CYBER SECURITY

SkillsUSA Championships Technical Standards

PURPOSE

The Esports & Cybersecurity Capture the Flag (CTF) Competition supports the officially approved Department of Education High School dual enrollment Information Technology Cluster Experience Based Learning Completer academic credit Career pathway Technical Education (CTE) track. In the customized esports and cyber security, capture the flag (CTF) competition, a unique and direct focus combines cybersecurity with the multi-billion-dollar gaming and esports career pathway industry through customized training exercises that thoroughly evaluate participants' skills and knowledge in various subdomains. Each Esports and Cybersecurity CTF challenges and tests participants' ability to find security vulnerabilities in a knowledge, skills, and abilities competitive gamification in a test IT environment. It also aims to find a hidden file or piece of information (the "flag") in either the gaming esports competition scenario, i.e., Call of Duty (COD), Rocket League, Madden, NBA2K, or another target environment.

CLOTHING REQUIREMENT

Class E: Competition Specific — Business Casual

- Official School District Esports Logo Team Jersey or Polo Shirt
- Khaki Pants, Black dress slacks, or black dress skirt (knee-length minimum)
- White Sneakers or an approved unified school color shoe.

Note: Wearing socks or a hose is no longer required. If worn, socks must be a unified color.

Note: Competitors must wear their official competition clothing to the competition orientation meeting.

These regulations refer to clothing items that are pictured and described:
https://www.unityprinting.com/BFG/.

If you have questions about clothing or other logo items, call 1-800-364-8610.

About Blaze Fire Games
Visit us at: https://blazefiregames.com/#!/

About Blaze Fire Games Esports Bus
https://bfgesportsbus.com/about

Blaze Fire Games Esports Bus Promo
https://www.youtube.com/shorts/Ax9fBt2N5IU

Contact

Blaze Fire Games
info@bfgesportsbus.com
8003648610

ELIGIBILITY (TEAM OF TWO)

Open to a team of two active SkillsUSA members enrolled in programs with Esports and Cyber Security Cyber Security, Information Security, or Systems and Networking Security Architecture as an occupational objective. Each participating school district in the state may send up to three high schools and one college/postsecondary team.

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee (This includes all reference materials, diagrams, and instruction required for the competition):
   a. Switch fabric for network connectivity
   b. USB Thumb Drives
   c. L2/L3 Managed Switches
   d. Enterprise Routers
   e. Network Server Systems
   f. Hardware Firewalls
   g. Wireless Access Points
   h. Wireless Network Capability
   a. Tablet PCs/Smartphones
   b. **GameDevHQ will provide a competition laptop for each participating Competition Team.**
   i. Write Blocker Device
   j. SD Card Reader
   k. Log files from PCs, access points, servers, and routers.
   l. Network Cables
   m. Console Cables

2. Supplied by the competitor:
   a. Blank Paper
   b. Writing Instrument
   c. Notebook PC with the following software installed:
   d. Dual-booting Windows 10/11 Pro and Kali Linux (or self-bootable Kali USB Thumb Drive): The Kali version must perform RDP operations.
   e. Putty Software
   f. Autopsy Software
   g. Access Data FTK Imager (Freeware version)
   h. Wireshark
   i. Nmap/Zenmap
   j. Wi-Fi Adapters Capable of Promiscuous Mode Operation
   Note: The competition notebook PC must possess an Ethernet port or a USB to Ethernet converter. This is required for access to the competition environment. Only software specified by the technical committee can be installed on the competitor machines used for the competition. The inappropriate games or content on the competition machine may result in disqualification.
   k. All competitors must create a one-page resume. See "Resume Requirement" below for guidelines.

RESUME REQUIREMENT

Competitors must create a one-page resume to submit online. SkillsUSA national competitors should submit their resumes by the deadline published on the competition updates page of our website to info@aperionglobalinstitute.com

The deadline and link for resume submission will be posted on http://updates.skillsusa.org. Failure to submit a resume will result in a 10-point penalty.

Your resume must be saved as a PDF file using the file name format of "Last Name First Name." For example, "John Hemby " would keep her resume as **Hemby_John**. If you need assistance saving your file as a PDF, visit the Adobe website for more information.

***Note*:** Check the Competition Guidelines and the updates page on the SkillsUSA website at http://updates.skillsusa.org.

PROHIBITED DEVICES

Cellphones, electronic watches, and other electronic devices not approved by a competition's national technical committee are ***NOT*** allowed in the competition area. Please follow the guidelines in each technical standard for approved exceptions. Technical committee members may also support exceptions onsite during the SkillsUSA Championships if deemed appropriate.

Penalties for Prohibited Devices

If a competitor's electronic device makes noise or if the competitor is seen using it at any time during the competition, an official report will be documented for review by the Director of the SkillsUSA Championships. If it is confirmed that the competitor used the device in a manner that compromised the competition's integrity, the competitor's scores may be removed.

SCOPE OF THE COMPETITION

The competition is defined by industry standards as determined from elements of the NIST Publication 800-181 Cyber Security Workforce Framework Categories, which include:

- Securely Provision (SP)
- Operate and Maintain (OM)
- Protect and Defend (PR)

KNOWLEDGE PERFORMANCE

Cognitive Domain Performance

Competitors will examine their knowledge of common cyber security tenets as defined by the objectives of CompTIA's Security+ or ETA's ITS certifications. This involves knowledge of standard cyber security tools, techniques, and practices. Questions cover critical cyber security systems and devices related to endpoint 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 lasts up to two hours.

SKILL 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. Competitors must complete assigned tasks at several
independent activity stations. The tasks are designed to provide a variety of cybersecurity.

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.

COMPETITION GUIDELINES

1. The competition requires a team (tactical unit) of two competitors. Each will have to display equivalent subject matter expertise in all competency areas. The stages of the competition are as follows:
2. Cognitive Domain — The knowledge/certification exam and the professional interview
3. Psychomotor Domain — Hands-on skills task stations.

COMPETITION STATIONS

These competition skill performance stations are created to be a scouting combine where competitors will demonstrate a wide range of skill sets needed in this industry. The competitors will rotate through the activity stations as determined by the technical committee.

Station 1: Cybersecurity Professional Certification Exam Station

Competitors will take the CompTIA Security+ or ETA ITS Certification exams for professional certification.

Station 2: Professional Activities Station

Competitors will provide verbal instructions or explanations to an evaluator for the task presented at the professional activities station.

1. Train a fellow employee on how to avoid phishing attempts associated with emails and websites. This should include user-level examples of things to look for to prevent everyday items from being used as bait.
2. Explain the requirements for (and methods of) creating solid passwords for senior management personnel in your company.
3. Provide legally sound advice and recommendations to management on various cybersecurity topics.
    a. Provide sound recommendations to management on a variety of cyber security policies.
        1). Separation of Duties Policies
        2). Acceptable Use Policies
        3). Mandatory Vacation Policies
    b. Conduct training of the organization's staff on various employee-centered cyber security activities.
        1). Use of Antivirus Software
        2). Use of Anti-Malware Products.
    c. Explain to a new employee the process for notifying first responders of the Computer Incident Response Team about the possible occurrence of a cyber event.

Station 3: Network Systems Hardening Station

This task contains activities related to hardening network systems, including different types of endpoints and network servers. Competitors will display knowledge of industry-standard processes and procedures for hardening an endpoint, stand-alone computing device, or network server. Devices may be running Windows, Linux, or Android operating systems.

Suggested Hands-On Activities Include:

1. Endpoint Hardening — Competitors will display knowledge of industry-standard processes and procedures for hardening an endpoint or stand-alone computing device.
    a. Configuring BIOS/CMOS settings to secure the outer perimeter of a personal computer.
        1). Configure BIOS Passwords to safeguard the CMOS Area and control access to the operating system
        2). Enable/Disable USB ports
        3). Manage Boot devices and boot order
    b. Take steps to harden an installed operating system – including Windows 10/11, Windows Server 2012/R2, 2019, and Linux distributions.
        1). Create secure passwords
        2). Given a scenario, configure lockout policies
        3). Given a scenario, create and manage local user policies
        4). Given a scenario, assign user privileges based on the principle of least privilege
        5). Disable vulnerable accounts
        6). Given a scenario, order services and ports securely
        7). Identify and remove unnecessary software applications
    c. Secure data at rest in a personal computer.
        1). Apply file and folder-level encryption.
        2). Apply disk-level encryption
    d. Install/configure antivirus/antimalware
        1). Perform secure local firewall configurations
        2). Write a rule to allow or deny specific traffic to pass through the local firewall.
        3). Given a scenario, perform secure browser configurations
2. Server Hardening — These tasks contain activities related to hardening servers against attack. Competitors will display knowledge of industry-standard processes and procedures for hardening a network server.
    a. Given a scenario, create and configure an administrative account to replace the default admin account.
    b. Configure permissions or rights for network users and groups applying the principle of least privilege
    c. Implement server security logging and auditing
    d. Take steps to harden an installed server operating system.
        1). Create and manage network user policies
        2). Assign user privileges based on the principle of least privilege
        3). Disable vulnerable/unnecessary user accounts
        4). Manage services and ports securely
    e. Secure data at rest in a server environment.
    f. Perform vulnerability scans and host-based service system calls on operating servers.
    g. Given a scenario, create virtual machines/networks on a server.

Station 4: Local Network Device Security

This task contains security-related activities associated with managed switches and enterprise routers. It includes activities related to accessing these devices, configuring them to create network security structures, and establishing security for the device itself.

Suggested Hands-On Activities Include:

1. Managed Switch Security
    a. Access a managed switch's management environment.
        1). Establish an IP Address for the switch's management VLAN
    b. Enable access security for the switch's admin environment.
        1). Configure an encrypted password for the switch.
    c. Create multiple VLANs to establish segmented network security zones
    d. Manage switch port security
        1). Given a scenario, configure MAC filtering on a managed switch
    e. Create an ACL to control access to different groups of switch ports or IP addresses
    f. Given a scenario, establish SSH administrative access to the switch.
2. Enterprise Router Security
    a. Access an enterprise router's management environment.
        1). Enable access security for the router's admin environment.
        2). Configure an encrypted password for the router.
    b. Create a routing scheme to route traffic from one designated network to another.
        1). Given a scenario, set up static routing
        2). Add a neighbor
    c. Configure a router to implement specified traffic control measures.
    d. Configure an enterprise router to log network system events for incident response auditing.

Station 5: Network Boundary Security

This task involves installing and configuring typical network boundary devices and structures to form an effective network zone or edge security system.

Suggested Hands-On Activities Include:

1. Access a hardware firewall's management environment
    a. Establish an IP Address for the firewall's management console
2. Enable access security for the switch's admin environment
    a. Configure an encrypted password for the switch
3. Given a scenario, use a hardware firewall to create and configure perimeter security that provides a boundary between two network zones with differing security levels.
    a. Implement a network perimeter firewall.
    b. Create a DMZ
4. Perform file hashing on a downloaded file to verify its integrity
5. Establish and configure an ACL on the firewall to limit or restrict access to assets as required by the organization's security policies
6. Enable NAT for specific types of network traffic
7. Create a VPN connection
8. Span a firewall port for monitoring purposes
9. Configure IPSec on the firewall

10. Configure IDS

Station 6: Scripting for Cybersecurity

This task contains activities associated with creating scripts to automate cybersecurity-related activities. Competitors should be prepared to develop Python, Ruby, Powershell 7, or Bash scripting language scripts.

Suggested Hands-On Activities Include:

1. Create scripts to automate Nmap scans to scan an entire network or a portion of a network
2. Create scripts to conduct reverse DNS lookups

Station 7: Wireless and Mobile Device Security

This task involves installing, configuring, and securing wireless access points and mobile devices.

Suggested Hands-On Activities Include:

1. Securely install, connect, and configure a wireless access point.
    a. Create a secure password for the AP/Router.
    b. Given a scenario, configure the most secure authentication protocol available.
    c. Turn off any guest networks.
2. Configure secure Wi-Fi operation of the AP
    a. Hide the SSID broadcast
    b. Change the default SSID
    c. Lower the antenna power to limit the usable distance of the Wi-Fi signal
    d. Configure MAC filtering to restrict access
3. Configure wireless router options
4. Configure wired AP/Router options
    a. Given a scenario, limit the DHCP pool size to control the number of wireless devices that can connect to the network.
    b. Establish secure Wi-Fi connections to an access point
    c. Create a secure password for the mobile device
    d. Configure locking specifications
    e. Given a scenario, configure the device's services and applications to provide secure operation.
5. Configure a WAN (Wireless Area Network)
6. Reset a typical access point

Station 8: Digital/Network Forensics

This task contains activities related to computer or network forensic activities associated with incident response actions. Competitors will use appropriate measures to collect information from various sources to identify, analyze, and report cyber events that occur (or might occur) to protect data, information systems, and networks from cyber threats.

Suggested Hands-On Activities Include:

1. Wireshark PCAP analysis
2. Given a set of log files created during a given activity, the competitor must be able to analyze the activity occurring, determine whether it is an event or not, and, if an event occurred, describe best practices for mitigating the event.
3. Collect, process, preserve, analyze, and present computer-related evidence in support of network vulnerability mitigation and criminal, fraud, counterintelligence, or law enforcement investigations.
4. Scan USB thumb drives or SD cards for deleted files
5. Create a forensic image of a drive.
6. Create a memory dump of a suspected computer.
7. Perform a live data acquisition.

Station 9: Pentesting

This task contains activities related to the process of penetration testing. The competitor will plan, prepare, and execute systems tests to evaluate results against specifications and requirements and analyze and report on test results.

Suggested Hands-On Activities Include:

1. Conduct a port scan on a designated device or network
2. Perform a network vulnerability scan
3. Perform a wireless sniffing operation
4. Perform a WireShark scan
5. Enumerate a network
6. Analyze collected information to identify vulnerabilities that pose the possibility of exploitation.
7. Perform a DoS attack against a specified target
8. Hack a specified file (flag) in a remote network
9. Perform steps to establish persistence in a compromised network or device

Station 10: Capture the Flag Competition

During times when the competitors are not actively participating at one of the other cyber security stations, they will engage in an online Capture the Flag (CTF) event. The competitors will log onto the designated CTF website, enroll themselves, and perform the CTF activity or activities presented.

Suggested possible CTF activities include:

1. Forensics paths
2. Cryptography
3. Web Exploitation
4. Reverse Engineering
5. Binary Exploitation

STANDARDS AND COMPETENCIES

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework https://niccs.cisa.gov/.

CY 1.0 — Outline principles and concepts of data storage and security (System Architecture SP-ARC002)

CY 2.0 — Demonstrate abilities to securely provision operating systems software and configure security at initial provisioning stages (Securely Provision SPDEV-001)

CY 3.0 — Assessments of systems and networks and identifies where those deviate from acceptable configurations, enclave policy, or local policy. Measure the effectiveness of architecture against known vulnerabilities. (Protect and Defend: Vulnerability Assessment and Management PRVAM-001)

CY 4.0 — Analyze data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, and network traffic logs.) analyze events that occur within their environments to mitigate threats (Protect and Defend: Defense Analyst PR-CDA-001)

CY 5.0 — Preparation and execution of tests against systems requirements to analyze results (Test and Evaluation SP-TST-001)

CY 6.0 — SkillsUSA Framework

The SkillsUSA Framework is used to pinpoint the Essential Elements in Personal Skills, Workplace Skills, and Technical Skills Grounded in Academics. Students must display or explain how they used some of these Essential Elements. Please reference the graphic, as you may be scored on specific elements applied to your project. For more, visit: www.skillsusa.org/who-we-are/skillsusa-framework/.

English and Language Arts

SC Standard A1. Reading: Literary Text Reading-
Literary Text: Principles of Reading (P)

Standard 1: Demonstrate understanding of the organization and basic features of print. Standard 2: Demonstrate understanding of spoken words, syllables, and sounds.
Standard 3: Know and apply grade-level phonics and word analysis skills when decoding words. Standard 4: Read with sufficient accuracy and fluency to support comprehension.

COMMITTEE IDENTIFIED ACADEMIC SKILLS

The technical committee has identified the following academic skills embedded in this competition.

Math Skills

- Use scientific notation.
- Use logarithms.
- Use statistics.

Science Skills

- Use knowledge of mechanical, chemical, and electrical energy.
- Use knowledge of temperature scales, heat, and heat transfer.
- Use knowledge of work, force, mechanical advantage, efficiency, and power.
- Use knowledge of principles of electricity and magnetism.
- Use knowledge of static electricity, current electricity, and circuits.
- Use knowledge of signal frequencies and baud rate.
- Use knowledge of communication modes (full/half duplex).

Language Arts Skills

- Organize and synthesize information for use in written and oral presentations. Demonstrate knowledge of appropriate reference materials.

CONNECTIONS TO NATIONAL STANDARDS

State-level academic curriculum specialists identified the following connections to national educational standards.

Math Standards

- Linear algebra
- Trigonometry
- Calculus
- Data analysis and probability
- Operational analysis
- Problem-solving
- Reasoning and proof

Source: *Careeronestop: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx. Select "Academic Competencies" from the model.*

Source: *NIST Publication 800-181 CyberSecurity Workforce Framework: https://doi.org/10.6028/NIST.SP.800- 181r1*

Science Standards

- Understands relationships among organisms and their physical environment
- Understands the sources and properties of energy

- Understands forces and motion
- Understands the nature of scientific inquiry

Source: *McREL compendium of national science standards. To view and search the compendium, visit www2.mcrel.org/compendium/.*

Language Arts Standards

- Students apply various strategies to comprehend, interpret, evaluate, and appreciate texts. They draw on their prior experience, their interactions with other readers and writers, their knowledge of word meaning and other texts, their word identification strategies, and their understanding of textual features (e.g., sound-letter correspondence, sentence structure, context, and graphics)
- Students adjust their spoken, written, and visual language (e.g., conventions, style, vocabulary) to communicate effectively with various audiences and for different purposes.
- Students use spoken, written, and visual language to accomplish their purposes (e.g., for learning, enjoyment, persuasion, and the exchange of information)

Source: IRA/NCTE Standards for the English Language Arts. To view the standards, visit http://www.ncte.org/standards/ncte-ira.

Skills/competencies to be tested by the contest (list 5 to 10):

- Network Defense
- Ethical Hacking
- Digital Forensics
- Software Development Principles
- Game Design & Creativity
- Team Collaboration
- Communication
- Critical Thinking

Which occupational titles in SkillsUSA's membership directly or closely relate to the competencies expected of competitors in this contest?

- VA
- AS
- CPSA
- CPSB
- CP
- CMT
- IAGD
- TECH
- CY
- CMT

What are the **titles** of the entry-level jobs appropriate to these skills?

Computer User Support Specialists (via O*NET)

Provide technical assistance to computer users. Answer questions or resolve computer problems for

clients in person, via telephone, or electronically. May assist in using computer hardware and software, including printing, installation, word processing, electronic mail, and operating systems.

Sample of reported job titles: Computer Specialist, Computer Support Specialist, Computer Technician, Desktop Support Technician, Help Desk Analyst, Help Desk Technician, Information Technology Specialist (IT Specialist), Support Specialist, Technical Support Specialist

Software Engineer / Software Developer
A Software Developer serves as a member of the software development team. They aid in the innovation and creation of company software and programs. Generally found in
tech-heavy industries and large corporations, a Software Developer will work alongside a team of programmers to code programs that meet the needs of the company or client. They seek to facilitate the proper design and implementation of software. From detailed

From computer coding to innovative design, a Software Developer is an asset when creating a seamless software experience for customers. The typical salary range can range from $70,000, with experienced and more senior positions earning over $175,000 yearly.

Game Developer / Programmer/Arcade Game Prototyping Tech/Engineer/Platform Engineer
Game developers often work on teams and help to make a game's concept or ideas come to life. They create a story, outline the design, and create game prototypes. They are responsible for designing and developing video games for units including a personal computer, a consul, or a mobile application. They code the base engine from the ideas of the game's design team and may be called upon to assist with character design with novel design animation and unit testing. The typical salary range for Interns and Junior Developers can range from $50,000, with experienced and more senior positions earning over $125,000 yearly.

Video Game Designer/UI/UX Video Game Artist
Game artists create art for one or more types of games and help make a game's visual elements, including characters, vehicles, surface textures, and clothing. They create compelling and emotionally impactful artwork that fits and enhances the game theme's established style and branding. They push creative projects from the concept through development into final execution. They collaborate with a team to execute large and small projects with the same enthusiasm and maintain existing products while providing assets for marketing purposes. These artists can use their talents to create video game characters and earn between $40,000 and $100,000 yearly.

Game Developer (Junior, Lead)/ Unity Game Developer/Game Systems Designer
As a Game Designer, you will create new sports games and use computer programming languages to write the required code. You will manage the software development teams/project team through the software development life cycle. Your passion for video gaming will show through your exceptional creative and artistic skills during client pitches and new product development meetings. Successful game designers can take anywhere from
$50,000 to over $100,000, depending on their experience and abilities.

Game/VR Producer/Producer - Gaming Media/ Multimedia - Games
As a game producer, this person deals with budgeting and project management and is also responsible for promoting the game to the "powers that be" within the gaming industry and the most influential people: the fans. Successful producers can make anywhere from $50,000 to over $140,000, depending on their experience and abilities.

Video Game Tester/QA Tester
This is the job that most can only dream of. Not only do they hire people to design the game, but they also hire people to play it! The position of a game tester is all about playing games, taking notes of any glitches in the system, and notating the consumer's expected experience playing the game. This is a lucrative job and one that is in high demand in the industry! Experienced testers can earn over $100,000 yearly.

What are the prospects for **industry growth** in demand for these skills?

Computer and Information Technology Occupations

https://www.bls.gov/ooh/computer-and-information-technology/home.htm

Newzoo. (2021). Global Games Market Report. Retrieved from https://newzoo.com/insights/trend-reports/newzoos-global-games-market-report-2021-light/

U.S. Bureau of Labor Statistics. (2021). Software Developers. Retrieved from

https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm

Unity Gaming Report 2022
https://create.unity.com/gaming-report-2022

What companies/organizations are **committed** to providing volunteers and equipment for a demonstration contest at the national SkillsUSA Championships?

3. www.eccouncil.org
4. www.blazefiregames.com

What companies/organizations should be approached shortly to provide volunteers and contest equipment and place winner prizes for a demonstration contest at the national SkillsUSA Championships?

5. https://IGDA.org
6. https://unity.com
7. https://gamedevhq.com
8. www.eccouncil.org
9. www.blazefiregames.com

Where can SkillsUSA state directors procure volunteers/contest equipment/prizes for a **state-level contest**?

10. www.eccouncil.org
11. www.blazefiregames.com