Please accept the attached document with cover letter in response to the NICE Framework Request for Comments.

Regards,
Jim Whitmore

ATTACHMENT: C&IS Knowledge & Curriculum Outline V1.0

13 January 2020

National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: NICE Framework Request for Comments

This letter and attached document are provided in response to the Request for Comments to the National Initiative for Cybersecurity Education (NICE)[1].

This response focuses on topics #3 and #4 in the section *Improvements to the NICE Framework*, namely: "Share any key concepts or topics missing from the current NICE Framework", and "Describe how the NICE Framework can be more useful to a variety of audiences (i.e. employers, employees, education and training providers, learners, small enterprises, etc.)".

My recommendation is to supplement the current NICE Workforce Framework document[2] with a reference resource covering cybersecurity concepts and practices. A cybersecurity knowledge reference would serve several purposes: it would foster consistency in academic and professional training programs; it would enable synergy of skills across job roles; and, it would guide businesses, agencies and enterprises to adopt mature cybersecurity programs.

A document entitled *Cyber and Information Security: An Outline for Academic Study and Professional Practice* is attached. This exemplar identifies and organizes important knowledge areas and activities associated with cybersecurity roles. The content represents applied knowledge and experience from a career in systems engineering, information technology architecture and independent research. It forms the basis or a multi-course curriculum offered several times in a cross-discipline undergraduate program. This material can be a valuable resource in delivering education and training, as well as, in implementing enterprise cybersecurity programs.

I am open to further discussion about the content and how it can be improved.

Regards,

Jim Whitmore, B.S.E.E, M.S., IEEE, ACM
Distinguished Certified Information Technology Architect (The Open Group)
Adjunct Faculty for Computer Science, Dickinson College, Carlisle PA
Email: jjwhitmore@computer.org LinkedIn: www.linkedin.com/in/whitmorejim

ATTACHMENT: C&IS KNOWLEDGE & CURRICULUM OUTLINE V1.0

[1] https://www.nist.gov/news-events/news/2019/11/nist-seeking-input-updates-nice-cybersecurity-workforce-framework
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Cyber and Information Security: An Outline for Academic Study & Professional Practice

J. Whitmore

Version 1.0

13 January 2020

1 Table of Contents

2 Introduction

2.1 Description

This document contains an outline of knowledge areas and related curriculum for the study and practice of Cyber and Information Security.

2.2 Rationale

Computing has evolved from isolated data centers to interconnected networks and global sharing of information built upon an open computing supply chain. The practice of Cyber and Information Security has grown as a patchwork discipline of process, tool, terminology and guidance that are mapped to organizational roles.

Addressing the technical and business aspects of Cyber and Information Security in a coordinated way requires a unifying paradigm of thought and a common set of reference materials that engages multiple organizational roles and disciplines.

This outline and curriculum offer the foundational concepts for a cohesive, cross-discipline course of study that is applicable to all organizations and organizational roles.

2.3 Notes

1. The outline on the following pages organize cybersecurity knowledge into three perspectives: Cyber Thinking, Cyber Enterprises and Cyber Systems. The concepts and terminology used throughout are assembled from authoritative sources including the Glossary by the Committee on National Security Systems.

2. The knowledge outline has been implemented in a curriculum consisting of two undergraduate special topics courses as described in Appendix A, with learning objectives and content to fit technical and non-technical audiences. The courses leverage material from well-known authoritative sources as listed in the References Appendix B.

3. The knowledge outline includes a section entitled *Advanced topics* that represents a detailed treatment of highly technical material. This content is integrated into the existing courses as appropriate. It is also the subject of ongoing research.

3 Cyber and Information Security Knowledge Outline

3.1 Basic Concepts

3.1.1 The Internet

1) What is the Internet?
2) What are the origins of the Internet?
3) How is the Internet is governed?

3.1.2 Interconnected Systems

1) What is meant by "interoperability"?
2) What are the elements of Interconnected Systems?
3) What makes "interoperability" among computer systems and services possible?
4) Provide examples of standards and guidelines related to interoperability.

3.1.3 Cyber & Information Security

1) What is Cyberspace?
2) What is the relationship between the Internet and Cyberspace?
3) What is the value of Cyberspace?
4) What is Cybersecurity?
5) What is Information Security?
6) Why are Cyber and Information Security important?

3.1.4 Motivations for Cyber & Information Security

1) What are the recent statistics and trends for Cyber and Information Security?
2) What are the top targeted industries?
3) What are the costs of Cybersecurity breaches? Globally? By industry?
4) How long did it take, on average, for an organization to discover and contain cyber breaches?
5) How many vulnerabilities in commercial-off-the-shelf IT products and services have been reported to NIST in the past 10 years?
6) What percentage of data breaches were caused by… Malicious or criminal attack? System Glitch? Human Error?
7) Who are the perpetrators of cyber-attacks?
8) What are the relative costs of fixing vulnerabilities at various stages of information system lifecycle? Implementation phase vs. design phase? Testing phase vs. design phase? Production vs. Design phase?
9) What is the impact and consequence of cyber insecurity on Nation states? Businesses? Industries? Populations?

3.1.5 Exploring Cybersecurity in Three Perspectives

1) **Cyber Thinking**: A view of relationships and dependencies among people, process, technology and information within environments where adversarial behavior is present.
2) **Cyber Enterprises**: A view of how organizations approach cybersecurity.
3) **Cyber Systems**: A view of information systems, information technologies, system management processes, security controls and security countermeasures.

3.2 Perspective 1: Cyber Thinking

3.2.1 A Reference Model for Security

1) Identify sources of security knowledge.
2) Describe a General Model for Security.

3.2.2 Owners, Assets and Operating Environments

1) Identify Owners, Organizational Roles and Other Parties.
2) Describe Assets: Information; Information Systems; Tangible Assets; Intangible Assets.
3) Describe Operating Environments.

3.2.3 Threat Actors, Threat Agents, Threats, Attacks and Abuses

1) Define Threat Actors and Threat Agents.
2) Define Threats and Attacks.
3) Explain Vulnerabilities, Weaknesses and Abuses.
4) Define Attack Surface.

3.2.4 Relationships & Dependencies

1) Explain the relationships between Owners, Roles and Assets.
2) Explain the relationships between Threat Agents, Threat Actors and Assets.
3) Explain Adversaries and Adversarial Behaviors.

3.2.5 Risk, Risk Analysis, Risk Mitigation and Risk Tolerance

1) Define Risk.
2) Describe dimensions of Risk.
3) Describe a Risk Analysis Process.
4) Explain Risk Tolerance.
5) Explain the concept of Risk Mitigation.
6) Describe ways to mitigate Risk.

3.2.6 Security Controls and Countermeasures

1) Define Governance.
2) Describe types of Governance.
3) Describe types of Security Controls and Security Countermeasures.
4) Explain Defense-in-Depth.

3.3 Perspective 2: Cyber Enterprises

3.3.1 Enterprise and Enterprise Structure

1) Discuss “enterprise” or “organization” as a generic term for any type of business, agency, or affiliated group, e.g., Government, Government Agency, Corporation, Business, Institution, Community, etc.
2) Discuss “enterprise mission” as a generic term for the purpose, charter, etc., of an organization.
3) Discuss “enterprise structure” as a set of functions with relationships and dependencies in an organization, e.g., Division; Operating Unit; Department; Office; etc.
4) Discuss “role” as a set of duties and responsibilities assigned to individuals in an enterprise or organization, e.g., Owners; Stakeholders; Relying Parties; Executives; Line Management; Operations; Employees; etc.

3.3.2 Enterprise Assets and Workloads

3.3.2.1 Enterprise Assets

1) Define Asset.
2) Explain Information Asset.
3) Explain Information Technology Asset.
4) Explain Tangible Assets and Intangible Assets.

3.3.2.2 Enterprise Workloads

1) Describe Enterprise Workloads as a function of enterprise mission.
2) Relate Enterprise Workloads to Business Application Patterns.
    a) Collaboration (User to User; System to System; Process to Process)
    b) Information Aggregation (User to Information; System to Information; Process to Information)
    c) Self-Service (User to Business; System to Business; Process to Business)
    d) Extended Enterprise (Business to Business; Process to Process)
3) Describe Business Application Topologies.
    a) Peer to Peer
    b) Hub and Spoke
    c) Mesh
    d) Linear Sequence

3.3.3 Enterprise Risk and Governance

3.3.3.1 Enterprise Risk

1) Risk for Government enterprises:
    a) National Defense; National Economy; Critical Infrastructure, Public Safety; etc.
2) Risk for Non-Government enterprises:
    a) Loss: Financial; Reputational; Operational; etc.
    b) Liability: Civil; Criminal; Regulatory non-compliance; etc.
3) Information Technology Risk
    a) Confidentiality: Loss of assets; Loss of privacy, etc.
    b) Integrity: Tainted Data; Tainted Systems; Loss of Provenance; Unpredictable Operations, etc.
    c) Availability: Loss of function; Loss of Capability; Loss of Access, etc.

3.3.3.2 Enterprise Governance

1) Describe Types of Governance.
   a) Enterprise Governance, to include: policies, standards and processes that guide and measure the operation of an enterprise against its mission, applicable laws, regulations, contractual agreements, risk tolerances, etc.
   b) Information Technology Governance, to include: policies, standards and processes that guide and measure the operation of information technology organization and systems against its mission, the mission of the enterprise.
   c) other
2) Explain Motivations for Governance.
   a) Internally driven: Organization Mission; Charter; Ethics; Social Responsibility; etc.
   b) Externally driven: Accountability to Stakeholders, Clients, Customers, General Public, etc.
   c) Legal: Criminal Law; Civil Law; Administrative Law; Contractual; Regulatory

3.3.4 Enterprise Security Programs

3.3.4.1 Enterprise Security Policies, Standards and Processes

1) Discuss Enterprise Security Programs: Security Polices, Standards and Processes.
2) List and Explain Enterprise Security Roles.
   a) Policy Maker, Risk Manager, Security Analyst, Security Engineer, Employee, etc.
3) Explain the need for and value of Standards for Cyber and Information Security
   a) Security Standards bodies ISO; NIST; Industry; etc.
   b) Security Standards: ISO/IEC 27001/2; NIST SP800-53R4; etc.
4) Discuss types of Security Controls and Countermeasures in an Enterprise Security Program
   a) Management consisting of policies, standards and processes
   b) Operational consisting of human and programmatic oversight of operational systems and processes
   c) Technical consisting of technology-based mechanisms and components within computers and physical systems and human machine interfaces.

3.3.4.2 Process Controls for Management and Operation

1) Security-related management processes
   a) Organization strategy and situational analysis:
      i) SWOT Analysis: Strengths, Weaknesses, Opportunities, Threats
      ii) OODA Loop: Observe, Orient, Decide, Act
      iii) CSF (Cyber Security Framework) process: Identify, Protect, Detect, Respond, Recover
   b) Development & integration IT Systems & Services:
      i) Supply Chain Management & Assurance
      ii) SDLC: Identify, Prioritize, Design, Implement, Test, Revise
   c) Service Management and Incident Response:
      i) MAPE loop: Monitor, Analyze, Plan, Execute
      ii) OODA Loop: Observe, Orient, Decide, Act

3.3.4.3 Process Controls for System Development and Supply Chain

1) Development Lifecycle (SDLC)
   a) Explain Information Systems and Information System Lifecycles.

b) Explain System Development Lifecycle.
c) Identify styles of System and Software Development.
d) Compare and Contrast styles of System and Software Development?
e) Describe security-related activities in System Development Lifecycle.
f) Describe management Controls in the System Development Lifecycle.

2) Supply Chain for Information Technology
   a) Explain the Information Technology Supply Chain.
   b) Describe IT Supply Chain for: Infrastructure; IT Components (HW & SW); IT Services.
   c) Describe management Controls for the IT Supply Chain.

3.3.4.4 Operational Controls and Technical Controls

1) Explain Security Mechanisms & Services (See 3.4.5 for detail).
2) Explain Systems Management Operations (See 3.4.5 for detail).
3) Explain Security Management Operations (See 3.4.5 for detail).

3.3.4.5 Data and Information Security

1) Information Classification and Control
   a) Define Data and Information.
   b) Explain Data & Information Risk.
   c) Explain Data & Information Classification & Control.
      i) Classification of data & information assets.
      ii) Policies and practices for control of data & information.
2) Information Privacy
   a) Define types of data: subject data, system data, operational data, metadata, information.
   b) Explain the lifecycle of data.
   c) Explain data ownership and provenance.
   d) Explain “digital footprint”.
   e) Explain “privacy risk”.
   f) Explain data aggregation.
   g) Explain data analysis and insights.
   h) Explain privacy laws and regulations.
   i) Describe controls for data protection and information privacy.

3.4 Perspective 3: Cyber Systems

3.4.1 Elements of Cyber Systems

1) Discuss Cyber systems as a system of: People, Technology, Process and Information.

3.4.2 People in Roles in Cyber Systems

1) List and describe Information technology related Roles.
2) List and describe IT Security Roles.
3) List and describe Relying Parties.

3.4.3 Cyber System Workloads

1) List and Describe examples of Internet-based Computing Systems.
   a) Enterprise Computing systems
   b) Client-server computing: Two-tier, three-tier and N-tier
   c) Internet Information, Transaction and Collaboration Services
   d) Cloud Computing, e.g., Private Cloud; Public Cloud; Hybrid Cloud
   e) Internet of Things (IoT), e.g., Sensor System, Actuator Systems, Sensor & Actuator Systems, etc.
   f) Industrial Control Systems (ICS), e.g., Supervisory Control and Data Acquisition (SCADA), Program Logic Controller (PLC), etc.
2) Explain Information Technology Topologies.
   a) Mesh, e.g., Network Routing, Domain Name Service, Message Transfer Systems, etc.
   b) Hub and spoke, e.g., Portal; Marketplace; Social Computing; Groupware; Web Services, IoT, etc.
   c) Fan-in / Fan-out, e.g., IoT, SCADA, PLC, etc.
   d) Linear Sequence, e.g., Supply Chain

3.4.4 Cyber System Processes and Technologies

3.4.4.1 IT Supply Chain Processes & Components

1) Explain IT Supply Chain Standards and Processes.
   a) NIST SP800-53R4 System and Services Acquisition
   b) ISO/IEC 20243 Trusted Technology Provider Standard
2) Explain IT Supply Chain patterns.
   a) Extended Enterprise (Business to Business; Process to Process)
   b) Collaboration (User to User; System to System; Process to Process)
   c) Explain Blockchain
      i) What is Blockchain?
      ii) What are Smart Contracts?
      iii) What Risks and Threats are addressed by Blockchain technology?
      iv) What Risks and Threats are not addressed by Blockchain?
3) Explain Components in Information technology Supply Chain.
   a) Hardware: Chips, Circuitry, System boards, Adapter boards, Hard Drives, Communication, Peripheral Devices
   b) Software: Microcode, Firmware, Bios, Kernel, Device Drivers, Operating Systems, Management and Admin Software, Applications
   c) Integrated Systems: IOT Devices, Storage Systems, Hubs, FW, Routers, Servers, Workstations, Mobile Systems

d) List sources of IT Systems and Components: Internally developed; 3rd party components; Open Source; Outsourced Services.

3.4.4.2 Infrastructure

1) Discuss Critical Infrastructure: Telecommunications; Chemical; Transportation Systems, including: mass transit, aviation, maritime, ground/surface, rail and pipeline systems; emergency services; postal; shipping.
2) Discuss IT Infrastructure: Physical locations, Facilities, Hardware and Communications Systems.
3) Examples of Communications Systems: Cellular: Wide Area Networks (WAN); Wireless Local Area Networks (WLAN or WiFi); Personal Area Networks (PAN); Wireless Sensor Networks (WSN / WSAN); Supervisory Control and Data Acquisition (SCADA).
4) Describe Communications Channels and Paths: wire, wireless, microware, satellite, GPS, etc.

3.4.4.3 IT Networks & Networking (Routing, Addressing & Naming, etc.)

1) Explain Internet Addressing.
   a) Internet Protocol (IP) Addresses are used by the Communications Infrastructure that does the routing from source to destination
2) Explain Internet Naming.
   a) Domain Names: character-oriented names assigned to IP addresses
3) Explain Private vs Public Networks.
   a) Some systems / devices need to be accessible by all on public networks
   b) Homes and enterprises create a network security perimeter
   c) Govt manages IP addresses; Administered by ISPs (Internet Service Providers
4) Describe Firewalls and Explain how they segment and isolate networks.
   a) Packet filter Firewall… rules that allow or deny access
   b) Network Address Translation (NAT) Firewalls… a Packet Filter firewall that changes the IP address in packets from private address to a public address
   c) Proxy Server…. Pretends to be systems on the private side to the destinations on the public side
5) Describe Network Computing Infrastructure.
   a) Information Packets structure and format
   b) Information Packet Sending, Routing & Delivery
      i) Information packets contain source and destination IP addresses
      ii) IP Addresses identify Networks and Hosts
      iii) Routing Tables contain paths from source to destination
      iv) Routing Protocols share status of paths among routers
   c) Domain Name Service
      i) DNS = Domain Name Server or Domain Name System
      ii) DNS Server answers questions from computers to provide the IP address associated with a domain name
      iii) DNS Server answers questions from SMTP Server on where to send emails
   d) Message Transfer Systems
      i) Electronic Mail across the Internet: Simple Mail Transfer Protocol (SMTP)
      ii) Email Addresses have the structure… user @DomainName
      iii) SMTP Servers Transfer email between SMTP Email Servers
      iv) SMTP Servers access Mail Exchange Records from Domain Name Servers

3.4.5 Operational Controls and Technical Controls

1) Explain IT Operational Controls.
   a) Explain the functions, roles and responsibilities in Systems Operations Centers.
   b) Explain the functions, roles and responsibilities in Security Operations Centers.
2) Explain IT Technical Controls.
   a) Explain Security Mechanisms.
   b) Explain Security Services.

3.4.5.1 Identity and Identity Management

1) Describe Identity: Something you have; Something you know; Something you are.
2) Describe forms of Identity: for human actors; for non-person entities.
3) Describe Identity Lifecycles.
4) Explain Identity lifecycle processes for human actors; for non-person entities.
5) Explain Identify Verification Systems.
6) Explain and provide examples of directories: System Files & Registries; LDAP.
7) Explain Federated Identity.

3.4.5.2 Access Control and Access Management

1) Explain elements of Access Control: Identification, Authentication, Authorization.
2) Explain Single and Multi-Factor Authentication.
3) Explain Mandatory and Discretionary Access Control.
4) Explain ways to evaluate Access Control policies.
5) Explain Privileges and Permissions, Access Control Lists, Authorization Matrix.

3.4.5.3 System & Network Integrity

1) Explain Software and System Flaw Prevention & Flaw Remediation.
2) Explain System Hardening.
3) Explain Segmentation and Isolation: facilities; rooms; networks; systems; software execution. environments; information
4) Explain Monitoring and Alerting and Audit Management: facilities; rooms; networks; systems; software execution environments; information

3.4.6 Information Protection

1) Describe protection of data at rest.
2) Describe protection of data in motion.
3) Describe the role of cryptography in data protection.
4) Describe how access control and data protection are related.

3.4.6.1 Information Flow Controls

1) Explain Communication Paths and Communication Path protections.
2) Explain Communications Channels and Communication Channel protections.
3) Explain endpoint identity and authentication.

3.4.6.2 Information Integrity Controls

1) Explain Message Digests.
2) Explain Secure Hash Algorithms.
3) Explain Data Signing and Verification.

3.4.6.3 Cryptography as a Security Control

1) Explain the elements of cryptography: algorithms; keys and key management.
2) Explain uses for cryptography.
   a) Confidentiality
   b) Access Control for data at rest and data in motion
   c) Data integrity mechanisms

3.4.7 Security Controls Strategy, Implementation and Verification

1) Explain IT Risk Management Strategies.
   a) Risk Awareness
   b) Strong Security Controls and Countermeasures
   c) Defense-in-Depth
   d) Minimum Attack Surface
   e) Operational Monitoring
   f) Rapid Detection and Response
   g) Vulnerability and Incident Management
   h) Continuous Improvement

2) Explain IT Risk Management Implementation.
   a) Management Controls
   b) Operational Controls
   c) Technical Controls
   d) Audit and Accountability

3) Explain IT Risk Management Verification.
   a) Compliance Reviews
   b) Technical Assessments
   c) Certification & Accreditation
   d) Signing & Signature Verification

3.5 Advanced Topics

3.5.1 Security Analysis in Enterprise Security Programs

3.5.1.1 Management Focused Security Analysis

1) List types of enterprise-oriented security analysis activities.
   a) Enterprise Business Risk Assessment
   b) Enterprise IT Risk Assessment
   c) Emergency/Incident Response
   d) Forensic Analysis

3.5.1.2 Systems Development Focused Security Analysis

1) List types of System Development-oriented security analysis activities.
   a) Development Threat Assessments: Threat Analysis/Modeling; Attack Analysis/Model
   b) Penetration Test & Ethical Hacking

3.5.1.3 Operations Focused Security Analysis

1) List types of Operations-oriented security analysis activities.
   a) Operational IT Risk Assessment
   b) Vulnerability & Incident Management
   c) Emergency/Incident Response
   d) Forensic Analysis

3.5.2 Security Analysis Practices and Methods

3.5.2.1 Security Analysis Practices

1) Enterprise IT Risk is a forward-thinking assessment of the intersection of business concerns with information technology concerns
2) Operational IT Risk is an introspective evaluation of the effectiveness of deployed policies, standards and practices that are intended to control risk
3) Threat Analysis/Model is an interpretation of Enterprise IT Risk that is often used in designing and assessing IT systems. Threat Models begin with a statement of risk and risk tolerance. Risks are associated with threats. Threats are organized by severity and likelihood. Threats are assigned a relevance based on risk tolerance. Mitigations are prescribed based on how threats may be realized. Risk Mitigation Plans based on Threat Models are validated by creating attacks that out-think the Threat Model.
4) Attack Analysis/Model is a statement of the impact of known attacks on an organization and its IT systems. Attack Models generally begin with a corpus of known attacks and attacker behaviors. Attacks are organized by relevance to the function of the target system. Attack scenarios are ranked by impact. Mitigations are assigned based the extent to which risk can be reduced. Risk Mitigation Plans based on Attack Models are validated by confirming the effectiveness of controls and countermeasures against attacks.

3.5.2.2 Security Analysis Methods

1) Informal Methods – Skills on Hand, often uses: Statistical Analysis
2) Formal Methods – Mathematical Proof, often for special purpose systems, to include: cryptography, OS Kernel

3) Engineering Methods – Optimized based on numerous conflicting requirements and constraints. Often uses: Fault Analysis, Structural Analysis, Scenario Analysis, Risk Analysis
4) Compare and Contrast Informal, Formal and Engineering Methods.
   a) Informal Methods are not well suited for cybersecurity because the output may vary from analyst to analyst or system to system; plus, adversaries do not follow to statistics
   b) Formal Methods are not well suited for cybersecurity because cyber systems are too complex and there are too many variables.
   c) Engineering Methods are technical well-suited for cybersecurity, however, when the analysis is done manually, time of analysis becomes an obstacle for most cyber systems.

3.5.2.3 Security Analysis Maturity Model

1) Level 1: Human Driven Analysis
2) Level 2: Automation Assisted Analysis
3) Level 3: Algorithmic Analysis
4) Level 4: Machine Learning
5) Level 5: Autonomous

3.5.3 Adversarial Thinking and Model Driven Attack Analysis

3.5.3.1 Adversarial Thinking

1) Explain Adversarial Thinking
2) Discuss the roles of Blue Teams and Red Teams in Enterprise Security Programs

3.5.3.2 Model Driven Attack Analysis

1) Explain the Nature of Cyber Conflict in terms of Attacker behaviors and Security Controls.

$$\textbf{Attacker behavior vs Controls}_{[\text{Supply Chain}]} + \textbf{Controls}_{[\text{SDLC}]} + \textbf{Controls}_{[\text{System Operations}]}$$

2) Explain Attacker Behaviors.
   a) Attack Use Case is a Data Object that joins information from several data sources.

$$\textbf{AttackUseCase} = (\text{Actor, Action, Target, Objective, Tactics, Result, Risk Index})$$

   b) Attack Scenario is a grouping of Attacks mapped to a set of phased objectives.

$$\textbf{AttackScenario}_i = (\text{Attack}_1, \text{Attack}_2, \text{Attack}_3, \text{Attack}_4)$$

   c) Attack Campaign is a grouping of Attack Scenarios.

$$\textbf{AttackCampaign}_j = (\text{AttackScenario}_1, \ldots, \text{AttackScenario}_n)$$

3) Explain Attack Patterns and attack-related data.
   a) Attack Patterns are data objects defined in the Mitre Common Attack Pattern Enumeration Catalog (CAPEC).
   b) Attack related data: known defects; known techniques & tactics, known controls, etc. from Mitre CWE, Mitre ATT&CK, NIST SP800-53R4, NIST National Vulnerability Database, etc.
   c) Attack related meta-data: attack vectors, mitigation potential, architectural decisions, etc.

3.5.3.3 Attack Domains and Attack Objectives

1) List and Describe Attack Domains.
   a) Attack Domains are Categories derived from domain overlay in Mitre CAPEC: Supply Chain; Physical Security; Communications; Hardware; Software; Social Engineering
2) List and Explain Attacker Objectives for each Attack Domain.
   a) IT Supply Chain: Taint Hardware or Software; Theft of Assets; Expose Sensitive Information.
   b) Infrastructure (Physical, Hardware and Communications): Theft of Assets; Expose Sensitive Information; Obstruct or Deny Service.
   c) Networking: Expose Sensitive Information; Obstruct or Deny Service; Take Control of System or Device.
   d) Network Computing: Expose Sensitive Information; Obstruct or Deny Service; Take Control of System or Device.
   e) Software & Applications: Expose Sensitive Information; Obstruct or Deny Service; Take Control of System or Device.
   f) Social Engineering: Affect Thinking and Judgement; Taint Hardware or Software; Expose Sensitive Information; Theft of Assets; Obstruct or Deny Service; Take Control of System or Device.

3.5.3.4 Attack Enumeration and Visualization

1) Describe Attack Maps as an organized group of Attacks and Attack Scenarios
2) Describe Attack Trees as a subset of an attack map that is relevant to a cyber system
3) Describe Attack Graph as a prioritized Attack Tree

4 Appendix A: Cyber and Information Security Curriculum Outline

4.1 Introductory Course: Cyber and Information Security

Course Description: Cybersecurity incidents represent a serious threat to governments, organizations and individuals. This course will explore the concepts and concerns that guide business executives, policy makers, and information technology professionals to address risks to computer systems and sensitive information. After reviewing industry, national and international security standards and practices, students will have the opportunity to analyze recent high impact incidents and craft cybersecurity plans for organizations and software development life cycles.

Learning Objectives: At the completion of this course successful students will demonstrate knowledge, presentation and writing skills for:

1) Cybersecurity Concepts, Standards and Models
2) Cybersecurity Risk
3) Cybersecurity Plans for Enterprises and Software Development
4) Information Technology and Internet Computing
5) Trustworthy Computing
6) Emerging Topics

Instructional Methods: Lectures describing Technical and Theoretical Concepts; Class discussions of Readings and Reference Materials; Student presentations; Online Analytical Tools

Course Prerequisites: Introduction to Computing (recommended)

Course Outline:

1) Unit 1: Concepts
2) Unit 2: Cyber Thinking
3) Unit 3: Cyber Enterprises
4) Unit 4: Elements of Cyber Systems

Audiences:

1) Academic
   a) Undergraduate Computer Science students
   b) Undergraduate non-Computer Science College students
2) Professional
   a) Software Engineers, Security Analysts,
   b) Business Manager, Policy Maker

4.2 Advanced Course: Cybersecurity Lecture/Lab

Course Description: Modern network connected devices are increasingly subject to malicious or unintentional threats that can affect system availability, integrity and the confidentiality of sensitive information. This course explores the topic of cybersecurity from a software designer's perspective. The lectures will investigate methods for threat analysis. The lab exercises will demonstrate a range of security related functions, flaws and mitigations that software developers need to consider when building software systems that operate in networked environments.

Learning Objectives: At the completion of this course, successful students will demonstrate knowledge and skill for:

1) Adversarial Thinking: Red Team / Blue Team roles
2) Applied Security Analysis
3) System configuration and operation in a lab environment
4) Configuration and Operation of security controls and countermeasures in a lab environment
5) Security attacks & attack mitigations in a lab environment
6) Emerging Topics

Instructional Methods: Lectures describing Technical and Theoretical Concepts; Lab Exercises; Class discussions; Lab Exercises, Online Analytical Tools

Course Prerequisites: Introduction to Computing; Programming Languages; Coding; Data Structures; Operating Systems; Networking

Course Outline:

1) Unit 1: Review of Concepts; Cyber Thinking; Cyber Enterprises; Elements of Cyber Systems
2) Unit 2: Analytical Methods; Adversarial Thinking; Security Analysis Methods
3) Unit 3: Cyber System Technologies: Lectures & Labs
4) Unit 4: Cyber System Vulnerabilities, Weaknesses, Controls & Countermeasures: Lectures & Labs

Audiences:

1) Academic: Undergraduate Computer Science students
2) Professional: Software Engineers, Security Analysts

5 Appendix B: References

[1] Cybersecurity Curricula 2017: *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Joint Task Force (JTC) on Cybersecurity Education. Version 1.0. December 2017. https://www.csec2017.org/

[2] Curricular Foundations for Cybersecurity. Sobel, A., Parrish, A., Raj, R. IEEE Computer Magazine., April 2019. DOI: 10.1109/MC.2019.2898240

[3] National Initiative on Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice

[4] National Cybersecurity Center of Excellence (NCCoE). https://www.nccoe.nist.gov/

[5] Trusted CI. The NSF Cybersecurity Center of Excellence. National Science Foundation (NSF). https://trustedci.org/

[6] Trust in Cyberspace. National Research Council. 1999. Washington, DC. National Academies Press. https://www.nap.edu/catalog/6161/trust-in-cyberspace

[7] Instruction 4009: Glossary. Committee on National Security Systems (CNSS). 2015. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

[8] National Vulnerability Database (NVD). National Institute of Standards and Technologies (NIST). https://nvd.nist.gov/

[9] Common Attack Pattern Enumeration and Classification (CAPEC). Mitre Corporation. http://capec.mitre.org/

[10] Common Weakness Enumeration (CWE). Mitre Corporation. http://cwe.mitre.org/

[11] Attack Knowledgebase (ATT&CK). Mitre Corporation. https://attack.mitre.org/

[12] Common Criteria. Part 1 General Model, Version 3.1. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[13] Common Criteria. Part 2 Security Functional Components, Version 3.1. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[14] Common Criteria. Part 3 Security Assurance Components, Version 3.1, p. 95. https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[15] Common Criteria. Certified Products List & Statistics. https://www.commoncriteriaportal.org/products/stats/

[16] Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technologies (NIST). https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

[17] ISO/IEC 27002:2013. Security Controls. 2013. Information technology -- Security techniques -- Code of practice for information security controls. https://www.iso.org/standard/54533.html

[18] ISO/IEC 20243:2018. Trusted Technology Provider Standard. Mitigating maliciously tainted and counterfeit products -- Part 1: Requirements and recommendations https://www.iso.org/standard/74399.html

[19] Thompson, M., Irvine, C. *Individualizing Cybersecurity Lab Exercises with Labtainers*. IEEE Security and Privacy. March/April 2018. https://www.computer.org/csdl/mags/sp/2018/02/msp2018020091.html

[20] Patterns for e-business: A Strategy for Reuse. Jonathan Adams, Srinivas Koushik, George Galambos, Guru Vasudeva. IBM Press, 2001. ISBN:978-1-931182-02-7.

[21] Security and E-Business: Is There a Prescription? Jim Whitmore. 1998. 21st National Information Systems Security Conference, Arlington, Virginia. http://csrc.nist.gov/nissc/1998/proceedings/paperD13.pdf

[22] A method for designing secure solutions. JJ Whitmore - IBM systems Journal, 2001. Volume: 40, Issue: 3, pp 747–768. https://ieeexplore.ieee.org/abstract/document/5386938

[23] Policy-Based Automation in the Autonomic Data Center. D Kaminsky, B Miller, A Salahshour, J Whitmore. 2008 International Conference on Autonomic Computing, pp 209-210. https://ieeexplore.ieee.org/abstract/document/4550847

[24] Threat Analysis in the Software Development Lifecycle. J. Whitmore, S. Türpe, S. Triller, A. Poller, C. Carlson. *IBM Journal of Research and Development*, vol. 58, no. 1, Jan.-Feb 2014. https://ieeexplore.ieee.org/document/6717070

[25] Improving Attention to Security in Software Design with Analytics and Cognitive Techniques. Jim Whitmore, William Tobin. *Cybersecurity Development (SecDev) 2017 IEEE*, pp. 16-21, 2017. https://ieeexplore.ieee.org/document/8077801