CYBER SECURITY

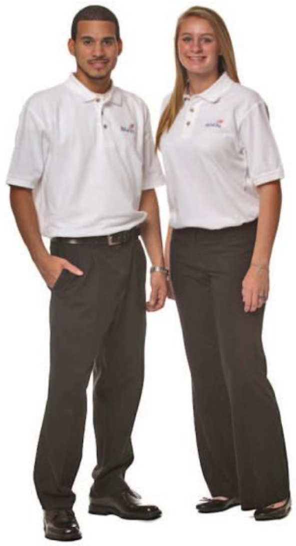
CONTEST DATE & LOCATION: Refer to the Kansas State Championship Conference Packet

PURPOSE: To evaluate each contestant's preparation for employment and to recognize outstanding students for excellence and professionalism with relation to the entry level skills within the field of Cybersecurity.

ELIGIBILITY: Team of two. Open to active SkillsUSA members enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture as the occupational objectives.

CLOTHING REQUIREMENT: There are specific clothing requirements, such as official SkillsUSA Kansas T-shirt with clean blue jeans. Although not required, contestants may wear the official uniform of SkillsUSA, or competition polo shirt and slacks. Clothing that identifies the school or that is inappropriate is prohibited.

Official SkillsUSA white polo attire



NOTE: The Official Kansas State T-shirt will be mailed to schools prior to the competition.

SCOPE OF THE CONTEST

The contest is defined by industry standards as determined from elements of the NIST Publication 800-181 Cyber Security Workforce Framework Categories included:

Securely Provision (SP)

Operate and Maintain (OM)

Protect and Defend (PR)

KNOWLEDGE PERFORMANCE

Cognitive Domain Performance – Contestants will take an examination covering their knowledge of common cyber security tenets as defined by the objectives of Comp TIA's Security+ or ETA's ITS certifications. This involves knowledge of common cyber security tools, techniques, and practices. Questions cover key cyber security systems and devices, including those related to-end point devices, software, managed switches, enterprise routers, wireless access points, firewalls, pen testing tools, and digital/network forensic activities. The exam consists of multiple-choice questions and last up to two hours.

SKILLS PERFORMANCE

Psychomotor Domain Performance – This portion of the competition consists of several Provisioning, Testing, Deployment, Operational and Maintenance, and Protection and Defensive procedures with the end goals set by the technical committee. Contestants must successfully complete assigned tasks at a number of independent Activity Station. The tasks are designed to provide a variety of Cyber Security challenges based on the recommended best practices of the industry. Identical tasks are used in high school and college/postsecondary categories. Approximately, 45 minutes are allowed at each station.

CONTEST GUIDELINES

The contest requires a team or tactical unit of Two: Each will have to display equivalent subject matter expertise in all competency areas. The contest will take place in two learning domains.

Professional Activities Station: Contestants will provide verbal instructions or explanations to an evaluator for the tasks presented at the Professional Activities Station.

End Point Security Station: Contestants will display knowledge of industry standards processes and procedures for hardening an end point or stand-alone computing device.

Managed Switch Security: Contestants will complete a task that contains security-related activities associated with managed switches.

Enterprise Router Security: Contestant will complete a task containing activities associated with accessing an enterprise router, configuring it to create network security structures and establish security for the router itself.

Server Hardening: Contestants will complete a task that contains activities related to hardening servers against attack.

Network Boundary Security: This task for contestants involves activities related to installing and configuring typical network boundary devices and structures to form an effective network zone or edge security systems.

Wireless and Mobile Device Security: Contestants will complete a task that contains activities related to installing, configuring and securing wireless Access Points and Mobile Devices.

Digital/Network Forensics: Contestants will complete tasks that contains activities related to computer or network forensic activities associated with Incident Response Actions. Contestants will use appropriate measures to collect information from a variety of sources to identify, analyze and report cyber events that occur (or might occur) to protect information, information systems, and networks from cyber threats.

Pentesting: Contestants will complete a task that contains activities related to the process of penetration testing. The contestant will plan, prepare and execute tests of systems to evaluate results against specifications and requirements as well as analyze and report on test results.