Schedule of Events
March 5-6, 2020
Public Safety & Security Sector Contests

College Advisor Check In	**Classroom Building**	**10:00 am- 11:00 am**
Demonstrations/Workshops/Simulators/Vendor	**On-Campus**	**10:30 am- 12:00 pm**
Kickoff Lunch (Special Guest Speakers)	**Dining Hall**	**12:00 am- 1:00 pm**
College Contests **Criminal Justice-** Classroom Building **Crime Scene Investigation-** Codes House **Cybersecurity-** Classroom Building **Urban Robotics Search and Rescue-** TBD **EMT-** Motlow EMT Building **Fire Fighting-** Simulations TBD	***See contest for location/map**	**11:00 am - 4:30 pm**
Battle of Champions	**On-Campus**	**4:30-6:00 pm**
Dinner/Awards Celebration	**Dining Hall**	**6:00-7:30 pm**
Overnight Guests- SURPRISE!	**On-Campus**	**8:00-10:00 pm**

Schools who would like to stay on-site at the Fire Academy need to submit a hotel planner including student name and gender.

All contestants will receive a SkillsUSA white polo to wear during competitions.
Students are to wear navy, black, or khaki pants with black boots or dress shoes.
**See Technical Standards for description*

All attendees will receive a SkillsUSA State T-Shirt, Lanyard, and State Pin as well!

Certificates will be awarded for the Highest Score in each contest segment.
Prizes and medals will be awarded for 1st, 2nd, 3rd place winners.
Trophies will be awarded to the Battle of Champion's Winners!

For questions, email your state director at Joy.Rich@TBR.edu

SkillsUSA

Public Safety & Security State Competition

NEW for 2020!

To provide more of our postsecondary students with the opportunity to demonstrate their SKILLS and connect with Industry Partners, we are hosting a sector-specific state competition for postsecondary students in the following areas:

- **Crime Scene Investigation**
- **Criminal Justice**
- **Cybersecurity**
- **Emergency Medical Technician**
- **Firefighting**
- **Robotics Urban Search & Rescue**

Technical standards for all competitions are attached to this email, and can be found at SkillsUSA.org
Registration available November 11-December 11, 2019 at SkillsUSA.org.

$99 Registration per attendee includes:
***All Meals *Entertainment *Conference T-Shirt *Conference Polo**
***Access to Industry Demonstrations *Professional Development**

Accommodations available on-site at TN Fire Service and Codes Academy for students and faculty located outside geographic region. Cost per attendee $65

March 5-6, 2020

Tennessee Fire Service and Codes Enforcement Academy
2161 Unionville- Deason Rd. Bell Buckle, TN 37020

How many contestants can my campus register per event?

Contestant count is based on the number of SkillsUSA members in the program
0-30 Members = 1 Contestant/Team 31-60+ Members = 2 Contestants/Team

**Verified through SkillsUSA.org site*

- **Crime Scene Investigation- Team of 3**
- **Criminal Justice- Individual**
- **Cybersecurity- Team of 2**
- **Emergency Medical Technician- Team of 2**
- **Firefighting- Individual**
- **Robotics Urban Search & Rescue- Team of 2**

Can I register observers?

Due to space limitation, we will not allow any observers to be registered.

Are meals included with registration cost?

YES! All meals are provided on-site at the TN Fire Service and Codes Academy

What is the appropriate attire?

Competitors must wear the conference polo and khaki, black, or navy pants during competition.
**Firefighting contestants may wear shorts/sweat pants with T-shirt during CPAT*.
All attendees should wear a polo with khaki, black, or navy pants to the Grand Awards luncheon, and wear their conference T-Shirt during evening entertainment.

How do I register for the conference?

Go to SkillsUSA.org and log in. Select Public Safety & Security State competition from the drop down menu and enter student/staff information. Submit your completed Housing Planning form to Joy.Rich@TBR.edu.
Housing Form: http://tnpsskillsusa.org/sites/default/files/2019-09/Public%20Safety%20%26%20Security%20Housing%20Form.pdf

How do I pay for the conference?

Payments for registration and housing will be made through LGIP transfer.

Should I bring copies of my resume?

YES! Students will have the opportunity to network with industry partners throughout the conference. Bring multiple copies of your resume to share with potential employers!

How many awards will be given?

- **Top 10 overall winners in each event and competition segments**
- **Prizes for Bronze, Silver, & Gold medalists! *Gold medal winners compete at NLSC**

For questions contact SkillsUSA Tennessee PS State Director
Joy.Rich@tbr.edu

SkillsUSA Master Schedule
Tennessee Fire Codes Academy, March 5, 2020

Crime Scene Investigation Schedule
Codes Building

Contest	MTSU Workshop	Lunch/ Guest Speakers	Observation Test	CSIPracticum	MNPD Demo	Simulations/ Employers	Battle of Champions	Dinner/ Awards
100	10:00-10:45 AM	11:00:00-12:00	12:15- 1:15 PM	1:30-2:30 PM	3:00-3:45 PM	10:00am -4:15 pm	4:30-6:00 PM	6:00-7:30 PM

Criminal Justice Schedule
Classroom Building

Contest	MTSU Workshop	Lunch/ Guest Speakers	Orientation	Stations	MNPD Demo	Simulations/ Employers	Battle of Champions	Dinner/ Awards
200	10:00-10:45 AM	11:00:00-12:00	12:15-12:45 PM	1:00-2:30 PM	3:00-3:45 PM	10:00am -4:15 pm	4:30-6:00 PM	6:00-7:30 PM

Cybersecurity Schedule
Classroom Building

Contest	Contest Orientation	Lunch/ Guest Speakers	Cyber Stations	Battle of Champions	Dinner/ Awards
300	10:00-10:45 AM	11:00:00-12:00	12:00:00 PM-4:00 PM	4:30-6:00 PM	6:00-7:30 PM

EMT Schedule
Motlow EMS Building

Contest	Orientation/ Kit Check	Lunch/Guest Speakers	Skills Stations (4)	Medical/Trauma Scenarios	MNPD Demo	Simulations/ Employers	Battle of Champions	Dinner/ Awards
400	10:00-10:45 AM	11:00:00-12:00	12:00-1:00 PM	1:00-3:00 PM	3:00-3:45 PM	10:00am -4:15 PM	4:30-6:00 PM	6:00-7:30 PM

Urban Robotics Search and Rescue
Classroom Building

Contest	MTSU Presentation	Lunch/ Guest Speakers	Technical Presentation Robot Check In	Practice /Timed Course	MNPD Demo	Simulations/ Employers	Battle of Champions	Dinner/ Awards
500	10:00-10:45 AM	11:00:00-12:00	12:00 -1:00 PM	1:00-3:00 pm	3:00-3:45 PM	10:00am -4:15 PM	4:30-6:00 PM	6:00-7:30 PM

Cyber Security

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.

First, refer to General Regulations, Page 9.

CLOTHING REQUIREMENT

Class E: Contest specific — Business Casual

- Official SkillsUSA white polo shirt
- Black dress slacks (accompanied by black dress socks or black or skin-tone seamless hose) or black dress skirt (knee-length, accompanied by black or skin-tone seamless hose)

These regulations refer to clothing items that are pictured and described at: www.skillsusastore.org. If you have questions about clothing or other logo items, call

800-401-1560 or 703-956-3723.

Note: Contestants must wear their official contest clothing to the contest orientation meeting.

ELIGIBILITY

(Team of 2*) Open to active SkillsUSA members enrolled in programs with Cyber Security, Information Security, or Systems and Networking Security Architecture as the occupational objectives.

EQUIPMENT AND MATERIALS

1. Supplied by the technical committee:

This includes all reference materials, diagrams, and instruction required for the contest.

a. Switch fabric for network connectivity

a. Personal Computers

b. USB Thumb Drives

L2/L3 Managed Switches

Enterprise Routers

Putty Software

a. Network Server System

a. Hardware Firewalls

a. Wireless Access Points

b. Wireless Network Capability

c. Tablet PCs/Smartphones

*Autopsy Software (Installed)

*AccessData FTK Imager (installed)

e. USB Thumb Drives

f. Write Blocker Device

g. SD Card Reader

a. Log files from PCs, access points, servers, and routers.

c. Network Cables

d. Console Cables

b. Bootable Kali USB Thumb Drives.

c. WiFi Adapters Capable of Promiscuous Mode Operation

2. **Supplied by the contestant:**

a. Resume

b. Blank Paper

c. Writing Instrument

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 include:

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 CompTIA'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, pentesting tools, and digital/network forensic activities. The exam consists of multiple-choice questions and lasts 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

1. 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. The domains of the contest are as follows:

The outcome and winners are determined by the combined scores from both domains

****

Standards and Competencies

Professional Activities Station

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

a. Train a fellow employee how to avoid phishing attempts associated with emails and web sites. This should include user level examples of things to look for to avoid common items used as bait.

b. Explain requirement for (and methods of) creating strong passwords to senior management personnel in your company.

c. Provide legally sound advice and recommendations to management on a variety of cyber security topics.

- d. Provide sound recommendations to management on a variety of cyber security policies.

- Separation of Duties Policies
- Acceptable Use Policies
- Mandatory Vacation Policies

- Conduct training of the organization's staff on a variety of employee cyber security activities.
  - Use of Antivirus Software
  - Use of Anti Malware Products.
- 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

SP 2.4 – Outline principles and concepts of data storage and security (System Architecture SP-ARC002)

Suggested Changes/Additions:

a. Form of documentation (handout/visual aid)
b. Timed presentation on set list of topics
Students will be informed of topics, prior to the competition

End-Point Security Station

Contestants will display knowledge of industry standard processes and procedures for hardening an end point or stand-alone computing device.

a. Configuring BIOS/CMOS settings to secure the outer perimeter of a personal computer.

*Configure BIOS Passwords to Safeguard the CMOS Area and Control Access to the Operating System

*Enable/Disable USB ports

* Manage Boot devices and boot order

b. Take steps to harden an installed operating system.

*Create Secure Passwords

*Given a Scenario Configure Lockout Policies

* Given a Scenario Create and Manage Local User Policies

* Given a Scenario Assign User Privileges based on the Principle of Least Privilege

*Disable Vulnerable Accounts

* Given a Scenario Manage Services and Ports Securely

*Identify and Remove Unnecessary Software Applications

c. Secure data at rest in a personal computer.

*Apply File and Folder Level Encryption

* Apply Disk Level Encryption

d. Install/configure antivirus/antimalware

*Perform Secure Local Firewall Configurations

*Write a Rule to Allow or Deny Specific Traffic to Pass Through the Firewall

* Given a Scenario Perform Secure Browser Configurations

SP 1.1 – Demonstrate abilities to securely provision operating systems, software, and configure security at initial provisioning stages (Securely Provision SPDEV-001)

Suggested Changes/Additions:

- Change/alter hardware capabilities
- Automate Grading

Managed Switch Security

This task contains security-related activities associated with managed switches.

a. Access a managed switch's management environment.

*Establish an IP Address for the Switch's Management VLAN

b. Enable Access Security for the Switch's Admin Environment.

*Configure an Encrypted Password for the Switch.

c. Create Multiple VLANs to Establish Segmented Network Security Zones

d. Manage Switch Port Security

*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 Telnet or SSH Administrative Access to the Switch.

Suggested Changes/Additions:

- Change/alter hardware capabilities
- Virtualize if possible (cisco packet tracer)
- Automate Grading

Enterprise Router Security

This task contains activities associated with accessing an enterprise router, configuring it to create network security structures and establish security for the router itself.

a. Access an Enterprise Router's Management Environment.

* Enable Access Security for the Router's Admin Environment.

*Configure an Encrypted Password for the Router.

b. Create a Routing Scheme to Route Traffic from one Designated Network to Another.

*Given a scenario Set up Static Routing

*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.

Suggested Changes/Additions:

- Change/alter hardware capabilities
- Virtualize if possible (cisco packet tracer)
- Automate Grading

Server Hardening

This task contains activities related to hardening servers against attack.

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.

*Create and Manage Network User Policies

*Assign User Privileges Based on the Principle of Least Privilege

*Disable Vulnerable/Unnecessary User Accounts

*Manage Services and Ports Securely

d. Secure Data at Rest in a Server Environment.

e. Perform Vulnerability Scans and host-based service system calls on Operating Servers

f. Given a Scenario Create Virtual Machines/Networks on a Server

SP 1.1 – Demonstrate abilities to securely provision operating systems, software, and configure security at initial provisioning stages (Securely Provision SPDEV-001)

Suggested Changes/Additions:

- Automate Grading
- Expand scenario
- Change difficulty
-

Network Boundary Security

This task contains activities related to installing and configuring typical network boundary devices and structures to form an effective network zone or edge security systems.

a. Access a hardware Firewall's management environment.

*Establish an IP Address for the Firewall's Management Console

b. Enable Access Security for the Switch's Admin Environment.

*Configure an Encrypted Password for the Switch.

c. Given a Scenario use a Hardware firewall to Create and Configure Perimeter Security that provides a boundary between two Network Zones that have Differing Security Levels.

*Implement a Network Perimeter Firewall

*Create a DMZ

d. Perform file hashing on a downloaded file to verify its integrity.

c. Establish and Configure an ACL on the firewall to limit or restrict access to assets as required by the organization's security policies.

e. Enable NAT for specific types of Network Traffic.

f. Create a VPN Connection.

g. Span a Firewall Port for Monitoring Purposes.

h. Configure IPSec on the Firewall.

i. Configure IDS/Splunk

Suggested Changes/Additions:

- Change/alter hardware capabilities
- Virtualize if possible (cisco packet tracer/pfSense)
- Automate Grading
- IDS/Splunk additions

Wireless and Mobile Device Security

This task contains activities related to installing, configuring and securing wireless Access Points and Mobile Devices.

Suggested Hands-On Activities Include:

a. Securely Install, Connect and Configure a Wireless Access Point.

*Create a Secure Password for the AP/Router

*Given a Scenario configure the most Secure Authentication Protocol Available

*Turn Off any Guest Networks

b. Configure Secure WiFi operation of the AP.

*Hide the SSID Broadcast

*Change the Default SSID

*Lower the Antenna Power to limit the Usable Distance of the WiFi signal

*Configure MAC Filtering to Restrict Access

c. Configure Wireless Router Options.

d. Configure Wired AP/Router Options.

*Given a Scenario Limit the DHCP Pool Size to Control the Number of Wireless Devices that can Connect to the Network

e. Configure a WAN (Wireless Area Network)

f. Reset a Typical Access Point.

Suggested Changes/Additions:

- Reimagine previous implementation
- No smart phones
- Change/alter hardware capabilities
- Virtualize if possible (cisco packet tracer)
- Automate Grading

Digital/Network Forensics

This task 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.

a. Wireshark PCAP analysis

a. Given a set of log files created during a given activity, the contestant must be able to analyze the activity occurring, determine whether it is an event or not, and describe best practices for mitigating the event if so.

b. Collect, process, preserve, analyze and present computer related evidence in support of network vulnerability mitigation and/or criminal, fraud, counter intelligence or law enforcement investigations.

c. Scan USB Thumb Drives or SD Cards for deleted files

d. Create a forensic image of a drive.

e. Create a memory dump of a suspected computer.

f. Perform a live data acquisition.

PR 5.1 – 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)

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 for the purposes of mitigating threats (Protect and Defend: Defense Analyst PR-CDA-001)

Pentesting

This task 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.

a. Conduct a Port Scan

b. Perform a Network Vulnerability Scan

c. Perform a Wireless Sniffing Operation

d. Perform a WireShark Scan

e. Enumerate a Network

f. Analyze Collected Information to Identify Vulnerabilities that Pose the Possibility of Exploitation.

f. Perform a DoS Attack Against a Specified Target

g. Hack a Specified file (flag) in a Remote Network

h. Perform Steps to Establish Persistence in a Compromised network or Device

SP 3.2 - Preparation and execution of tests against systems requirements to analyze results (Test and Evaluation SP-TST-001)

Committee Identified Academic Skills

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

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 academic standards.

Math Standards

• Linear algebra

• Trigonometry

• Calculus

• Data analysis and probability

• Operational analysis

• Problem solving

• Reasoning and proof

Source: CareerOne stop https://www.careeronestop.org/competencym

odel/comp etency-models/cybersecurity.aspx Select “Academic Competencies” from model.

Source: NIST Publication 800-181 CyberSecurity Workforce Framework http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-181.pdf Page 60 Reference K0052

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: https://www.mcrel.org/standards-curriculum/

Language Arts Standards

• Students apply a wide range of 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 of 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 use of spoken, written and visual language (e.g., conventions, style, vocabulary) to communicate effectively with a variety of audiences and for different purposes

• Students use spoken, written and visual language to accomplish their own 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

SkillsUSA State Competition

Below is information to help you prepare your students for our upcoming SkillsUSA competition on March 5th, 2019 at the TN Fire Codes Academy in Unionville, TN.

Students will need to bring one laptop and one "clean" USB/Flash Drive for the team. The laptop must have the following software downloaded prior to arrival:

- Wireshark
- Zenmap
- Nmap
- Owasp Zap
- Kali (optional)
- Autopsy
- Volatility
- Network Miner

(NetworkMiner is a Network Forensic Analysis Tool for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.)

- Nessus (optional)

(The Nessus Project was started by Renaud Deraison in 1998 to provide to the Internet community with a free remote security scanner. ... Today, the product still exists in two formats; a limited, free version and a full-feature paid subscription option. Nessus is available for Linux, Windows, and Mac OS X)

The competition is composed of four different stations that will test a particular set of skills by solving a specific problem. The software listed could be used in any of the stations.

Review the attached document that lists all possible competencies that may be tested. I suggest creating scenarios for your students to practice based on the competencies listed. Once a station is completed, contestants will have captured a "flag". The teams who capture the most flags in the given time will be our winners!

JSCC Student Participants:

Matthew Nelson

Benjamin Wallis

SkillsUSA Membership

Computer Technology

Advisor: Randall Callahan rcallahan1@jscc.edu

Academic Year: 2019

Anthony, Justin

Ard, Billy

Cavasin, Jerrold

Garrett, Samuel

Hicks, Joseph

Isaachsen, Michael

Jamison, Stephen

Kolanda, Patrick

Massey, Brent

Mireles Valdes, Margarito

Nelson, Matthew

Stafford , Chris

Vires, Matthew

Wallis, Benjamin

Health Sciences

Advisor: Kenneth Oxford koxford@jscc.edu

Academic Year: 2019

Allen , Taylor

Burg, Brianna

Hock, Ryan

Hylton, Justin

Sumler, Hope

SkillsUSA Tennessee PS 2020 Update

Feb 10, 2020	*Registration Deadline for Public Safety & Security Competition* *https://www.skillsusa-register.org*
February 2-8, 2020	National SkillsUSA Week
February 10-March 1, 2020	*Registration for State Conference AND CNC Haas competition* *https://www.skillsusa-register.org*
February 10-11, 2020	**Human Services Sector State Competition** Hosted at TCAT Dickson- Clarksville Campus
March 1, 2019	National SkillsUSA Membership Deadline Chapter of Excellence Submission Deadline
March 5-6, 2020	**Public Safety and Security State Competition** TN Fire Codes Academy, Unionville, TN
April 16, 2020	**CNC Competitions** at HAAS, Franklin, TN * m*ore details to come*
April 19-22, 2020	**SkillsUSA Tennessee Leadership and Development Conference** Chattanooga Convention Center
April 23-May 6, 2020	*Registration for NLSC https://www.skillsusa-register.org*
June 23-26	**National Leadership and Skills Conference** Louisville, KY, KEC

Additional Updates:

ADVISOR OF THE YEAR QUALIFICATIONS

1) Chapter Excellence Level 2: Chapter of Distinction In order to submit an AOY application, the Advisor's school must have completed Level 2 of the Chapter Excellence Program and submitted the CEP Application online. More information on the Chapter Excellence Program can be found here:

2) Joined Professional Member of SkillsUSA. In addition, the AOY applicant must have joined SkillsUSA as a Professional Member in the year of their National nomination. The new process requires that the advisor has completed the level 2 Chapter of Excellence application before the link for the Advisor of the Year application will activate.

Teachers are now allowed to nominate themselves and complete the application process. There are six primary essay-type questions to complete for each AOY application. Advisors should enter their responses for each question, clicking Save periodically. Some advisors may want to

craft responses to these questions in an offline Word document then copy/paste into the website.

Our state winner will go on to compete against our region, and if the win, they will move forward to the National Advisor of the Year competition. This award is a great honor to bestow upon our advisors, and I hope you apply, and/or encourage your best of the best SkillsUSA advisors to apply!

In order to advance an application to the regional level, you must supply three letters of support, one from a School Administrator, one from a Student, and one from the SkillsUSA State Director. For the state competition, you only need to upload the School Administrator and student letter.

The **deadline to receive applications is March 1, 2020**. The regional scoring will take place April 1, 2020. We will acknowledge our Advisor of the Year on stage at the state conference in Chattanooga!

If you have any questions, please email **support@skillsusa-register.org**

Contest Updates

Keep checking back to our state conference page for updates to state contests. I will send out a group email periodically, but to stay ahead of the game, make sure you or your students are watching the site! Click link below for first update

Additive Manufacturing

NEW this Year at State Conference

This year our VIP Dinner will take on a transformation to become the **#REDisMYcolor VIP Dinner**!

"Transformation Highlights"

- Attire can be SkillsUSA Blazer/Professional, **OR** Red semi-formal cocktail attire! Think "Red and Glitzy"!
- We will have a professional DJ and Dance Floor for **Postsecondary attendees** to celebrate your Chapter of Excellence and New Chapter successes!
- To secure your invitation to this notable event, you must complete your **Chapter of Excellence** application by March 1, 2020. Each institution will receive 5 complimentary tickets to the dinner/dance, and can purchase additional dickets for $40 each.

	Room	Check in Date	Check Out Date	Total Number of Nights	Occupant	Gender	Program Area	Competition
1	Single	3/5/2020	3/6/2020	1	MATTHEW NELSON	MALE	CYBERSECURITY	CYBERSECURITY
2	Single	3/5/2020	3/6/2020	1	BENJAMIN WALLIS	MALE	CYBERSECURITY	CYBERSECURITY
3	Single	3/5/2020	3/6/2020	1	RANDY CALLAHAN	MALE	CYBERSECURITY	INSTRUCTOR
4	Single	3/5/2020	3/6/2020	1				
5	Single	3/5/2020	3/6/2020	1				
6	Single	3/5/2020	3/6/2020	1				
7	Single	3/5/2020	3/6/2020	1				
8	Single	3/5/2020	3/6/2020	1				
9	Single	3/5/2020	3/6/2020	1				
10	Single	3/5/2020	3/6/2020	1				
11	Single	3/5/2020	3/6/2020	1				
12	Single	3/5/2020	3/6/2020	1				
13	Single	3/5/2020	3/6/2020	1				
14	Single	3/5/2020	3/6/2020	1				
15	Single	3/5/2020	3/6/2020	1				
16	Single	3/5/2020	3/6/2020	1				
17	Single	3/5/2020	3/6/2020	1				