2025-2026 Competitive Events Guidelines

Cybersecurity

Cybersecurity challenges members to demonstrate their knowledge of protecting systems and data from digital threats such as viruses, malware, phishing, and spyware. Through an objective test, members explore foundational cybersecurity principles, tools, and best practices used to defend against cyberattacks.

Event Overview

Division	High School
Event Type	Individual
Event Category	Objective Test
Event Elements	50-minute test, 100-multiple choice questions

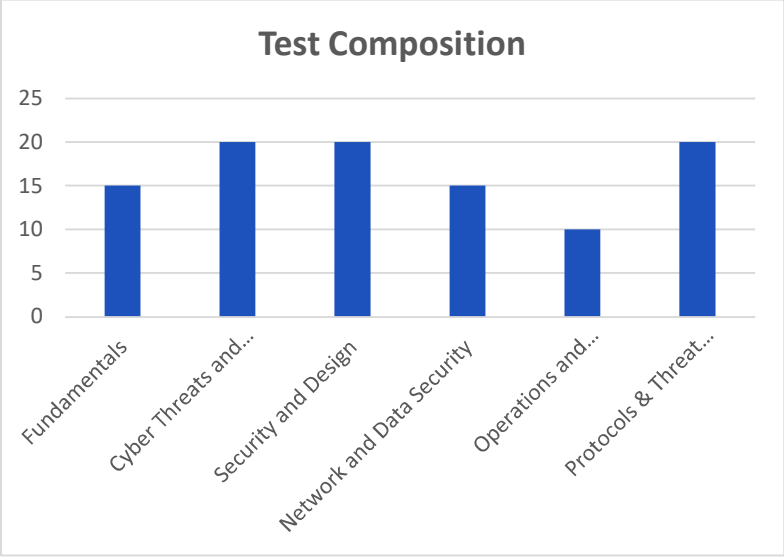
Educational Alignments

Career Cluster Framework Connection	Digital Technology
NACE Competency Alignment	Career & Self-Development, Critical Thinking, Professionalism, Technology

Knowledge Areas

- Security Fundamentals
- Cyber Threats and Vulnerabilities
- Security and Design
- Network and Data Security
- Security Operations and Management
- Security Protocols and Threat Mitigation

Test questions are based on the knowledge areas and objectives outlined for this event. Detailed objectives can be found in the study guide included in these guidelines.



Region

Each chapter may enter two students in this event. Testing is school-site and proctored with careful monitoring to ensure the integrity of the test.

State

Top three (3) qualifiers of each region are eligible to compete at the State Leadership Conference.

2025-2026 Competitive Events Guidelines

Cybersecurity

National

Required Competition Items

Items Competitor Must Provide	Items FBLA Provides On-site
• Sharpened pencil • Fully powered device for online testing • Conference-provided nametag • Photo identification • Attire that meets the FBLA Dress Code	• One piece of scratch paper per competitor • Internet access • Test login information (link & password provided at test check-in)

Important FBLA Documents

- *Competitors should be familiar with the Competitive Events Policy & Procedures Manual, Honor Code, Code of Conduct, and Dress Code.*

Eligibility Requirements

To participate in FBLA competitive events at the National Leadership Conference (NLC), the following criteria must be met:

- **Membership Deadline**: FBLA national membership dues must be paid to the specific division by 11:59 p.m. Eastern Time on March 1 of the current school year.
- **Repeat Competitors**: Members may only compete in an event at the NLC more than once if they have not previously placed in the top 10 of that event at the NLC. If a member places in the top 10 of an event at the NLC, they are no longer eligible to compete in that event at future NLCs, unless the event has been modified beyond a name change. Chapter events are exempt from this procedure.
- **Conference Registration**: Members must be officially registered for the NLC and must pay the national conference registration fee to participate.
- **Official Hotel Requirement**: To be eligible to compete, competitors must stay within the official FBLA housing block.
- **State Entry Limits**: Each state may submit up to four entries per event.
- **Event Participation Limits**: Each member may participate in:
    - One individual or team event, and
    - One chapter event (e.g., *Community Service Project* or *Local Chapter Annual Business Report*).
- **Participation Requirement**: To be eligible for an award, each competitor must complete all components of the event at the National Leadership Conference.
- **Identification at Check-in**: Competitors must present valid photo identification (physical or digital) that matches the name on their conference name badge. Acceptable forms include a driver's license, passport, state-issued ID, or school ID.
- **Late Arrivals**: Competitors will be allowed to compete until such time that the results are finalized, or participation would impact the fairness and integrity of the event, as determined by Competitive Events staff. Five penalty points will be assessed for late arrivals in any competitive event.
- **Event Schedule Notes**:
    - Some events may begin before the Opening Session.
    - All schedules are posted in local time for the NLC host city.

- Schedule changes are not permitted.

Event Administration

- **Test Duration:** 50 minutes
- **Format:** This event consists of an online objective test that is proctored and completed on-site at the National Leadership Conference (NLC).
- **Materials:** Reference or study materials are not permitted at the testing site.
- **Calculators:** Personal calculators are not allowed; an online calculator will be available within the testing platform.
- **Question Review:** Competitors may flag questions within the testing platform for review prior to the finalization of results at the NLC.

Scoring

- Each correct answer is worth one point.
- No points are deducted for incorrect answers.
- Tiebreakers are determined as follows: (1) The number of correct responses to 10 pre-selected tiebreaker questions will be compared. (2) If a tie remains, the number of correct responses to 20 pre-selected questions will be reviewed. (3) If a tie still remains, the competitor who completed the test in the shortest amount of time will be ranked higher.
- Results announced at the National Leadership Conference are considered official and will not be changed after the conclusion of the National Leadership Conference.

Penalty Points

- Competitors may be disqualified if they violate the Code of Conduct or the Honor Code.
- Five points are deducted if competitors do not follow the Dress Code or are late to the testing site.

Recognition

- The number of competitors will determine the number of winners. The maximum number of winners for each competitive event is 10.

Americans with Disabilities Act (ADA)

- FBLA complies with the Americans with Disabilities Act (ADA) by providing reasonable accommodations for competitors. Accommodation requests must be submitted through the conference registration system by the official registration deadline. All requests will be reviewed, and additional documentation may be required to determine eligibility and appropriate support.

Electronic Devices

- Unless approved as part of a documented accommodation, all cell phones, smartwatches, electronic devices, and headphones must be turned off and stored away before the competition begins. Visible devices during the event will be considered a violation of the FBLA Honor Code.

Sample Preparation Resources

- Official sample test items can be found in FBLA Connect. These sample items showcase the types of questions that may be asked on the test and familiarize competitors with the multiple-choice item options.

Study Guide: Knowledge Areas and Objectives

Security Fundamentals (15 test items)

1. Describe Confidentiality, Integrity, and Availability
2. Describe measures for establishing digital trust (e.g., identity proofing, non-repudiation, attestation)
3. Explain the concepts of authentication, authorization, and accounting
4. Provide examples of Zero Trust
5. Describe examples of deception and disruption technology for defending against attackers (e.g., honeypots, honeynets, honeyfiles)
6. Explain how binary, hexadecimal, and decimal are used in cryptography
7. Explain the purpose of least privilege principles

Cyber Threats and Vulnerabilities (20 test items)

1. Describe web and software sources of security vulnerabilities (e.g., injections, overflows, jailbreaking, race conditions)
2. Discuss attributes of threat actors and their goals (e.g., internal and external threats, financial gain, espionage, data theft)
3. Describe types of viruses
4. Discuss types of security vulnerabilities (e.g., backdoors, zero-days, unpatched software)
5. Discuss social engineering scams and attacks (e.g., phishing, phone scams, email scams)
6. Describe the purpose, methods, and mechanics of a DDoS attack
7. Describe the characteristics of types of malware (e.g., viruses, Trojans, worm, logic bombs)
8. Describe cryptographic attacks (e.g., downgrades, collisions, birthday attacks)
9. Discuss vulnerabilities of wireless networks

Security and Design (20 test items)

1. Explain how using cloud infrastructure affects system security
2. Discuss the security implications of microservice architecture (e.g., more attack surfaces, authentication, increased complexity)
3. Differentiate between logical and physical segmentation
4. Explain how containerization and virtualization can increase security
5. Describe security risks and challenges associated with the Internet of Things
6. Describe the concepts of backups, RAID, and UPS
7. Identify examples of the CIA triad in network design (e.g., UPS, encryption, data integrity)
8. Explain the role of testing in building secure cyber architecture

Network and Data Security (15 test items)

1. Describe the purpose of cryptography
2. Differentiate between public and private key cryptography
3. Discuss shift ciphers, Caesar ciphers, and substitution ciphers
4. Describe the three states of data
5. Describe the importance and use of access control models (e.g., MAC, DAC, RBAC)
6. Discuss authentication and authorization of network resources (e.g., multifactor, certificates, tokens)
7. Describe how blockchains and hashing can be used for authentication and data integrity

Security Operations and Management (10 test items)

1. Describe common security policies (e.g., acceptable use, information security, business continuity, disaster recovery)
2. Discuss elements of disaster prevention and recovery plans
3. Describe types of firewalls (e.g., network-based, NGFW, WAF)
4. Explain the use of firewall access lists and rules to increase security
5. Describe best practices for company messaging, email, and data security
6. Describe the impact of change management on security

Security Protocols and Threat Mitigation (20 test items)

1. Provide examples of secure protocols (e.g., SSH, HTTPS, TLS, WPA2)
2. Describe the purpose of intrusion prevention and detection systems
3. Describe policies and practices to prevent viruses, phishing and email scams
4. Explain methods of obfuscation (e.g., tokenization, data masking, steganography)
5. Describe how strong passwords increase security
6. Describe the purpose of digital certificates and Certificate Authorities (CAs)
7. Describe the importance of patches, updates, and version control for security
8. Explain the use of pen testing for increasing security

References for Knowledge Areas & Objectives

Adelaide University. *Cyber security basics: Exploring the fundamentals of cyber security.* https://online.adelaide.edu.au/blog/cyber-security-fundamentals

Association for Computing Machinery. *Cybersecurity Curricula 2017.* https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf

Codecademy. *Introduction to cybersecurity.* https://www.codecademy.com/learn/introduction-to-cybersecurity

CompTIA. *Security+ Certification Exam Objectives.* https://assets.ctfassets.net/82ripq7fjls2/6TYWUym0Nudqa8nGEnegjG/0f9b974d3b1837fe85ab8e6553f4d623/CompTIA-Security-Plus-SY0-701-Exam-Objectives.pdf

Cybersecurity Guide. *Mastering the basics: A comprehensive guide to cybersecurity 101 for the digital age.* https://cybersecurityguide.org/resources/cybersecurity-101/

The Academic Initiative of the Cyber Innovation Center. *K-12 Cybersecurity Learning Standards.* https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf