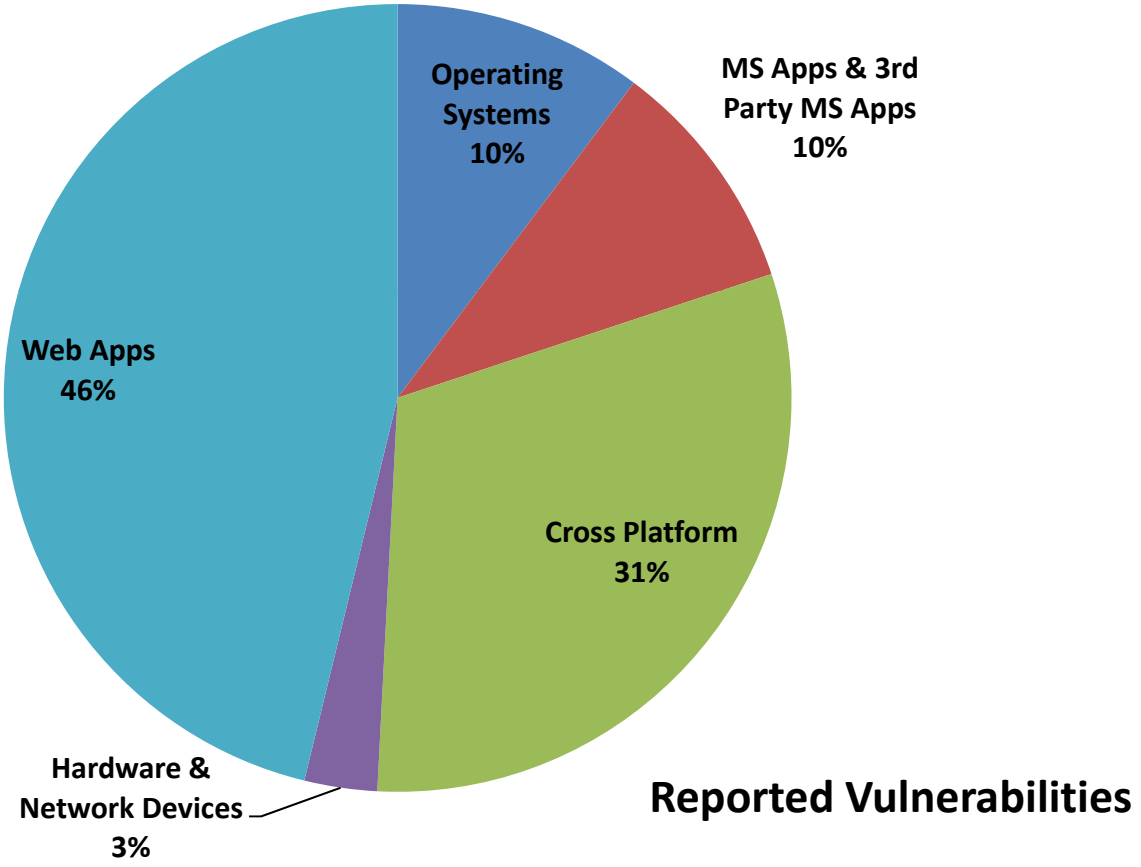
Securing Software Applications

How the Acquisition Project Leader
Helps Build-In Security

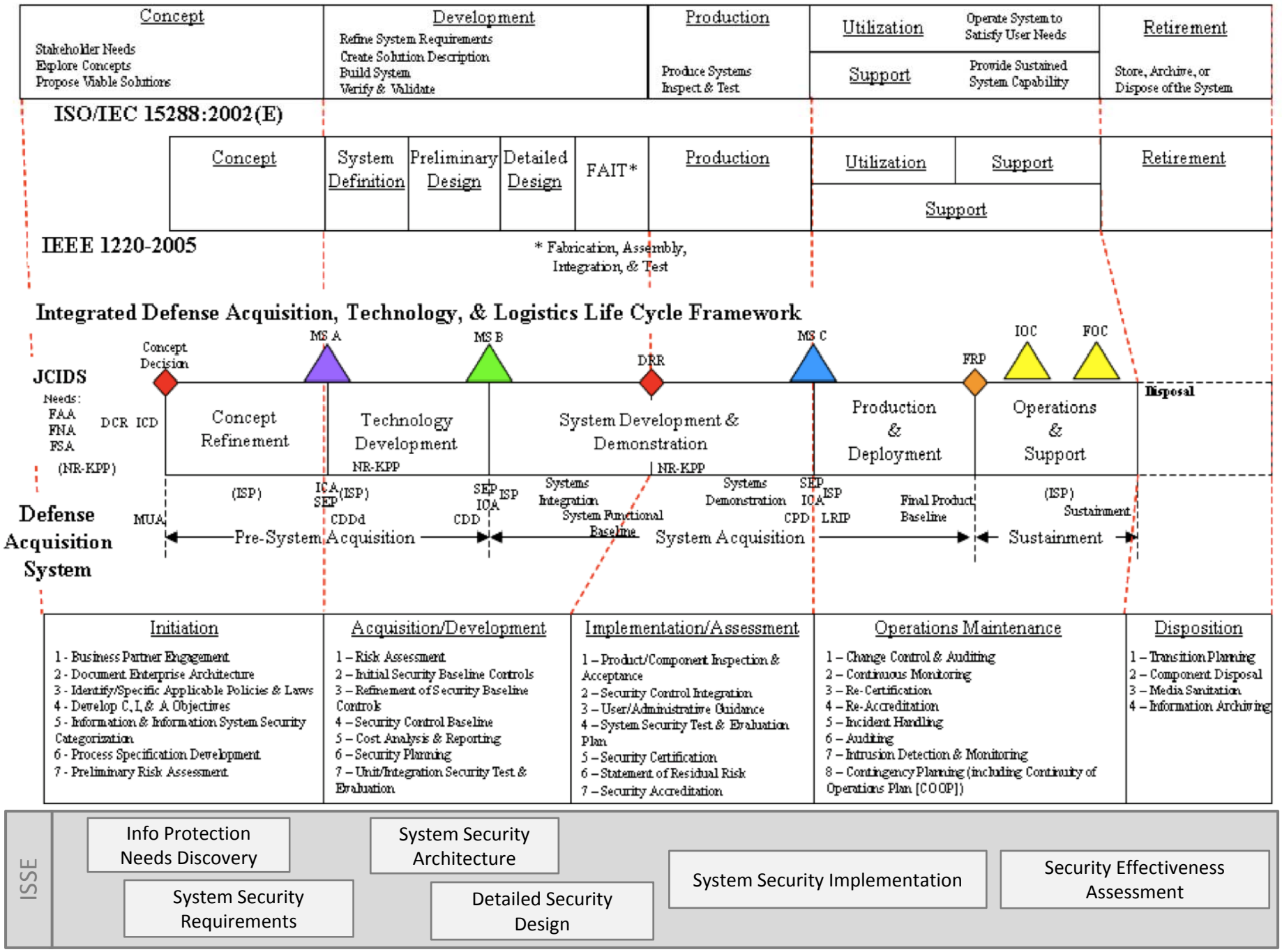
Why Worry about Applications?



Source: SANS@RISK: The Consensus Security Vulnerability Alert

Securing the Applications – In the Beginning

- Pick a lifecycle, any lifecyle
- Build on
  - People,
  - Process and
  - Technology
- Yes, its worth the time and effort if the organization values its data, reputation, or money


Concept
Stakeholder Needs
Explore Concepts
Propose Viable Solutions
Development
Refine System Requirements
Create Solution Description
Build System
Verify & Validate
Production
Produce Systems
Inspect & Test
Utilization
Operate System to Satisfy User Needs
Support
Provide Sustained System Capability
Retirement
Store, Archive, or Dispose of the System
ISO/IEC 15288:2002(E)
Concept
System Definition
Preliminary Design
Detailed Design
FAIT*
Production
Utilization
Support
Support
Retirement
IEEE 1220-2005
* Fabrication, Assembly, Integration, & Test
Integrated Defense Acquisition, Technology, & Logistics Life Cycle Framework
JCIDS
Needs:
FAA
FNA
FSA
(NR-KPP)
DCR ICD
Concept Decision
MS A
MS B
DRR
MS C
FRP
IOC
FOC
Disposal
Concept Refinement
Technology Development
NR-KPP
System Development & Demonstration
NR-KPP
Production & Deployment
Operations & Support
Defense Acquisition System
MUA
(ISP)
ICA
SEP
(ISP)
CDDd
SEP
IOA
ISP
CDD
Systems Integration
System Functional Baseline
Systems Demonstration
SEP
IOA
ISP
CPD
LRIP
Final Product Baseline
(ISP)
Sustainment
Pre-System Acquisition
System Acquisition
Sustainment
Initiation
1 - Business Partner Engagement
2 - Document Enterprise Architecture
3 - Identify/Specific Applicable Policies & Laws
4 - Develop C, I, & A Objectives
5 - Information & Information System Security Categorization
6 - Process Specification Development
7 - Preliminary Risk Assessment
Acquisition/Development
1 – Risk Assessment
2 – Initial Security Baseline Controls
3 – Refinement of Security Baseline Controls
4 – Security Control Baseline
5 – Cost Analysis & Reporting
6 – Security Planning
7 – Unit/Integration Security Test & Evaluation
Implementation/Assessment
1 – Product/Component Inspection & Acceptance
2 – Security Control Integration
3 – User/Administrative Guidance
4 – System Security Test & Evaluation Plan
5 – Security Certification
6 – Statement of Residual Risk
7 – Security Accreditation
Operations Maintenance
1 – Change Control & Auditing
2 – Continuous Monitoring
3 – Re-Certification
4 – Re-Accreditation
5 – Incident Handling
6 – Auditing
7 – Intrusion Detection & Monitoring
8 – Contingency Planning (including Continuity of Operations Plan [COOP])
Disposition
1 – Transition Planning
2 – Component Disposal
3 – Media Sanitation
4 – Information Archiving
ISSE
Info Protection Needs Discovery
System Security Architecture
System Security Implementation
Security Effectiveness Assessment
System Security Requirements
Detailed Security Design

What the SDLC?!

- Concept, Stakeholder Needs, Concept Refinement – in other words, *Requirements*
- Business needs drive requirements and Security is now a business need
- Mandates to secure IT systems are generally handed down from above (FISMA, HIPAA)
  - Or public pressure
- Security requirements are generalized through NIST, DoD, PCI-DSS, or community best practices

Requirements Refinement

- Put in the time - upfront
- Reusability from project to project
- Example: SQUARE Methodology from the Software Engineering Institute at Carnegie Mellon
- Start early, create clear usable security requirements – Easy!

Common Requirements

- NIST SP 800-53 (SI-10) Information Input Validation
  - Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands .
- PCI – DSS
  - Protect Stored Card Holder Data, Don't store authentication data and Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).
- DoD 8500.2 DCSQ Software Quality SDLC
  - Ensure that all required software development life cycle documentation is current and approved, and it reflects the use of code reviews and/or accepted software quality control practices that verify the security of software source code.

People, Process & Technology

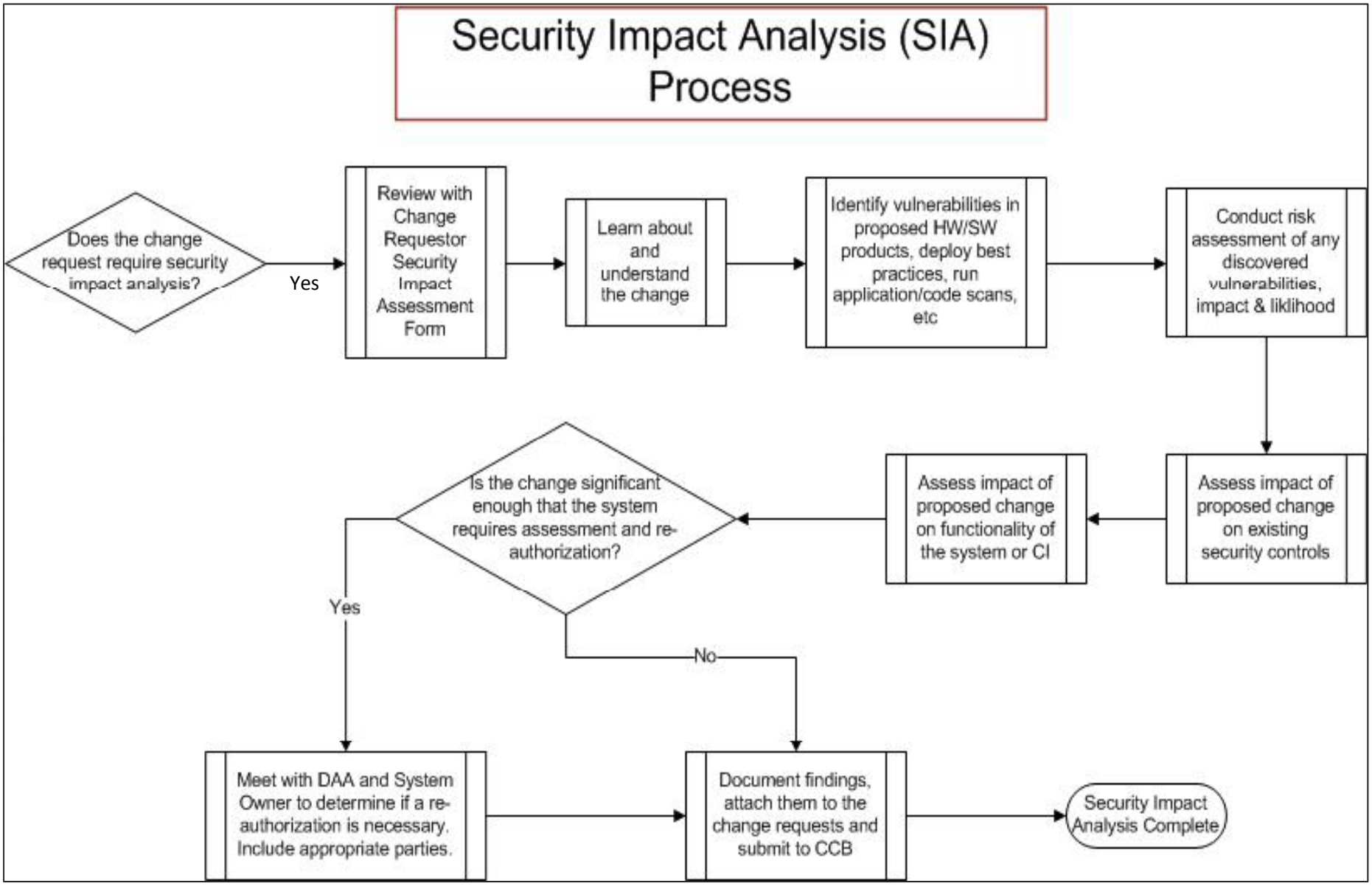
- It’s not all about Developers
- Team Approach
- Develop or Matrix specific set of Knowledge, Skills and Abilities (KSAs)
- Identify specific process flow areas to implement security
- Build a toolbox of complimentary tools

People

- Important KSA's
  - Information System Security Engineer
  - Code Reviewers for "top 25"
    - http://www.sans.org/top25-software-errors/
    - http://cwe.mitre.org/top25/index.html
  - Use of automated tools for scanning code and systems
  - RPF, SOW, Contract Language
  - Penetration Tester/Ethical Hacker
- Outsourcing
- Training & Development

Process

- Defined Process for specific parts/people on the project
  - System Security Engineering
  - Security configuration management (ECP)
    - Security Impact Analysis
  - Code Review (manual, automatic, specific to security)
- Locate appropriate injection points for security review or input into existing processes
- Adapt, modify or create from scratch



Modified from NIST SP 800-128,
Guide for Security Configuration Mangement of Information Systems

Process (cont.)

- Developing Reusable Security Requirements (SQUARE Methodology)
- Identifying Mandates & Requirements
  - Regulatory include FISMA, HIPAA, SOX, CCA and their changes (FISMA 2.0)
  - "Requirements" include NIST SP 800-53, DoD 8500.2, PCI-DSS
- Identifying emerging threats, evolving hacker methods
- Measures of Success – Metrics

Technology

- Tools for automated scanning of code and systems for errors, flaws, configuration issues, patch levels
- Not all tools are created equal – need multiple tools to adequately discover issues
- Cost of Toolsets can be HIGH
  - Developers (code review)
  - ISSE (configuration and vulnerability scanning)
  - Pen Tester (vulnerability discovery and exploitation)
- Outsourcing
  - Open Source
- Programming Language
  - http://www.cs.cornell.edu/projects/fabric/index.html

Questions ?

Useful Resources

- https://buildsecurityin.us-cert.gov/bsi/securecoding.html
- https://buildsecurityin.us-cert.gov/swa/downloads/Contract_Language_PocketGuide_Print.pdf
- http://www.msisac.org/scada/documents/4march08scadaprocure.pdf
- https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex
- http://www.sans.org/top25-software-errors
- http://www.sans.org/appseccontract/
- http://www.stsc.hill.af.mil/consulting/sw_estimation/estimatingguidebook.html
  http://www.veracode.com/images/pdf/sample%20contract%20language.pdf
- http://www.disa.mil/forge/

Acronyms

- C&A – Certification and Accreditation
- CCA – Clinger Cohen Act
- ECP - Engineering Change Proposal
- CEH - Certified Ethical Hacker
- CISSP-ISSEP – Certified Information System Security Professional – Information System Security Engineering Professional
- DAA – Designated Approval Authority
- DoD – Department of Defense
- FISMA -Federal Information Systems Management Act
- HIPAA – Health Insurance Portability and Accountability Act
- IAO/M – Information Assurance Officer/Manager
- ISSE – Information Systems Security Engineer
- KSAs - Knowledge Skills & Abilities
- NIST SP – National Institute of Standards and Technology Special Publications
- PCI – DSS – Payment Card Industry Data Security Standards
- RFP – Request for Proposal
- SANS – SysAdmin, Audit, Network, Security Institute
- SDLC – System Development Lifecycle
- SIA – Security Impact Assessment(Analysis)
- SOW – Statement of Work
- SOX – Sarbanes Oxley