2025-2026 Competitive Events Guidelines

Cybersecurity (Collegiate)

Cybersecurity challenges members to demonstrate their understanding of how to protect systems, networks, and data from digital threats such as viruses, malware, phishing, and spyware. Through an objective test, members explore cybersecurity concepts, tools, and best practices used to defend against and respond to cyberattacks.

Event Overview

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

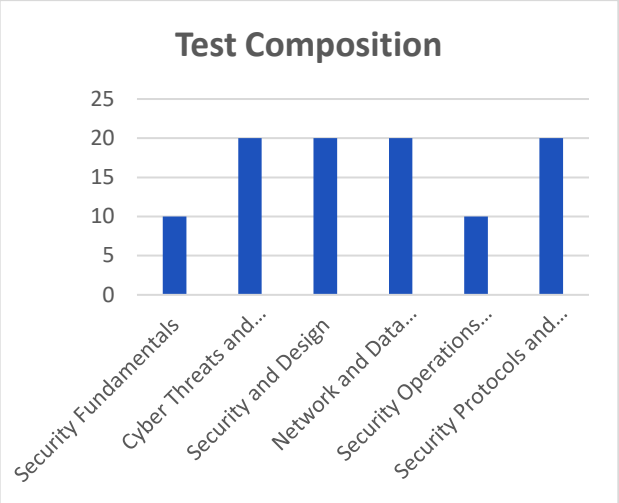
Educational Alignments

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.



State

Testing will take place prior to the State Leadership Conference. Testing must occur at school under the supervision of an adult proctor. Check the Call to Conference for specific instructions and deadlines.

2025-2026 Competitive Events Guidelines

Cybersecurity (Collegiate)

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.
- **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 *State of Chapter Presentation*).
- **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.

Security Fundamentals (10 test items)

1. Describe examples of confidentiality, integrity, and availability in cybersecurity operations
2. Discuss measures for establishing digital trust (e.g., identity proofing, non-repudiation, attestation)
3. Explain how authentication, authorization, and accounting are implemented in practice
4. Analyze principles of Zero Trust present in security architectures
5. Discuss examples of binary and hexadecimal in cybersecurity
6. Perform basic arithmetic involving binary and hexadecimal
7. Analyze examples of least privilege principles

Cyber Threats and Vulnerabilities (20 test items)

1. Analyze the causes of SQL injection and buffer overflow vulnerabilities (e.g., poor input validation, memory management)
2. Analyze the causes, mechanics, and consequences of race conditions (e.g., critical sections, information leak, crash)
3. Discuss attributes of threat actors and their goals (e.g., internal and external threats, financial gain, espionage, data theft)
4. Analyze how different viruses infiltrate systems and spread (e.g., boot sector, polymorphic, macro)
5. Analyze how backdoors, zero-days, and outdated software can lead to cybersecurity incidents
6. Discuss social engineering scams and attacks (e.g., phishing, phone scams, email scams)
7. Describe the purpose, methods, and mechanics of a DDoS attack
8. Analyze effects of and defense against types of malware (e.g., viruses, Trojans, worms)
9. Describe the consequences and mechanics of cryptographic attacks on enterprise systems
10. Evaluate the security of a wireless network

Security and Design (20 test items)

1. Analyze the security benefits and drawbacks of cloud infrastructure (e.g., IaaS, SaaS, PaaS)
2. Recommend changes to cybersecurity policies based on system architecture (e.g., microservice, cloud-based, hybrid)
3. Discuss use cases and examples of logical and physical segmentation (e.g., VLANs, subnets, air-gapped systems)
4. Analyze security use cases for containerization and virtualization in enterprise systems
5. Recommend a backup schedule based on an organization's needs (e.g., differential, incremental, full)
6. Recommend RAID levels based on an organization's needs (e.g., level 0, level 5)
7. Discuss types of testing used in cybersecurity
8. Analyze the impact of physical network design decisions on cybersecurity
9. Discuss key considerations in designing secure systems (e.g., availability, resilience, cost, responsiveness)
10. Discuss ways to increase resilience and recovery in design (e.g., load balancing, clustering, multi-cloud, platform diversity, backups)

Network and Data Security (20 test items)

1. Discuss the role of cryptography in ensuring confidentiality, integrity, authentication, and non-repudiation
2. Analyze the benefits and drawbacks of public and private key cryptography
3. Describe the mechanics of public and private key cryptography
4. Discuss types of ciphers (e.g., shift, Caesar, substitution)
5. Discuss logical access control methods (e.g., access control lists, group policies, passwords)
6. Analyze differences between access control models (e.g., MAC, DAC, RBAC)
7. Analyze network authentication methods (e.g., multifactor, certificates, tokens)
8. Describe the characteristics of effective and ineffective hash functions (e.g., collisions, distribution, efficiency)
9. Discuss the advantages and disadvantages of using blockchain for data integrity and authentication

Security Operations and Management (10 test items)

1. Discuss common security policies (e.g., acceptable use, information security, business continuity, disaster recovery)
2. Discuss elements of disaster prevention and recovery plans
3. Discuss the use cases of different types of firewalls (e.g., network-based, NGFW, WAF)
4. Evaluate messaging, email, and data security policies for risk management
5. Describe change management practices

Security Protocols and Threat Mitigation (20 test items)

1. Describe the purposes of SSH, HTTPS, TLS, and WPA protocols
2. Explain how intrusion detection and prevention systems work (e.g., signature-based, anomaly-based, NIDS)
3. Evaluate the effectiveness of policies and practices for preventing viruses, phishing, and email scams
4. Analyze different types of obfuscation (e.g., code, data, network)
5. Explain how digital certificates and Certificate Authorities (CAs) contribute to security
6. Explain how patches, updates, and version control prevent attacks
7. Discuss examples of penetration testing
8. Describe a VPN and its uses in cybersecurity
9. Describe security protocols used by VPNs and their characteristics (e.g., TLS, OpenVPN, L2TP, IPsec)

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