Intro to Information Security Testing and Assessment

Karen Scarfone

Scarfone Cybersecurity

Scarfone Cybersecurity

Agenda

- Assessment
- Why do assessment?
- Risk Management Framework
- Assessment methodology phases
- Technical assessment techniques

Content from NIST Special Publication 800-115

Assessment

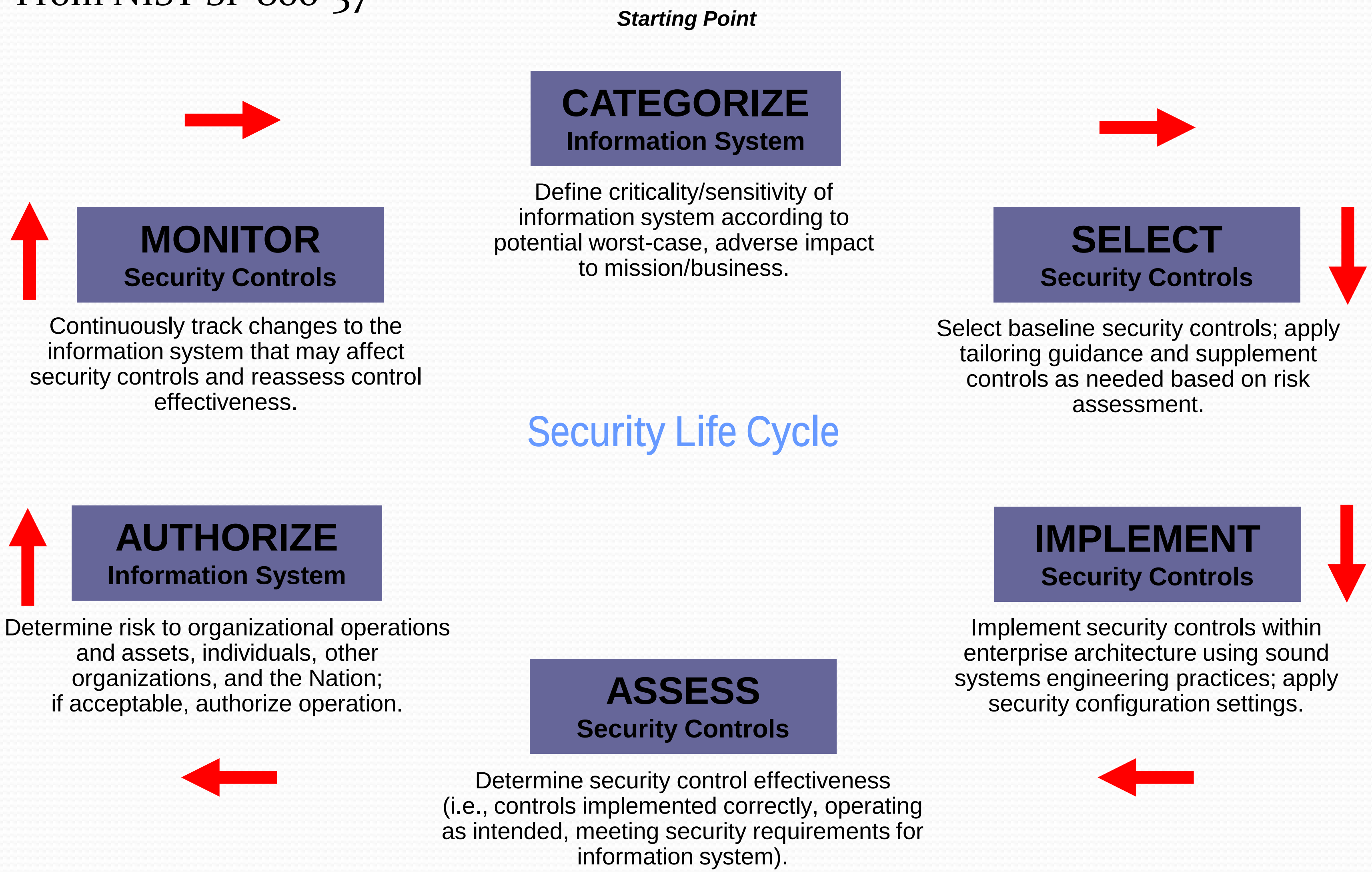
- Determining how effectively an entity being assessed meets specific security objectives
- Gaining understanding, achieving clarification, or obtaining evidence
- Three types of assessment methods
    - Testing: exercising one or more assessment objects to compare actual and expected behaviors
    - Examination: checking, inspecting, reviewing, observing, studying, or analyzing assessment objects
    - Interviewing: conducting discussions

Why do assessment?

- Help confirm that systems are properly secured
- Identify any organization security requirements that are not met, and other security weaknesses that should be addressed
- Meet requirements to periodically assess systems
- Not intended to take the place of implementing security controls and maintaining system security

Risk Management Framework

From NIST SP 800-37



Starting Point

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

Security Life Cycle

Assessment methodology phases

- Planning: Gather information needed for assessment execution and develop the assessment approach
    - Should treat an assessment as any other project
- Execution: Identify vulnerabilities and validate them when appropriate
- Post-Execution: Analyze identified vulnerabilities to determine root causes, establish mitigation recommendations, and develop a final report
- Several accepted methodologies for conducting different types of security assessments

Technical assessment techniques

- Review Techniques
  - Examination techniques, generally conducted manually
  - Evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities
  - Techniques include
    - Documentation review
    - Log review
    - Ruleset and system configuration review
    - Network sniffing
    - File integrity checking

Technical assessment techniques (cont.)

- Target Identification and Analysis Techniques
  - Testing techniques, generally performed using automated tools
  - Identify systems, ports, services, and potential vulnerabilities
  - Techniques include
    - Network discovery
    - Network port and service identification
    - Vulnerability scanning
    - Wireless scanning
    - Application security examination

Technical assessment techniques (cont.)

- Target Vulnerability Validation Techniques
  - Testing techniques that corroborate the existence of vulnerabilities
  - May be performed manually or with automated tools
  - Techniques include
    - Password cracking
    - Penetration testing
    - Social engineering
    - Application security testing

Combinations of techniques

- No one technique can provide a complete picture of the security of a system or network
- Organizations should combine appropriate techniques
  - One technique often relies on others
  - Multiple ways exist to meet an assessment requirement, such as determining whether patches have been applied properly
- Organizations have the flexibility to choose the techniques that best meet their requirements

Questions?

- karen@scarfonecybersecurity.com

LOCKHEED MARTIN

Introduction to Information Security Testing and Assessment

5th Annual Safeguarding Health Information:
Building Assurance through HIPAA Security

June 7, 2012

Richard L. Metzer D.Sc.

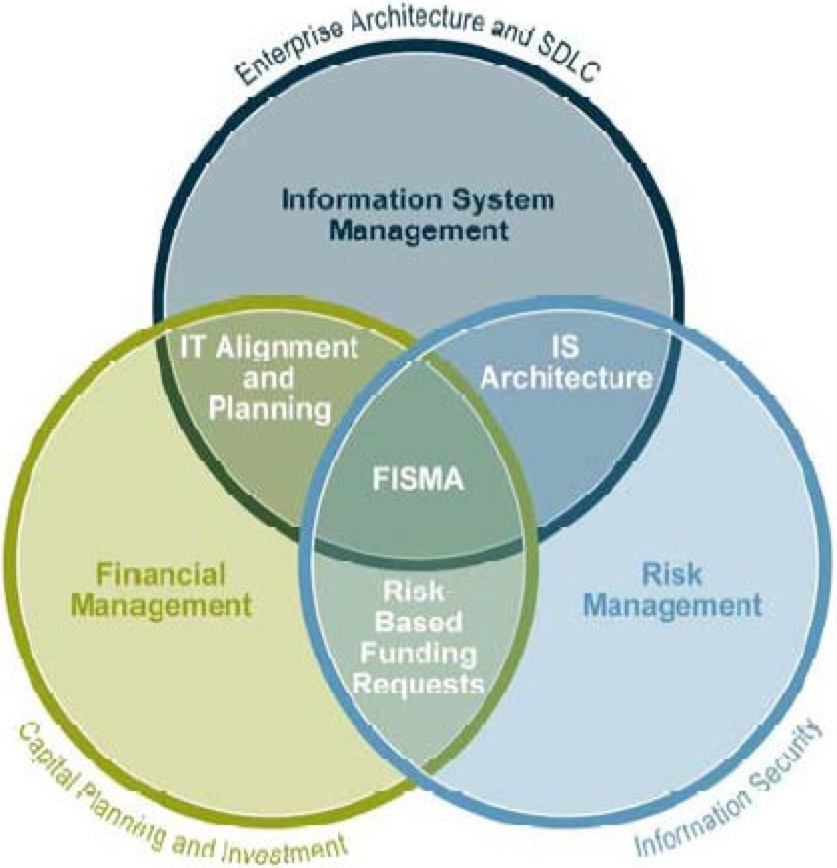
Agenda

- *Background*
- *Risk Management*
- *Threats*
- *Vulnerabilities*
- *Assessment and Testing*
  - *Vulnerability Scanning*
  - *Classical Security Testing*
  - *Penetration Testing*
  - *Fuzzing*

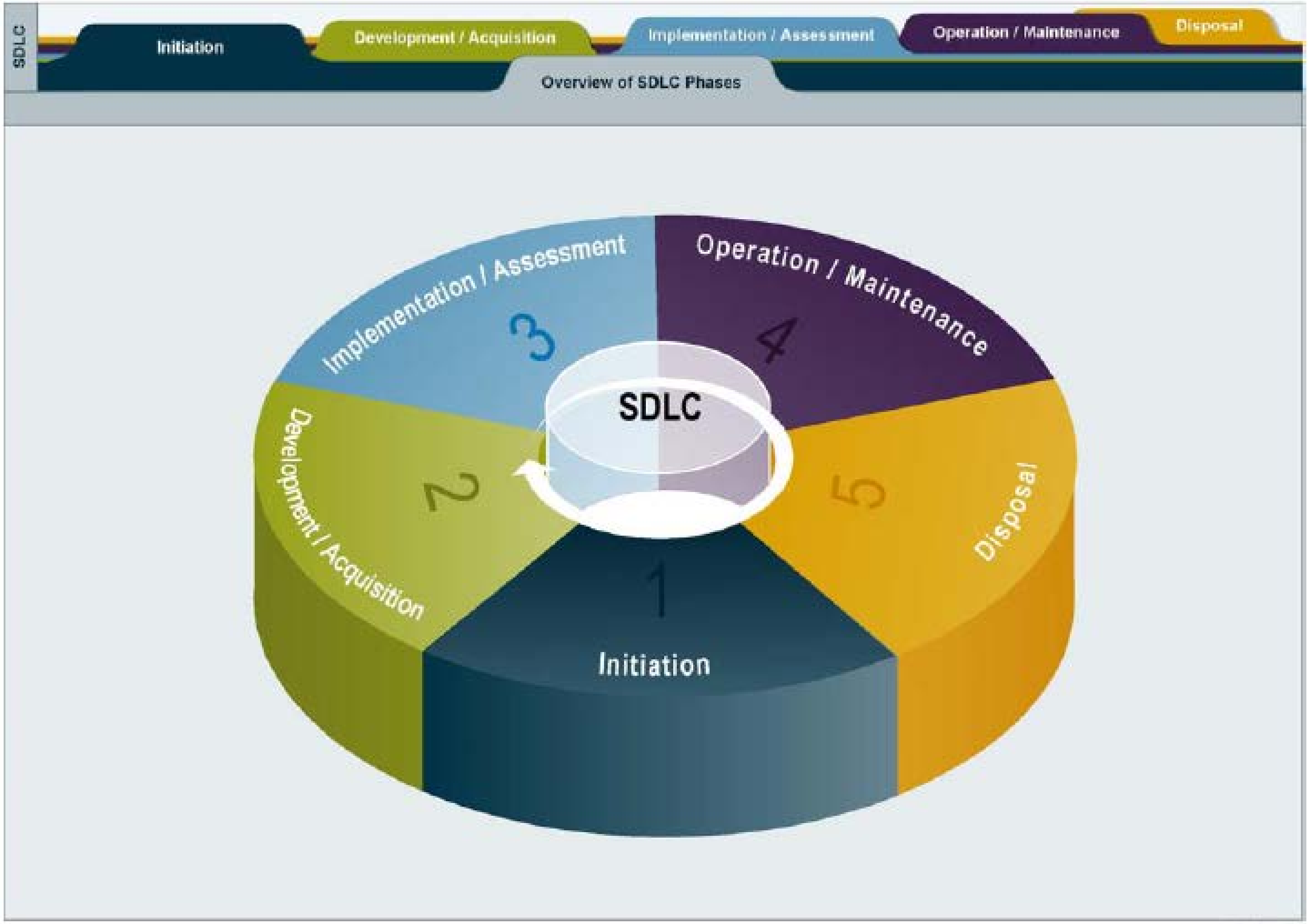
Background

- *Overarching Considerations*
  - *Business Mission, Tasks and Functions*
    - *Strategy and Tactics*
  - *Measurement*
  - *Risk Management*
  - *HIPAA as an Example*
- *Risk Management*
  - *Assets*
  - *Threats*
  - *Vulnerabilities*
  - *Impact*
- *System Development Life Cycle (SDLC)*

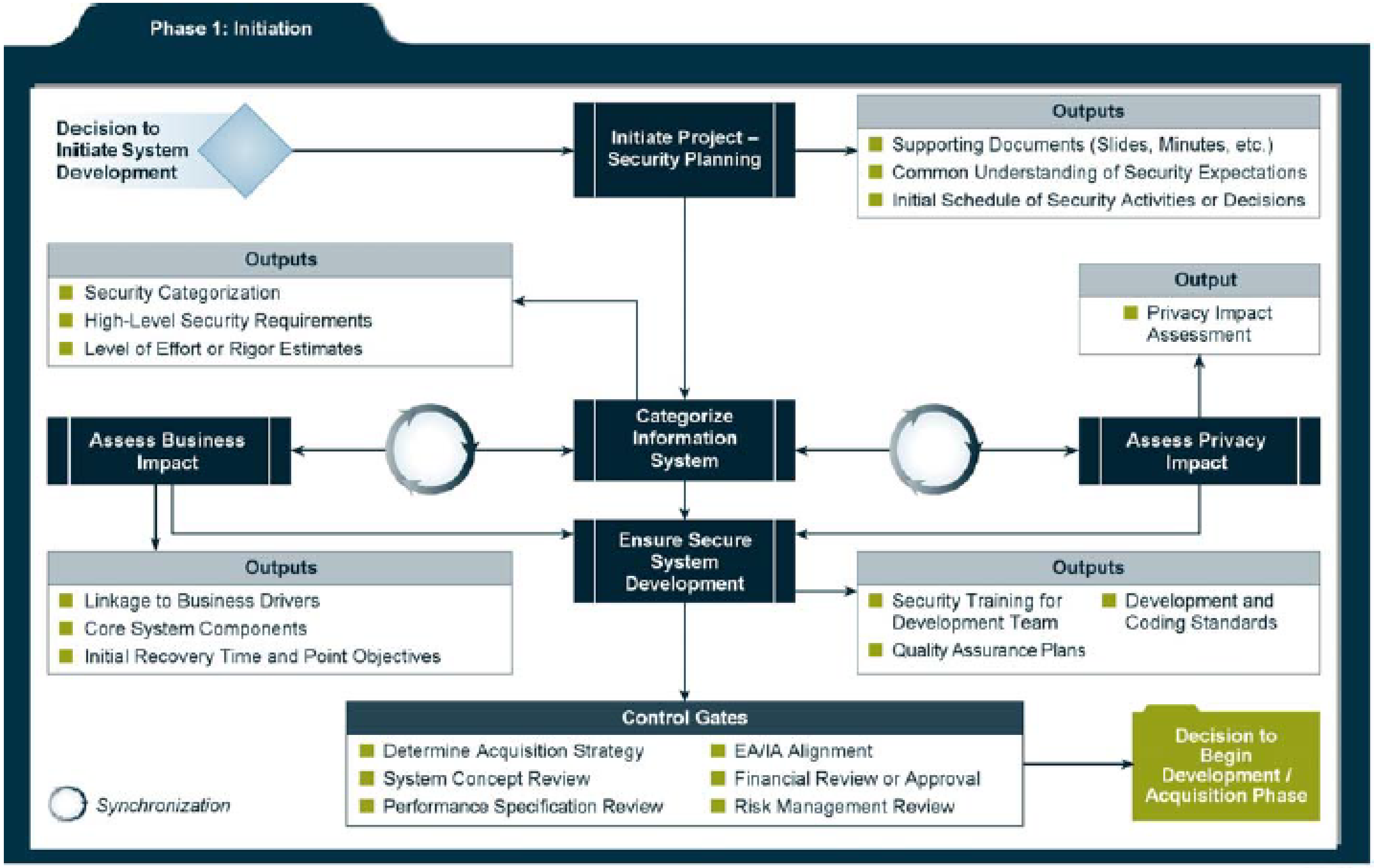
Positioning Security Considerations[3]


Enterprise Architecture and SDLC
Information System Management
IT Alignment and Planning
IS Architecture
FISMA
Financial Management
Risk Based Funding Requests
Risk Management
Capital Planning and Investment
Information Security

The SDLC: A Conceptual View



Relating Security in the Initiation Phase[3]



Phase 1: Initiation

Decision to Initiate System Development

Initiate Project – Security Planning

Outputs
- Supporting Documents (Slides, Minutes, etc.)
- Common Understanding of Security Expectations
- Initial Schedule of Security Activities or Decisions

Outputs
- Security Categorization
- High-Level Security Requirements
- Level of Effort or Rigor Estimates

Output
- Privacy Impact Assessment

Assess Business Impact

Categorize Information System

Assess Privacy Impact

Ensure Secure System Development

Outputs
- Linkage to Business Drivers
- Core System Components
- Initial Recovery Time and Point Objectives

Outputs
- Security Training for Development Team
- Development and Coding Standards
- Quality Assurance Plans

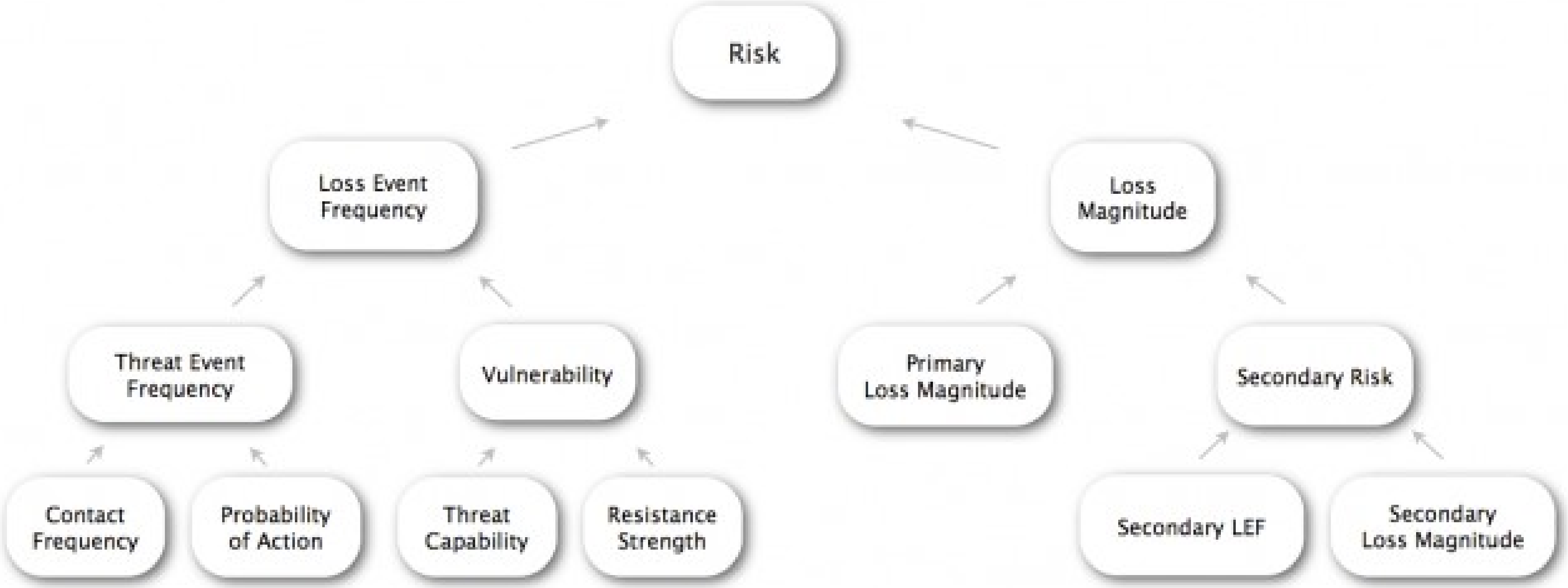
Control Gates
- Determine Acquisition Strategy
- System Concept Review
- Performance Specification Review
- EA/IA Alignment
- Financial Review or Approval
- Risk Management Review

Decision to Begin Development / Acquisition Phase

Synchronization

Risk Model [1]

Factor of Risk Diagram



IS&GS CIVIL

Threat Agent Components - Example

Subsets of the overall threat agent population that share key characteristics[1]

The notion of threat communities is a powerful tool for understanding who and what we're up against as we try to manage risk. For example, consider the following threat community profile:

Motive: ideology
Primary intent: damage/destroy
Sponsorship: unofficial
Preferred general target characteristics: entities or people who clearly represent a conflicting ideology
Preferred specific target characteristics: high profile, high visibility
Preferred targets: human, infrastructure (buildings, communications, power, etc.)
Capability: varies by attack vector (technological: moderate)
Personal risk tolerance: high
Concern for collateral damage: low

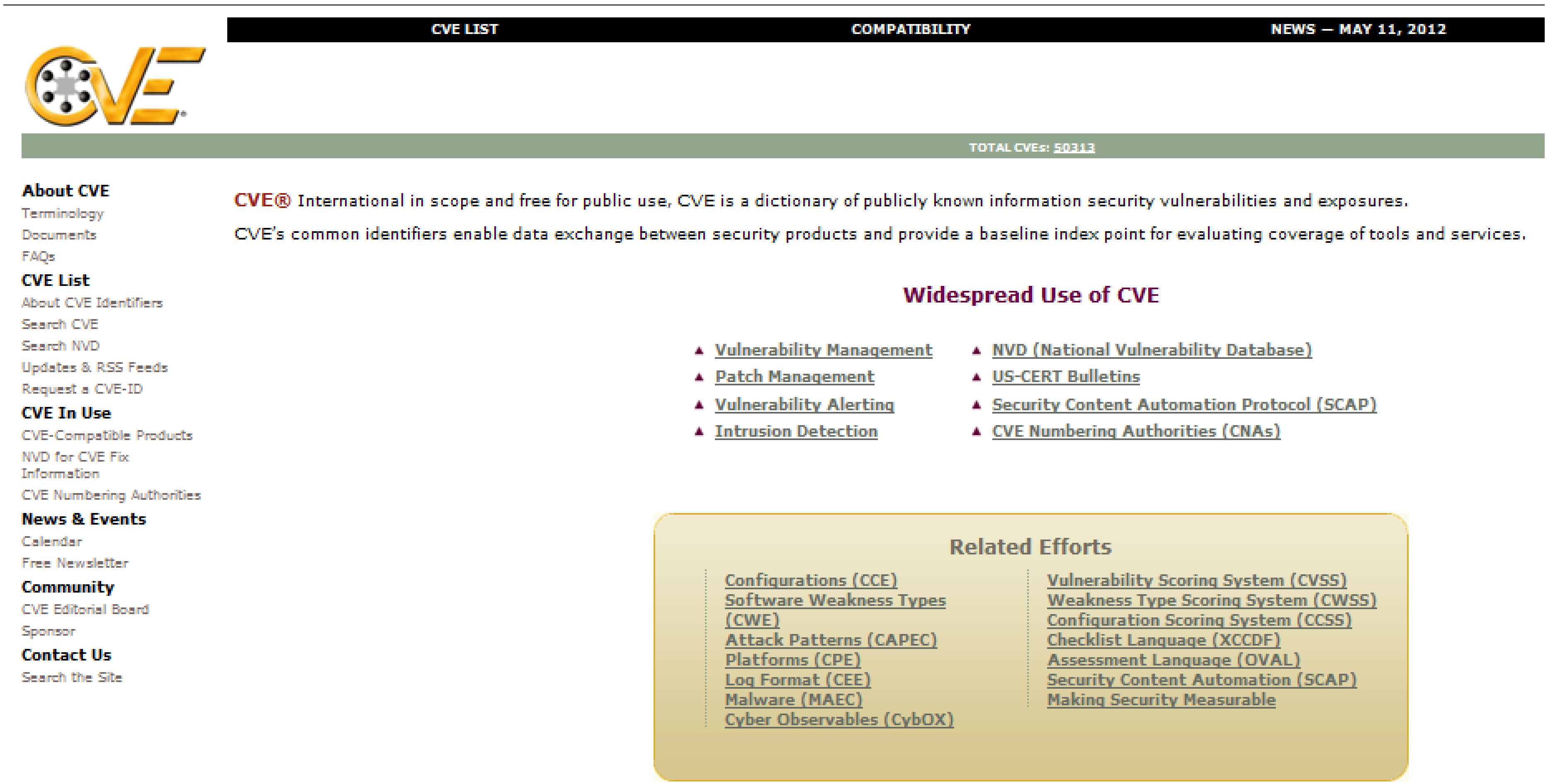
Threat Agent Characteristics – Example [1]

There are four primary components of our risk taxonomy that we want to identify threat agent characteristics for, those characteristics that affect:

- The frequency with which threat agents come into contact with our organizations or assets
- The probability that threat agents will act against our organizations or assets
- The probability of threat agent actions being successful in overcoming protective controls
- The probable nature (type and severity) of impact to our assets

It's important for us to understand the factors that drive these differentiating characteristics in order to effectively assess the probability of being subject to attack and, if subjected to attack, the likely nature, objective, and outcome of the attack. We'll examine these factors a bit more as we go along.

Common Vulnerabilities and Exposures (CVE)



CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Use of CVE

- ▲ Vulnerability Management
- ▲ Patch Management
- ▲ Vulnerability Alerting
- ▲ Intrusion Detection
- ▲ NVD (National Vulnerability Database)
- ▲ US-CERT Bulletins
- ▲ Security Content Automation Protocol (SCAP)
- ▲ CVE Numbering Authorities (CNAs)

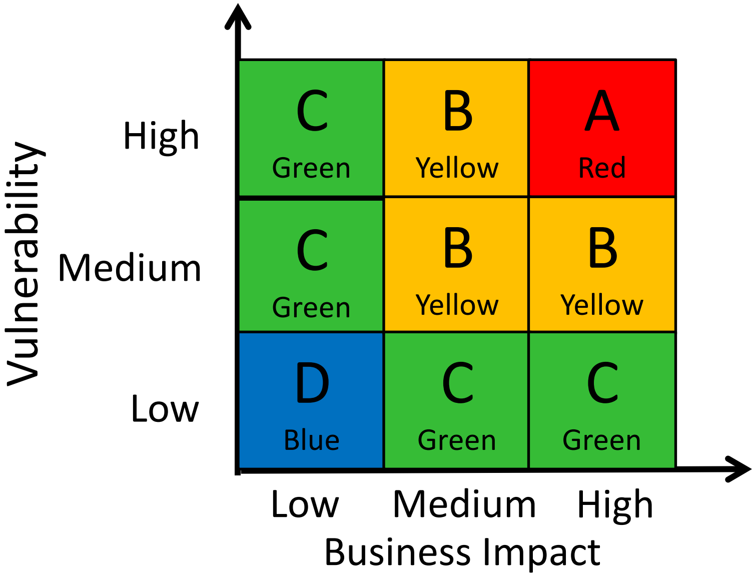
Related Efforts

- Configurations (CCE)
- Software Weakness Types (CWE)
- Attack Patterns (CAPEC)
- Platforms (CPE)
- Log Format (CEE)
- Malware (MAEC)
- Cyber Observables (CybOX)
- Vulnerability Scoring System (CVSS)
- Weakness Type Scoring System (CWSS)
- Configuration Scoring System (CCSS)
- Checklist Language (XCCDF)
- Assessment Language (OVAL)
- Security Content Automation (SCAP)
- Making Security Measurable

http://cve.mitre.org/

Mapping Risk Category to Impact and Vulnerability[2]

- *Business Impact Likelihood is the product of two probabilities**
  - *Probability event will occur (Threat Level)*
  - *Probability controls will fail when event occurs (Vulnerability Level)*
    - *Assessments difficult without historical data*
    - *There are no guarantees that history will repeat itself*
    - *Previously learned method (High, Medium, Low) summarized in the figure below*



Vulnerability	Low	Medium	High
High	C Green	B Yellow	A Red
Medium	C Green	B Yellow	B Yellow
Low	D Blue	C Green	C Green

Business Impact

- *Vulnerability assessments vary with circumstances but include: testing, auditing, scanning, penetration testing, dependency tree modeling and brain storming.*

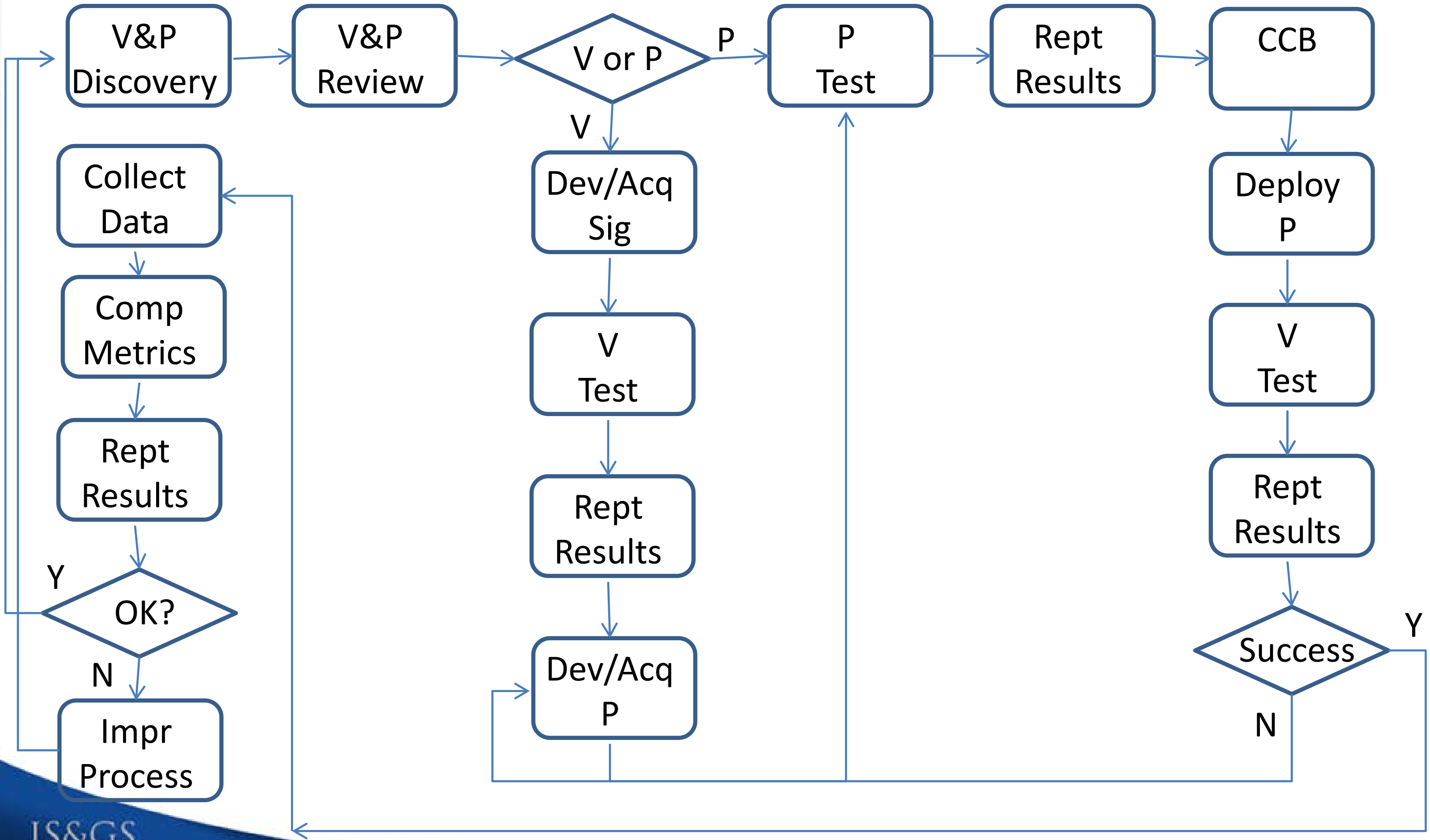
[2] Enterprise Security Architecture, Figure 9-3, p.208

Vulnerability and Patch Management

- *Several NIST Special Publications on the topic*
  - *800-24 PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does;*
  - *800-40 Creating a Patch and Vulnerability Management Program; and*
  - *800-51 Guide to Using Vulnerability Naming Schemes.*
- *Establish Goals/Metrics*
- *Develop a Process*
- *Acquire Tools*
- *Security Content Automation Protocol (SCAP)*
- *Hold Personnel Accountable*

Jenny is located in the Herndon/Ashburn area so Arlington is not good for her. She'll probably want to teleconference. Arlington is fine for me – Ballston, Rosly
Rick Metzer

Sample Vulnerability (V) and Patch (P) Management Process



IS&GS CIVIL

Vulnerability Assessment

- ***Types of Vulnerabilities***
  - *Physical, Personnel, and Technical*
- ***Physical***
  - *Typically Examination/Inspection methods (e.g., Locks, Visitor Access Control, etc., physical searches, OPSEC (Dumpster Dives))*
  - *May include Technical (e.g., Wireless Scanning)*
- ***Personnel***
  - *Typically involves all three methods (e.g., examination of training records, interviews with personnel to determine knowledge of security policies, processes, etc., and execution of password cracking tools).*

Vulnerability Assessment (Continued)

- *Technical*
  - *Typically Examination (e.g., Documentation, Demonstration of Security Tools, and Tool Outputs), Technical (e.g., execution of vulnerability scanning software, Security Test and Evaluation (ST&E) tests).*

Vulnerability Scanning Software

- *Types of Vulnerability Scanning Software Include*
  - *Network Scanning Software identifies weak networking device settings (e.g., vulnerable ports left open, default passwords)*
  - *Web Application Scanning software identifies weak web application settings, failure to implement patches to known web application vulnerabilities etc.*
  - *Database Scanning Software identifies similar weaknesses in database management systems and database applications.*
- *One list of Scanning Software and Vendors can be found at:*

  http://www.timberlinetechnologies.com/products/vulnerability.html

Security Testing and Evaluation

- *Classical Security Testing Method*
  - *Use the FIPS 199 Security Category and NIST SP 800-53 to create a list of security controls for the system*
  - *Decompose each control into specific security requirements that can be tested (e.g., Strong Passwords (IA-5) lists several specific requirements each of which requires one or more tests to verify proper functioning (password length (minimum & maximum), variety of character types, age of password, etc.)*
  - *Develop tests and test them to ensure they work correctly.*
    - *Some tests require test data*
    - *Test rerun/expected results problem*
  - *Organize tests for maximum efficiency and automate execution and recording of results as much as possible*

IS&GS CIVIL

Security Testing and Evaluation (continued)

- *Classical Security Testing Method*
  - *Validate tests with Designated Accrediting Authority or designee if possible prior to certification/acceptance testing*
  - *Store tests in a test library for future use (e.g., new releases of software, patch testing, new systems)*
  - *Retain test results for auditors*
    - *Some tests require test data*
    - *Test rerun/expected results problem*

Penetration Testing

- *Definition – Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.*[4]
- *Process*
  - *Planning and Preparation*
    - *Authority*
    - *Reconnaissance*
    - *Vulnerability Identification and Prioritization*
    - *Tactical Planning*
    - *Weaponization*
    - *Delivery/Penetration*

Penetration Testing (Continued)

- *Process (Continued)*
  - *Assessment*
    - *Exploitation*
    - *Installation*
    - *Command and Control*
    - *Actions on Objectives*
  - *Reporting and Cleanup*
    - *Prepare and Present Findings*
    - *Clean up all pen testing artifacts*

Fuzz Testing or Fuzzing

- *History*
  - *Professor Barton Miller, Univ. of Wisconsin, 1988 class project*
  - *Software testing technique that automatically inputs invalid, random, unexpected data to software to determine it's reaction. (e.g., where software expects 1-12 alphabetic characters for username fuzzer automatically inputs 0-2K of random alphanumeric and special characters or non-ascii characters)*
  - *Originally tested operating system command line input handling then progressed to GUI tools, APIs and network protocols*
    - o *Good for testing software that has no control over input*
    - o *Can test simple features but not complex software code*

Fuzz Testing (Continued)

- *Features*
  - *Good for testing software that has no control over input*
  - *Used to test simple features but not complex software code*
  - *Fuzzer Technology Still Requires High Level of Skill to Use*
    - *Individual Fuzzers For Each Protocol or Application*
    - *Requires Deep Protocol or Application Knowledge & Software Development Skills*
  - *Free & Open Source Fuzzing Software is Free Not Open Source*

Bibliography

1. FAIRWIKI, The Definitive Guide to the Factor Analysis of Information Risk (FAIR) Risk Landscape Components, http://fairwiki.riskmanagementinsight.com/?page_id=10
2. Sherwood, J., Clark, A., Lynas, D. (2005). *Enterprise security architecture: A business-driven approach*. San Francisco:CMP*Books.*
3. Kissel, R., Stine, K., Sholl, M., Rossman, H., Falsing, J. & Gulik, J. (2008). *Security considerations in the system development life cycle*. Gaithersburg, MD 20899-8930:NIST Special Publication 800-64 Rev. 2. National Institute of Standards and Technology, U.S. Dept. of Commerce.
4. Committee on National Security Systems. (2003). *National information assurance glossary: CNSS Instruction No. 4009.* Ft Meade, MD:CNSS Secretariat (142), National Security Agency, U.S. Dept. of Defense.