Wayne County Generation Cyber Curriculum
Crosswalk
NICE Workforce

Wayne County Generation Cyber utilized the National Cybersecurity Workforce Framework as a curriculum design for the Cybersecurity Program. The KSA's identified by the National Initiative for Cybersecurity Education (NICE) were then mapped to both the Securely Provision and Operate and Maintain domains. WCCCD Skills Commons contribution are for the Network + and Security + curriculum.

Network+ The domains identified in this document will assist student preparation for the CompTIA Network+ exam and the TestOut Network Pro exam.	**NICE Area - Securely Provision KSAs**	**NICE Area - Operate and Maintain KSAs**
1.0 Network Architecture		
1.1 Compare the layers of the OSI and TCP/IP models.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. NICE organizes cybersecurity into seven high-level categories*: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on *are Securely Provision and Operate and Maintain*. The KSAs for Network Architecture that align with each of the **Securely Provision** specialty areas (see below) are identified in the National Cybersecurity Workforce	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. *Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on are *Securely Provision and Operate and Maintain*. The KSAs for Network Architecture that align with each of the **Operate and Maintain** specialty areas (see below) are identified in the National Cybersecurity
1.2 Classify how application, devices, and protocols relate to the OSI model layers.		
1.3 Explain the purpose and properties of IP addressing.		
1.4 Explain the purpose and properties of routing and switching.		
1.5 Identify common TCP and UDP default ports.		

1.6 Explain the function of common networking protocols.	identified in the National Cybersecurity Workforce Framework included in this section. **Secure Acquisition** **Software Engineering** **System Security Architecture** **Technology Research & Development** **Systems Requirement Planning** **Test & Evaluation** **System Development**	identified in the National Cybersecurity Workforce Framework included in this section. **Data Administration** **Customer Service & Technical Support** **Network Services** **System Administration** **System Security Analysis**
1.7 Summarize DNS concepts and its components.		
1.8 Given a scenario, implement the network troubleshooting methodology.		
1.9 Identify virtual network components.		
2.0 Network Operations		
2.1 Given a scenario, install and configure routers and switches.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. NICE organizes cybersecurity into seven high-level categories*: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on *are Securely Provision and Operate and Maintain*. The KSAs for Network Operations that align with each of the **Securely Provision** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Secure Acquisition** **Software Engineering** **System Security Architecture** **Technology Research & Development** **Systems Requirement Planning** **Test & Evaluation** **System Development**	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. *Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on are *Securely Provision and Operate and Maintain*. The KSAs for Network Operations that align with each of the **Operate and Maintain** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Data Administration** **Customer Service & Technical Support** **Network Services** **System Administration** **System Security Analysis**
2.2 Given a scenario, install and configure a wireless network.		
2.3 Explain the purpose and properties of DHCP: Static vs. dynamic IP addressing, Reservations, Scopes, Leases, Options.		
2.4 Given a scenario, troubleshoot common wireless problems.		
2.5 Given a scenario, troubleshoot common router and switch problems.		
2.6 Given a set of requirements, plan and implement a basic SOHO network.		
3.0 Network Media		

3.1 Categorize standard media types and associated properties: Fiber, Copper, Plenum vs. non-plenum, media converters, broadband over powerline.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. NICE organizes cybersecurity into seven high-level categories*: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. *Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas.
3.2 Categorize standard connector types based on network media: Fiber (ST, SC, LC, MT-RJ), Copper (RJ-45, RJ-11, BNC, F-connector, DB-9 (RS-232), Patch panel, 110 block (T568A, T568B).		
3.3 Compare and contrast different wireless standards: 802.11 a/b/g/n standards (Distance, Speed, Latency, Frequency, Channels, MIMO, Channel bonding).	The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on *are Securely Provision and Operate and Maintain*. The KSAs for Network Media that align with each of the **Securely Provision** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Secure Acquisition** **Software Engineering** **System Security Architecture** **Technology Research & Development** **Systems Requirement Planning** **Test & Evaluation** **System Development**	The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on are *Securely Provision and Operate and Maintain*. The KSAs for Network Media that align with each of the **Operate and Maintain** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Data Administration** **Customer Service & Technical Support** **Network Services** **System Administration** **System Security Analysis**
3.4 Categorize WAN technology types and properties: Types (T1/E1, T3/E3, DS3, OCx, SONET, SDH, DWDM, Satellite, ISDN, Cable, DSL, Cellular, WiMAX, LTE, HSPA+, Fiber, Dialup PON, Frame relay, ATMs), Properties (Circuit switch, Packet switch, Speed, Transmission media, Distance).		
3.5 Describe different network topologies: MPLS, Point to Point, Point to Multipoint, Ring, Star, Mesh, Bush, Peer-to-peer, Client-server, Hybrid.		
3.6 Given a scenario, troubleshoot common physical connectivity problems: Cable problems (Bad connectors, Bad wiring, Open, short, Split cables, DB loss, TXRX reversed, Cable placement, EMI/interference, Distance, Cross-talk.		

3.7 Compare and contrast different LAN technologies: Types (Ethernet, 10BaseT, 100BaseT, 1000BaseT, 100BaseTX, 100BaseFX, 1000BaseX, 10GBaseSR, 10GBaseLR, 10GBaseER, 10GBaseSW, 10GBaseLW, 10GBaseEW, 10GBaseT), Properties (CSMA/CD, CSMA/CA, Broadcast, Collision, Bonding, Speed, Distance).		
3.8 Identify components of wiring distribution: IDF, MDF, Demarc, Demarc extension, Smart jack, CSU/DSU.		
4.0 Network Troubleshooting		
4.1 Explain the purpose and features of various network appliances: Load balancer, Proxy server, Content filter, VPN concentrator.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. NICE organizes cybersecurity into seven high-level categories*: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on *are Securely Provision and Operate and Maintain*. The KSAs for Network Troubleshooting that align with each of the **Securely Provision** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Secure Acquisition**	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. *Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on are *Securely Provision and Operate and Maintain*. The KSAs for Network Troubleshooting that align with each of the **Operate and Maintain** specialty areas (see below) are identified the National Cybersecurity Workforce Framework included in this section. **Data Administration** **Customer Service & Technical Support** **Network Services** **System Administration**
4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues: Cable tester, Cable certifier, Crimper, Butt set, Toner probe, Punch down tool, Protocol analyzer, Loopback plug, TDR, OTDR, Multimeter, Environmental monitor.		
4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues: Protocol analyzer, Throughput testers, Connectivity software, Ping, Tracert/traceroute, Dig, Ipconfig/ifconfig, Nslookup, Arp, Nbtstat, Netstat, Rout.		

4.4 Given a scenario, use the appropriate network monitoring resources to analyze traffic: SNMP, SNMPv2, SNMPv3, Syslog, System logs, History logs, General logs, Traffic analysis, Network sniffer.	**Secure Acquisition** **Software Engineering** **System Security Architecture** **Technology Research & Development** **Systems Requirement Planning** **Test & Evaluation** **System Development**	**System Administration** **System Security Analysis**
4.5 Describe the purpose of configuration management documentation: Wire schemes, Network maps, Documentation, Cable management, Asset management, Baselines, Change management.		
4.6 Explain different methods and rationales for network performance optimization: Methods (QoS, Traffic shaping, Load balancing, High availability, Caching engines, Fault tolerance, CARP), Reasons (Latency sensitivity, High bandwidth applications (VoIP, Video applications, Unified communications), Uptime.		
5.0 Industry Standards, Practices, and Network Theory		
5.1 Given a scenario, implement appropriate wireless security measures: Encryption protocols (WEP, WPA, WPA2, WPA Enterprise), MAC address filtering, Device placement, Signal strength.	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. NICE organizes cybersecurity into seven high-level categories*: Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on *are Securely Provision and Operate and Maintain*. The KSAs for Network Architecture that align with each of the	The National Initiative for Cybersecurity Education (NICE) identifies Knowledge, Skills and Abilities (KSAs) that align with the certification content area. *Securely Provision, Operate and Maintain, Protect and Defend, Investigate, Collect and Operate, Analyze and Oversee and Govern.* Each comprised of several Specialty Areas. The two high-level categories that Wayne County Generation Cyber (WCGC) focuses on are *Securely Provision and Operate and Maintain*. The KSAs for Network Architecture that align with each of the **Operate and Maintain** specialty areas (see below) are identified in the Cybersecurity Workforce
5.2 Explain the methods of network access security: ACL (MAC filtering, IP filtering, Port filtering), Tunneling and encryption (SSL VPN, VPN, L2TP, PPTP, IPSec, ISAKMP, TLS, TLS2.0, Site-to-site and client-to-site), Remote access (RAS, RDP, PPPoE, PPP, ICA, SSH.		

5.3 Explain the methods of user authentication: PKI, Kerberos, AAA (RADIUS, TACACS+), Network access control (802.1X, Posture assessment), CHAP, MSCHAP, EAP, Two-factor authentication, Multifactor authentication, Single sign-on.	Network Architecture that align with each of the **Securely Provision** specialty areas (see below) are identified in the National Cybersecurity Workforce Framework included in this section. **Secure Acquisition** **Software Engineering** **System Security Architecture** **Technology Research & Development** **Systems Requirement Planning** **Test & Evaluation** **System Development**	Framework included in this section. **Data Administration** **Customer Service & Technical Support** **Network Services** **System Administration** **System Security Analysis**
5.4 Explain common threats, vulnerabilities, and mitigation techniques: Wireless (War driving, War chalking, WEP cracking, WPA cracking, Evil twin, Rogue access point), Attacks (DoS, DDoS, Man in the middle, Social engineering, Virus, Worms, Buffer overflow, Packet sniffing, FTP bounce, Smurf), Mitigation techniques (Training and awareness, Patch management, Policies and procedures).		
5.5 Given a scenario, install and configure a basic firewall: Types (Software, Hardware), Port security, Stateful inspection vs. packet filtering, Firewall rules (Block/allow, Implicit deny, ACL), NAT/PAT, DMZ.		
5.6 Categorize different types of network security appliances and methods: IDS and IPS (Behavior based, Signature based, Network based, Host based), Vulnerability scanners (NESSUS, NMAP), Methods (Honeypots, Honeynets).		