NEW YORK CITY SKILLSUSA Area V

CYBER SECURITY

PURPOSE

To assess each competitor's readiness for employment and to recognize exceptional students for demonstrating excellence and professionalism in entry-level cyber security skills.

ELIGIBILITY (TEAM OF TWO)

Open to a team of two (2) active SkillsUSA members from the same school enrolled in programs with **Cyber Security**, **Information Security**, or **Systems and Networking Security Architecture** as an occupational objective. Each school may send one team. A full team must be registered. See General Regulations for more information about substitution and penalty rules.

CLOTHING REQUIREMENT

Class E: Competition Specific — Business Casual

- Official SkillsUSA white polo shirt or other related apparel
- Black dress slacks or black dress skirt (knee-length minimum)
- Black closed-toe dress shoes

Note: Wearing socks or hose is not required. If worn, socks must be black dress socks and hose must be either black or skin-tone and seamless/nonpattern.

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee:
    a. Laptop computer with Wi-Fi
    b. All reference materials, diagrams, and instruction required for the competition
2. Supplied by the competitor:
    a. Pencils/writing utensils
    b. Notepad or blank paper
    c. Wi-Fi Adapter

PROHIBITED DEVICES

Cellphones, electronic watches and/or 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 approve exceptions onsite during the event if deemed appropriate.

PENALTIES FOR PROHIBITED DEVICES

If a competitor's electronic device emits any sound, or if the competitor is observed using the device at any point during the competition, an official incident report will be filed for review. If it is determined that the device was used in a way that compromised the integrity of the competition, the competitor's scores may be invalidated or the competitor may be disqualified.

SCOPE OF THE COMPETITION

The competition is defined by industry standards as determined from elements of NIST Special Publication 800-181 (NICE Cybersecurity Workforce Framework). The competition emphasizes workforce categories including:

- Securely Provision (SP)
- Operate and Maintain (OM)
- Protect and Defend (PR)
- Analyze (AN)
- Security Test and Evaluation (SP-TST)

Hands-on components also reflect security control implementation principles outlined in NIST SP 800-53 and technical security assessment methodologies consistent with NIST SP 800-115.

This event is designed to evaluate each team's ability to apply cybersecurity knowledge, implement defensive controls, secure cloud resources, and perform structured penetration testing activities in a controlled environment.

KNOWLEDGE PERFORMANCE

Cognitive domain performance will include an individual assessment evaluating knowledge of foundational cybersecurity concepts aligned with industry-recognized certification objectives similar to CompTIA Security+ and CySA+.

Each station will assess participants' knowledge of cybersecurity tools, techniques, and best practices, covering areas such as threat detection, risk assessment, system hardening, network security fundamentals, cloud security concepts, foundational cryptography, and incident response processes.

SKILL PERFORMANCE

Psychomotor domain performance consists of integrated cybersecurity tasks involving secure provisioning, configuration management, defensive implementation, cloud security remediation, and penetration testing procedures.

Competitors will demonstrate the ability to:

- Harden Windows and Linux endpoint and server operating systems
- Apply security best practices while maintaining required system functionality
- Secure cloud infrastructure resources using proper access controls and monitoring
- Conduct structured black-box penetration testing activities from reconnaissance through exploitation and reporting

Hands-on activities simulate real-world cybersecurity responsibilities aligned with entry-level workforce expectations. All skill performance components are to be completed within the allotted three-hour competition window.

COMPETITION GUIDELINES

1. The competition requires a team (tactical unit) of two competitors from the same local chapter. Each competitor must demonstrate subject matter expertise across all competency areas. The competition includes an individual knowledge assessment and multiple integrated hands-on cybersecurity challenges.

2. Rather than rotating through independent activity stations, teams will complete a structured sequence of challenges designed to evaluate defensive, administrative, cloud security, and offensive security skill sets.
3. During hands-on activities, teams may divide responsibilities strategically; however, both competitors are expected to actively contribute. Certain components require individual performance, while others require coordinated teamwork.
4. All activities must be conducted strictly within the provided competition environment. Internet access and unauthorized electronic devices are prohibited unless explicitly authorized by the technical committee.
5. Competitors must maintain professionalism, preserve required system functionality while implementing security controls, and document findings or actions where required. Security configurations that unnecessarily disrupt required services may result in score deductions.
6. Competitors must strictly follow all written and verbal instructions provided by the technical committee. Activities must remain within the defined scope of the assigned systems and targets. Failure to comply will result in immediate disqualification.

Station 1: Cybersecurity Knowledge Assessment
Competitors will complete an individual cybersecurity knowledge examination designed to assess foundational understanding of industry-recognized security principles consistent with objectives similar to CompTIA Security+ and CySA+.

The assessment will measure knowledge of cybersecurity tools, techniques, and best practices related to system security, network defense, cloud security, cryptography fundamentals, risk management, and incident response.

Note: Access to cell phones, internet resources, AI tools, or external materials is not permitted during this assessment.

Station 2: Network and System Hardening
This task contains activities related to hardening endpoint and server systems in accordance with industry-recommended security best practices. Devices may include Windows and Linux based operating systems.

Competitors will demonstrate the ability to securely configure and defend systems while maintaining required service functionality.

Suggested Hands-On Activities Include:

1. Endpoint Hardening — Secure configuration of Windows and Linux workstations.

2. Remove or disable unnecessary services and applications.
3. Configure password complexity and account lockout policies.
4. Create and manage local users and groups using least privilege principles.
5. Disable or secure default and administrative accounts.
6. Configure host-based firewall rules to allow or deny specified traffic.
7. Secure open ports and disable unnecessary services.
8. Enable and configure logging and auditing policies.
9. Apply file-level and disk-level encryption where appropriate.
10. Secure a pre-installed application running on the server.
11. Configure secure remote administration settings.
12. Implement patch management and update procedures.
13. Review system configurations for potential vulnerabilities.
14. Document system modifications for evaluation.

Station 3: Cloud Security Configuration
This task contains activities related to securing a cloud-based infrastructure environment. Competitors will be provided access to a preconfigured AWS environment containing multiple deployed services.

Competitors must identify security misconfigurations and implement appropriate remediation measures while maintaining operational integrity.

Suggested Hands-On Activities Include:

1. Review and secure IAM roles, users, and permissions.
2. Apply least privilege access controls.
3. Identify and remediate publicly exposed services.
4. Configure and secure security groups and network access controls.
5. Enable logging and monitoring services.
6. Secure storage resources and data access permissions.
7. Implement multi-factor authentication where applicable.
8. Apply network segmentation principles.
9. Review audit logs to identify potential security concerns.
10. Document identified risks and corrective actions taken.

Station 4: Penetration Testing (Red-team)
This task contains activities related to structured black-box penetration testing. Competitors will use a provided attacker machine to assess designated vulnerable systems within the environment.

Competitors will plan, prepare, execute, and document testing activities consistent with accepted penetration testing methodologies.

Suggested Hands-On Activities Include:

1. Conduct reconnaissance and information gathering.
2. Perform network scanning and service enumeration.
3. Identify potential vulnerabilities and misconfigurations.
4. Perform controlled exploitation of identified weaknesses.
5. Capture designated proof-of-compromise artifacts (flags).
6. Analyze exploitation impact and security implications.
7. Demonstrate understanding of post-exploitation considerations.
8. Prepare a concise report summarizing findings and recommended mitigations.

Note: Competitors must strictly limit testing activities to designated targets within the competition environment. Any attempt to access other unauthorized systems than what's been mentioned will result in disqualification.

STANDARDS AND COMPETENCIES

CY 1.0 — Outline principles and concepts of data storage, system architecture, and secure configuration management (Securely Provision – SP-ARC002).

CY 2.0 — Demonstrate the ability to securely provision, configure, and harden operating systems and services at initial deployment and during operational maintenance (Securely Provision – SP-DEV001; Operate and Maintain – OM-ADM001).

CY 3.0 — Assess systems, cloud resources, and networks to identify deviations from secure baselines and measure effectiveness against known vulnerabilities (Protect and Defend – PR-VAM001).

CY 4.0 — Analyze logs, system outputs, and security tool results to detect and interpret potential threats and recommend mitigation strategies (Protect and Defend – PR-CDA001; Analyze – AN-ASA001).

CY 5.0 — Plan, execute, and document structured security testing activities including vulnerability assessment and controlled penetration testing (Security Test and Evaluation – SP-TST001).

CY 6.0 — Demonstrate professionalism, ethical conduct, teamwork, communication skills, and adherence to defined scope and competition rules consistent with industry expectations and workforce readiness standards.

CY 7.0 — SkillsUSA Framework
The SkillsUSA Framework is used to pinpoint the Essential Elements found in Personal Skills, Workplace Skills and Technical Skills Grounded in Academics. Students will be expected to display or explain how they used some of these Essential Elements. For more, visit: skillsusa.org/who-we-are/skillsusa-framework/.

COMMITTEE IDENTIFIED ACADEMIC SKILLS

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

Math Skills

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

Science Skills

- 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.