Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
	Secondary Competency Task List	
100	**NETWORK TECHNOLOGIES**	
101	Explain the function of common networking protocols, including TCP,FTP, UDP, TCP/IP suite, DHCP, TFTP, DNS, HTTP(S), ARP, SIP (VoIP), RTP (VoIP), SSH, POP3, NTP, IMAP4, Telnet, SMTP, SNMP2/3, ICMP, IGMP, TLS.	
102	Identify commonly used TCP and UDP default ports, including TCP ports: FTP – 20, 21, SSH – 22, TELNET – 23, SMTP – 25, DNS – 53, HTTP – 80, POP3 – 110, NTP – 123, IMAP4 – 143, HTTPS – 443 UDP ports: TFTP – 69, DNS – 53, BOOTPS/DHCP – 67, SNMP – 161.	
103	Identify the following address formats, including IPv6, IPv4, MAC addressing.	
104	Given a scenario, evaluate the proper use of addressing technologies and addressing schemes, including: Subnetting: Classful vs. classless (e.g. CIDR, Supernetting), NAT, PAT, SNAT, Public vs. private, DHCP (static, dynamic APIPA) Addressing schemes: Unicast, Multicast, Broadcast.	
105	Identify common IPv4 and IPv6 routing protocols, including Link state: OSPF, IS-IS Distance vector: RIP, RIPv2, BGP Hybrid: EIGRP.	
106	Explain the purpose and properties of routing, including IGP vs. EGP, Static vs. dynamic, Next hop, Understanding routing tables and how they pertain to path selection, Explain convergence (steady state).	
107	Compare the characteristics of wireless communication standards, including 802.11 a/b/g/n: Speeds, Distance, Channels, Frequency Authentication and encryption: WPA, WEP, RADIUS, TKIP, AES.	
200	**NETWORK MEDIA AND TOPOLOGIES**	
201	Categorize standard cable types and their properties, including Type: CAT3, CAT5, CAT5e, CAT6 STP, UTP, Multimode fiber, single-mode fiber Coaxial: RG-59, RG-6 Serial Plenum vs. Non-plenum Properties: Transmission speeds, Distance, Duplex, Noise immunity (security, EMI), Frequency.	
202	Identify common connector types, including RJ-11, RJ-45, BNC, SC, ST, LC, RS-232.	
203	Identify common physical network topologies, including Star, Mesh, Bus, Ring, Point to point, Point to multipoint, Hybrid.	
204	Given a scenario, differentiate and implement appropriate wiring standards, including 568A, 568B, Straight vs. cross-over, Rollover, Loopback.	
205	Categorize WAN technology types and properties, including Type: Frame relay, E1/T1, ADSL, SDSL, VDSL, Cable modem, Satellite, E3/T3, OC-x, Wireless, ATM, SONET, MPLS, ISDN BRI, ISDN PRI, POTS, PSTN Properties: Circuit switch, Packet switch, Speed, Transmission.	
206	Categorize LAN technology types and properties, including Types: Ethernet, 10BaseT, 100BaseTX, 100BaseFX, 1000BaseT, 1000BaseX, 10GBaseSR, 10GBaseLR, 10GBaseER, 10GBaseSW, 10GBaseLW, 10GBaseEW, 10GBaseT Properties: CSMA/CD, Broadcast, Collision, Bonding, Speed, Distance.	
207	Explain common logical network topologies and their characteristics, including Peer to peer, Client/server, VPN, VLAN.	
208	Install components of wiring distribution, including Vertical and horizontal cross connects, Patch panels, 66 block, MDFs, IDFs, 25 pair, 100 pair, 110 block, Demarc, Demarc extension, Smart jack, Verify wiring installation, Verify wiring termination.	
300	**NETWORK DEVICES**	
301	Install, configure and differentiate between common network devices, including Hub, Repeater, Modem, NIC, Media converters, Basic switch, Bridge, Wireless access point, Basic router, Basic firewall, Basic DHCP server.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
302	Identify the functions of specialized network devices, including Multilayer switch, Content switch, IDS/IPS, Load balancer, Multifunction network devices, DNS server, Bandwidth shaper, Proxy server, CSU/DSU.	
303	Explain the advanced features of a switch, including PoE, Spanning tree, VLAN, Trunking, Port mirroring, Port authentication.	
304	Implement a basic wireless network, including Install client, Access point placement, Install access point: Configure appropriate encryption, Configure channels and frequencies, Set ESSID and beacon Verify installation.	
400	**NETWORK MANAGEMENT**	
401	Explain the function of each layer of the OSI model, including Layer 1 – physical, Layer 2 – data link, Layer 3 – network, Layer 4 – transport, Layer 5 – session, Layer 6 – presentation, Layer 7 – application.	
402	Identify types of configuration management documentation, including Wiring schematics, Physical and logical network diagrams, Baselines, Policies, procedures and configurations, Regulations.	
403	Given a scenario, evaluate the network based on configuration management documentation, including, Compare wiring schematics, physical and logical network diagrams, baselines, policies and procedures and configurations to network devices and infrastructure, Update wiring schematics, physical and logical network diagrams, configurations and job logs as needed.	
404	Conduct network monitoring to identify performance and connectivity issues, including Network monitoring utilities (e.g. packet sniffers, connectivity software, load testing, throughput testers), System logs, history logs, event logs.	
405	Explain different methods and rationales for network performance optimization, including Methods: QoS, Traffic shaping, Load balancing, High availability, Caching engines, Fault tolerance Reasons: Latency sensitivity, High bandwidth applications; VoIP, Video applications Uptime.	
406	Given a scenario, implement network troubleshooting methodologies, including Information gathering – identify symptoms and problems, Identify the affected areas of the network, Determine if anything has changed, Establish the most probable cause, Determine if escalation is necessary, Create an action plan and solution identifying potential effects, Implement and test the solution, Identify the results and effects of the solution, Document the solution and the entire process.	
407	Given a scenario, troubleshoot common connectivity issues and select an appropriate solution, including Physical issues: Cross talk, Nearing crosstalk, Near End crosstalk, Attenuation, Collisions, Shorts, Open impedance mismatch (echo), Interference Logical issues: Port speed, Port duplex mismatch, Incorrect VLAN, Incorrect IP address, Wrong gateway, Wrong DNS, Wrong subnet mask Issues that should be identified but escalated: Switching loop, Routing loop, Route problems, Proxy arp, Broadcast storms Wireless Issues: Interference (bleed, environmental factors), Incorrect encryption, Incorrect channel, Incorrect frequency, ESSID mismatch, Standard mismatch (802.11 a/b/g/n), Distance, Bounce, Incorrect antenna placement.	
500	**NETWORK TOOLS**	
501	Given a scenario, select the appropriate command line interface tool and interpret the output to verify functionality, including Traceroute, Ipconfig, Ifconfig, Ping, Arp ping, Arp, Nslookup, Hostname, Dig, Mtr, Route, Nbtstat, Netstat.	
502	Explain the purpose of network scanners, including Packet sniffers Intrusion detection software, Intrusion prevention software, Port scanners.	
503	Given a scenario, utilize the appropriate hardware tools, including Cable testers, Protocol analyzer, Certifiers, TDR, OTDR, Multimeter, Toner probe, Butt set, Punch down tool, Cable stripper, Snips, Voltage event recorder, Temperature monitor.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
600	**NETWORK SECURITY**	
601	Explain the function of hardware and software security devices, including Network based firewall, Host based firewall, IDS, IPS, VPN concentrator.	
602	Explain common features of a firewall, including Application layer vs. network layer, Stateful vs. stateless, Scanning services, Content filtering, Signature identification, Zones.	
603	Explain the methods of network access security, including ACL: MAC filtering, IP filtering Tunneling and encryption: SSL VPN, VPN, L2TP, PPTP, IPSEC Remote access: RAS, RDP, PPPoE, PPP, VNC, ICA.	
604	Explain methods of user authentication, including PKI, Kerberos, AAA: RADIUS, TACACS+, Network access control: 802.1x, CHAP, MS-CHAP, EAP.	
605	Explain issues that affect device security, including Physical security, Restricting local and remote access, Secure methods vs. unsecure methods: SSH, HTTPS, SNMPv3, SFTP, SCP; TELNET, HTTP, FTP, RSH, RCP, SNMPv1/2.	
606	Identify common security threats and mitigation techniques, including Security threats: DoS, Viruses, Worms, Attackers, Man in the middle, Smurf, Rogue access points, Social engineering (phishing) Mitigation techniques: Policies and procedures, User training, Patches and updates.	
700	**NETWORK ADMINISTRATION**	
701	Establish and document dial-in procedures for remote users.	
702	Document security requirements and procedures used to protect the network from malicious tampering or accidental damage.	
703	Establish a process to record technical information and regularly update technical documentation to support reliable network performance.	
704	Determine availability of resources assigned to users to maintain access in accordance with network usage policy.	
705	Describe how to disseminate necessary documentation to users to assist them in successfully accessing resources on the network.	
706	Document virus-scanning procedures used to protect the computer system and files from corruption.	
707	Establish, perform and document necessary steps used to successfully implement user backup procedures to avoid data loss.	
708	Develop & maintain an administrative log to document day-to-day network administrative tasks.	
709	Describe how to ensure compliance of network procedures with organizational requirements.	
710	Research and interpret organizational structure to determine categories of users.	
711	Make recommendations for user accounts based on an organization framework.	
712	Assign proper characteristics to network accounts to maintain network security and allow users to perform tasks effectively.	
713	Plan and implement group and user file/directory permissions and resolve any conflicts.	
714	Create and document user access in accordance with organization requirements.	
715	Establish and document user-friendly login procedures and provide instructions for user access to the network.	
716	Monitor resource sharing & user permissions to maintain network application security.	
717	Recommend usage policies that support network security.	
718	Establish group account controls that meet network and organization usage policies.	
719	Establish password authentication rules and policies to secure the network.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
720	Propose user help-desk access procedures to provide technical assistance and improve customer relations.	
721	Design and implement methods to monitor user accounts.	
722	Design and Set up directories on the network to store user files for a given situation.	
800	**NETWORK PLANNING**	
801	Propose a design for a network that meets organizational needs for a given situation.	
802	Design a network wiring schematic for a proposed network design.	
803	Assess and present to management the benefits and risks associated with implementation of a specific network design.	
804	Propose an intranet architecture for processing information within a specific organization.	
805	Design a physical layout for an organized wiring closet.	
806	Design a network architecture using multiple protocol suites to enable communication with other network-connected machines.	
807	Evaluate a buildings structure for proper cabling installation.	
808	Research and apply building and wiring codes to design a physical network topology.	
809	Analyze & document bandwidth requirements to plan for increased network capacity.	
810	Interview customers to identify organizational constraints affecting the design of a network.	
811	Analyze and document customer and organizational requirements as they relate to network architecture.	
812	Identify, select and document a logical topology to meet system requirements and organizational needs.	
813	Explain and document the advantages and limitations of various network operating systems to support selection of an operating system.	
814	Identify and interview vendors to research available hardware components and their cost for a given network upgrade.	
815	Compare quality of service of various hardware vendors and make recommendations.	
900	**NETWORK IMPLEMENTATION**	
901	Develop a proposed network implementation plan to meet client needs.	
902	Develop and implement a test plan for a specific network after implementation.	
903	Produce an implementation plan document that includes network implementation schedule, and project management charts.	
904	Interpret blueprints to evaluate the feasibility of network implementation plan.	
905	Present a network implementation plan to team members and management.	
906	Organize tasks and team members for a network implementation plan.	
907	Present a proposed network implementation plan to users in non-technical terms.	
908	Determine future network equipment requirements based on network usage trends and growth plan.	
909	Gather and analyze user feedback to determine whether a network implementation meets client requirements.	
910	Assess the effectiveness of the implementation and document areas for improvement.	
911	Develop alternative solutions to a given network implementation problem.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
912	Estimate and document the costs and benefits associated with a given network implementation plan.	
913	Document physical constraints to a given implementation and present to management in non-technical terms.	
914	Evaluate power requirements and availability to ensure necessary capacity for network.	
915	Evaluate and document HVAC and other environmental constraints in the development of the network installation plan.	
916	Interpret blueprints and user requirements to identify the appropriate physical location for network servers and other devices.	
917	Develop and document a plan for the physical security of servers on the network.	
918	Draw sketches of proposed wire runs and assess their compatibility with the network installation plan.	
919	Create an accurate and complete wire list schema from a network installation plan.	
920	Evaluate and select appropriate mount outlets for installation of required equipment.	
1000	**NETWORK MAINTENANCE**	
1001	Prioritize network maintenance service requests according to user requirements and level of impact on users and system.	
1002	Describe how to promptly address network problems as they are identified through maintenance reports.	
1003	Describe how to Seek & incorporate feedback to develop effective solutions to identified maintenance issues.	
1004	Properly use performance and monitoring tools to assess network performance.	
1005	Evaluate & document results of maintenance performed to solve specific failures.	
1006	Create a network maintenance schedule that regularly assesses performance of network components.	
1007	Develop hardware/software maintenance plan to meet user needs & system specifications.	
1008	Develop and implement a test plan for checking network system operations after maintenance.	
1009	Interpret & update network maintenance reports that document current network performance.	
1010	Read and interpret warranty information; document impact on maintenance plan and schedule.	
1011	Accurately fill out warranty forms to guarantee compliance with vendor requirements.	
1012	Assess the costs and benefits of repairing versus replacing equipment and make recommendations.	
1013	Develop a contingency plan for network failure; propose an effective recovery strategy.	
1014	Effectively communicate with end-users and administration to coordinate a maintenance schedule.	
1015	Select and coordinate equipment needed to implement a network maintenance plan.	
1016	Interview users to determine the effectiveness of maintenance; interpret and document feedback.	
1017	Estimate the budgetary impact of a network maintenance plan and make recommendations to team and management.	
1018	Organize maintenance tasks & team members to follow appropriate maintenance plan.	
1019	Identify & document hardware required to maintain and improve network performance.	
1020	Identify and develop criteria for network maintenance baseline performance.	
1021	Effectively use hardware and software tools to identify network media problems.	
1022	Identify and obtain appropriate software upgrades, drivers and patches using available vendor resources to maintain system performance.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
1100	**NETWORK MONITORING AND OPTIMIZATION**	
1101	Select and implement procedures to resolve traffic bottlenecks within the network and document the results.	
1102	Evaluate hardware and software malfunctions, prioritize the problems according to importance and propose resolution plan.	
1103	Identify changes in network performance and compare against specifications.	
1104	Implement monitoring procedures from a remote location in accordance with organization procedures.	
1105	Analyze network performance trends and synthesize results to determine areas for optimization.	
1106	Identify and monitor potential environmental hazards that could impact network performance.	
1107	Analyze and summarize collected monitoring data to determine system performance.	
1108	Identify monitoring requirements, and develop and document monitoring procedures.	
1109	Properly use monitoring tools according to vendor specifications.	
1110	Follow industry standards and use appropriate tools to monitor the system.	
1111	Gather and analyze data to verify that changes to the network achieved optimization goals.	
1112	Create statistical report of problems and solutions with necessary graphs to present to management.	
1113	Estimate time and budgetary impacts of optimization and make recommendations to management.	
1114	Compare network performance to baseline data to identify problems and optimize system performance.	
1115	Develop and implement a comprehensive schedule to optimize and monitor network performance.	
1116	Install and run monitoring software to optimize network performance.	
1117	Identify and document abnormal system performance and implement a solution with minimal disruption to user productivity.	
1118	Develop, document, and implement testing and troubleshooting procedures in accordance with organizational requirements.	
1119	Document sources of malfunctions and solutions implemented.	
1200	**NETWORK OPERATING SYSTEMS**	
1201	Identify and document existing network standards related to operating systems to ensure compliance.	
1202	Develop and implement acceptance tests to verify that the operating system is performing according to specifications.	
1203	Document network operating system installation procedures and server configuration.	
1204	Configure the network operating system to meet user and organizational requirements.	
1205	Develop and implement a directory replication procedure to maintain a master set of directories and files.	
1206	Create emergency startup disks and boot procedures to restart the system in case of system failure.	
1207	Create and interpret system logs to identify problems in the network operating system.	
1208	Implement and review appropriate logging procedures and resolve logging errors.	
1209	Identify and apply appropriate patches and upgrades to the operating system according to vendor specifications.	
1210	Compare network performance to baseline data and identify network operating system problems.	
1211	Develop and implement network operating system backup procedures to prevent loss of data.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
1212	Determine and implement the most appropriate disk file system based on user and security needs.	
1213	Identify and use appropriate tools to test a network operating system.	
1214	Use diagnostic tools according to troubleshooting procedures to test a network operating system.	
1215	Document operating system backup procedures and make recommendations for improvement.	
1300	**NETWORK OPERATIONS**	
1301	Implement backup procedures to secure user data and system configurations.	
1302	Properly use system measurement techniques including probes and performance and protocol monitoring tools.	
1303	Set up file systems and directory structures to support network users.	
1304	Select and use server tools to administer the network and document results.	
1305	Produce operational reports using network documentation application, word processing and chart programs.	
1306	Prepare and present a report of necessary upgrades to enhance hardware and software to meet user requirements and optimize system.	
1307	Evaluate hardware problems and test the operation of hardware components to verify functionality according to specifications.	
1308	Implement and document solutions to problems at the server level.	
1309	Evaluate hardware or software malfunctions, prioritize the problems in order of importance and propose resolution strategy.	
1310	Create a security assessment checklist and implement procedures to assess system security.	
1311	Identify and correct connectivity and protocol problems to enhance network performance.	
1312	Simulate various problems locally to assess their impact on the network and test solutions.	
1400	**NETWORK RECOVERY**	
1401	Identify and train individuals who will perform backup and recovery operations.	
1402	Develop a disaster recovery plan in cooperation with network team and vendors, and present to management for approval.	
1403	Apply appropriate fault tolerance methods to the current network to optimize network response.	
1404	Describe the differences between primary and backup servers and explain their respective roles during disaster recovery.	
1405	Select & install uninterruptible power supply hardware and software to prevent data loss.	
1406	Develop & implement an effective network recovery and backup training plan for users.	
1407	Effectively reconfigure hardware and software after recovery to reestablish optimal performance.	
1408	Analyze and interpret data retrieved from error log files to troubleshoot problem areas.	
1409	Create a network recovery disk to protect against data loss.	
1410	Utilize software to assist in the analysis of error log files.	
1411	Identify and repair network media faults.	
1412	Identify specific network media failures and implement an effective recovery process.	
1413	Identify & recover from virus and other security-related issues with minimal downtime.	
1414	Recognize the differences between hardware and software problems to implement appropriate recovery procedures.	

pennsylvania
DEPARTMENT OF EDUCATION

High School Graduation Years 2010, 2011 and 2012

Computer System Networking and Telecommunications
CIP 11.0901
Task Grid

Unit/Standard Number		Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level
1415	Restore data backup storage after system failure and document procedures.	
1416	Analyze and implement the necessary steps to backup a primary and backup server.	
1417	Develop and implement a contingency plan to restore stability to the network after a system failure.	
1418	Identify conflicting or erroneous data after a system failure and reconcile with backup.	
1419	Document system deficiencies and implement appropriate software patches to improve network reliability.	
1420	Discuss the importance of server synchronization and explain how it affects recovery.	
1500	**NETWORK SECURITY**	
1501	Identify and document secure locations for servers and printer resources on an existing network.	
1502	Evaluate installation procedures and server configurations to prevent system tampering.	
1503	Determine and establish appropriate client privilege access levels according to security policies.	
1504	Research and document applicable organization security policies and make recommendations to team and management.	
1505	Create and implement security logs to monitor usage and unauthorized access.	
1506	Identify and document potential password vulnerabilities and make recommendations for improvement.	
1507	Establish and document firewalls to protect network against external tampering and unauthorized access.	
1508	Identify security risks within the current system and make recommendations for improvement.	
1509	Identify and document the current network security configurations to establish a baseline.	
1510	Select and apply standard testing tools and techniques to verify security configurations.	
1511	Analyze the current system to determine if the levels of security meet organization requirements.	
1512	Analyze security logs to identify potential risks and security violations.	
1513	Schedule and perform periodic security reviews to identify security risks.	
1514	Analyze current firewall system to determine if it meets the organization needs and make recommendations for improvement.	
1515	Identify and document vulnerabilities in software security and apply appropriate patch.	
1516	Apply the appropriate security software updates when needed.	
1517	Configure and document various user password parameters to establish access rights to company data.	
1518	Monitor vendor websites to obtain security patches and upgrades.	
1519	Develop and implement procedures for updating virus software and security patches on the system.	
1600	**UPGRADING A NETWORK**	
1601	Analyze current system and organization requirements to identify system upgrade requirements.	
1602	Obtain and document equipment costs for a given network upgrade.	
1603	Develop and implement an upgrade plan that meets organizational needs.	
1604	Perform upgrade installation, test effectiveness and functionality of upgrade, and document results.	
1605	Develop a plan for multi-vendor installation and make recommendations to management for approval.	

Unit/Standard Number	pennsylvania DEPARTMENT OF EDUCATION **High School Graduation Years 2010, 2011 and 2012** **Computer System Networking and Telecommunications** **CIP 11.0901** **Task Grid**	**Proficiency Level Achieved: (X) Indicates Competency Achieved to Industry Proficiency Level**
1606	Identify and select vendor products that meet system requirements.	
1607	Identify vendor, product and service alternatives to resolve network problems and make recommendations.	
1608	Evaluate trends in network vendors and products to plan for future network support and growth.	
1700	**NETWORK VENDORS AND PRODUCTS**	
1701	Document the products installed on a specific network and their respective vendors.	
1702	Evaluate and document strengths and limitations of specific vendors and their products and services.	
1703	Research, select and document vendors, products, and services that meet organizational, user, and technical needs for a given situation.	