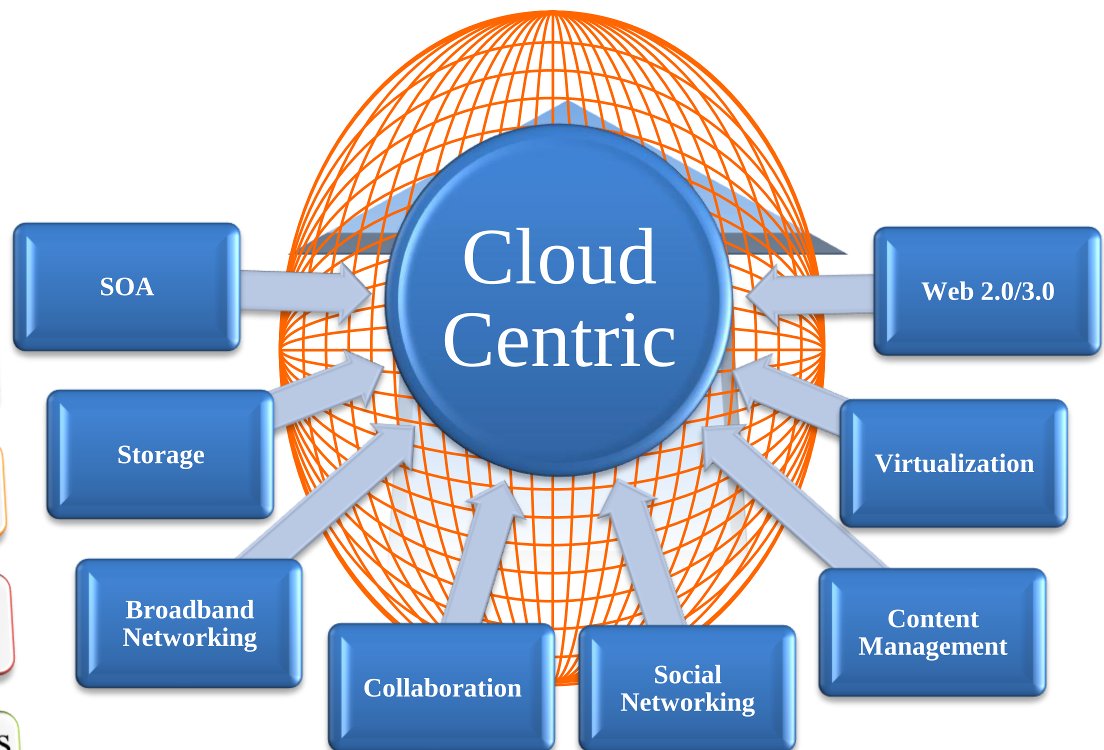
EMERGING TRENDS

Emerging Trends - 1

Cyber Environment Growth

1. Increasing access to infrastructure assets via Internet based technologies
2. Increase in Users (Internal & External, Global)
3. Advent of Cloud Computing
4. Advances in Social Networking Technologies
5. Multiple Security Domains
6. Dynamic nature of Enterprise Systems (SoS, NCES)
7. Conversion of Legacy Applications as Service

Using



And Increasing ……………….

Emerging Trends - 2

Emerging Threats

- Increase in system complexity
- Increase in standards and regulation compliance requirements
- Shortcomings in Proprietary Authentication
- Increase in Unauthorized Retrieval of Information for personal/ monitory Gain
- Increase of Vulnerabilities in Security Products
- Release of Beta version of system components

- 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

Security attacks, software vulnerabilities, and hardware failure can all lead to security threats

Emerging Trends - 3

Caused By Increase in ……

Hackers

Criminals

Terrorist

Software Components

Network Components

Technology Advances

Threat Agents

Employees

Business Partners

Sub-Contractors

“State” Sponsored

Natural Disasters

Industry Regulations

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

Emerging Trends - 4

Causing loss of control and disruption in

Transport Media	• Routers, Switches, Antenna, Towers,
Protocols	• Standard, Proprietary
Gateways	• Proxy Servers, Firewalls
Systems	• Cyber Systems, Industrial Control Systems
Storage	• Multiple formats of Text, Audio, Video data
Facilities	• Local, International

Growth of cyber technologies have changed threat environment forever.....

Emerging Trends - 5

Creating Impacts….

Legal Liabilities

National Security

System Destruction

Customer Confidence

Improper Data Disclosure

Loss of Revenue

Delays and Denial of Services

Loss of Productivity

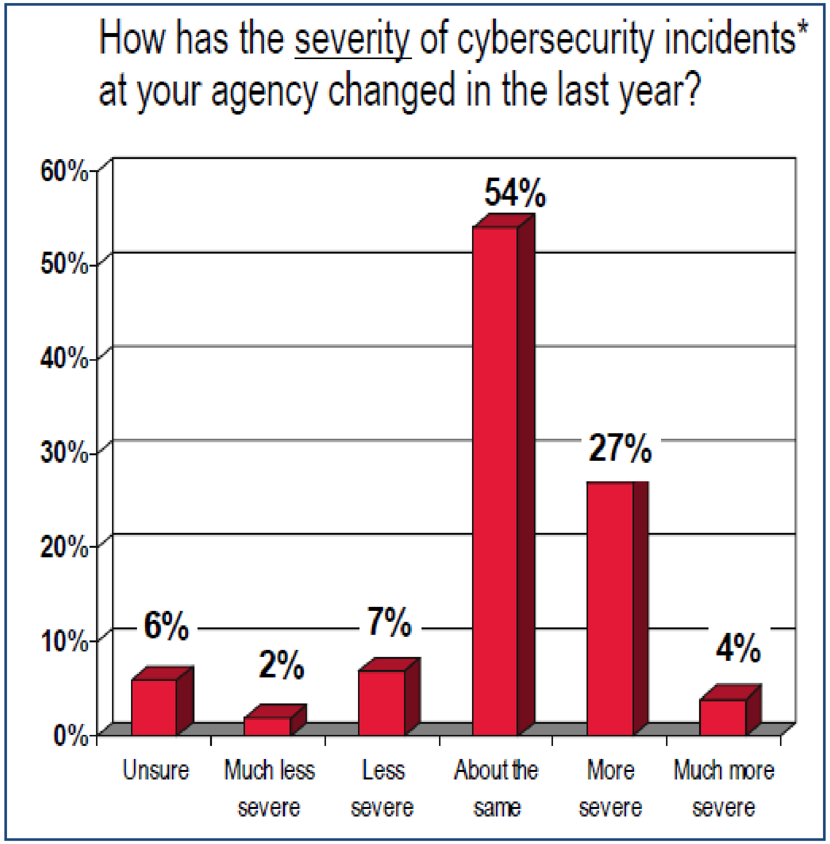
Economic Uncertainty

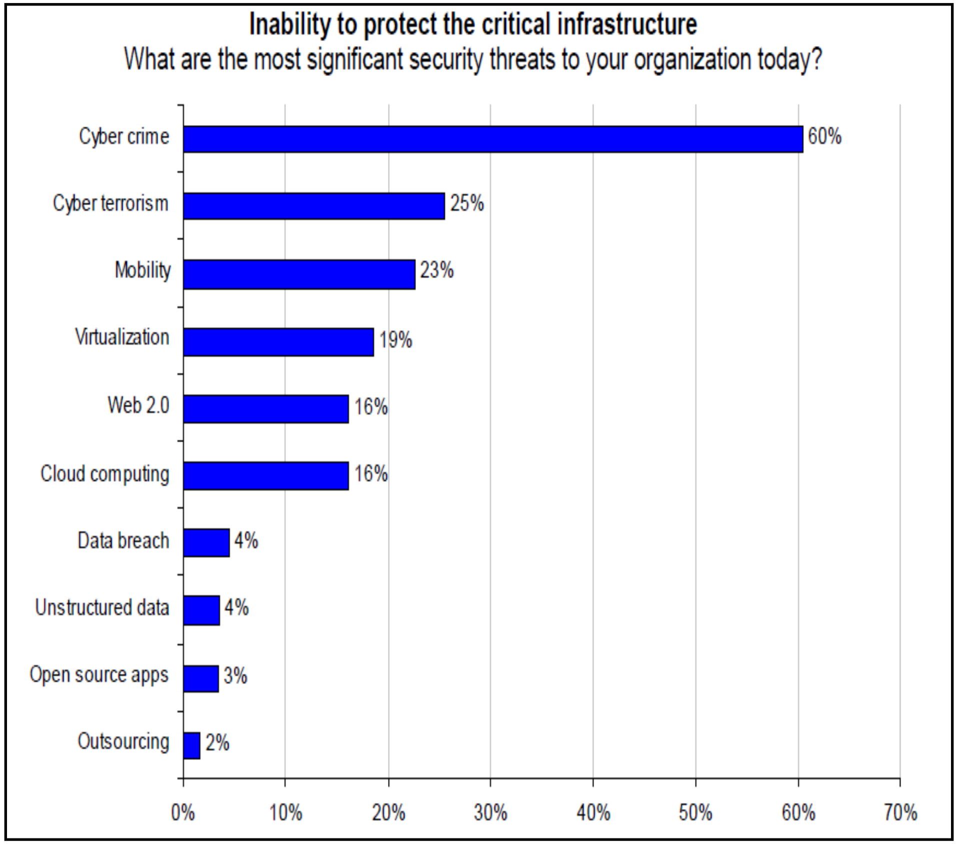
High Cost of Maintenance

And Numerous Cascading Effect because of Domain Interdependencies

Emerging Trends - 6

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%202%20%282%29.pdf

Incident related to Cyber Crimes are on rise

Emerging Trends - 7

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

Integration with Systems Engineering Life Cycle

- 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 Requirements

Principles	To Ultimately Support
Confidentiality	Enterprise Networks
Integrity	Enterprise Services
Availability	Enterprise Information
Authentication	Enterprise Systems
Authorization	Enterprise Domains
Auditing	Nation's Economy and Security
Non-Repudiation	

And Build Trust and Confidence in system environment

Cyber Security Standards &Regulations

For Applicable Enterprise Domain

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

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

International
- ISO
- ITU
- <more…>

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

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

And Growing Day by Day……………….

Cyber Security Controls

Management	Technical	Operational	Monitoring	Maintenance
Risk Assessment	Identification	Physical Protection	Risk Assessment	IDS and IPS
Business Continuity Planning	Authentication	Environmental Protection	Physical Access	Patch Management
Disaster Recovery Planning	Access Control	Personnel Security	Media Access	Change Management
Incident Management	Accounting	Communication Protection	Remote Access	
Awareness & Training	Auditing	Configuration Management	Environmental Controls	
Security Assessment	System Protection	Media Protection	Suspicious Activities	
C&A	Communication Protection	Incident Response		
	Encryption and Key Management			

Security Controls are action or procedure that provide CIA of system environment

CYBER SECURITY ASSESSMENT FRAMEWORK

Assessment Objectives

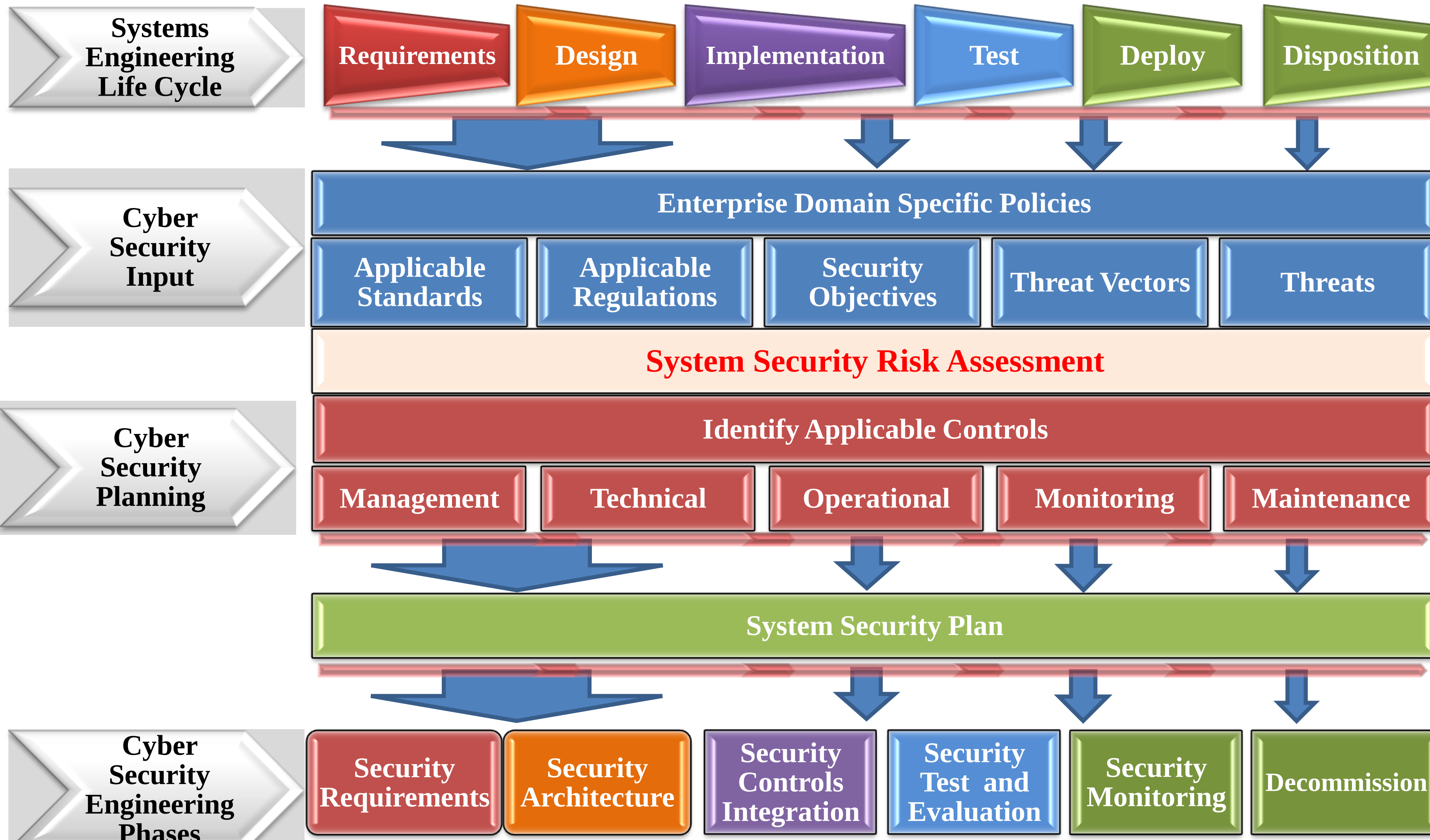
Cyber Security Assessment

The test and evaluation of the cyber environment 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 protection against security vulnerabilities and threats
2. Ensure compliance to legislative and regulatory Standards
3. Ensure the confidentiality, integrity and availability of the data
4. Identify problem areas and provide reasonable options
5. Ensure enterprise infrastructure is reliable, recoverable and resilient

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

Cyber Security Engineering



Security must be a key part of the life cycle processes for any system:

Cyber Security Assessment Plan

Assessment Plan

1. Select/Obtain sponsorship
2. Define objectives
3. Select policy and guideline for assessment
4. Define roles and responsibilities

1. Select/Define Assessment Process
2. Select Assessment Tools
3. Define measurement metrics and reports
4. Identify and gather documentation

Security Controls Assessment Plan

Plan and Gain an understanding of security needs

Cyber Security Assessment

Systems Engineering Life Cycle	**Requirements**	**Design**	**Implementation**	**Test**	**Deploy**	**Disposition**
Cyber Security Assessment Phases	**Identify**	**Inspect**	**Investigate**	**Test**	**Monitor**	**Disposition**
Assessment Activities	**Review Require ments**	**Review Documents**	**Review Controls Integration**	**Conduct Testing**	**Monitor Operation**	**Dispositi on Assets**
Assessment Activity Elements	Security Policies Security Standards Security Regulations Requirements	Security Architecture Security Design Security Functions DR/COOP	Static Analysis Controls Integration Configuration Procedures Redundancy & Recoverability	User Interface Test Black Box Testing Vulnerability Test Penetration Test	Configuration Management Patch Management Incident Management Performance Management	Disposal Process Critical Assets Disposal Sensitive Data Disposal Media Disposal
Assessment Activity Reports	**Requirements Analysis Report**	**Security Design Review Report**	**Security Integration Report**	**Security Testing Report**	**Security State Report**	**Assets Disposition Report**

←-----------Security Risk Assessment Throughout-------------→

Cyber Security Assessment Process

Define System Mission Threads

Identify Cyber Services Used

Identify Functions Executed

Identify Information Flow

Define Possible Threat Scenarios

Generate Assessment Data

Develop Assessment Cases

Setup Assessment Environment

Identify Assessment Members

Identify Assessment Tools

Execute Assessment Cases

Analyze and Report Results

Actively managing the "security process" is a key part of achieving security

Cyber Security Controls Assessment

- **Verification**
  - Security Plan
  - Risk Assessment
  - Physical Protection
  - Environmental Protection
  - Media Protection
  - Contingency Planning
  - Incident Response
  - Awareness and Training
- **Validation**
  - Access Control
  - Accountability
  - Auditing
  - Identification
  - Authentication
  - System Protection
  - Communicatio n Protection
  - Routine Maintenance
- **Web Services Specific**
  - External Users
  - Internal Users
  - Key Management
  - Cloud-to-Cloud
- **Vulnerability Testing**
  - Hidden Fields Manipulation
  - Invalid Input
  - SQL Injection
  - Buffer Overflow
  - Cross Site Scripting
  - Session Hijacking
  - Error Handling
  - Parameter Tempering
- **Penetration Testing**
  - IP Attacks
  - ICMP Attacks
  - TCP Attacks
  - Routing Attacks
  - DoS Attacks
  - Spam Attacks
  - Social Attacks

Gain an understanding of State of System Security

Cyber Security Testing Tools

- **Network Assessment**
  - Foundstone
  - Nessus
- **Network Mapping**
  - NMap
  - NetsTumbler
- **Wireless Network Analysis**
  - AirSnort
- **Host Configuration Analysis**
  - Solarwinds
  - SuperScan
- **Traffic Analysis**
  - EtherReal
  - Sniffer
- **Access Control**
  - GetAdmin
  - Pwdump2
- **Web Application Scan**
  - AppScan
  - WebInspect
- **Web Services Scan**
  - SOAPUI
- **Database Scan**
  - WebInspect
  - Internet Scanner
- **Data Retrieval**
  - Planning
- **Password Cracking**
  - Crack 5
  - L0pht
- **File Integrity**
  - TripWire
  - LANGuard

Plan and Gain an understanding of security needs

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
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. 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%202%20%282%29.pdf
6. 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
7. 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
8. 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*
9. 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*
10. NERC Critical Infrastructure Protection Standards 002-009, at *http://www.nerc.com/page.php?cid=2|20*

Acronyms

1. CAG – Consensus Audit Guidelines (SANS 20 security controls)
2. CFATS – Chemical facility Anti-terrorism Standards
3. CIA – Confidentiality, Integrity, Availability
4. CIP – Critical Infrastructure Protection
5. COTS – Commercial Off The Shelf
6. DIACAP - DoD Information Assurance Certification and Accreditation Process
7. DCS – Distributed Control System
8. FERC – Federal Energy regulatory Commission
9. FISMA – Federal Information Security Management Act
10. HIPAA - Health Insurance Portability and Accountability Action
11. ICS – Infrastructure Control System
12. IEC – International Electrochemical Commission
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. SANS - SysAdmin, Audit, Network, Security
26. SCADA – Supervisory Control and Data Acquisition System
27. SOX - Sarbanes-Oxley Act