Appendix 16 – Alignment Document

Cybersecurity CTAG Alignment

This document contains information about one proposed Career-Technical Articulation Numbers (CTANs) for the proposed Information Technology Career-Technical Assurance Guide (CTAG).
The CTANs are:

1. Cybersecurity Fundamentals

1. Cybersecurity Fundamentals Potential CTAN alignment with the Information Technology Pathway in the Career Field Technical Content Standards of the Ohio Department of Education.

General Course Description: This course will provide the student with basic knowledge of cyber security dynamics and is designed to be the entry point for students desiring to major in Computer Security Systems. The course will address issues involving hackers, malware, social theories, protocols, firewalls, and intrusion detection. In addition, this course will discuss the prevention and containment of intrusion incidents, the incident response process, and the forensic examination of a computer.

Advising Notes*:*

- Must access credit within 3 years of program completion

Proposed Semester Credit Hours: 3

Proposed Alignment:

Proposed Learning Outcomes The student will be able to:	Competencies and/or Descriptors from the Information Technology Pathway of the Career Field Technical Content Standards
1. Discuss the social theories of computer-enabled abuse and the role of compliance framework in mitigating abuse.	9.1.1 Identify the goals, objectives and purposes of Cyber Security. 9.1.2 Describe the concepts of malware attack vectors. 1.12.2 Differentiate between appropriate and inappropriate information 1.12.3 Interpret security policies through job specific training, and training updates 9.1.3 Maintain data security using data labeling, handling, and disposal as prescribed by policy and law 1.12.4 Apply secure password behavior 1.12.5 Apply physical and virtual situational awareness (e.g., clean desk policies, shoulder surfing, social engineering, tailgating) 9.1.4 Mitigate threats by remaining abreast of industry information 9.1.5 Identify types of controls (e.g., Deterrent, Preventive, Detective, Compensating, Technical, and Administrative 9.2.1 Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions).
2. Discuss the malicious user's motivation such as social engineering and cyber warfare.	9.3.1 Identify Application Vulnerabilities (e.g. Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Integer overflow, Zero-day, Cookies and attachments, Locally Shared Objects (LSOs), Flash cookies, Malicious add-ons, Session hijacking, Header manipulation, Arbitrary code execution/remote code execution).
3. Compare worms, trojans, viruses, spyware and other types of malicious software.	9.5.1 Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware). 9.5.2 Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks). 9.5.3 Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid Birthday attacks, rainbow tables). 9.5.4 Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole).
4. Evaluate how encryption can be used and abused.	9.4.7 Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators). 9.4.5 Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures).

	9.4.6 Use of algorithms/protocols with transport encryption (e.g.,SSL, TLS,IPSec ,SSH ,HTTPS)
5. Describe standard communication protocols.	9.5.1 Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware). 9.5.2 Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks). 9.5.3 Configure defenses for Password attacks (e.g., Brute Force, Dictionary attacks, Hybrid Birthday attacks, rainbow tables). 9.5.4 Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole). 9.7.1 Recognize digital reconnaissance techniques (e.g., packet capture, OS fingerprinting, topology discovery, DNS harvesting). 9.4.2 Secure use of network Protocols (e.g., IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SCP, ICMP). 9.4.3 Apply principles of IPv4 and IPv6 securely. 9.7.4 Collect digital evidence according to established policies and protocols (e.g., system image, packet captures).
6. Categorize various types of network and computer attacks.	9.5.1 Locate and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware). 9.5.2 Discover vulnerabilities to and mitigate network attacks. (e.g.,Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks).
7. Compare Firewalls, intrusion detection and intrusion prevention.	9.2.7 Inventory devices 9.3.4 Implement secure application configuration (e.g., Application hardening, Application patch management). 9.3.6 Differentiate between Server-side vs. client-side validation. 9.4.8 Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators) 9.4.10 Monitor and manage network Unified Threat Management.
8. Examine how information security can be used to mitigate cyber-crimes.	9.2.1 Perform authorization control (e.g., least privilege, separation of duties, mandatory access, discretionary access, rule-based access control, role-based access control, time of day restrictions, location distractions). 9.2.2 Implement authentication techniques (e.g., Tokens, Common access card, Smart card, Multifactor authentication, Single sign-on, Biometrics, Personal identification verification card, Username, Federation, Transitive trust/authentication). 9.2.3 Use authentication factors (e.g., Something you are, Something you have, Something you know). 9.2.5 Implement Data Loss Prevention (DLP).

	9.3.6 Differentiate between Server-side vs. client-side validation. 9.4.4 Apply wireless security configurations (e.g., Disable SSID broadcast, TKIP, CCMP, Antenna placement, Power level controls.) 9.4.5 Manage PKI and certificates (Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures). 9.4.6 Use of algorithms/protocols with transport encryption (e.g., SSL, TLS, IPSec, SSH, HTTPS). 9.4.7 Install and configure network devices (firewalls, switches, load balancers, proxies, web security gateways, VPN concentrators). 9.4.8 Install and configure network security devices. 9.4.9 Implement port security. 9.4.10 Monitor and manage network Unified Threat Management. 9.4.11 Mitigate network threats (e.g., Flood guards, Loop protection, Implicit deny, Network separation, Log analysis, Unified threat management, peripheral, and removable media). 9.4.12 Apply the principles of secure Network Design (e.g., DMZ, Subnetting, NAT/PAT, Remote access, Telephony, Virtualization).
9. Create a plan to defend against cyber-attacks.	9.5.1 Describe, locate, and mitigate security threats (e.g., Adware, Viruses, Spyware, Trojan, Rootkits, Logic bomb, Botnets, Ransomware, Polymorphic malware). 9.5.2 Describe and discover vulnerabilities to and mitigate network attacks. (e.g., Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Spit and other attacks). 9.5.4 Describe, appraise for, and mitigate Social Engineering attacks (e.g., Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Phishing, Spear Phishing, Whaling, Vishing, Principles, URL hijacking, Watering Hole). 9.8.1 Design and implement network segmentation 9.8.2 Differentiate between detection controls and prevention controls (e.g., IDS vs. IPS, Camera vs. guard). 9.8.3 Use discovery tools and utilities to identify threats (e.g., Protocol analyzer, Vulnerability scanner, Honeypots, Honeynets, Port scanner). 9.8.4 Create, edit, and use roles and system management tools 9.8.5 Implement endpoint security 9.8.6 Implement Access Control Lists (ACL). 9.8.7 Deploy a server hardening plan. 9.8.8 Implement a Network Access Control (NAC) plan. 9.8.9 Interpret alarms and alert trends. 9.8.10 Apply incident response procedures (e.g., Preparation, Incident identification , Escalation and notification , Mitigation steps, Lessons learned, Reporting, Recovery

	procedures, First responder, Incident isolation, Quarantine, Device removal, Data breach). 9.8.11 Differentiate between types of Penetration testing (e.g., Black box, White box, Gray box).