

# ***Regional Advisory Committee Meeting***

Region 14 Education Service Center  
Taylor Room – 10:00 a.m. – November 4, 2020

**8:30 – WTTC Meeting – Nolan Room**  
**10:00 – RAC Business – Dr. Dana Marable, Chairman of RAC**

## **A G E N D A**

### **Center for Instructional Improvement/Administration – *Shane Fields***

- . Introduce Guests
- . BCSA Business - Mid Winter Conference - *virtual*
- . BCSA Dues
- . Evaluation Surveys
- . ACP Program Information - *flyer*

### **Center for Technology Services – *Robb McClellan***

- . Digital Innovation Update
- . Technology Update
- . WTTC Update

### **Center for Instructional Leadership & Federal Programs - *Emilia Moreno***

- . Administrative Updates
- . Curriculum Updates
- . Federal Information
- . Training Opportunities

### **Center for Teaching and Learning – *Lisa White***

- . Special Education Update

### **BCSA Officers**

**President - Dr. Dana Marable - DeLeon ISD**  
**President-Elect - Dr. David Young - Abilene ISD**  
**Past President - Bobby Easterling - Jim Ned CISD**  
**First Vice-President - Dr. Jason Cochran - Eastland ISD**  
**Second Vice-President - Jonathan Scott - Albany ISD**



# Region 14 Education Service Center Alternative Certification Program

## Tina Wyatt

Program Coordinator  
Teacher Certification  
Master of Education  
Associates Degree Program  
(325) 675-7026  
[twyatt@esc14.net](mailto:twyatt@esc14.net)

## Billie McKeever

Superintendent Program  
(325) 675-7014  
[bmckeever@esc14.net](mailto:bmckeever@esc14.net)

## Greg Priddy

Principal Program  
Office: (325) 675-8684  
[gpriddy@esc14.net](mailto:gpriddy@esc14.net)

## Programs Offered

- Teacher Certification  
*Now Enrolling for 2020-2021 Cohort Through December 1st, 2020.*
- Principal Certification
- Master of Education with Principal Certification
- Superintendent Certification
- Associates Degree in Child Development  
*In collaboration with Cisco College - An opportunity for educational aides to earn an associates degree in child development while continuing to work!*
- GED Testing

*Questions?  
Contact us!*

**Candice Escobar** Administrative Assistant - (325) 675-7020 [cescobar@esc14.net](mailto:cescobar@esc14.net)

See more at [https://www.esc14.net/page/acp\\_home](https://www.esc14.net/page/acp_home) or [bit.ly/312FgNR](https://bit.ly/312FgNR)



## FIELD SERVICE ANNOUNCEMENTS FOR NOVEMBER

Rick Howard, Field Service Representative

We have a lot going on in the way of training and services right now so please review the items below.

### [Legal Seminar, November 5-6](#)

As with all our other training this fall, the annual Legal Seminar will be presented in virtually. The attorneys from TASB Legal Services are providing up to six hours of continuing education credit (CEC) for registered attendees. Two topics will be broadcast on Thursday, November 5, and two topics on Friday, November 6. During the broadcasts, presenters will be available online to answer your questions. In addition, both sessions will be followed by a live Q&A panel for up to two hours of credit. All sessions will be recorded and available to registered attendees for 30 days after the broadcast.

### [XG Conference, November 9-10](#)

The XG Summit highlights current research and promising practices related to school governance and student success. TASB hosts this convening of national thought leaders with Texas trustees and administrators. Trustees and superintendents share their examples of promising practices related to leading governance research. Attend the summit to learn more about the latest research and what that looks like in Texas public school governance.

### [Teacher Incentive Allotment Strategic Planning Workshop, November 17-18](#)

Hear from the experts at TASB HR Services and Kreuz Consulting Group about TIA and effective models of educator incentive programs.

Topics covered:

- Determining steps and decisions to prepare for TIA implementation
- Planning strategically for TIA system development
- Coordinating educator evaluation systems and student growth measures
- Implementing and managing a student learning objective (SLO) process
- Transforming your district's talent management processes into an integrated system
- Examining Human Capital Management Systems and lessons learned across the nation

### [Student Video Contest, Opens Dec 1](#)

Back by popular demand, we hope this year's Student Video Contest is bigger and better than ever! Make a creative video showing how your school has learned and grown in the face of adversity. Rural, urban, big, small—every school community faces its own unique set of challenges each school year. The goal of the video is to highlight how your school has boldly overcome barriers to support students, teachers, and public education as a whole. Previous year submissions are available at the link for models to consider. In each category (elementary, middle/junior, and high school) there will be a first prize of \$5,000 and a second prize of \$2,500 awarded to the school to be used in the winners' classroom. Submission closes on January 21, 2021.

## [Business Recognition Program, Opening Soon](#)

Texas public schools benefit tremendously from the generous support of businesses and organizations in their community, especially through this most difficult set of circumstances. Whether they choose to champion a specific event, activity, program, campus, the education foundation, Partners in Education, or the entire district, local businesses and community groups are vitally important to the success of public schoolchildren in our state. Express your appreciation by recognizing entities in your community that contribute valuable support to your district. Historical files are available at the link for the past 3 years for you to refresh your memory about the businesses you have honored before.

## [School Board Recognition Month—January](#)

If not already, you should be receiving your School Board Recognition Planning Kit very soon. It's not too early to begin your preparations for honoring your school board in January. Take full advantage of the opportunity to lavish them with meaningful recognition for their service!

And Lastly!

## [Local Policy Review](#)

The Policy Consultants that work with your districts recommend a complete review of all your LOCAL policies every 5-8 years or any time any significant change in leadership occurs on the board or among campus and district administrators. Sixty to 75% of you have not had a Policy Review within the last 5 years. You may ask why it is necessary when you are faithful to adopt the updated LOCAL policies included in the periodic updates. The best answer to the question is that only the LOCAL policies related to the LEGAL updates are reviewed by staff attorneys. That leaves a lot of LOCAL policies at risk of not being reviewed until a Local Policy Review is conducted. The **Review** is an exercise that matches practice with adopted policy and everyone knows that when the two don't agree, it is a fatal flaw and quickly overturned by a judge, hearing officer or Commissioner—imagine a Val/Sal controversy! It may also be an opportunity to implement best practice that your consultant has identified in another district. The consultants are scheduling now for next summer and that was my preferred time to do it as a superintendent. If interested in a proposal, either contact me or your policy consultant. Either of us can also provide the date of your last review.

Now to close—keep up the great work and now that we are approaching the Thanksgiving holiday, look for your blessings to be thankful for and be sure to express your gratitude!



**Rick Howard**

*Field Service Representative*

Texas Association of School Boards  
12007 Research Blvd. • Austin, Texas 78759-2439  
512.505.2474, ext. 2474 • 800.580.8272  
CELL 325.642.5180

Region 14 ESC  
RAC Meeting  
November 2020

# Center For Technology Services

Robb McClellan, Director



# DIGITAL INNOVATION



*Supporting Non-Traditional Instructional Strategies  
through Modern Learning Experiences*

- G Suite for Education
- MakerEd
- Coding
- COMPILE
- Social Media
- PBL
- Design Thinking
- AR/VR in EDU
- BreakoutEDU
- Drones
- Robotics
- 3D Design and Printing
- Laser Design
- CNC Production
- Video and Podcast
- Discovery Education
- Tech Apps
- Dig Inn! Collaboration
- Digital Docs - On Call!
- ENDLESS DESTINATIONS!

## Digital Innovation Consultants

*Christy Cate*

[ccate@esc14.net](mailto:ccate@esc14.net)

(325) 675-7028

*Hilary Miller*

[hmiller@esc14.net](mailto:hmiller@esc14.net)

(325) 675-8630

*Shawn Schlueter*

[sschlueter@esc14.net](mailto:sschlueter@esc14.net)

(325) 675-8645



*Let's enjoy  
the ride*



<https://goo.gl/Ry1UJZ>

November 2020



# DIGITAL INNOVATION



## Summer PD

### Google Galore!

- ❑ 74 Teachers Requesting Assignments
- ❑ 177 Individualized Assignments Completed
- ❑ 16 Google Apps to Choose



Enjoy the Showcase

## PANDEMIC RESOURCES



Google's hub of information to help teachers during COVID-19



COVID-19 Educational Resources App - search by content and age group

- ❑ School Closure Planning Documents by Nicole Zumpano
- ❑ Online Learning Doctrine by Jennifer Pearson



More Guides and Resources Available



<https://sites.google.com/esc14.net/remote-learning>



<https://goo.gl/Ry1UJZ>

November 2020



# DIGITAL INNOVATION



## Professional Development

### PD to Start the Year

#### Haskell-Knox SSA

- Oh the Places You'll Go with Virtual Learning
- Google Slides Interactivity
- Pear Deck and Google Slides



Enjoy the [Playlist](#)

#### Hawley

- Google Classroom Overview



Classroom [Playlist](#)

### Consortium Spotlight

#### BrightBytes

- Single platform for all educational data
- Determine best places to allocate resources
- Monitor trends and progress over time



[ESC 14 Presentation](#)

### Google Meet Enterprise

Aspermont, Clyde and Merkel teachers received training:

- Breakout Rooms
- Q & A
- Polls
- Noise Cancellation



[Google Meet](#)







# DIGITAL INNOVATION



## Discovery Education

### Does your district need training?

- |                                       |   |
|---------------------------------------|---|
| <input type="checkbox"/> Abilene      | <input type="checkbox"/> Lueders-Avoca        |
| <input type="checkbox"/> Albany       | <input type="checkbox"/> <b>Merkel</b>        |
| <input type="checkbox"/> Baird        | <input type="checkbox"/> Moran                |
| <input type="checkbox"/> Blackwell    | <input type="checkbox"/> Paint Creek          |
| <input type="checkbox"/> <b>Clyde</b> | <input type="checkbox"/> Rule                 |
| <input type="checkbox"/> Comanche     | <input type="checkbox"/> Sidney               |
| <input type="checkbox"/> Cross Plains | <input type="checkbox"/> Snyder               |
| <input type="checkbox"/> Eastland     | <input type="checkbox"/> St. John's Episcopal |
| <input type="checkbox"/> Gustine      | <input type="checkbox"/> Stamford             |
| <input type="checkbox"/> Hawley       | <input type="checkbox"/> Trent                |
| <input type="checkbox"/> Lorraine     | <input type="checkbox"/> Wylie                |



**Discovery  
Education**

Email [ccate@esc14.net](mailto:ccate@esc14.net)

## Google Jamboard

### Have you explored the features?

- Online whiteboard
- Core G Suite service
- Built into Google Meet
- Saves automatically to Drive
- Collaborative
- App with autoshape and auto handwriting recognition



**ESC 14  
Training video with  
Presentation in  
Description**





# DIGITAL INNOVATION



## THL 3.0's SCHOOLOGY vs. GOOGLE CLASSROOM



**Schoolology**

### PROS

- Pre-built lessons (when available)
- Campus-wide overviews

### CONS

- 4-8 week set-up
- Complex interface
- Costs (after 2 yrs.)



**Google Classroom**

### PROS

- Already utilized
- Integrated with G Suite applications
- Simple interface
- No cost (always)

### CONS

- Limited campus/district-level reporting

- What do you expect to need from your Remote Learning solution?
- Which LMS reduces the “doubling” of work by teachers and IT at your district, serving in-class and at-home students simultaneously?

## TCEA

**TCEA**  
CONVENTION & EXPOSITION

**We have some BIG ideas for 2021. Explore them all.**  
February 1-5, 2021 • In-Person + Online • Dallas, Texas

Dallas Convention Center  
REGISTRATION IS OPEN





# DIGITAL INNOVATION



## Service Station Check-Out is Going Strong!



**\*Region 14 ESC has thoroughly cleaned the tech resources you are utilizing.** Please employ your districts COVID-19 policy in regard to sharing technology devices and cleaning between access. If you are uncertain about proper cleaning techniques or acceptable chemical solutions, please contact Shawn Schlueter at [sschlueter@esc14.net](mailto:sschlueter@esc14.net).

Reach out to continue extending non-traditional instructional resources to ALL students.

- ❑ **Google Expeditions** - already traveled to Merkel, heading to Abilene soon
- ❑ **Ozobots** - already headed to Wylie, heading to Abilene soon
- ❑ **Magnastix, Tinker Toys and Strawbees** - heading to Abilene before Christmas
- ❑ **Drones** (jumping and flying) - prepping for Abilene right after Thanksgiving
- ❑ **Rubiks Cubes** - scheduled for Abilene

Virtual Trips to the Service Station are possible!

- ❑ Merkel High School enjoyed virtual exploration of the CNC router.



Click [here](#) for reservations!



<https://goo.gl/Ry1UJZ>

November 2020



## **E-rate Update November 2020**

470 window is open now.

The official “2021 Eligible Services List” has not been released yet but expects to be unchanged from last year.

Schools can use their numbers from last year.

They all have a new pot of C2 money for the next 5 years and can see that amount in the the EPC portal or multiply their total student count by \$167.

There is no more campus budget, just a district budgets.

The 471 window is scheduled to open in early to mid January.



# E-rate Update

## August 1, 2020

To login, a user will first enter their regular username and password. The system will then send the user a temporary security passcode to be entered as shown below.



### Email Authentication

USAC requires multifactor authentication to add an additional layer of security when signing in to your account.

✔ Passcode has been sent to the following email address!

Email Address

Enter passcode

[Re-send Email](#)

[Verify](#)



# E-rate Update

## August 1, 2020

### **Closer to Home:**

To provide your district the most effective and efficient E-rate service we have created a system called TechTrack. Anytime you have an erate question or issue just submit a TechTrack ticket through [District Depot](#) and we'll respond as quickly as possible. The goal is to provide timely communication as well as accurate documentation. Your login credentials should be the same as your Pitstop credentials. Click on the Region 14 TechTrack icon and follow the prompts.

Link to District Depot:

<https://districtdepot.esc14.net/DistrictDepot/Login.aspx?ReturnUrl=%2fDistrictDepot%2f>



# E-rate Update

## August 1, 2020

### What is E-rate?

E-rate: Universal Service Program for Schools and Libraries:

The FCC's E-rate program makes information services more affordable for schools and libraries. With funding from the [Universal Service Fund](#), E-rate provides discounts for Internet access and internal connections to eligible schools and libraries.

The ongoing proliferation of innovative digital learning technologies and the need to connect students, teachers and consumers to jobs, life-long learning and information have led to a steady rise in demand for bandwidth in schools and libraries.

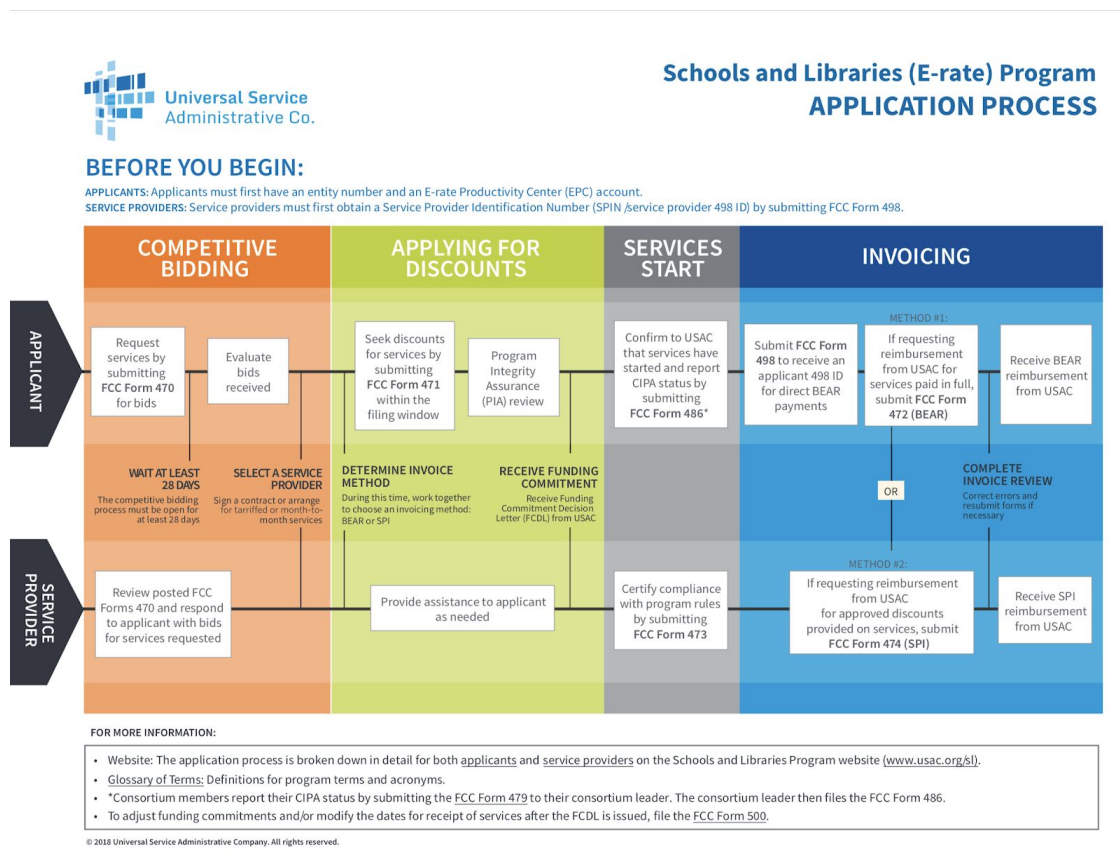
In recent years, the FCC refocused E-rate from legacy telecommunications services to broadband, with a goal to significantly expand Wi-Fi access. These steps to modernize the program are helping E-rate keep pace with the need for increased Internet access. Eligible schools and libraries may receive discounts on Internet access, as well as internal connections, managed internal broadband services and basic maintenance of internal connections. Discounts range from 20



# E-rate Update August 1, 2020

to 90 percent, with higher discounts for higher poverty and rural schools and libraries. Recipients must pay some portion of the service costs.

## Erate Process at a glance:



I look forward to assisting you in any way I can.

Brit Pursley  
ESC 14 / E-rate  
325-675-8627  
bpursley@esc14.net







## *Security Coop*

October 30, 2020

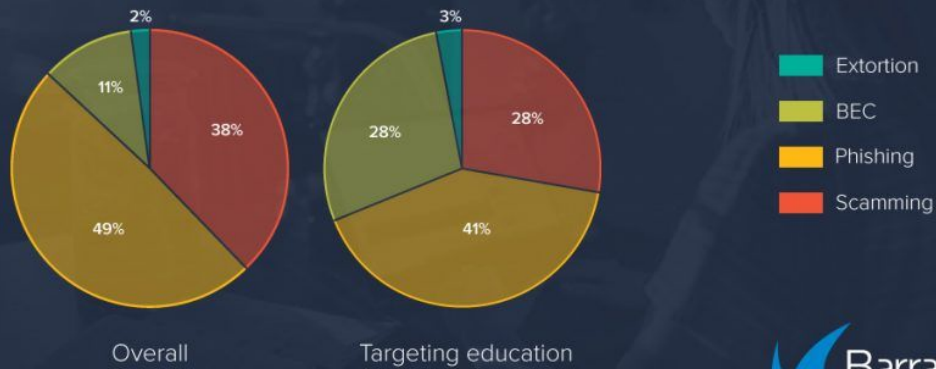
### **Schools hit with Data Breaches in September 2020**

During the month of October 2020, there have been **35 publicly-disclosed school incidents**, including student and staff data breaches, ransomware/other malware outbreaks, phishing attacks, other social engineering scams, denial-of service attacks, and a wide variety of other incidents. During National Cyber Security Month Barracuda Networks data shows that K12 schools are more than twice as likely to get hit with a business email compromise (BEC) than any other companies outside of education. According to Barracuda Network, “BECs accounted for 28% of all spear-phishing attacks aimed at educational institutions, while for all other verticals it was 11%. In addition, within education 57% of malicious emails came from internal – primarily students’ – email accounts.” I will have the pie charts below. I will also provide the link to the 4 ways to protect your school district.

[How to Protect Your Educational Organization](#)

# Types of spear-phishing attacks

June–September 2020



# Spear-phishing attacks targeting education

June–September 2020



---

## **Ports that are being Blocked:**

Cisco is set up to block the following.

Dynamic list of known ransomware domains and IP addresses. Block all countries except Canada and the US. Only allow DNS for root servers and known good DNS.


- BLOCKED PROTOCOLS
- SMB
- QUIC
- ICMP
- Ping
- SNMP
- SMTP
- DNS
- IPSec
- SSH-Tunnels
- TELNET
- NTP

---

**Steps we are taking to protect you:**

- **Implement the 46 policies into your security plan.**
- **Goal to complete new policies and procedures for this year.**
- **Being behind our Firewall.**
- **Training users with KnowBe4.**
- **Blocking sites with Smoothwall.**
- **Integrating Perch Security to our networks**
- **Vulnerability and Penetration Testing**

**Steps we will take in the future:**

- **Make sure all staff is aware of the district policies and procedures.**
  - **Using SendSafely or Gmail to send sensitive information through email.**
  - **Weekly newsletters from Perch Security**
  - **24/7/365 Network monitoring**
- 



---

# Attacks Risk Report

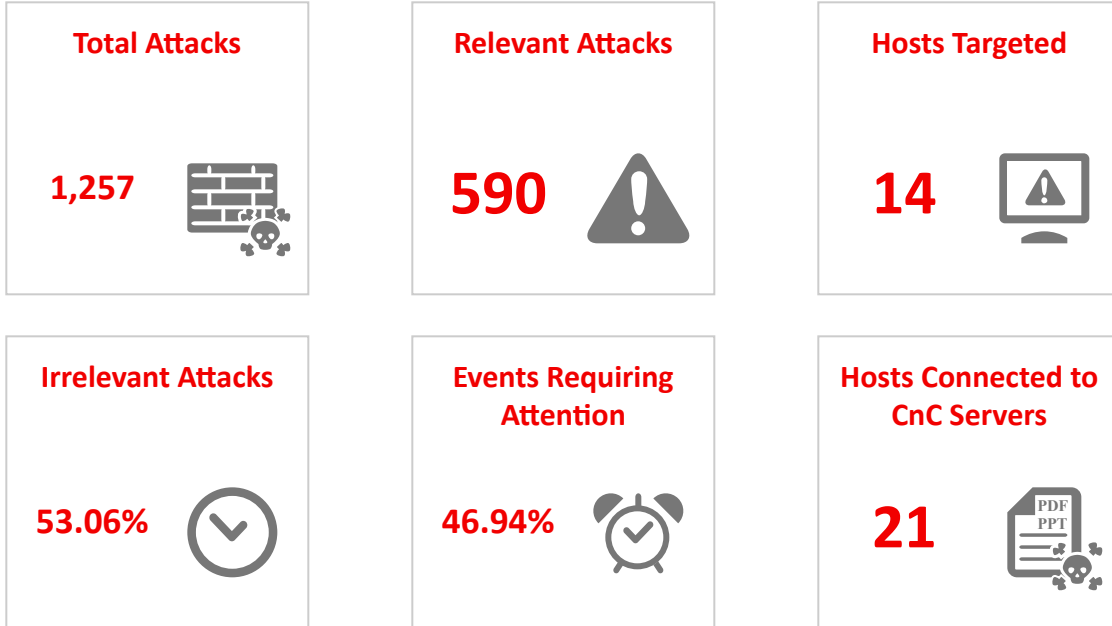
Friday, October 30, 2020



# I. EXECUTIVE SUMMARY

Cisco has determined that your company is at a high risk due to the observation of attacks on the network targeting hosts that may be vulnerable. These attacks and hosts require further investigation to help lower the risk.

**Assessment Period: Fri Oct 23 2020 14:13:04 to Fri Oct 30 2020 14:13:04**



## RELEVANT ATTACKS CARRY THE FOLLOWING RISKS

CLASSIFICATION	COUNT
A Network Trojan was Detected	1,016
Web Application Attack	83
Attempted User Privilege Gain	67
Potential Corporate Policy Violation	33
Detection of a Denial of Service Attack	32

Cisco recommends that your company deploy Cisco Firepower Appliances to:

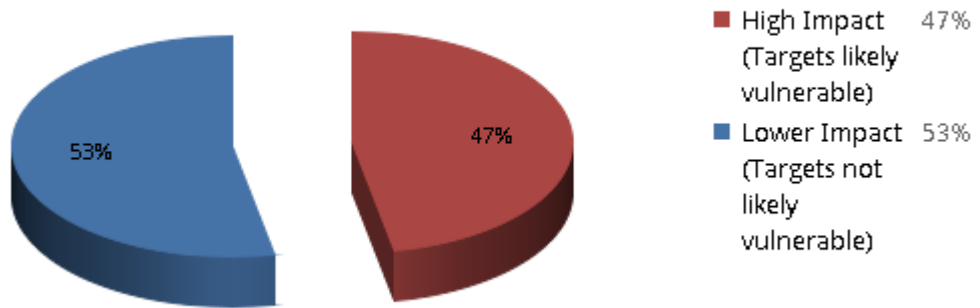
1. Establish continual visibility into its network attack risks
2. Implement automated protections in order to mitigate this risk going forward



## II. ASSESSMENT RESULTS

### IDENTIFYING CRITICAL ATTACKS USING IMPACT ANALYSIS

Of the 1,257 total attacks on your network, 590 (46.94%) of them were considered high impact. That means they targeted machines that were likely vulnerable to these attacks. These events are the most critical to investigate, and Cisco automatically identifies them for you. Cisco identifies high impact events automatically by correlating attacks with target risk, which is determined by passively profiling your network devices and their vulnerabilities in real time. This saves time and money over traditional solutions, which require you to qualify all events manually or import scan data from other systems. If a staff member's time is worth \$75 per hour and each attack takes 10 seconds to qualify, then each attack costs \$0.21 to manually qualify. The difference in qualification time and cost between Cisco and traditional solutions is substantial.



ATTACKS TO QUALIFY / YEAR	COST TO QUALIFY	COST TO QUALIFY ALL ATTACKS
65,544 estimated total attacks	\$0.21	\$13,764.15
30,764 estimated high impact attacks	\$0.21	\$6,460.50

**Year #1 Cost Savings: \$7,303.65**  
**Year #5 Cost Savings: \$36,518.25**

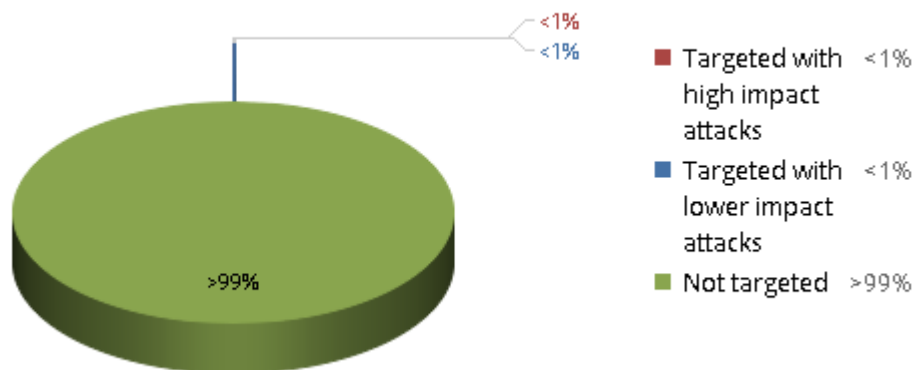
## HIGH IMPACT ATTACKS

The following attacks are very important to investigate because they directly target machines that have been identified as potentially vulnerable. The target machine's operating system version, running services, and potential vulnerabilities all match what the threat is designed to attack.

EVENT TYPE	DETAILS	POTENTIALLY VULNERABLE HOSTS
A Network Trojan was Detected	MALWARE-BACKDOOR JSP webshell backdoor detected (1:39058:2)	13
A Network Trojan was Detected	MALWARE-CNC Win.Adware.BrowserAssistant variant outbound connection (1:51593:1)	2
A Network Trojan was Detected	MALWARE-CNC Andr.Spyware.iSpyoo variant post-compromise outbound connection (1:50435:1)	1
A Network Trojan was Detected	MALWARE-CNC Andr.Spyware.iSpyoo variant post-compromise outbound connection (1:50436:1)	1
A Network Trojan was Detected	MALWARE-CNC Win.Trojan.Azorult outbound connection (1:48552:1)	1

## HOSTS AT HIGH RISK

0.04, 0.09% of your monitored hosts have been targeted with high impact attacks during the assessment period. They are at high risk of infection. The attacks should be investigated and the machines assessed to ensure proper controls are in place. An additional {2}% of the machines discovered on your network were targeted with some form of attack.





## HOSTS ALREADY COMPROMISED

---

Special attention should be paid to computers already compromised by malware as they are likely to be exfiltrating information from your private systems. Systems that fall into this category likely have had malware residing on them for some time already and the initial infection has been missed by existing security protections.

SAMPLE LIST OF COMPROMISED DEVICES	TOTAL HOSTS CONNECTED TO CNC SERVERS
10.6.255.2	<b>21</b>
10.16.255.4	
10.17.0.174	
10.22.0.76	
10.33.0.201	

The systems listed above are exhibiting signs of compromise as they are connecting outbound to known Command and Control (CnC) servers tracked by Cisco Talos. You should take action to remediate or restore these systems.

## AUTOMATING THE TUNING EFFORT

---

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	266,468
A new host was added to the network	4,463
A device started using a new transport protocol	4,463
A device started using a new network protocol	8,790

As network changes are made, Cisco solutions automatically adjust policy so new operating systems, hosts, and protocols are protected. Cisco automates the tuning process by monitoring networks in real time and observing changes, and then making appropriate policy changes as a result. For example, if Windows 2000 hosts running IIS appear on the network, Cisco ensures that rules protecting against Windows 2000 and IIS vulnerabilities, and not irrelevant rules that may cause false positives, protect these hosts.

## APPLICATIONS ASSOCIATED WITH ATTACKS

---

The following applications have been identified as associated with attacks. You should identify applications in this list that have low business relevance and evaluate whether it would be helpful to control them on your network.

APPS ASSOCIATED WITH HIGH IMPACT EVENTS	COUNT	APPS ASSOCIATED WITH LOWER IMPACT EVENTS	COUNT
Android browser	541	Chrome	236
Web browser	31	Web browser	188
cURL	13	Mobile Safari	140
Chrome	2	Firefox	37
Firefox	2	RealAudio	10

## TOP ATTACKERS AND TARGETS

---

The top attackers and target machines observed in the attack attempts on your network are listed below. For high impact attacks in particular, you should ensure that targets are well protected from potential attackers by patching these machines and blocking potentially malicious traffic.

### High Impact Events

ATTACKERS	ATTACKS
10.100.65.171	544
208.76.225.82	15
20.57.170.186	12
208.76.225.75	10
10.16.255.4	5

TARGETS	ATTACKS
69.64.81.98	346
69.64.91.29	195
10.100.71.9	25
52.90.52.15	3
54.209.84.18	3

### Lower Impact Events

ATTACKERS	ATTACKS
10.16.255.4	362
10.30.128.9	75
35.213.181.65	27
45.79.225.74	26
45.41.134.96	22

TARGETS	ATTACKS
10.16.255.4	109
139.45.196.27	86
139.45.195.164	77
139.45.196.89	67
139.45.195.43	63

## IPv6 ATTACKS AND TRAFFIC

---

IPv6 traffic is a potential avenue for attacks that is often left unprotected by organizations. Network security is often thought of strictly from an IPv4 perspective, yet hosts may communicate internally and even externally to an organization over IPv6, exposing them to attack risks. The following communications were observed over IPv6 during the assessment period.

HOSTS USING IPv6 IN YOUR NETWORK (MONITORED)
<b>24</b>

ATTACKS SEEN OVER IPv6
<b>0</b>



## III. BUSINESS RISK OF ATTACKS

---

### BUSINESS RISK OF INTRUSION ATTEMPTS

---

Different types of attacks were detected on the network, each introducing different business risks. Here are the most common attack types observed along with the risks each introduces.

ATTACK CLASSIFICATION	NUMBER OF EVENTS	RISK ASSOCIATED WITH THE ATTACK
Potential Corporate Policy Violation	33	Information Theft: These events indicate usage of apps and protocols in ways that may be prohibited by organizational policy.
A Network Trojan was Detected	1,016	Infrastructure Damage, Information Theft: A trojan is a program that appears to be benign to an end user but is in fact malicious. It can be used to steal information or cause damage.
Denial of Service	32	System Degradation, Denial of Service: Denial of service (DoS) attacks attack the reliability of your network infrastructure, causing service to be denied to legitimate users.
Administrator/User Privilege Gain	93	Information Theft, Infrastructure Damage: Users on network machines who gain privileges illicitly may be able to steal information and control machines.



## IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, critical attacks are taking place and placing your organization at risk. New countermeasures and security controls are required to mitigate the risk.

Cisco recommends deployment of network-based protections via the threat-focused Cisco Firepower Next Generation Firewall and NGIPS Appliances to complement existing protections. These will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Real-Time Contextual Awareness	Profile hosts, applications, users, and network infrastructure in real time. Assess potential vulnerabilities and identify network changes.
Automatic Impact Assessment	Determine the risk of any attack to your business in real time in order to optimize response to it.
File Identification and Control	Detect and optionally block files by file type. Capture files for offline analysis, if desired.
Advanced Malware Protection (AMP)	Protect against malware with AMP for networks, which includes integration with AMP ThreatGRID for superior sandboxing, security intelligence and advanced file analysis. Also, AMP for Endpoints provides endpoint protection to offer defense in depth.
URL filtering	Enforce acceptable use of the internet.
Application Visibility and Control	Identify and control over 3000 applications. By leveraging OpenAppID, application detectors can be created for custom application. Furthermore, Snort rules can be written to address specific applications.
Security Intelligence	With unparalleled visibility into the Internet, Cisco Talos provides dynamic IP and URL black list to protect against malicious websites.
Automatic Policy Tuning	Automatically tune IPS protections in response to changes in your network composition.
Association of Users with Security and Compliance Events	Associate users with activity on the network, including attacks and application usage, through integration with Active Directory servers.
Collective Intelligence	Get rapid detection and insight into emerging threats so that defenses stay effective.
Virtual Protection	Protect VM-to-VM communications the same as physical networks.

In addition, Cisco offers optional Advanced Malware Protection for networks and hosts, and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.



---

## ABOUT CISCO

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It's more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For over three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

Cisco delivers intelligent cybersecurity for the real world.

## CONTACT US

Want to learn more about getting this information on your network? Go to [cisco.com/go/security](https://cisco.com/go/security) and request a live demo.



---

# Network Risk Report

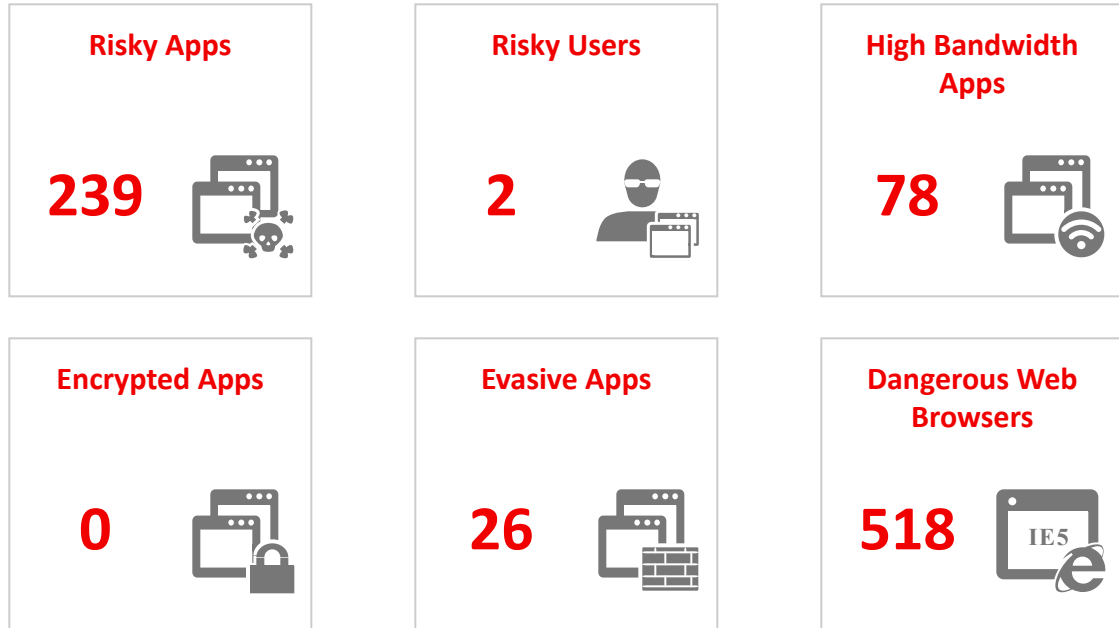
Friday, October 30, 2020



# I. EXECUTIVE SUMMARY

Cisco has determined that your company is at a high risk due to the use of applications that are potentially dangerous to the enterprise yet have low business relevance. These applications may leave your network vulnerable to attack, carry malware, or waste bandwidth.

**Assessment Period: Fri Oct 23 2020 14:15:56 to Fri Oct 30 2020 14:15:56**



## YOUR NETWORK PROFILE

<b>10</b>	<b>86</b>	<b>2,000</b>	<b>29</b>
Operating Systems	Mobile Devices	Applications in Use	File Types Transferred

## RECOMMENDATIONS

Cisco recommends your company deploy Cisco Firepower Appliances (NGIPS/NGFW) with App Control and URL Filtering to:

1. Reduce your application attack surface
2. Granularly control applications, bandwidth, URL access and acceptable use policies
3. Get visibility into network risks and usage, including mobile devices and BYOD risk



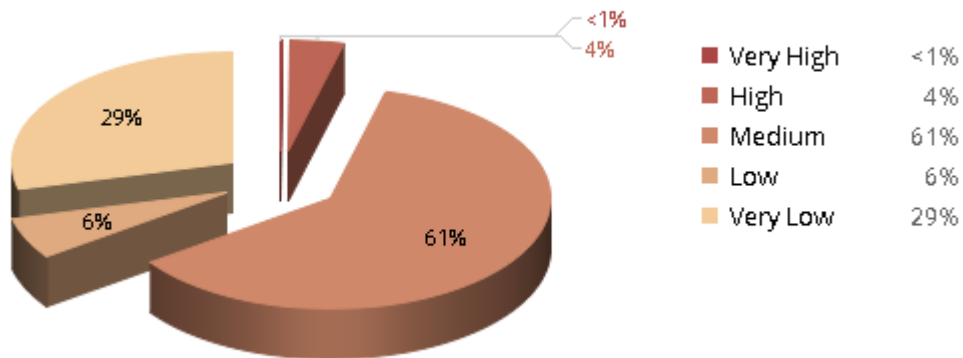
## II. APPLICATION RISK

### APPLICATIONS WITH HIGH RISK AND LOW BUSINESS RELEVANCE

Some applications carry high risk because they can be vectors for malware into the organization, possess recent vulnerabilities, use substantial network resources, or hide the activities of attackers. Other applications have low business relevance: they are not relevant to the activities of a typical organization. When an application has high risk and low business relevance, it is a good candidate for application control to reduce your application risk. You should investigate these applications to determine whether they are important to control.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
BitTorrent	264,534	Very High	Very Low	22,064.85
Googlebot	22,742	Very High	Very Low	1,803.81
Bingbot	15,913	Very High	Very Low	871.67
Yahoo! Slurp	7,207	Very High	Very Low	471.37
PornHub	5,669	Very High	Very Low	37.69

### SUMMARY OF ALL NETWORK CONNECTIONS BY APPLICATION RISK





## HIGH BANDWIDTH APPLICATIONS

---

Some applications use a substantial amount of network bandwidth. This bandwidth usage can be costly to your organization and can negatively impact overall network performance. You may want to restrict the usage of these applications to particular networks: for instance, a wireless network may not be well suited for video streaming. Or, you can shut down these applications entirely or simply get visibility into how your bandwidth is being used.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
YouTube	3,013,751	High	Very Low	3,113,175.15
Netflix stream	291,246	Very Low	Very Low	881,031.16
Disney Plus	170,220	Low	Very Low	730,765.74
Microsoft Update	4,594,517	Medium	Low	312,936.27
Prime Video	519,791	Medium	Low	277,031.11

## EVASIVE APPLICATIONS

---

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
BitTorrent	264,534	Very High	Very Low	22,064.85
CyberGhost VPN	629	Very High	Low	135.40
Ultrasurf	3	Very High	Low	0.25
Hideman Login	770,553	Very High	Medium	6,006.43
Windscribe	724	High	Very Low	160.89

## OTHER APPLICATIONS OF INTEREST

---

Other applications were observed that may be of interest and possibly candidates for control. Users may use anonymizers and proxies to bypass your network security or cloak their identities. Gaming applications may be distractions to productivity and use excessive bandwidth. Peer-to-peer applications are often malware vectors. And remote administration applications may allow malicious users to control machines in your environment.

### Anonymizers and Proxies (accesses):

No Data

### Games and Recreation (accesses):

*Facebook(2,158,033), Instagram(463,048),  
Messenger(2,114), TweetDeck(494),  
MySpace(213), Flixster(121), Facebook*

### Peer-to-Peer and Sharing (accesses):

*cURL(960,383), Instagram(463,048),  
MSN(423,379), Pinterest(417,549),  
TikTok(247,055), Windows Live(159,304),*

### Remote Administration and Storage (accesses):

*HTTPS(266,377,363), HTTP(70,239,838),  
BitDefender(42,937,395), iCloud(2,038,601),  
Google Hangouts(1,485,506),*

## DANGEROUS WEB BROWSER VERSIONS

A profile of your network revealed the following old web browsers in use. Outdated web browsers are a major vector for network malware and it is important to update them (or encourage users to). These browsers often have unpatched vulnerabilities or carry other risks.

BROWSER	VERSION	NUMBER OF HOSTS
Internet Explorer	10.0, 10.0Microsoft	33
Google Chrome	1079.0.3945.136, 1080.0.3987.99, 1083.0.4103.106, 1084.0.4147.89, 1085.0.4183.127, 1086.0.4240.110, 1086.0.4240.114, 1086.0.4240.75, 1086.0.4240.99, 1186.0.4240.110, 1186.0.4240.99, 24.0.1312.52, 28.0.1500.72, 32.0.1700.102, 33.0.1750.117, 39.0.2171.36, 4.030.0.0.0, 4.055.0.2883.91, 4.059.0.3071.125, 4.061.0.3163.98, 4.075.0.3770.143, 4.076.0.3809.132, 4.079.0.3945.116, 4.084.0.4147.89, 4.085.0.4183.101, 4.085.0.4183.127, 4.086.0.424, 4.086.0.4240., 4.086.0.4240.110, 4.086.0.4240.114, 4.086.0.4240.75, 4.086.0.4240.99, 4.4.481.0.4044.138, 41.0.2272.118, 45.0.2454.85	326
Safari	10.1, 11.1, 12.1.1, 13.0.4, 13.0.5, 13.1.1, 13.1.2, 13.1.3, 14.0, 2.4.0, 5.0, 534.34, 6.0.2	110
Firefox	24.0, 3.6.18, 38.0, 41	49

## RISKY WEB BROWSING

The following web communications were identified that correspond to risky activity. Malware sites, open proxies and anonymizers, keyloggers, phishing sites, and spam sources are all Web activities that can put your networks at risk. It is wise to evaluate the use of URL filtering technologies to detect and control communications to risky sites.

URL CATEGORY	CONNECTIONS	BLOCKED	DATA INBOUND (KB)	DATA OUTBOUND (KB)
Social Networking	5,121,860	0	741,393,420.48	39,774,552.38
Filter Avoidance	225,846	0	1,240,688.43	297,387.23
Malware Sites	70,000	0	866,196.02	88,150.74
Professional Networking	46,548	0	11,564,475.89	270,560.04
Adult	15,711	0	255,254.40	19,178.14
Cheating and Plagiarism	6,607	0	228,722.38	25,545.92
Hacking	2,071	0	182,678.57	4,366.18
Peer File Transfer	1,915	0	200,212.86	3,367.76
Phishing	1,740	4	20,656.27	2,287.36
Extreme	32	0	4,268.46	58.24

## THE APPLICATIONS ON YOUR NETWORK

---

This is a list of the riskiest applications discovered in use on your network. Three types of applications are identified and listed here: client applications (including web browsers), web applications (such as Facebook), and application protocols (such as HTTP). Full visibility over all application types enables you to get a better perspective on how your networks are currently utilized.

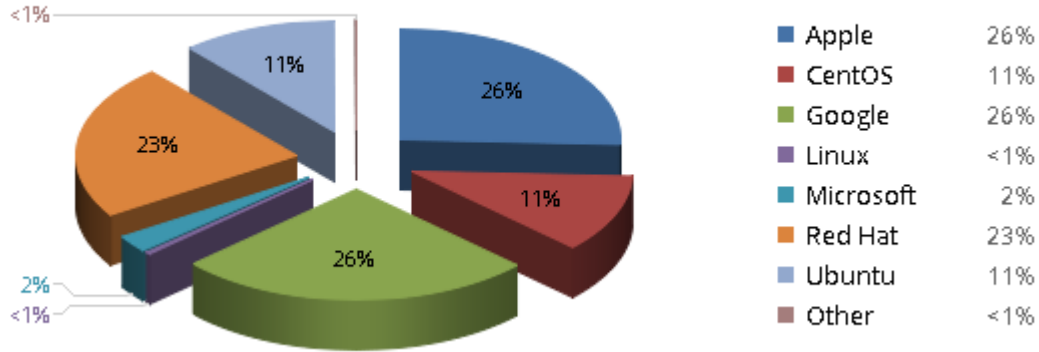
CLIENT APPLICATIONS	WEB APPLICATIONS	APPLICATION PROTOCOLS
Client applications include web browsers and other desktop applications that access the network.	Web applications are carried over web-related protocols such as HTTP and HTTPS. Many web applications operate on port 80 and/or port 443.	Application protocols are the means by which other applications communicate over your network. Examples include HTTPS and SSH.
<b>Total: 512</b>	<b>Total: 1,537</b>	<b>Total: 735</b>
Betternet client, Bingbot, BitCoin, BitComet, BitTorrent, ...	Adult Friend Finder, Betternet, Bingbot, BitCoin, BitComet, ...	Adult Friend Finder, Betternet, Bingbot, BitCoin, BitTorrent, ...



### III. ASSET PROFILE

#### THE OPERATING SYSTEMS ON YOUR NETWORK

The operating systems below were observed on your network. You should identify any operating systems that fall outside your IT policy and investigate them further as to whether they should be permitted.



#### THE MOBILE DEVICES ON YOUR NETWORK

The following mobile devices were profiled on your network. Mobile devices may be vulnerable, especially older or jailbroken versions. It is important to be aware of how mobile devices are used and set appropriate security policies.

OS VENDOR	OS VERSION	COUNT
Google	7.0	21
Red Hat	7.5, 7.6	10
Apple	13.1.2	9
Google	4.4.2	8
Google	5.1	8

## THE FILES TRAVERSING YOUR NETWORK

---

### Downloads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Archive	MSCAB	HTTP	544,243
Archive	JAR	HTTP	67,480
Multimedia	MP3	HTTP	56,675
Archive	ZIP	HTTP	16,033
Multimedia	SWF	HTTP	9,896

### Uploads

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
Archive	GZ	HTTP	7,223
Archive	ZIP	HTTP	151
Executables	MSEXE	HTTP	36
PDF files	PDF	HTTP	11
System files	DMP	HTTP	6

### Misc

FILE CATEGORY	FILE TYPE	PROTOCOL	COUNT
PDF files	PDF	SMTP	1,873
PDF files	PDF	POP3	21
Multimedia	MP3	POP3	15
Office Documents	MAIL	SMTP	12
Archive	ZIP	FTP Data	2



## IV. RECOMMENDATIONS

Despite existing protections, your organization's application usage exposes it to added risks. This assessment, which contains a profile of your network, has identified risky assets. New countermeasures and security controls are required to mitigate the risks to these assets.

Cisco recommends that Firepower Appliances with Application Control and URL Filtering are deployed to:

1. Establish continuous network visibility into its application and asset risk
2. Augment its existing controls in order to mitigate this risk

### 1. ESTABLISH CONTINUOUS NETWORK VISIBILITY INTO APPLICATION RISK

Existing security infrastructure provides inadequate protection against application and asset risks. Cisco recommends deployment of network-based protections via Firepower Appliances (NGIPS/ NGFW). These will provide the following new capabilities and benefits to augment your network visibility:

NEW CAPABILITY	BENEFIT
Network Map	Profiles hosts on the network, including network infrastructure, desktops, servers, mobile devices, virtual machines, and many others.
Application Visibility and Control	Identify and control over 3000 applications. By leveraging OpenAppID, application detectors can be created for custom application. Furthermore, Snort rules can be written to address specific applications.
Security Intelligence	With unparalleled visibility into the Internet, Cisco Talos provides dynamic IP and URL black list to protect against malicious websites.
Mobile Awareness	Identifies and profiles mobile devices, including iOS, Android, Amazon, Blackberry, and other mobile device types. Identifies jailbroken devices.
Real-time Contextual Awareness	Profiles hosts and identifies communications that are of unusual bandwidth or hosts that are running inappropriate applications for the environment.

### 2. AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk applications pose. These measures may entail reduction of the application threat surface and blocking risky URLs. Cisco recommends deployment of network-based protections via Firepower Appliances with Application Control and URL Filtering. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Granular Application Control	Reduce potential area of attack through granular control of thousands of applications.
File Identification and Control	Detect and optionally block files by file type. Capture files for offline analysis, if desired.
URL Filtering	Control on a database of millions of URLs, by risk or productivity characteristics
Virtual Protection	Protect VM-to-VM communications the same as physical network

In addition, Cisco offers NGIPS capabilities and optional Advanced Malware Protection for networks and hosts, to help better protect against the latest threats. Please contact your Cisco representative or reseller for more information.



---

## ABOUT CISCO

It's no secret that today's advanced attackers have the resources, expertise, and persistence to compromise any organization at any time. As attacks become more sophisticated and exploit a growing set of attack vectors, traditional defenses are no longer effective.

It's more imperative than ever to find the right threat-centric security products, services, and solutions for your current environment. These solutions must also easily adapt to meet the evolving needs of your extended network, which now goes beyond the perimeter to include endpoints, mobile devices, virtual machines, data centers, and the cloud.

For over three decades, Cisco has been a leader in network security protection, innovation, and investment. Our expertise and experience helps us increase intelligence and expand threat protection across the entire attack continuum for a level of security you can build your business on.

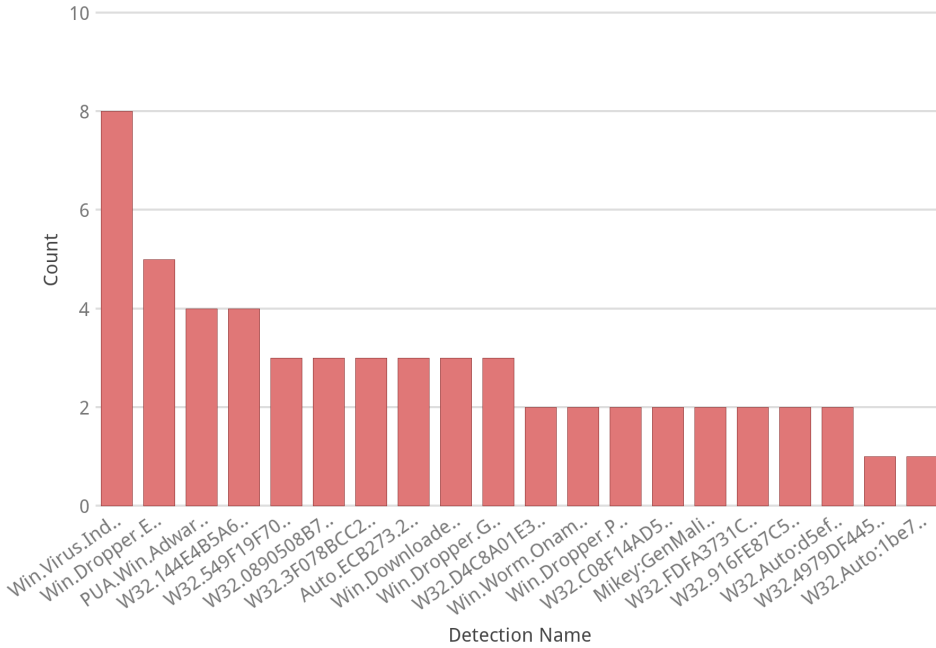
Cisco delivers intelligent cybersecurity for the real world.

## CONTACT US

Want to learn more about getting this information on your network? Go to [cisco.com/go/security](https://cisco.com/go/security) and request a live demo.

# Malware Threats

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40

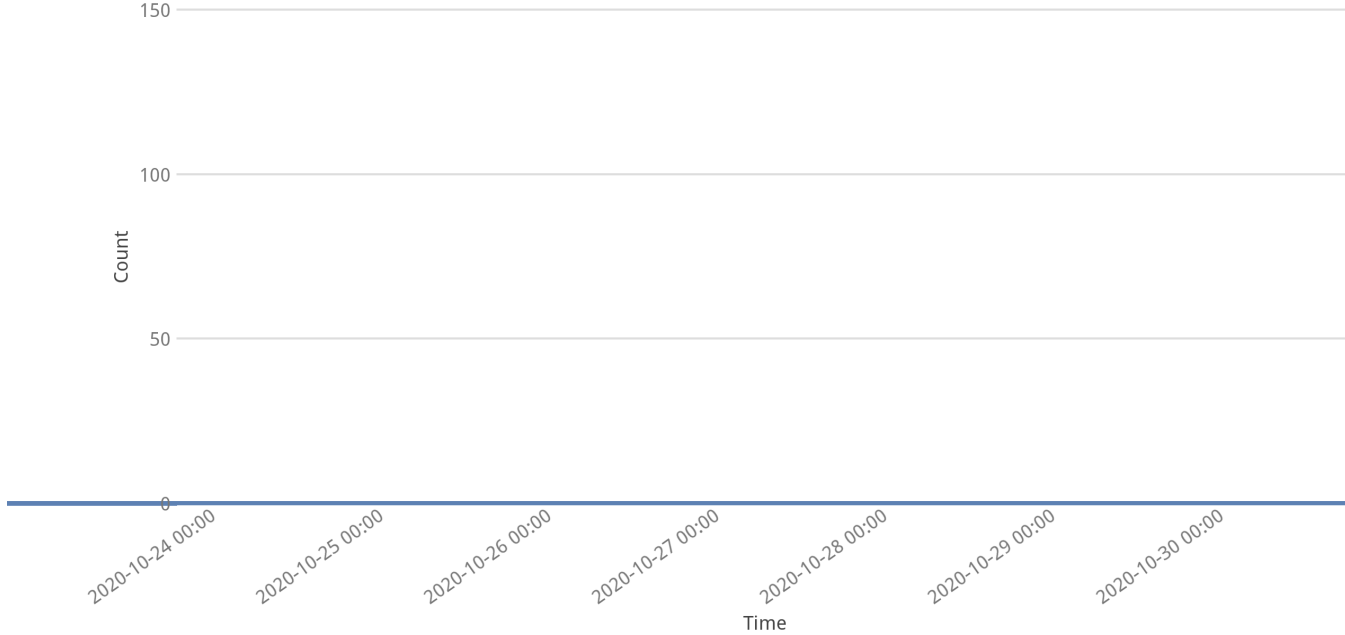


Detection Name	Count
Win.Virus.Induc::1201	8
Win.Dropper.Ez...	5
PUA.Win.Adwar...	4
W32.144E4B5A6...	4
W32.5A9F19F70...	3
W32.0890508B7...	3
W32.3F078BCC2...	3
Auto.ECB273.2...	3
Win.Downloader.Farfli::Dynamer.tht.talos	3
Win.Dropper.Generic::1201	3
W32.D4C8A01E31-100.SBX.TG	2
Win.Worm.Onamu::1201	2
Win.Dropper.Poorweb::in03.talos	2
W32.C08F14AD5D-95.SBX.TG	2
Mikey:GenMaliciousA-tpd	2
W32.FDFA3731C6-95.SBX.TG	2
W32.916FE87C5B-95.SBX.TG	2
W32.Auto:d5ef44.in03.Talos	2
W32.4979DF4457-95.SBX.TG	1
W32.Auto:1be727ebce.in03.Talos	1

# Threat Detections over Time

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40

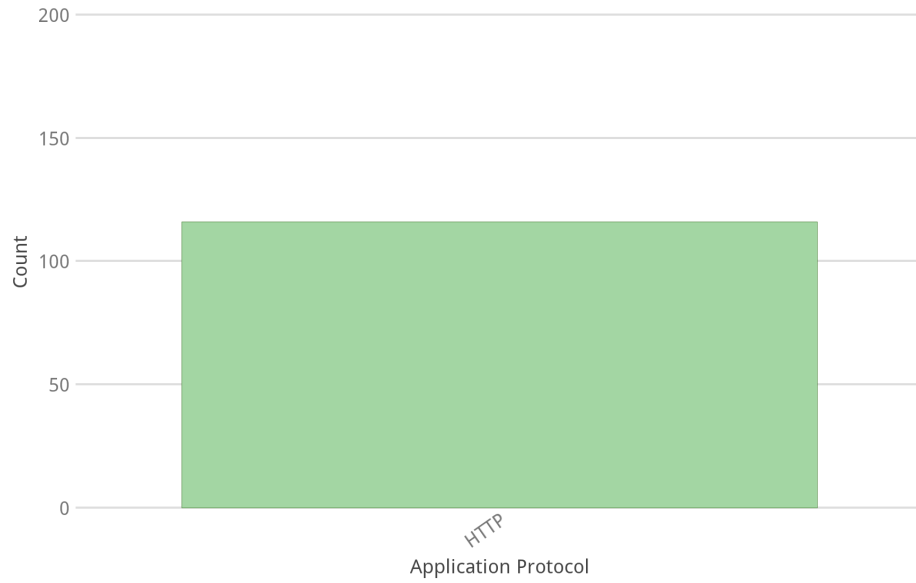
Constraints: Event Type = Threat Detected





# Application Protocols Transferring Malware

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40

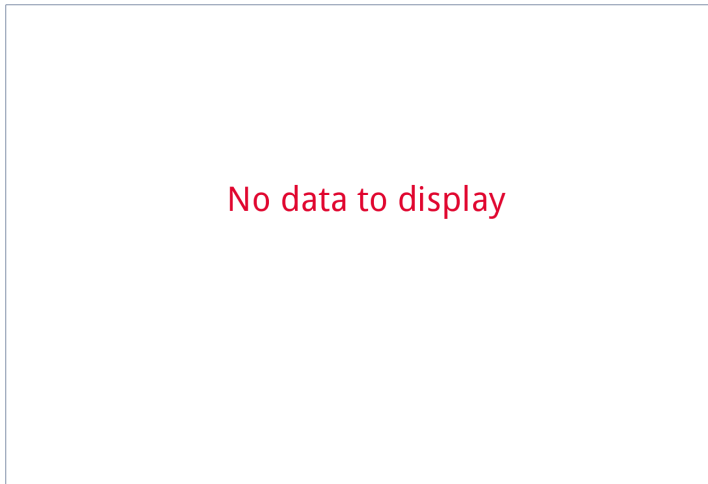


Application Protocol	Count
HTTP	116

# Hosts Receiving Malware

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40

Constraints: Event Type = Threat Detected

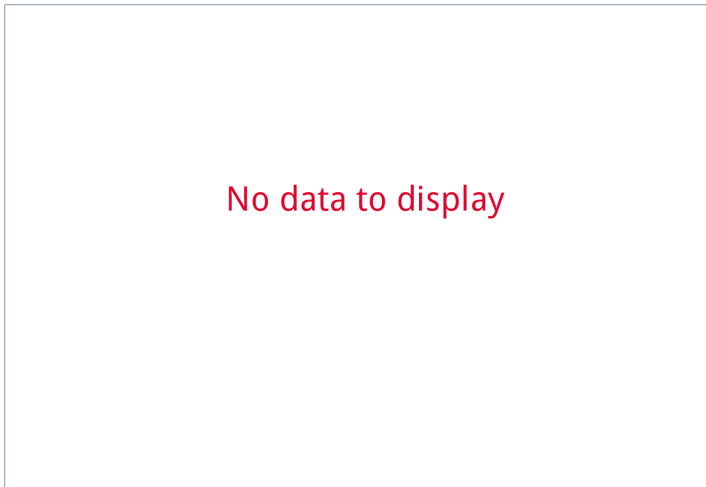


Receiving IP	Count
--------------	-------

## Hosts Sending Malware

**Time Window:** 2020-10-23 14:10:40 - 2020-10-30 14:10:40

**Constraints:** Event Type = Threat Detected

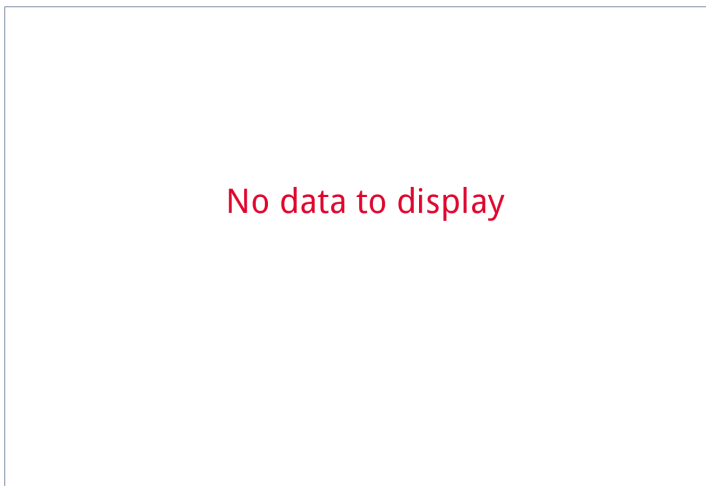


Sending IP	Count
------------	-------

## Users Affected by Malware

**Time Window:** 2020-10-23 14:10:40 - 2020-10-30 14:10:40

**Constraints:** Event Type = Threat Detected

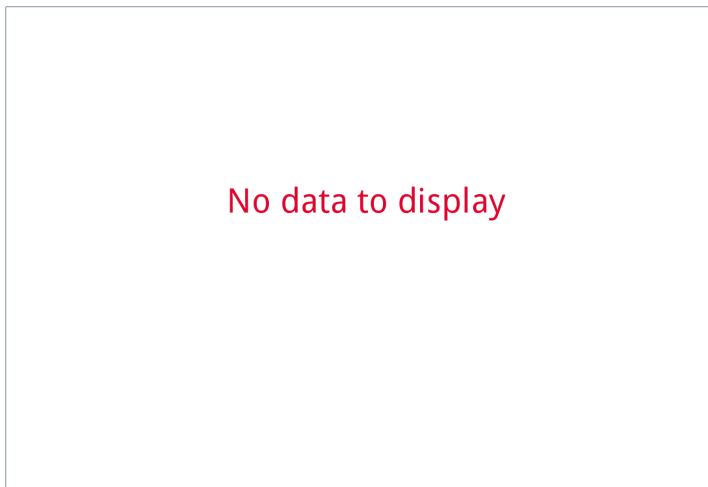


User	Count
------	-------

# Malware Intrusions

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40

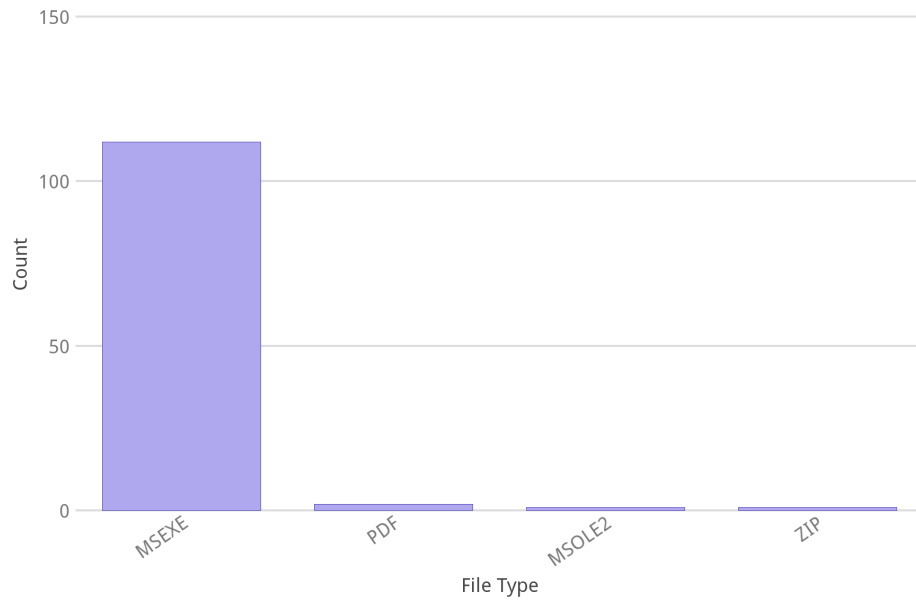
Constraints: Message = BLACKLIST,MALWARE



Message	Count
---------	-------

# File Types Infected with Malware

Time Window: 2020-10-23 14:10:40 - 2020-10-30 14:10:40



File Type	Count
MSEXE	112
PDF	2
MSOLE2	1
ZIP	1





2020-10-25 09:17:26	5.79.75.210	10.16.255.4	80	45782	No Authentication Required	Threat Detected in Network File Transfer	Auto.44A6C8.212338.in02	0bxt0nImNIAYPzFjpuQLhgBfodlv1	Malware	44a6c840150ff86f1237a20c76bfff2cee442667ce484129495eb88ee006e0fc	MSEXE	Executables	839.0000	/0bxt0nImNIAYPzFjpuQLhgBfodlv1	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-25 08:56:03	5.79.75.210	10.16.255.4	80	44628	No Authentication Required	Threat Detected in Network File Transfer	Win.Dropper.Ursu:.in03.talos	Y2kHKPi8zio2UX5cE1HNbhoPHOPCOw	Malware	e24ae4d40041b2219b6c0c50f9d46560dafbb3718897d8e33ebbc0ffa1916d42	MSEXE	Executables	247.5000	http://5.79.75.210/Y2kHKPi8zio2UX5cE1HNbhoPHOPCOw	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-25 08:15:09	157.185.145.131	10.16.255.4	80	42045	No Authentication Required	Threat Detected in Network File Transfer	Win.Downloader.Farll::Dynamer.tht.talos	abuuiabblgaag0utvuwoquqlhac	Malware	6ea27426ff47b4abd8a8e53f7d3452c981aa6fe86ca07ef15e45f6f8cae3108	MSEXE	Executables	648.0000	http://157.185.145.131/2865400.s21d-2.faiusrd.com/0/abuuiabblgaag0utvuwoquqlhac?wsiphost=ipdb&wsrid_tag=5e6b817b_psmgbsdbos1ts66_36329-6535	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-25 06:21:43	5.79.75.210	10.16.255.4	80	45089	No Authentication Required	Threat Detected in Network File Transfer	W32.Lojack.21gd.1201	Q16i7oUqjIP2iqRULAI2whKRCL0Tp6	Malware	dcblfd12321fa7c4fa9a72486ced578dc00dcae79e6d95aa481791f044a55af3	MSEXE	Executables	17.0000	http://5.79.75.210/Q16i7oUqjIP2iqRULAI2whKRCL0Tp6	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-25 04:21:21	157.185.144.118	10.16.255.4	80	50291	No Authentication Required	Threat Detected in Network File Transfer	Win.Downloader.Farll::Dynamer.tht.talos	abuuiabblgaag0utvuwoquqlhac	Malware	6ea27426ff47b4abd8a8e53f7d3452c981aa6fe86ca07ef15e45f6f8cae3108	MSEXE	Executables	648.0000	http://157.185.144.118/2865400.s21d-2.faiusrd.com/0/abuuiabblgaag0utvuwoquqlhac?wsiphost=ipdb&wsrid_tag=5e6853a0_psmgzjgord1de87_5849-22973	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-25 00:19:39	5.79.75.210	10.16.255.4	80	39847	No Authentication Required	Threat Detected in Network File Transfer	MIkey.GenMaliciousA.tpd	exMtexHP7IaxUwzH4gTz0hoXIVauKY	Malware	92e4863e9cd484117c1288ceb692823a6d86c0b3a09f29a5cbc4af6a83a03415	MSEXE	Executables	259.7197	http://5.79.75.210/exMtexHP7IaxUwzH4gTz0hoXIVauKY	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 21:08:14	5.79.75.210	10.16.255.4	80	49640	No Authentication Required	Threat Detected in Network File Transfer	Win.Dropper.Snojan.:100.sbx.vioc	p61tpwsDRtaeHL8UBNizmh4dtXYUgP	Malware	e416ad91acbc386bf67dc551fb36b9d95a195d8b656cfe4001325b8b5f07624e	MSEXE	Executables	567.9063	/p61tpwsDRtaeHL8UBNizmh4dtXYUgP	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 20:42:08	209.134.25.150	10.16.255.4	80	60591	No Authentication Required	Threat Detected in Network File Transfer	Win.Dropper.Gandcrab.in07.talos	tracking_number.pdf..exe	Malware	fec01eclbc95ba154b19c1e9bb93edaa4bbe6628380b6670afe130e4b05c58b	MSEXE	Executables	217.5127	http://scheff.com/trackinglist/tracking_number.pdf..exe	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 18:48:42	5.79.75.210	10.16.255.4	80	55200	No Authentication Required	Threat Detected in Network File Transfer	Win.Dropper.Danti:~95.sbx.tg	N2wCoNum7UBXuPoFqA18QHpgtKEcRn	Malware	705409bc11fb45fa3c4e2fa9dd35af7d4613e52a713d9c6ea6bc4baaf49aa74a	MSEXE	Executables	53.0000	http://5.79.75.210/N2wCoNum7UBXuPoFqA18QHpgtKEcRn	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 17:11:32	5.79.75.210	10.16.255.4	80	53822	No Authentication Required	Threat Detected in Network File Transfer	Win.Dropper.Necurs:~95.sbx.tg	WJ4t1bi34c1ziPzI62ie6hxgI3QSYD	Malware	b049148acf2380a57401ba6ba546e7cf3e64f9ce2a7fb77111a14277dc8e1184	MSEXE	Executables	259.5000	http://5.79.75.210/WJ4t1bi34c1ziPzI62ie6hxgI3QSYD	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 16:54:16						Threat Detected in Network File Transfer (Retrospective)			Malware	4b3be3b3c414b83ec18f6500197151b035957760467b2abfb29d8e6dc1986463							Malware Detected by Local Malware Analysis	firepower
2020-10-24 16:53:15	10.16.255.4	174.20.4.138	8080	54943	No Authentication Required	Threat Detected in Network File Transfer (Retrospective)		Wen Du Ri Ji .exe	Malware	4b3be3b3c414b83ec18f6500197151b035957760467b2abfb29d8e6dc1986463	MSEXE	Executables	79.0859	http://https://s.hearty.app/dl/win/chrome.x86%E6%BA%AB%E5%BA%A6%E6%97%A5%E8%A8%98.exe	HTTP	SHA	Retrospective Event (Local Malware Analysis), Sat Oct 24 21:54:16 2020(UTC), Old Disp: Neutral, New Disp: Malware, Threat Name: Win.Malware.Jaik-6917323-0;	Region14-FTD-SM40-Two
2020-10-24 16:46:00	5.79.75.210	10.16.255.4	80	54953	No Authentication Required	Threat Detected in Network File Transfer	W32.1DAB395830-95.SBX.TG	Y2kHKvi8YcoBFXOUegcNbh0PhOPCOw	Malware	1dab39583011142746095f5938fa9c318a27974796a434492b7f0866016c580	MSEXE	Executables	115.7109	http://5.79.75.210/Y2kHKvi8YcoBFXOUegcNbh0PhOPCOw	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 16:23:51	8.211.23.107	10.16.255.4	80	50193	No Authentication Required	Threat Detected in Network File Transfer	W32.3070F7636C-100.SBX.VIOC	6.exe	Malware	3070f7636c684ab48a7e4882ca5b4c4b20159710461d1b78aaeaa1943738865	MSEXE	Executables	372.1875	http://xerrload02.top/downloadfiles/6.exe	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 15:46:41	5.79.75.210	10.16.255.4	80	35163	No Authentication Required	Threat Detected in Network File Transfer	GenericKD:Trojan-tpd	xkaspOFgeTYVuuNceX11EngOfmkINW	Malware	cc8e42372ef2df10f26bc075cf363ca73cad573bb0eb3dfa67991e79df9d5ccd	MSEXE	Executables	83.5000	http://5.79.75.210/xkaspOFgeTYVuuNceX11EngOfmkINW	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 15:28:16	5.79.75.210	10.16.255.4	80	58260	No Authentication Required	Threat Detected in Network File Transfer	W32.Variant.21fy.1201	N2wCo5ImXsBecPOuqpU8QHpgtKEcRn	Malware	861b6bc1f9869017c48930af5848930dd037fb70fc506d8a7e43e1a0dbd1e8cb	MSEXE	Executables	249.5000	http://5.79.75.210/N2wCo5ImXsBecPOuqpU8QHpgtKEcRn	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 15:26:47	185.126.178.243	10.16.255.4	80	34657	No Authentication Required	Threat Detected in Network File Transfer	W32.Auto:25499537f8.in03.Talos	Rina_AC.exe	Malware	25499537f84389814f15e8d5d2e429ab95d2f2c6b037565717450717d3e12265	MSEXE	Executables	270.0000	http://185.126.178.243/data/Rina_AC.exe	HTTP	SHA	Region14-FTD-SM40-Two	
2020-10-24 14:38:23	75.127.1.211	10.16.255.4	80	44432	No Authentication Required	Threat Detected in Network File Transfer	W32.Auto:4c9daefcd4.in03.Talos	kmk.exe	Malware	4c9daefcd476a1a197393e0bc78c10152090116893ac4f08dd681fb36fe41431	MSEXE	Executables	575.5000	http://75.127.1.211/kmk.exe	HTTP	SHA	Region14-FTD-SM40-Two	



# Zoom Usage Guidelines

August 20, 2020

## Introduction

In early 2020, Zoom's user base expanded exponentially in response to increased demand for virtual collaboration tools caused by the COVID-19 pandemic. During this time, several major security issues were identified with the Zoom platform. In response to these issues and concerns, Zoom halted feature development and committed to an aggressive 90-day security improvement plan. This plan was initiated on April 1, 2020, and outlined seven commitments to secure and harden the platform, and to remediate the identified security and privacy issues.

Zoom recently completed this 90-day plan. In a July 1, 2020, [message to customers](#), they outlined the status of the seven commitments made to improve the security and privacy protections of the Zoom application. Additionally, they outlined key leadership changes and additions, additional offers of Zoom for Government (hosted in Amazon Web Services Government Cloud), and additional U.S.-based product engineering teams to support the company's continued growth.

Based on the platform's new security stance, it is appropriate for Region 14 to implement a Zoom usage guidance. This updated document provides suggestions and guidance on the use of Zoom and other virtual collaboration tools. As with any technology, organizations should always consult the most recent documentation from the technology platform developer.

## Region 14 Usage Position

Region 14 has reviewed Zoom's progress on the implementation of the security plan. Region 14 has also conducted and reviewed additional third-party research and analysis on the Zoom platform. Based on the currently available evidence, Region 14 has concluded Zoom is now a viable candidate for online collaboration and is an acceptable platform for conducting state business involving both public and sensitive communications. Region 14 continues to strongly recommend against using Zoom for highly confidential conversations, meetings, or data transfer. Additionally, Region 14 recommends against using the recording feature for sensitive and confidential meetings. While it may be appropriate to host and record a public webinar or board

meeting using Zoom, the risks of recording a sensitive internal meeting using the platform may be prohibitive.

Region 14 encourages all organizations currently using or considering the use of Zoom to explore Zoom for Government, which has been granted [FedRAMP Moderate Authorization](#).

**Note: That both the U.S. Department of Homeland Security (DHS) - Cybersecurity & Infrastructure Security Agency (CISA) and the U.S Department of Defense (DoD) have established guidelines for the authorized use of Zoom in their respective organizations. The guidance provided in this document aligns with these federal usage guidelines.**

### **Security Points of Consideration for Agency Use**

Zoom does not encrypt meeting traffic over its own internal network and servers. This practice is required to support the cloud-based recording of meetings and webinars, a key business function for Zoom. Session recordings are processed after the meeting and encrypted when stored. They can also be password protected or shared to members of your organization; however, during the recording process, the session is available on Zoom's infrastructure unencrypted. Should their systems be compromised, any live recording or open session would be exposed to the attack.

As meeting traffic is internally unencrypted, each organization should evaluate the risk of exposure for sensitive or confidential meeting traffic. Region 14 recommends against recording these meetings or sharing documents as attachments through the meeting platform.

Each organization must evaluate the use of any virtual collaboration platform against the security requirements of that organization. When in doubt, users should consult with their IT professionals and management to ensure the platform does not present an unacceptable risk to the organization. Region 14 reminds users to always follow their organization's policies addressing virtual meetings, inform/url meetings.

Virtual collaboration tool administrators should carefully review their system, group, and user configurations and reach out to their vendors for support as needed. As with any technology, it is critical to update software and apply security patches on a regular basis. End users are encouraged to review the [DIR Virtual Collaboration Tools Security Tips](#) document for additional guidance.

### **General Virtual Collaboration Tool Configuration Recommendations**

Virtual collaboration tools are feature-rich programs with many configurations that can support open collaboration or communication based on how the tool is configured. Below are general configuration recommendations to support security and reduce the chance of meeting disruption.



- Schedule meetings that require a password to join. Distribute passwords to attendees separately, via email.
- Turn on the “waiting room” feature to view and control which users are admitted into the meeting.
- Users can enable waiting rooms when scheduling the meeting or as a system-wide configuration.
- Lock meetings once all participants have joined. This will prevent unauthorized users from gaining entry while the meeting is in session.
- After locking the meeting, review the list of participants and expel any unknown participants before sharing your content.
- Expel disruptive individuals from your meeting.
- If supported by your system, disable the feature that allows participants who have been previously removed to rejoin.
- Disable participants’ ability to record the meeting.
- Disable participant screen or file sharing. This will prevent your meeting from being disrupted by others and the sharing of inappropriate or potentially malicious content.
- Disable the chat feature prior to the start of the meeting.
- Put all attendees in mute mode and suspend privileges for participants to unmute themselves until needed.
- Avoid using personal meeting IDs for public-facing meetings.
- Consider publishing the meeting link via email to the desired attendees, rather than posting the link on public websites or calendars.
  - For public and other open meetings, such as board meetings, consider scheduling a webinar and requiring attendee registration.
- Avoid posting photos or screenshots of your meetings. This could provide threat actors with the associated meeting ID and information on who is attending your meetings.

### **Alternative Services Available through DIR**

DIR has multiple collaboration software services available. A list is provided below:

<https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Cooperative%20Contracts%20for%20Remote%20Access.xlsx>

According to, they do not DIR endorse the use of any specific product or solution. It is incumbent upon each organization to evaluate the use of any virtual collaboration platform against the security requirements of the organization.

# ESC 14 App Services

<https://goo.gl/8AaAUd>



## **HOT TOPICS**

### **● TimeKeeper - Calendar Month Report**

- TimeKeeper now features 'Calendar Month Summary' for TRS reporting.

### **● TxEIS transmittal-prep version update**

- Nightly updates from TxEIS

- Staff Info, Sub Info

- Leave balances



- Update Staff/Sub lists throughout all App Services - (TimeKeeper, TimesAway, etc.)

### **● Staff Absence Report -TkSubMatch**

- TkSubMatch - Cross reference sub TimeKeeper actions with TimesAway sub assignments.
- Highlights missed sub assignments or absence request submissions.

# R14 School Directory App



Region 14  
Education Service Center

Search...



Service for World Class Schools

Departments

Programs & Services

R14 Districts

PITStop

Jobs

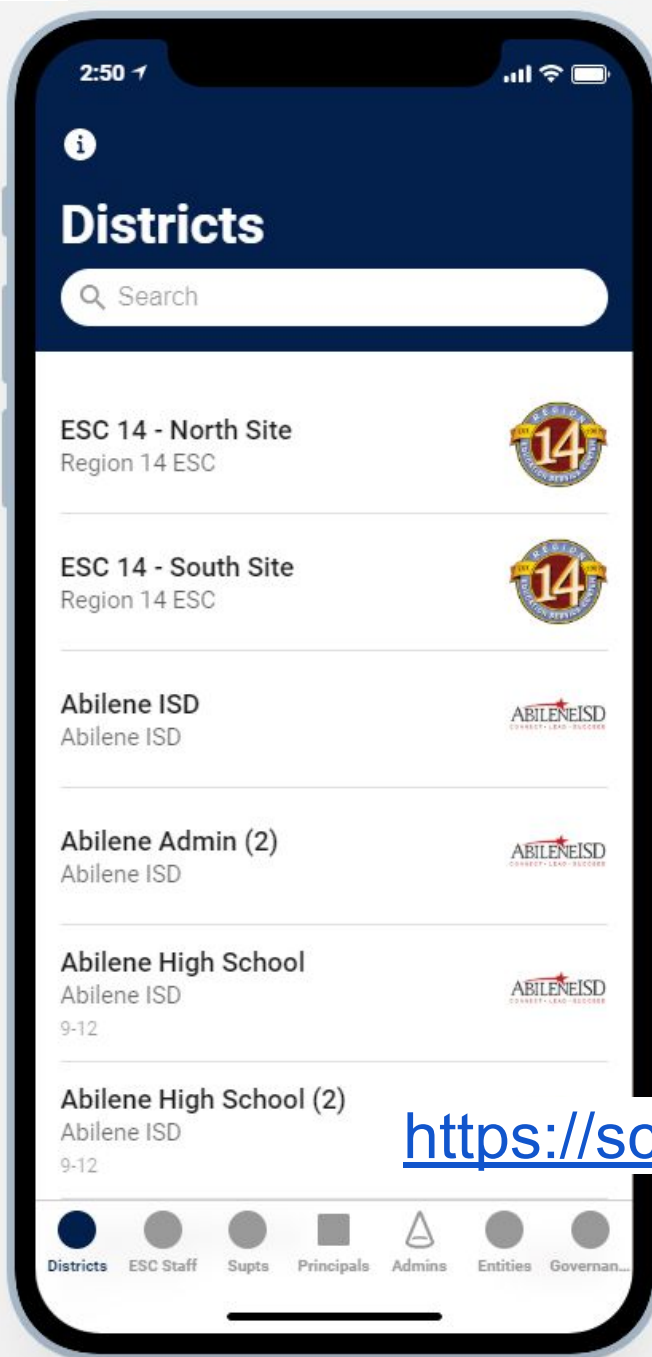
ESC Employees

About Us

<http://www.esc14.net>



Scan with camera to install app.



## R14 School Directory

by App Script

Region 14 ESC School Directory

SHARE APP

<https://schooldirectory.esc14.net/>

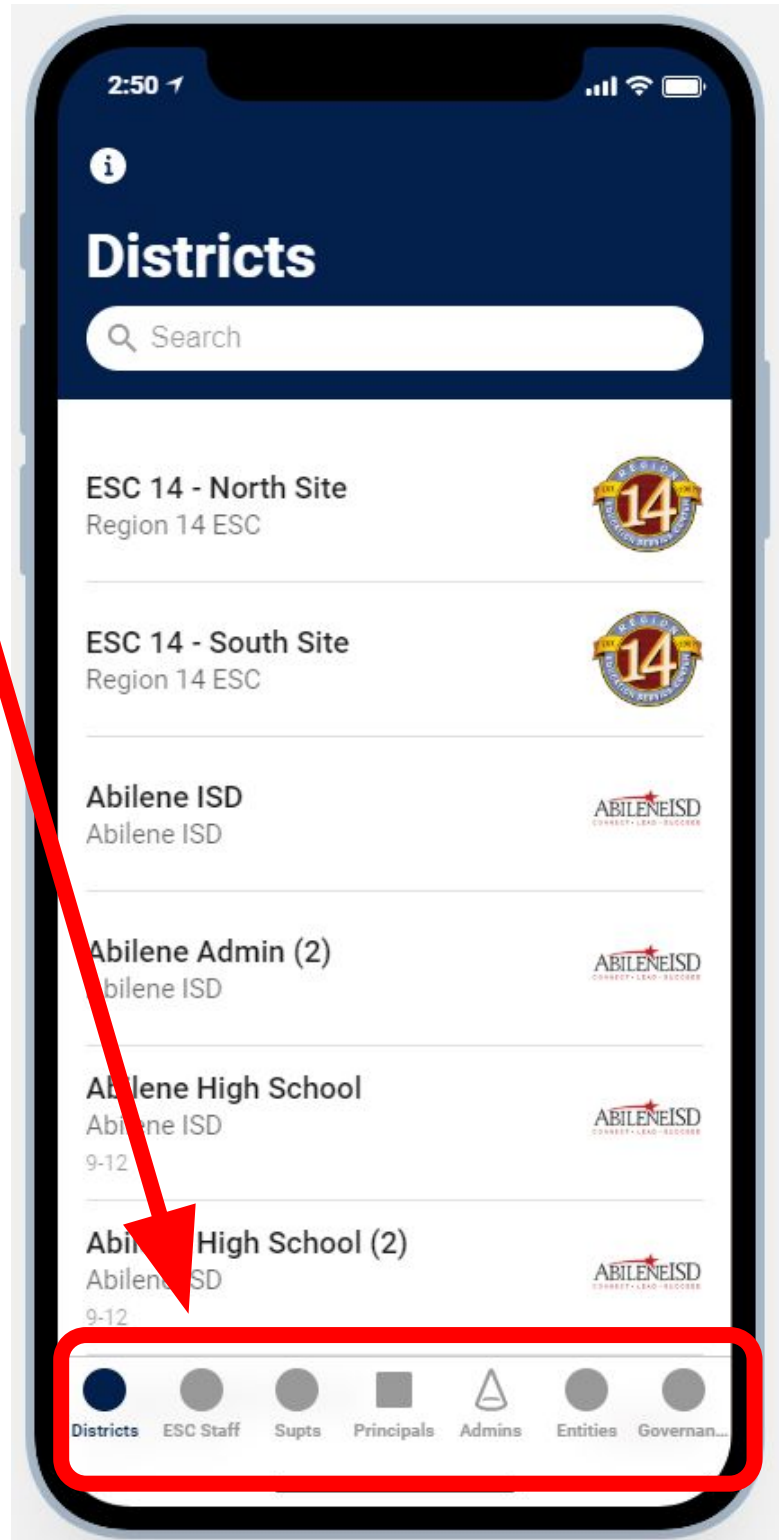
# R14 School Directory App

## Searchable tabs:

- Districts
- ESC Staff
- Supts
- Principals
- Admins
- Entities
- Governance

## Updates ESC 14 distribution lists:

- Supts.
- Supt. Secretaries
- Curriculum
- Erate
- Secondary Principals
  - Grades 6-12
- Elementary Principals
  - Grades EE-5



## ESC 14 Contact to update your info:

- Melissa Morales
- [mmorales@esc14.net](mailto:mmorales@esc14.net)
- 325-675-8608

# ESC 14

# App Services

# Info Site

[www.esc14.net](http://www.esc14.net)

The screenshot shows the ESC 14 website interface. At the top left is the logo for Region 14 Education Service Center, established in 1967. To the right is the text "Region 14 Education Service Center" and a search bar. Below the header is a navigation menu with items: Departments, Programs & Services, R14 Districts, PITStop, Jobs, R14 Service Station, ESC Employees, and About Us. A red box highlights "Departments" with an arrow pointing to a dropdown menu. The dropdown menu contains: Technology Services - Home, Technology Services - Staff, Programs, and Bomgar. A red box with the number "1." points to "Technology Services" in the dropdown. A second red box with the number "2." points to "Programs" in the dropdown. A third red box with the number "3." points to the "Apps Services" icon in a grid of service icons. The grid includes: Apps Services (highlighted), Digital Innovation, Distance Learning, eRate, Library Services / Media Services, Media Production Lab, Network Services, TSDS, TxEIS Student, and WTTC. The main heading "Technology Services Programs" is displayed in large blue text.

David Watkins [dwatkins@esc14.net](mailto:dwatkins@esc14.net)

# ESC 14

# App Services

# Info Site

<https://goo.gl/8AaAUd>

## App Services Home



Select Icon Links below for Information on Specific Services



[TimesAway](#)



[TimeKeeper](#)



[TransTrack](#)



[HelpTrack](#)



[TravelTrack](#)



[App Services](#)

[Overview and Contact Info](#)

David Watkins [dwatkins@esc14.net](mailto:dwatkins@esc14.net)

# ESC 14 App Services

<https://goo.gl/8AaAUd>

- District Custom G-Suite applications

- **TimesAway**



- Absence from Duty/Sub requests



- **TimeKeeper**



- Hourly time clock system

- **HelpTrack**



- Support requests(tech, maint, etc.)

- **TransTrack**



- Transportation requests/assignments

- **TravelTrack** - designed with co-ops in mind



- Mileage tracking/reimbursements

## Staff/Student Upload Services

- **ESTAR/MSTAR** <https://goo.gl/jDapu8> **ESTAR/MSTAR**
- **PITStop**
- **Eduphoria**
- **Library Services**
- **TEA's Roster Validation Data**
- **misc district requests for third party applications**
- **based on TxEIS export .sql scripts**

# TimeKeeper - Time Management



Date	Time	Daily Calculations	TimeKeeper Action	Name	Employee Number	Job Code	Additional Info	Resolved Note
5/9/2016	1:08 PM		Clock In	Staff Names	Empl. #s	Maintenance/Custodian		
5/9/2016	2:58 PM	1.84	Clock Out			Maintenance/Custodian		
5/9/2016	2:58 PM		Clock In			Transportation		
5/9/2016	4:22 PM	1.39	Clock Out			Transportation		
5/10/2016	6:00 AM		Clock In			Transportation		
5/10/2016	7:35 AM	1.58	Clock Out			Transportation		
5/10/2016	7:35 AM		Clock In			Maintenance/Custodian		
5/10/2016	11:34 AM	4	Clock Out			Maintenance/Custodian		
5/10/2016	1:02 PM		Clock In			Maintenance/Custodian		
5/10/2016	2:57 PM	1.93	Clock Out			Maintenance/Custodian		
5/10/2016	2:58 PM		Clock In			Transportation		
5/10/2016	4:21 PM	1.39	Clock Out			Transportation		
5/11/2016	6:08 AM		Clock In			Transportation		
5/11/2016	7:36 AM	1.47	Clock Out			Transportation		
5/11/2016	7:36 AM		Clock In			Maintenance/Custodian		
5/11/2016	11:40 AM	4.06	Clock Out			Maintenance/Custodian		
5/11/2016	1:07 PM		Clock In			Maintenance/Custodian		
5/11/2016	2:56 PM	1.81	Clock Out			Maintenance/Custodian		

- Easy Clock In/Out Management
- Error notifications/flags

Select Employee	1/29/2017	2/4/2017		2/5/2017		2/11/2017		2/12/2017		2/18/2017		2/19/2017		2/25/2017		Pay Period Totals		
	Job Code Hours	Ttl Hrs	Reg Hrs	Prem Hrs	Ttl Hrs	Reg Hrs	Prem Hrs	Ttl Hrs	Reg Hrs	Prem Hrs	Ttl Hrs	Reg Hrs	Prem Hrs	Ttl Hrs	Reg Hrs	Prem Hrs	Reg Hrs	Prem Hrs
Alde																		
Bus_Driver	5.95	5.16	0.79	6.12	5.34	0.78	4.93	4.93									15.43	1.57
Cafeteria																		
Maintenance	40.16	34.84	5.32	39.74	34.66	5.08	31.93	31.93									101.43	10.40
Secretary																		
Student_Worker																		
Substitutes																		
Teacher																		
Technology																		
UIL																		
YHU																		
Total Hours	46.11	40.00	6.11	45.86	40.00	5.86	36.86	36.86			0.00			0.00			116.86	11.97
>Sub-Total Regular Weekly Hours	40			40			36.86				0.00			0.00				
>Sub-Total Premium Hours	6.11		13.25%	5.86		12.78%												

## Weekly Job Code Subtotals

- OT hours auto-proportioned
- Assists with Blended Rate Calculations



# TimeKeeper - Calendar Month Summary



- **Calendar Month Summary:**



- Summary report by employee based on calendar month
- Disregards district' pay period
- Summarizes:
  - TimeKeeper hours
  - TimeKeeper days
  - Job Code hours
- Aides with TRS reporting



## App Services

### TxEIS Transmittal file creation:

- **Actual Hours file**

- File created for TxEIS import for TRS reporting





# TimeKeeper - My TimeKeeper Site

## Employee Access

- Today's TimeKeeper Actions
- Current Pay Period Total and Weekly Summary
- TimeKeeper Actions for entire pay period

### MY CURRENT PAY PERIOD SUMMARY

#### Today's TimeKeeper Actions

Print

Date	Time	Action	Name	Empl. Number	Job Code	Additional Info
2017/05/23	4:59 AM	Clock In	[Redacted]	542	500 Maintenance/Custodian	

#### Current Pay Period Summary

Print

User_Name	Pay Period Reg. Hrs.	Pay Period OT Hrs.	Week 1 Reg. Hrs	Week 1 Extra Hrs.	Week 2 Reg. Hrs	Week 2 Extra Hrs.	Week 3 Reg. Hrs	Week 3 Extra Hrs.	Week 4 Reg. Hrs	Week 4 Extra Hrs.	Week 5 Reg. Hrs	Week 5 Extra Hrs.
[Redacted]	94.09	13.46	40	6.5	40	6.96	14.09					

#### Current Pay Period TimeKeeper Actions

Print

Date	Time	TimeKeeper Action	Daily Calculations	Name	Employee Number	Job Code	Additional Info	Resolved Note
2017/05/08	4:16 AM	Clock In		[Redacted]	542	500 Maintenance/Custodian		
2017/05/08	8:00 AM	Clock Out	3.73	[Redacted]	542	500 Maintenance/Custodian		
2017/05/08	10:17 AM	Clock In		[Redacted]	542	500 Maintenance/Custodian		
2017/05/08	3:10 PM	Clock Out	4.88	[Redacted]	542	500 Maintenance/Custodian		
2017/05/09	4:45 AM	Clock In		[Redacted]	542	500 Maintenance/Custodian		

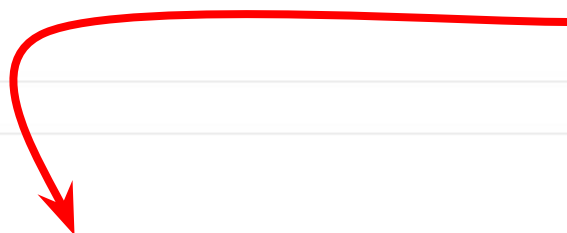
# Campus Access - Sub Search Site



## TODAY'S SUBS

Print

Substitute	Start Date	Day(s)	Staff Member	Reason	Request ID
<b>Subs</b>	03/23/2017	1	<b>Staff</b>	SCHOOL BUSINESS	1703_10110455
	03/23/2017	1		STATE PERSONAL	1703_21023519



## UPCOMING SUBS NEEDED

Print

Staff Member	Start Date	Day(s)	Sub Assign	Status	Reason	Request ID
<b>Staff</b>	03/28/2017	1	<a href="#">Sub Assign Link</a>	PENDING	STATE PERSONAL	1703_21113007
	04/06/2017	1/2 (pm only)	<a href="#">Sub Assign Link</a>	PENDING	STATE PERSONAL	1703_10113507
	05/04/2017	1	<a href="#">Sub Assign Link</a>	PENDING	SCHOOL BUSINESS	1703_07100401

## SUB SEARCH



Choose a Date then View List for Campus subs that are not booked on that day.

View List



# My TimesAway Site



## Employee Access

MY TIMESAWAY - PREVIOUS, CURRENT AND UPCOMING

Print

Name	Start Date	End Date	Days	Edit/Cancel	Reason	Substitute	Requ ID	State
Staff Name	2017/02/22	2017/02/22	1/2 (pm only)		STATE PERSONAL	Subs Name	1703_01103708	APPROVED
	2017/02/27	2017/02/27	1		STATE PERSONAL		1703_07083336	APPROVED
	2017/03/03	2017/03/03	1		STATE PERSONAL		1703_07085542	APPROVED
	2017/03/06	2017/03/06	1		STATE PERSONAL		1703_07085932	APPROVED
	2017/03/07	2017/03/07	1		STATE PERSONAL		1703_07090502	APPROVED
	2017/03/08	2017/03/08	1		STATE PERSONAL		1703_07090758	APPROVED
	2017/05/04	2017/05/04	1	<a href="#">Edit/Cancel link</a>	SCHOOL BUSINESS		1702_23010500	APPROVED

# My Sub Assignments Site

MY CURRENT AND UPCOMING SUB ASSIGNMENTS

Substitute Access



Select Name, Enter Employee Number and select VIEW to see current and upcoming assignments.

Select Name...

Print

Name	Campus	Start Date	End Date	Days	Substitute	Requ ID	State
Staff Names	Elementary	2017/03/08	2017/03/08	1	My Name	1703_07090947	APPROVED
	Elementary	2017/03/09	2017/03/09	1		1703_03114456	APPROVED
	Elementary	2017/03/20	2017/03/20	1		1703_19043150	APPROVED
	Elementary	2017/03/29	2017/03/29	1		1703_10111512	APPROVED
	Elementary	2017/04/06	2017/04/06	1		1703_10113715	APPROVED
	Elementary	2017/04/11	2017/04/11	1		1703_10114248	APPROVED
	Elementary	2017/04/26	2017/04/26	1/2 (am only)		1703_22092501	APPROVED
	Elementary	2017/05/03	2017/05/03	1		1703_11022313	APPROVED
	Elementary	2017/05/04	2017/05/04	1		1703_11022529	APPROVED
	Elementary	2017/05/19	2017/05/19	1		1703_07102829	APPROVED

# Staff Absence Report



Name:	Substitute	Start Date of Absence:	End Date of Absence:	Category	Staff Days charged	Sub - Number of Days	Campus	Reason for absence:	Event Details:	Absence / Sub Confirmed	Sub Hours Day 1	Sub Hours Day 2	Sub Hours Day 3	Sub Hours Day 4	Sub Hours Day 5
Staff1	Sub1	1/30/2017	2/3/2017	STATE PERSON	5	5	Elementary	Personal	Personal	Yes	8.13	8.38	7.28	8.05	8.1
Staff2	Sub2	1/30/2017	1/30/2017	DISTRICT LEAVE	1	1	Junior High	Personal	personal	Yes	7				
Staff3	Sub3	1/30/2017	1/30/2017	STATE PERSON	1	1	High School	Personal	SICK	Yes	8.1				

- HR confirmation and compilation report

- Combines:



- TimesAway info from each absence
- TimeKeeper sub hours if applicable

- Allows Campus level confirmation

- Enhanced error notifications/flags

Name:	Substitute	Start Date of Absence:	End Date of Absence:	Category	Staff Days charged	Sub - Number of Days	Request Id	Event Details:	Position	Absence / Sub Confirmed	Sub Hours Day 1
Staff4	Sub7	1/17/2017	1/17/2017	02 LOCAL PER	1.0	1.0	1701_17022052		Support Sta	Remove	4.2
Staff4	Sub7	1/17/2017	1/17/2017	02 LOCAL PER	1.0	0.5	1701_17022052		Support Sta	Yes	4.2



Staff Absence Report Help Page:

<https://goo.gl/mVbUfq>

# Staff Abs - TkSubMatch (1)



tkSubstitute	Date	Hours	Staff Member	StaffAbs Length	Check - 26
Subs with TimeKeeper Clock In days	2019/1/18	7.75	Staff member and absence length from matching day sub assignment on Staff Absence Report		
	2019/1/21	7.75			
	2019/1/22	7.75			
	2019/1/24	7.75			
	2019/1/25	4.87			
	2019/1/7	7.97			
	2019/1/8	7.77			
	2019/1/9	7.48			
	2019/1/14	4.6			
	2019/1/15	8.17			
	2019/1/16	7.9			
	2019/1/17	4.02			
	2019/1/18	4.3			
	2019/1/21	7.75			
	2019/1/22	7.83			
	2019/1/23	4.33			

- **Substitute - TimeKeeper Actions**
  - Lists each day with hours when a substitute clocked in.
- **Confirms day match on Staff Absence Report**
  - Lists Staff Member and absence length for days matched to a sub assignment
  - Highlights row in yellow if no day match is found on Staff Absence Report



# Staff Abs - TkSubMatch (2)



TimeKeeper Subs	Days - Clocked In	Days - Hrs. Est.	StaffAbs Total
	5	4.5	3
	13	11	9
	1	1	0
	5	5	3
	3	3	2
	4	3.5	1.5
	6	5.5	4
	6	5	5
	5	4	3
	2	2	2
	1	1	1
	7	7	4.5
	10	9.5	8.5
	2	1.5	1.5
	4	4	2
	3	2.5	0.5
	5	4.5	3
	10	9	8
	4	3.5	3
	12	11.5	9.5

Substitutes  
with  
TimeKeeper  
Clock In days

- **TimeKeeper Subs**
- **Days - Clocked In**
  - TimeKeeper total day count
- **Days - Hrs. Est.**
  - Estimates the number of sub days based on daily hours clocked in.
    - Less than 5.5 hours =  $\frac{1}{2}$  sub day
    - 5.5+ hours = full sub day
- **StaffAbs Total**
  - Total Staff Absence sub assigned days

# ESC 14 App Services



## ● **TxEIS transmittal-prep version update**



**TxEIS prep - Nightly updates from TxEIS**

- Staff Info
- Sub Info
- Leave balances



**Update lists throughout App Services**



■ TimeKeeper, TimesAway, etc.

■ Staff lists

■ Sub lists

■ TxEIS Prep

- Displays current leave balances

**Schedule a demo for the TxEIS Prep version update when your district is ready to check on the transition.**



# RAC Notes

## Network Services

### **Network Services**

Network Services is a contracted service to include assistance, support and training to administer the local area network with personal visits, remote, email or telephone support.

Network Services assists with servers, desktop PCs, routers, switches, Smoothwall filter, printers, wireless devices, cabling, and other in-house network components. All districts will have access to the Barracuda backup solution and Virus software.

### **Network Services Contacts:**

**Tim Willis**

[twillis@esc14.net](mailto:twillis@esc14.net)

Network Service

325-675-7027

**Joe Hall**

[jhall@esc14.net](mailto:jhall@esc14.net)

WAN Engineer

325-675-8657

**Mike Wetsel**

[mwetsel@esc14.net](mailto:mwetsel@esc14.net)

WTTC Administrator

325-675-8662



## **What's New In TSDS?** November 4, 2020

It is time for Fall PEIMS! The due date is December 3, 2020.

Fall PEIMS School Start Window AND Snapshot are on the same day this year due to COVID! October 30<sup>th</sup>

ECDS Kindergarten submission due date is January 28<sup>th</sup>, 2020.

KG should be using one of two suggested reading instruments. TX-KEA(CLI) or mCLASS Texas Edition(Amplify) Districts who are not using one of these instruments will not submit ECDS KG this year.

### OTHER TSDS Submissions:

Class Roster (CR)

State Performance Plan Indicator 14 (SPPI-14)

Special Education Language Acquisition (SELA)

Residential Facility (RF) Tracker

[mccllellan@esc14.net](mailto:mccllellan@esc14.net)

325-675-8681

[lhatch@esc14.net](mailto:lhatch@esc14.net)

325-675-8611

[gdickerson@esc14.net](mailto:gdickerson@esc14.net)

325-675-8668

[cpolk@esc14.net](mailto:cpolk@esc14.net)

325-675-7015

[spriddy@esc14.net](mailto:spriddy@esc14.net)

325-675-8639

## **Trainings 2020-2021**

**August 6<sup>th</sup> Zoom meeting on new Attendance codes**

**August 13 Session 108673 TSDS Unique ID Enrollment Tracking Trex**

**August 18 – Session 108674 TSDS TWEDS – PEIMS Data Standards  
Student Records and Teacher Responsibility**

**September 3 Session 108675 PEIMS Update & Attendance Handbook**

**September 29 – Session 108678 TSDS Technical & PEIMS Training**

**October 1 – Session 108679 TSDS Technical Training and Core  
Applications (not PEIMS)**

**Additional Workshops may be added.**

**For handouts and other resources go to the Region 14 ESC  
Website.**

**Go to the TSDS and TxEIS Student icons on the Technology  
Services Program page. Each icon will take you to a new page  
that has documents and handouts uploaded from the  
trainings.**

### **What is TSDS?**

The Texas Student Data System (TSDS), a major initiative by the Texas Education Agency, is a new statewide system that modernizes and improves the quality of data collection, management, and reporting in Texas education.

## What is TWEDS?

TWEDS is a Web-Enabled version of the Texas Education Data Standards. TEDS includes all data elements, code tables, business rules, and data validations needed to load local education agency education data to all TSDS applications.

## What is TSDS Unique ID?

LEAs use Unique ID numbers to load student and staff information to the TSDS Education Data Warehouse (EDW). Each student and staff member will have a single unique 10-digit identifier for his or her entire career within the Texas educational system. Individuals will retain the same unique identifier even if they leave the Texas education system and return years later or transition from being a student to a staff member.

TSDS Unique ID is necessary in order to integrate the various subsystems of TSDS smoothly and accurately.

## TSDS Required Trainings:

**TSDS PEIMS Training** – This training provides participants the knowledge on how to get your data into the Validation Tool to the Data Transfer Utility, To the Data Manager, to the TSDS PEIMS Application

**TSDS ECDS Training**– Early Childhood Data System

This is to provide participants the knowledge on how to get your Kindergarten and Pre-K data uploaded into the TSDS system.

**TSDS Unique ID** – This training provides the most up to date information on the Unique ID process and how to use the application.

**TSDS TIMS** – TSDS Incident Management Escalation Process  
This training explains how a district person writes a ticket after calling the ESC and the problem is escalated to TEA. TEA requires a ticket system for workflow. The district must begin the ticket and escalate the ticket to Level 2 (ESC), we then escalate to Level 3 (TEA) for further assistance.

**TSDS Technical Resources**-This training instructs personal on how your data goes through the Validation Tool to the Data Transfer Utility, To the Data Manager, to the TSDS PEIMS Application

## Pricing for TSDS

TEA set a standard price of \$21,280.00 for Region Centers to charge each district no matter the size. Region 14 worked hard to discount that price and use the ADA of our districts to customize the price for each district. Robb worked out a formula that is all inclusive of technical support and trainings that includes consultants traveling to districts to help as needed. When districts are not a part of our contracted services they are charged \$95.00 an hour for support and training. A workshop is 6 hours and would cost a district \$575.00 per person to attend.

## Terms to Know

- **Unique ID** - the TSDS module for managing identification numbers
- **Operational Data Store** – the ODS, the system's data store, will include a wide range of educational data from the LEAs, spanning multiple years.
- **Dashboard Data Mart** – the DDM is a voluntary repository for multiple years of performance data that uses information loaded by participating LEAs to the ODS to calculate performance metrics and power the optional [studentGPS® Dashboards](#).

- [TSDS PEIMS](#) – the replacement for EDIT+, TSDS PEIMS is a repository for PEIMS data and enables the selective loading, validation, and reporting required to finalize and submit a PEIMS collection.
- [Core Collections](#) - the application that houses all other TEA data collection in TSDS, such as the Early Childhood Data System (ECDS), SPPI-14, Residential Facility (RF) Tracker, Class Roster, and SELA.
- [Texas Web-Enabled Education Data Standards](#) – TWEDS provides specifications for loading LEA educational data into the EDW for reporting and analysis purposes. TWEDS is based on the national Ed-Fi standards and is more expandable and widely compatible than the legacy PEIMS standards



## **What is the TPEIR?**

The Texas P-20 Public Education Information Resource is a longitudinal data warehouse that links students from pre-K through enrollment and graduation from Texas colleges (P-20). It is managed by TEA in partnership with the Texas Higher Education Coordination Board.

In addition to **20+ years** of P-12 and higher education data from Texas colleges and universities and information on teacher certification and teacher preparation programs, the warehouse has been expanded to link critical missing **pre-kindergarten, college readiness, and workforce** (wage, industry, and employment) data.





# Texas Goes TxEIS

Secure Web-based Software for Texas Schools



**Awarded as a state-sponsored student information system**

**Secure your future – upgrade to TxEIS Plus**



## TxEIS-sized Hosting

We're upgrading your hosting experience by adding backup TCC data centers!

A fully integrated, Web-based product, **TxEIS PLUS** can be hosted at a regional ESC data center – providing **EXCLUSIVE** access to these hosting advantages:

- + Redundant systems keep the hosting environment up and running
- + Guaranteed business continuity and disaster recovery
- + Maintenance-free hosting managed by ESC technical experts
- + Data access remains district controlled
- + Automatic backups, upgrades and new releases
- + Eliminates expenses to maintain and upgrade your on-site servers

## TxEIS-sized Service

With over 40 years of experience providing service in Texas, **TxEIS PLUS** offers superior quality support from your trusted ESC representatives.

Our support services include:

- + Phone and email support
- + Training/Workshops
- + Training Documents/User Guides
- + Inclusion on Distribution Lists
- + Problem Resolution

Select your ideal support package from the following options:



Platinum



Gold



Silver



Bronze

## TxEIS-sized Value

As part of our continued service to our loyal customers, ESC representatives are eager to work with each school district and charter school to ensure that **TxEIS PLUS** fits comfortably within your budget.

**Contact your local ESC for pricing information.**

(Please see back page for contact information.)



## Texas Goes TxEIS

# PLUS

### Secure Your Future

Seeing the news images of the devastation from major hurricanes and tornadoes, do you wonder about it happening in your community? Most of us don't. But stop and think about your own surroundings. Is there ever heavy rain, snow, or hail? Could a gas leak cause a potential explosion? Could a water main break cause flooding? Could a fire caused by nature or by arson wreak havoc on your facilities?

What would you do? Do you have current backups of your student and financial data? Are they in what was advertised as a "fire proof" vault? Are they stored at least five miles away from your district or charter school? Have you made arrangements to bring up your computer environment in another location with the hardware capacity you need? Will you have staff available who can configure the equipment and restore the necessary software programs, along with the data, to get you back in operation - without missing the next payroll or report card due date?

Most schools do not have a disaster recovery plan in place that would address all of these vulnerabilities.

You do not have to live in an area at risk for hurricanes to need disaster recovery.

**No matter where you are, you need it!**

### What Are My Options?

If you are one of the almost 900 LEAs using TxEIS, or you are considering TxEIS as your software of choice, here are some benefits you should know:

#### Option 1

Most ESCs offer a hosting option, where your data is housed in a secure, protected environment.

- Your data is backed up nightly and sent to one of the two TxEIS Data Centers.
- The TxEIS Data Centers replicate the backed up data between each other, offering a third degree of protection.
- Weekly backups of data are created and maintained by TxEIS Data Center staff for 90 days at a secure off-site facility.
- In the event of a disaster at your host ESC, one of the Data Centers will have you back in operation in 48 hours or less as of the last backup received at the TxEIS Data Center.



**TxEIS: The only administrative software designed exclusively for Texas schools**

#### Offering:

- Secure hosting - leave the hardware and maintenance to others
- Disaster recovery/business continuity
- Texas-specific software at the best value in Texas
- Premier support from your local ESC
- Service Level Agreements with guaranteed response times

#### Option 2

A second hosting option is to be hosted at one of the two TxEIS Data Centers located at the ESCs in San Antonio (ESC-20) and Fort Worth (ESC-11). The TxEIS Data Centers were designed for the purpose of hosting multiple tenants with security, high-availability, backup, and disaster recovery. The architecture is built around Cisco and Dell industry-leading technologies as a multisite, fully redundant design with automated disaster recovery failover from each site to the other site. Included in the architecture is a comprehensive security solution using state-of-the-art Cisco firewalls, security appliances, and switches.

- Your data is backed up nightly and sent to the other TxEIS Data Center.
- Additionally, incremental backups are made and sent every two hours to the other TxEIS Data Center.
- Weekly backups of data are created and maintained for 90 days at a secure off-site facility.
- In the event of a disaster at one TxEIS Data Center, the other center will have you back in operation within a matter of hours, with two hours or less loss of data, guaranteeing business continuity.
- The TxEIS Data Centers have been certified by an SSAE-16 SOC2 Type 1 audit of internal controls, providing peace of mind regarding security and availability.
- You are still supported by your local ESC!



# Texas Computer Cooperative (TCC)

***A Tradition of Performance***

***A Vision for the Future***

Turn to the leader in the most comprehensive administrative software available for Texas schools, and let us give you the proper tools to manage your school district's future.



## iTCCS

With over 45 years of public education and software development experience, iTCCS applications provide you with powerful tools for managing your school district's future. iTCCS applications are widely used in the state of Texas servicing the needs of over 335,000 students. iTCCS is managed by the Texas Computer Cooperative (TCC) offering a comprehensive range of business and student administrative applications written specifically for Texas school districts and charter schools. iTCCS is your school management software partner for the future: a cooperative effort that is attentive to your needs and offers you qualified expertise, a full product line, and comprehensive service, support, consulting, and training.

Visit [tcc-itccs.net](http://tcc-itccs.net) for more information.



## TxEIS

TxEIS offers a state-sponsored Student information system, as well as a complete range of Business applications, designed exclusively for Texas local education agencies (LEAs). TxEIS is a fully integrated solution that streamlines operational needs and simplifies reporting requirements. And why not add secure data center hosting, with disaster recovery, supported by trained service technicians. TxEIS gives you localized support from 19 Education Service Centers across Texas who have expertise in the needs of their local LEAs and dedication to local customer support. With TxEIS, you'll get complete peace of mind.

The Texas Computer Cooperative (TCC) is a cooperative of 19 of the Texas Education Service Centers (ESCs) currently serving 875 districts across the state and over 1.1 million Texas students. For nearly 50 years the TCC has been the leader in delivering products and services that support Texas LEAs in managing student and business information. The TCC has been working with strategic partners to develop a comprehensive Business Plan that will ensure we continue to provide the best products and services to you, our clients.

By 2021, the TCC will establish a single new product suite, merging the functionality of the current TxEIS and iTCCS products. This new product suite will build on our success as the leader in the state in compliance and reporting, provide an enhanced user experience, and further empower LEAs to easily make informed decisions and engage stakeholders through powerful yet flexible tools and applications.

Current iTCCS clients can expect continued high quality, responsive support. The TCC and your ESC support team will ensure a smooth transition to the new product, which will offer new functionality as well as a significantly improved user interface and navigation. ESC support teams will work with each client individually to develop a customized transition plan.

Current TxEIS clients can expect the same ease of use and navigation with more robust integration with third party software. We will continue to introduce new software features and enhancements. Clients will experience a seamless transition to the new product.

Future TCC clients can expect a top quality business and student Enterprise Information System that meets the needs of *all* Texas LEAs. We will continue to outperform our competitors with the largest, most knowledgeable business and student support teams who can be onsite at any client location in the state in under three hours. TCC software is developed specifically for Texas LEAs. No competitor matches our understanding of and compliance with Texas school business rules and requirements.

Sincerely,

Jeff

**Jeff Goldhorn, Ph.D.**

Executive Director

Education Service Center, Region 20

1314 Hines Avenue, San Antonio, Texas 78208

[jeff.goldhorn@esc20.net](mailto:jeff.goldhorn@esc20.net)

Ph: (210)370-5600

Cell: (210)363-8024

## **TxEIS & TSDS Fall 2020 Workshops**

You may find these trainings in PitStop on the Region 14 website!

**November 10 - Session 109064 – Fall PEIMS Workday** - This is a workday for Student users to complete the Fall PEIMS submission. Fall Submission is Due December 6<sup>th</sup>.

**November 17 - Session 108974 – Fall PEIMS Workday** - This is a workday for Student users to complete the Fall PEIMS submission. Fall Submission is Due December 6<sup>th</sup>.

**December 15- Session 108682 TxEIS End of Semester and Grade Averaging**- This workshop will provide end of Semester 1 Grading Procedures as well as teach how to run Grade Averaging and Class Ranking.

**January 21 – TxEIS Personal Graduation Plans** - Training will be on the TxEIS PGP application. This is a great training for your campus secretaries, counselors, or anyone that would be working in the PGP application. **NOT IN PITSTOP YET**



# ***ESC Region 14 School Finance November 2020***



***November 5th --PEIMS workday-- sign up on Tx&IS Business Webpage***

***November 10th--PEIMS workday-- sign up on Tx&IS Business Webpage***

***November 11th--PEIMS workday-- sign up on Tx&IS Business Webpage***

***November 12--Fall PEIMS due to ESC for review***

***November 19th--Business Forum + Consortium training on TRS-- Session #109040***

***November 20th - Annual Fingerprinting Certification and Statement of Compliance  
due***

***December 1st--Operations Transportation Report due***

***December 2nd--Consortium Training on PEIMS data impacts-- Session #108814***

***December 3rd--Fall PEIMS due to TEA***

***December 9th--Tx&IS workday-- sign up on Tx&IS Business Webpage***

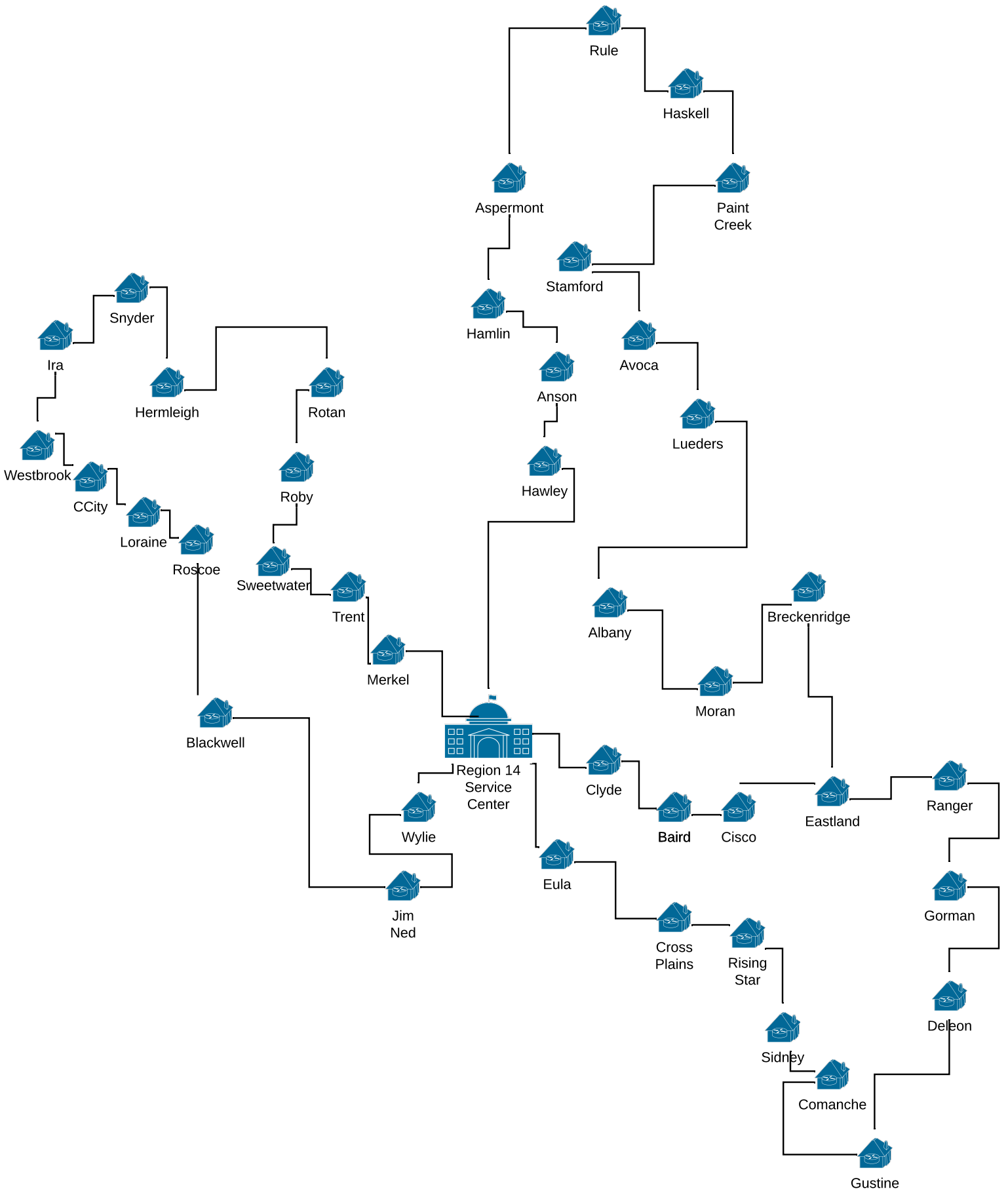
***December 10th--Business Forum + T&SB BuyBoard presentation***

***December 16th--W-2, 1099, ACA workshop for Tx&IS users --Session 109113***

### WTTC Board of Directors - 2020-2021

Name	Category	Organization	Years Served	Fax #	E-mail	Phone #
Bill Alcorn	K-12	Haskell CISD	2	940-864-8096	balcorn@haskell.esc14.net	940-864-2602
Bryan Allen	K-12	Merkel ISD	2	325-928-3910	ballen@merkelisd.net	325-928-5813
Jay Baccus	K-12	Anson ISD	1	325-823-6371	jbaccus@anson.esc14.net	325-823-4444
Kenny Berry	K-12	Clyde CISD	2	325-893-4222	kjberry@clydeisd.org	325-893-4024
Patti Blue*	K-12	Gustine ISD	3	325-667-7303	pblue@gustine.esc14.net	325-667-7281
Randy Burks	K-12	Hamilin ISD	3	325-576-2722	rburks@hamlin.esc14.net	325-576-2152
Sheron Caton	Higher Education	Cisco College	1		sheron.caton@cisco.edu	325-794-4530
Greg Decker	K-12	Rotan ISD	2	325-735-2332	gdecker@rotan.esc14.net	325-35-2686
Shane Fields	Gov't Agencies	Region 14 Ed. Srv. Cntr.	3	325-675-8659	sfields@esc14.net	325-762-3974
Scott Hamm	Higher Education	Hardin Simmons	1		Scott.E.Hamm@hsutx.edu	325-670-1099
Joey Light	K-12	Wylie ISD	2	325-695-3438	jlight@wylie.esc14.net	325-692-4353
Mary Ross	Gov't Agencies	West Central Texas Workforce Center	3	325-795-4300	mary.ross@workforcesystem.org	325-795-4301
Bob Spikes	K-12	Lueders Avoca CISD	2	325-228-4211	bspikes@lueav.esc14.net	325-228-4513
Glen Teal	K-12	Jim Ned ISD	2	325-554-7740	gteal@jimned.esc14.net	325-554-7500
Mike Thompson	K-12	Ranger ISD	1	254-647-5215	mthompson@ranger.esc14.net	254-647-1187
* - Board Chair						
** - Vice Chair						
Robb McClellan	Director of CTS	Region 14 Ed. Srv. Cntr.		325-675-8659	mcclellan@esc14.net	325-675-8681
Mike Wetsel	WTTC Administrator	Region 14 Ed. Srv. Cntr.		325-675-8659	mwetsel@esc14.net	325-675-8662

# Region 14 Wide Area Network Layout





---

**Meeting Minutes**  
**August 5, 2020**

**Call to order:**

Meeting was called to order at 9:01 a.m. by Bryan Allen

Board members present: Bryan Allen, Patti Blue, Shane Fields, Bill Alcorn, Jay Baccus, Joey Light, Glen Teal, Greg Decker, Mary Ross, Sharon Caton , Scott Hamm, Bob Spikes, Jonathan Scott and Kenny Berry

**WTTC Administrator:** Mike Wetsel; **WTTC Director:** Robb McClellan

**Visitors:** Christy Cate, Hilary Miller, @jrutkowski, Jason Carter, and Dana Marible

**Introduction of Guests:** Welcome new Board Member Sharon Caton

**Approval of Minutes:**

Bill Alcorn made a motion to approve the minutes from February 5, 2020. Motion was seconded by Joey Light. Motion was approved unanimously.

**Financial Report:**

Mike stated that everything is in good shape putting us back at about 60%. Jay Baccus made the motion to approve the Financial Report. Glen Teal seconded. Motion was approved unanimously.

**Budget:** More supplies have been added to the Maker Space. This year the bill will be higher because we are needing to purchase a firewall. Robb stated that we could discuss other billing options in the future. One option would be to spread the budget over a five year period, to make billing more consistent. Bill Alcorn stated that it would be best in his opinion, to go ahead purchase the Firewall. Sharon agreed and also mentioned discussing a more consistent billing process going forward. Bill Alcorn made a motion to approve the budget and Bob Spikes seconded. Motion was approved unanimously.

**2020-2021 Elections** There are 2 Board Member vacancies. Mike will send out an email to the Superintendents for anyone interested in being a WTTC Board Member. They will be voted on at the next board meeting.

**WAN Update:** Mike stated that he is in contact with Texas Lonestar Network to help provide services for students out of range. Mary Ross stated that the Federal Reserve Bank in Dallas is also looking at resources to address the digital divide.

Mike stated that the wide area network was good overall and the only thing he would add is a UPS at each district.

**Other:**

**Adjourn:**

Motion made to adjourn by Jay Baccus and seconded by Bryan Allen. Approved by all at 9:23 a.m.



---

**Agenda**  
**Wednesday, November 4, 2020**  
**via Zoom**

<https://us02web.zoom.us/j/84458042598>

- Call to Order
- Introduction of Guests
- Roll Call for DL Participants
- Minutes from August 5, 2020
- New Vice-Chair
- Financial Report
- WAN Update
- USAC Update
- Other

**Next meeting – February 3, 2021**

**Adjourn**

## WTTC Package

The WTTC is much more than just Internet Access. We provide training, instructional technology, network security, network monitoring, as well as Internet Access. Our staff has over 180 years of experience in Education and Technology to support you. According to an Internet Security Officer dealing with over half of the other Region Centers, we are far ahead of most with our security and other services.

Instructional Technology – about 34% of your WTTC fee.

We currently have 3 Instructional Technology Specialists. They provide Google Certifications for Educators, Interactive Education Resources Training, Technology Innovations Training, Technology Content Training, Professional Development Training and access and training on resources such as our K-12 Makerspace at our Region 14 Service Station. Professional development classes are included in your fee.

Christy Cate 12 years at ESC14, 24 years in Education, 20 years in technology

Shawn Schlueter 13 years at ESC14, 26 years in Education including 3 years as Technology Director, 13 years at ESC14 and 10 years as a Science Specialist

Hilary Miller 2 years at ESC14, 17 years in education, 11 years in Technology

WTTC Network - about 66% of your WTTC fee

Internet Access from 2 Internet POPs ensuring that if one provider goes down, you still have Internet access from another provider. Dual 1 gig fiber routes back to Region 14. All traffic is protected by a state of the art firewall. Traffic is monitored 24x7 by a third party service to notify us of any instances warranting action. A product called SecureX ties all of our firewall, endpoint protection, traffic monitoring as well as third party evaluations into a seamless portal to monitor and protect the network. The fiber network was purchased for 3 cents on the dollar. The firewall was obtained at an unheard price of 81% discount and other services are heavily discounted as well. We also provide distance learning opportunities through traditional DL as well as Zoom.

Joe Hall – Network Engineer 12 years at ESC14, 24 years in technology

Jeremiah Mahaffey – Distance Learning Specialist – 19 years at ESC14

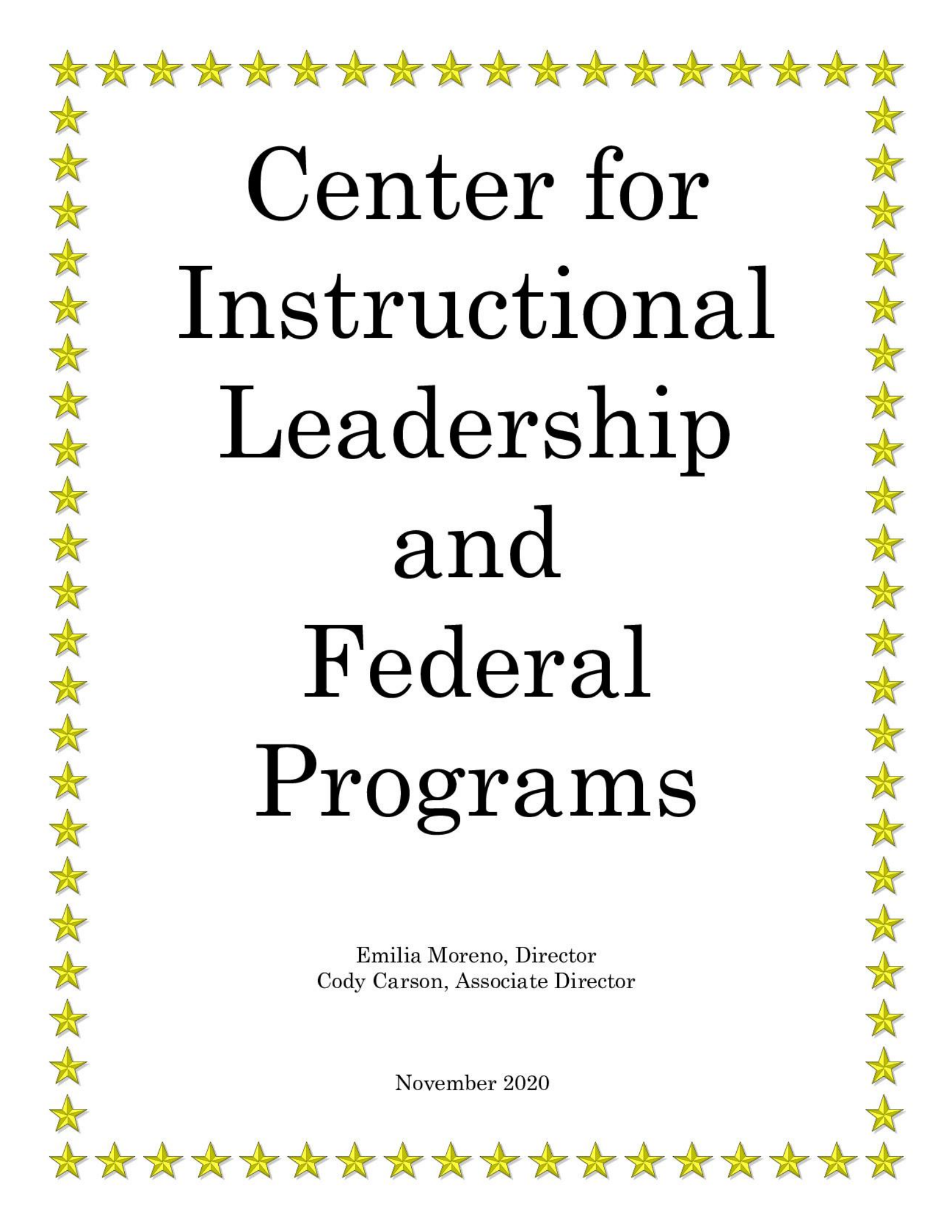
Tim Willis – Network Support – 20 years at ESC14, 20 years in Technology

Jeremy Jones – Server and Network Security 3 years at ESC14, 6 years in technology

Dontay Raglin – Network Security 1 year at ESC14, 3 years in technology

Mike Wetsel – WTTC Administrator 11 years at ESC14, 26 years in Education, 34 years in technology

Robb McClellan – WTTC Director – 20 years at Region 14, 32 years in Education and 23 years in technology.



# Center for Instructional Leadership and Federal Programs

Emilia Moreno, Director  
Cody Carson, Associate Director

November 2020

**Instructional Leadership & Federal Program Updates  
November 2020**

---

**2021-22 Mentor Program Allotment – Cycle 2**

Optional program that provides LEAs with funds to build or sustain beginning teacher mentor programs

- Cycle 2 District Application – **November 2** window opens
- Application Deadline – **December 18**
- TEA notifies districts of MPA application approval – February 2021
- MPA funding begins – September 2021

**Additional information:**

- ✓ Awarded LEAs must abide by TEC 48.114;
- ✓ If LEA interest & eligibility exceed the state funding amount:
  - **Priority points** based on – LEA size, rural status, requirement to submit an ESSA Equity Plan, and percentage of LEA’s student population that qualifies as ECO Dis

*For additional information or assistance, please contact Cody Carson @ 325-675-7031.*

\*\*\*\*\*

**Grant Update**

**Safety & Security Grant:**

- ✓ Public schools, including the School for the Blind and Visually Impaired and the School for the Deaf may only expend funds for:
  1. exterior doors with push bars;
  2. metal detectors at school entrances;
  3. erected vehicle barriers;
  4. security systems that monitor and record school entrances, exits, and hallways;
  5. campus-wide active shooter alarm systems that are separate from fire alarms;
  6. two-way radio systems;
  7. perimeter security fencing;
  8. bullet-resistant glass or film for school entrances; and
  9. door-locking systems

Eligible funding amount for most LEAs: \$25,000

Last date for an amendment: **March 2, 2021**; if the needs assessment has changed for this funding then district will want to amend the application

Grant end date: **May 31, 2021**

### **Elementary & Secondary School Emergency Relief Fund (ESSER) Grant:**

- ✓ All activities charged to the ESSER grant must be reasonable and necessary to meet the overall purpose of the program, which is “to prevent, prepare for, and respond to” the COVID-19 pandemic.

#### ESSER Key Dates:

March 13, 2020 – Pre-award allowed

March 27, 2020 – CARES Act signed

May 15, 2020 – TEA received federal award

**May 15, 2021** – TEA must issue NOGAs to LEAs

**September 30, 2021** – ESSER funds end date

**September 30, 2022** – 12- month carryover

### ***ESSER Random Validation (RV) Training:***

- TEA staff will provide training to ESCs in January 2021.
- ESCs will train selected LEAs as a requirement of the ESC ESSER Technical Assistance Grant by the end of February 2021
- **MARCH 19, 2021: DEADLINE TO SUBMIT DOCUMENTATION FOR VALIDATION**

Some indicators include:

- LEA can **provide date(s) that the needs assessment** was developed or the date(s) that the needs assessment was reviewed and/or revised
- **Needs Assessment should include:**
  - 1)How the LEA will determine its most important educational needs as a result of COVID-19;
  - 2)The LEA’s proposed timeline for providing services and assistance to students and staff in both public and non-public schools (as applicable);
  - 3)How the LEA intends to assess and address student learning gaps resulting from the disruption in education services
- Sample Types of Documentation:
  - Documentation of compensation to employees and contractors during the period of closures related to COVID-19
  - Title to materials, equipment and property purchased with ESSER funds

## **Kindergarten & Prekindergarten Program Requirements**

The Early Childhood Data System (ECDS) is a state reporting feature in the Texas Student Data System (TSDS). Unless specifically exempted by a waiver, all public schools and open-enrollment charter schools (LEAs) must report assessment data, aligned with the Texas Education Data Standards (TEDS), that are collected using assessments that are on the commissioner's list of approved assessments.

- ECDS application will be available for LEAs to load *kindergarten data* from **November 9, 2020 - January 28, 2021**
- ECDS application will be available for LEAs to load *prekindergarten (PK) data* from **November 9, 2020 - June 24, 2021**

### **Public Kindergarten Programs (11-9-20 through 1-28-21)**

The reporting of kindergarten program data into ECDS is **mandatory for all LEAs** that administer an approved tool from the commissioner's list, which currently includes the following:

- ✓ Texas Kindergarten Entry Assessment (TXKEA) by CLI Engage
- ✓ mCLASS Texas Edition by Amplify Education

### **Public Prekindergarten Programs (11-9-20 through 6-24-21)**

The reporting of public prekindergarten program data into ECDS is **mandatory for LEAs** that administer a prekindergarten program

- Type of curriculum:
  - The Texas DLM Early Childhood Express
  - Opening the World of Learning: Texas Comprehensive Pre-K
  - Big Day for PreK Texas Program
  - High Scope Preschool Curriculum and Assessment
  - Frog Street Pre-K
  - Texas System Teaching Strategies System for Pre-K, Texas Edition
  - Other

\*\*\*\*\*

## **2020 Results Driven Accountability (RDA)**

The 2020-21 determination levels for local education agencies (LEAs) for the bilingual education/English as a second language (BE/ESL/EL), other special populations (OSP), and special education (SPED) program areas will be available on October 16, 2020 through the Ascend application in the Texas Education Agency Login (TEAL).

### ***Summary of Indicators***

---

***(Red – No DATA or Report Only for RDA in 2020)***

#### ***BE/ESL/EL***

Domain I	Indicator #1 (i-v)	BE STAAR 3-8 Passing Rate
	Indicator #2 (i-v)	ESL STAAR 3-8 Passing Rate
	Indicator #3 (i-v)	EL (Not Served in BE/ESL) STAAR 3-8 Passing Rate
	Indicator #4	EL Dyslexia STAAR 3-8 Reading Passing Rate
	Indicator #5 (i-v)	EL Years-After-Exit (YsAE) STAAR 3-8 Passing Rate
	Indicator #6 (i-iv)	EL STAAR EOC Passing Rate
	Indicator #7	TELPAS Reading Beginning Proficiency Level Rate
	Indicator #8	TELPAS Composite Rating Levels for Students in U.S. Schools Multiple Years
Domain II	Indicator #9	EL Graduation Rate
	Indicator #10	EL Annual Dropout Rate (Grades 7-12)
Domain III	Indicator #11	EL Dyslexia Representation (Ages 6-21)

---

#### ***Other Special Populations (Foster Care/Homeless/Military)***

Domain I	Indicator #1 (i-v)	OSP STAAR 3-8 Passing Rate
	Indicator #2	OSP Dyslexia STAAR 3-8 Reading Passing Rate
	Indicator #3 (i-iv)	OSP STAAR EOC Passing Rate
Domain II	Indicator #4	OSP Graduation Rate
	Indicator #5	OSP Annual Dropout Rate (Grades 7-12)
Domain III	Indicator #6	OSP Dyslexia Representation (Ages 6-21)

---

#### **RDA Timeline:**

##### October

- Results Driven Accountability (RDA) Data Released

##### November

- Superintendent identifies District Coordinator of School Improvement (DCSI)
- Superintendent and DCSI establish District Leadership Team (DLT)
- Department of Review and Support contacts LEAs with Determination Level (DL) 3 or higher to schedule teleconference to review RDA data, Root Cause Analysis, COVID-19 Impact Protocol and Strategic Support Plan (SSP) development (optional)



- DCSI, DLT, and relevant stakeholders engage in planning activities and develop SSP

December/January

- DCSI, Education Service Center (ESC) staff, and TEA staff conduct teleconference to discuss initial SSP submission \*DL 3 or higher for BE/ESL/EL or OSP\*
- Superintendent submits DCSI qualifications in Ascend: Due Dec. 1st
- DCSI submits SSP in Ascend: **Due Dec. 18th**  
\*Submissions Required for Determination Levels 3 or 4 in BE/ESL/EL or OSP\*

TEA webinar training link for the following RDA related areas:

- Results Driven Accountability Training – October 13, 2020
- EL Self-Assessment Overview – December 9, 2020
- Dyslexia Program Evaluation – October 29, 2020 & December 15, 2020
- Dyslexia Monitoring Overview – October 27, 2020

<https://tea.texas.gov/academics/special-student-populations/review-and-support/review-and-support-resources>

**Ascend Application on TEAL**

The 2020-21 determination levels (DLs) for LEAs for the BE/ESL/EL, other special populations (OSP), and SPED program areas were made available on October 16, 2020 through the Ascend application in TEAL. Add this application to your TEAL account to view Ascend report for your LEA.

*For additional information or assistance, please contact Emilia Moreno @ 325-675-8674.*

\*\*\*\*\*

**Comparability Assurance Document**

ALL districts receiving federal funds are required to submit an ONLINE SURVEY. This survey is due **November 20!**

*For additional information or assistance, please contact Lucy Smith @ 325-675-8641.*

# Strengthening Classroom Outcomes

YEARLY SUBSCRIPTION PURCHASED THROUGH  
REGION 14

Get 6 Ebooks and 2 On-Demand Workshops  
Annual Subscription **\$60**

Your Pace, Your Schedule. Online. On-Demand.  
**START TODAY**

EMOTIONAL poverty  
a framework for UNDERSTANDING POVERTY  
RESEARCH-BASED STRATEGIES  
BOYS in Crisis  
WORKING with STUDENTS  
BEFORE YOU QUIT TEACHING

**RUBY PAYNE, PhD**

12-month subscription includes 2 on-demand PD trainings and 6 ebooks accessible any time during the 12-month period.

**REGISTER NOW!**

**HOW TO REGISTER:**

**[www.esc14.net](http://www.esc14.net)**

**Select: District Depot**

**Log In: Using Your Pitstop Info**

**Select: aha! Process Subscriptions**

**REGISTER NOW!**



## **2020-2021 Counselor of the Year**

Nominations now open for the  
ESC 14 Counselor of the Year.  
Counselor honors will be given  
in the following areas:

- K-12 Campus
- Secondary Campus
- Elementary Campus

To nominate your counselor:

<https://bit.ly/3drPZqD>

**Deadline to Nominate Wednesday, November 18th**

## Counselor Consortium Workshops

### December 1st- Consortium Exclusive

- Presenter: Author Julia Cook
- Request a Spot: <https://bit.ly/371mDOQ>

### December 9th- Coffee & Conversation

- Accountability Updates w/TEA
- Register here: <https://bit.ly/2GTHTLF>

### January 20th- Reality Therapy

- Presenter: Dr. Brenda Faulkner
- Register here: <https://bit.ly/2SudLC4>

### February 24th- Counselor Mini Conference

- Presenter: Betty White
- Registration coming soon

### Counselor of the Year Nominations

- Due November 18th
- Nominate a counselor <https://bit.ly/3drPZqD>

### Counselor Consortium Contact

Zan Wilson

[zwilson@esc14.net](mailto:zwilson@esc14.net)

325-675-8620



TITLE A

TITLE B

TITLE C

TITLE D

TITLE E

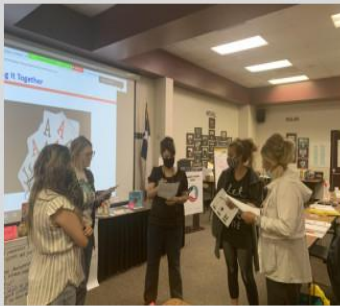
TITLE F



Contact Us:

Cody Carson  
[ccarson@esc14.net](mailto:ccarson@esc14.net)  
325-675-7031

Amy Kotara  
[akotara@esc14.net](mailto:akotara@esc14.net)  
325-675-7038



Region 14 is a TEA authorized provider. We can assist you in implementing HB3 Reading Academies through various pathways including:

- Blended
- Comprehensive
- Biliteracy
- Administrator
- Local Implementation

Come join the fun!

Launching new academy cohorts  
Summer 2021!

We can support you through:

- Deep dive training
- Individualized coaching
- PLC Support
- Artifact Coaching



# Bus Driver Training Winter 2021

## Registration Fees:

\$60 for 8-hour recertification

\$150 for 20-hour certification

Additional \$150 out of region

## 8 Hour Recertification

Minimum enrollment for trainings must be at least 10 participants.

Additional trainings will be scheduled as needed.

## 20 Hour Bus Driver Certification

[Session # 109057](#) - February 1-3, 2021

5:30 - 9:30

### ESC 14 Bus Driver Training Coordinators:

Alan Richey, 325-675-8622 [arichey@esc14.net](mailto:arichey@esc14.net)

Alicia Gonzales, 325-675-7001 [agonzales@esc14.net](mailto:agonzales@esc14.net)

# Title I, Part A & ESSA Updates

## Comparability Submission

There are two parts to the annual Comparability obligations:

1. **Comparability Assurance Document (CAD)**- required for **ALL districts receiving federal funds**. This is an [online survey](#) where LEAs state whether or not they are exempt and acknowledge compliance with a couple of requirements. **This survey is due November 20**
2. **Comparability Computation Form (CCF)**- required for non-exempt districts. Due in November

## Title I Zoom Recordings

- All Title I contacts received an email from Lucy on 10/6/20 with two Title I zoom recordings.
- Please send Lucy an email detailing which zooms you viewed, if any, in order for your district to receive credit

## NEW! "Title I Talks" w/ Lucy & Zan

- Short zoom sessions to address current issues/updates on Title I, Part A
- Nov 13 @ 1:30 [Register](#)
- Dec 11 @ 1:30 [Register](#)

## Highly Qualified Paraprofessionals

- Follow the link to find the requirements for paras performing instructional duties on a Title, I Part A Schoolwide served campus
- **NOTE:** The paraprofessional must also meet the state's paraprofessional certification exam and requirements.
- <https://bit.ly/3j343lw>

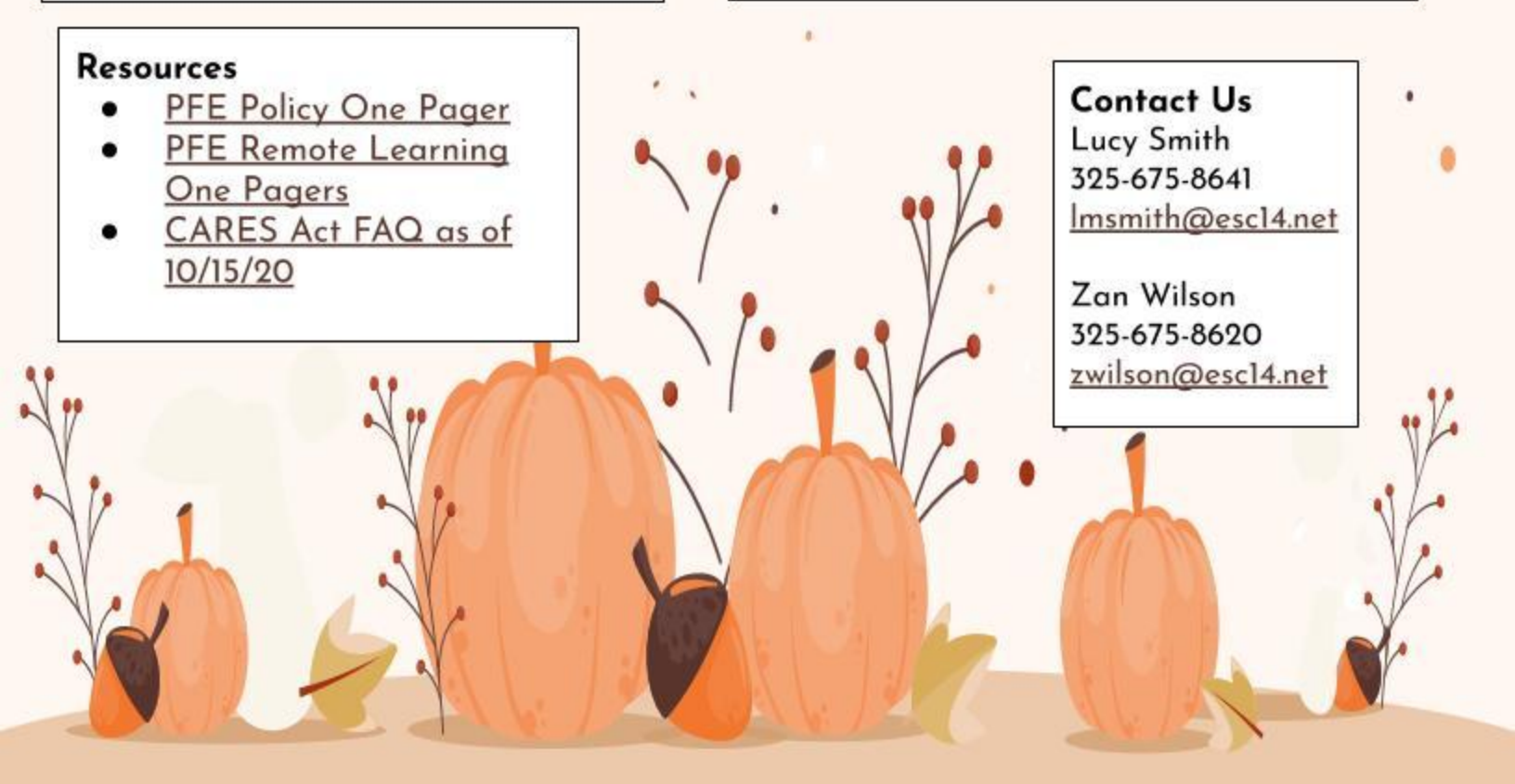
## Resources

- [PFE Policy One Pager](#)
- [PFE Remote Learning One Pagers](#)
- [CARES Act FAQ as of 10/15/20](#)

## Contact Us

Lucy Smith  
325-675-8641  
[lsmith@escl4.net](mailto:lsmith@escl4.net)

Zan Wilson  
325-675-8620  
[zwilson@escl4.net](mailto:zwilson@escl4.net)



# Career and Technical Education Updates

November 2020

## Upcoming CTE Professional Development

Region 14 Perkins V SSA  
Updates-Nov. 3rd

(11:00 a.m. -12:00 p.m.) Zoom only  
[Registration link](#)

New CTE Teacher Cohort-Nov. 6th  
(9:00-12:00)

In Person & Zoom [Registration link](#)

Counselor Chat-November 6th  
(1:00-2:00 p.m.)

Zoom only [Registration link](#)

CTE Leadership Meeting-Dec. 2nd  
(9:00-12:00)

In Person & Zoom [Registration link](#)

## Business/Industry Partner

[BIG COUNTRY MANUFACTURING ALLIANCE](#)

Contact Info:  
Vicki Hayhurst  
Region 14 CTE  
Specialist  
325-675-8669  
[vhayhurst@esc14.net](mailto:vhayhurst@esc14.net)

## Reporting IBCs in TSDS PEIMS

May report IBCs earned between  
9/1/2019-5/31/2020

In the 2020-2021 TSDS PEIMS Fall  
Submission

One-time reporting submission  
extension for the above reporting  
time. Must be in the PEIMS Fall  
Submission resubmission deadline.  
(FINAL)

### IBC Exam Fee Data Element

- Does not permit decimals
- Follow standard rounding rules
  - >0.50 round up to the nearest whole number
  - <0.49 round down to the nearest whole number

## Administrator CTE Resources Links

- [Texas Perkins V CTE State Plan](#) (Summary)
- [Programs of Study](#) (updated)
- [Chapter 231 Teacher Certifications](#) (updated)
- [CTE Innovative Courses](#) (updated)





# HIGHLY MOBILE AND AT-RISK STUDENT PROGRAMS DIVISION WEBINAR

**Thursday, November 5th, 2020 | 1:00 pm - 3:00 pm**

**Register via Zoom**

Education Service Centers, School District staff, and Open-Enrollment Charter School staff are encouraged to attend!

Please join us to hear important information for the 20-21 school year!

Topics include:

- Mental and Behavioral Health Updates
- Safe and Supportive School Program
- Highly Mobile Student Engagement
- Transition Assistance for Foster Care and Homeless Students
- Student Programs Updates
- and more...

Please send any questions to: [Jordan.Brown@tea.texas.gov](mailto:Jordan.Brown@tea.texas.gov)

# McKinney Vento 101 Training

*Who: District liaisons or school staff who has not had McKinney Vento 101 training this year*

*When: Thursday, November 5, 2020 , Time: 9:30- 12:00pm*

*Where: Virtual*

*Why: McKinney Vento Act requires LEAs to identify students experiencing homelessness to ensure equitable services.*

*[Register here](#)*

*Contact: Tina Haywood, [thaywood@esc14.net](mailto:thaywood@esc14.net), 325.675.8624*

# REGION 14

## SCHOOL HEALTH SERVICES

Guidance for conducting  
bleeding control training  
under COVID-19 conditions

- Senate Bill 11
- Updated September 2020
- Includes Virtual flexibilities
- Find more information [here](#)



## CERTIFICATIONS

Hearing

Vision

Spinal

Re-certification



# CHILD NUTRITION PROGRAM

## Region 14

Cynthia Whitfield  
Barbara Braden  
Lori Muzquiz  
Cody Polk

### Verification Report

The **Preliminary Verification Report** will open November 1st and is due November 15th. This is a JotForm and the link to the Jotform will be provided in an email to CEs and in Download Forms on TX-UNPS (SNP-123).

The count of students reported on the Preliminary Verification Report **MUST** equal the count of students reported on the SFA Verification Report.

### Summer Mandate

If requesting a waiver, state law requires\* board of trustees to send written notice of the district's intention to the district's local school health advisory council (SHAC) no later than November 30, 2020.

\*Subject to change, based on COVID-19 guidance.



# PY21

# CACFP LIVE

Texas Education Service Center's Live • Interactive • Virtual • Environment

OCT  
14

REGISTER

## Start Today! Preparing for the Administrative Review

When Contracting Entities (CEs) receive an Engagement Letter from the Texas Department of Agriculture (TDA) for an Administrative Review (AR), a Document Request Packet (DRP) is attached. In the DRP, there are lists of Program documents that must be available for review; many will need to be uploaded in TX-UNPS for a desk review that will take place prior to the scheduled review date. In order to improve Program compliance and efficiency, participants will look at the historical requirements of the DRP in order to map out an ongoing and up-to-date digital storage plan for potentially required documents. In addition, participants will diagram and list the steps necessary to upload DRP documents in TX-UNPS.

## CACFP in Adult Day Care Centers

Participants will practice identifying required elements for enrollment, Meal Production Records, and allowable costs. In addition, participants will evaluate scenarios in order to identify the ones that demonstrate the proper use of Offer-Versus-Serve Meal Service.

NOV  
11

REGISTER

## Income and Expenses in the DRP, Part I

Participants will practice identifying required documentation necessary in order to track income and expenses in a nonprofit food program account separately. In addition, participants will evaluate scenarios and identify the ones that demonstrate that enough allowable food was purchased in order to support the claims made.

DEC  
9

REGISTER

**Schedule:**

**2nd Wednesday of the Month  
10:30AM - 12PM**



**Center  
for  
Teaching and  
Learning**

**November 4, 2020**

**Lisa White - Director**

# Review and Support Updates

- Cyclical Monitoring Schedule for Cycles 3-6 have been released and can be found on the TEA webpage  
<https://tea.texas.gov/academics/special-student-populations/review-and-support/differentiated-monitoring-and-support-dms>
- ALL districts PL1-4 are required to submit a DCSI into ASCEND by December 1, 2020
- Self-Assessment will be released in January 2021 for all LEA's to complete by April/May 2021
- SPED Self-Assessment Overview webinar- December 16, 2020

# Differentiated Monitoring and Support Cyclical Monitoring Schedule for Special Education

<https://tea.texas.gov/academics/special-student-populations/review-and-support/differentiated-monitoring-and-support-dms>

## Region 14

Cycle 1 Reviews 2019-2020	Cycle 2 Reviews 2020-2021	Cycle 3 Reviews 2021-2022
<b>Group 1 (Oct.-Dec.)</b>	<b>Group 1 (Oct.-Dec.)</b>	<b>Group 1 (Oct.-Dec.)</b>
NA	Roscoe Collegiate ISD	Breckenridge ISD
<b>Group 2 (Jan.-Mar.)</b>	Texas College Prep. Academies	Gorman ISD
Albany ISD	<b>Group 2 (Jan.-Mar.)</b>	<b>Group 2 (Jan.Mar.)</b>
Cisco ISD	Colorado ISD	Cross Plains ISD
Eastland ISD	Loraine ISD	Hawley ISD
<b>Group 3 (Apr.-June)</b>	<b>Group 3 (Apr. June)</b>	Westbrook ISD
Baird ISD	NA	Comanche ISD
Clyde CISD		<b>Group 3 (Apr.-June)</b>
Stamford ISD		Aspermont ISD
		Sidney ISD
Cycle 4 Reviews 2022-2023	Cycle 5 Reviews 2023-2024	Cycle 6 Reviews 2024-2025
<b>Group 1 (Oct.-Dec.)</b>	<b>Group 1 (Oct.-Dec.)</b>	<b>Group 1 (Oct.-Dec.)</b>
Eula ISD	Anson ISD	Rule ISD
Merkel ISD	Blackwell CISD	Paint Creek ISD
Jim Ned CISD	Hermleigh ISD	De Leon ISD
<b>Group 2 (Jan.-Mar.)</b>	Rotan ISD	<b>Group 2 (Jan.Mar.)</b>
Haskell CISD	<b>Group 2 (Jan.-Mar.)</b>	Lueders-Avoca ISD
Trent ISD	Ira ISD	Roby ISD
Hamlin ISD	Wylie ISD	<b>Group 3 (Apr.-June)</b>
<b>Group 3 (Apr.-June)</b>	Highland ISD	Ranger ISD
Sweetwater ISD	Moran ISD	Gustine ISD
	<b>Group 3 (Apr.-June)</b>	Rising Star ISD
	Abilene ISD	
	Snyder ISD	



# Dyslexia Monitoring

--NEW--

- SB2075 - Relating to public school compliance with dyslexia screening, reading instrument requirements, and parent notification
- Will follow the Special Education Cyclical Monitoring schedule
- Will begin with Cycle 2 Group 2 in January 2020
- Dyslexia Monitoring Overview for LEA's was recorded and will be posted on TEA website <https://tea.texas.gov/academics/special-student-populations/review-and-support/review-and-support-resources>
- Questions? Sharon Anglin- [sanglin@esc14.net](mailto:sanglin@esc14.net)  
325-675-7032

# Special Education RDA Requirements



## 2020-21 Results Driven Accountability Intervention Requirements

### Special Education (SPED)

Determination Level (DL)	Establish a DCSI and DLT	Engage in Continuous Improvement	Submit Strategic Support Plan (SSP) to the Texas Education Agency
<b>Determination Level 1</b> Meets Requirement	YES	YES	NO
<b>Determination Level 2</b> Needs Assistance	YES	YES	YES
<b>Determination Level 3</b> Needs Intervention	YES	YES	YES
<b>Determination Level 4</b> Needs Substantial Intervention	YES	YES	YES

- **ALL LEA'S** must complete and submit a Self- Assessment. (Opens January 2021 in ASCEND)
- Determination Levels 2-4 will participate in regularly scheduled support conferences with TEA.
- Determination Levels 3-4 will include Targeted Desk Reviews and possible On-Site Reviews.
- Strategic Support Plan (SSP) Webinar recording- <https://www.youtube.com/watch?v=GjFyaMFo1xc&feature=youtu.be>
- SSP's due December 18th

# Remote Instruction Reminders

## New Guidance on Remote Instruction Needs for Special Education/504 Students

<https://tea.texas.gov/sites/default/files/covid/SY-20-21-SPED-FAQ.pdf> (page 2)

- 6. If my school system chooses not to offer remote instruction to the general student population, how should my school system address COVID-19-related remote instruction needs for a special education student or a student subject to Section 504? *NEW October 15, 2020***

NEW  
10/15/2020

If a district chooses not to offer remote instruction to its students generally, it does not have to do so for an individual student, such as a special education student, unless, after a request by the parent/guardian or another member of the special education student's admission, review and dismissal (ARD) committee, the committee determines as part of the student's individualized education program (IEP) that remote instruction is required to receive a free and appropriate public education (FAPE). The same general considerations would apply to a student receiving accommodations under Section 504. (Please see the Remote Attendance Requirements section of the SY 20-21 Attendance and Enrollment FAQ on the TEA COVID-19 Support and Guidance site for more information on providing remote instruction for students generally.)

<https://tea.texas.gov/sites/default/files/covid/SY-2020-21-Attendance-and-Enrollment.pdf> (page 17 question 19)

- 19. Is my school system required to offer remote instruction? *NEW October 15, 2020***

NEW  
10/15/2020

No, school systems are not required to offer remote instruction to the general student population. Please note, however, that remote instruction may be required for individual students, if a particular student's individualized education program (IEP) or Americans with Disabilities Act accommodation requires remote instruction. (For more information about considerations for students receiving special services, please see the SY 20-21 Special Education

17

tea.texas.gov



FAQ on the [TEA COVID-19 Support and Guidance site](#).) Providing remote instruction to the general student population is a local decision and one that can be modified by the LEA during the school year. As indicated in the guidance provided within this FAQ, any parent may request that their student be offered virtual instruction from any school system that offers such instruction. However, this does not mean that school systems are required to provide remote instruction throughout the school year. If a parent requests virtual instruction and the school does not offer it, the **parent may enroll in another school system** that does offer it for transfer students.

- 20. Are there specific requirements LEAs must follow to discontinue providing remote instruction as an instructional model? *NEW October 15, 2020***

NEW  
10/15/2020

Yes. If an LEA decides to discontinue providing remote instruction, they must give a 14-day notice to parents and notify parents of the option to transfer to another district for remote instruction. Those school systems that have discontinued remote instruction prior to the date of this clarification, even if remote instruction were discontinued without adequate advance notice, must still ensure parents are aware of their options to continue remote instruction by transferring to another school system.

# Supplemental Special Education Services

<https://tea.texas.gov/academics/special-student-populations/special-education/supplemental-special-education-services-ses>



Search

[A - Z Index](#) [Contact](#) [Employment](#) [Sign Up for Updates](#) [TEA Correspondence](#)



About TEA



Texas Schools



Academics



Finance & Grants



Reports & Data



Student Assessment



Texas Educators

[Home](#) / [Academics](#) / [Special Student Populations](#) / [Special Education](#)

## Supplemental Special Education Services (SSES)



### About Supplemental Special Education Services

Supplemental Special Education Services (SSES) are on-line accounts made available to eligible parents of students with disabilities that have been impacted by COVID-19 school closures. Families of students with eligible disabilities can use the on-line accounts to obtain goods and services up to a specific dollar amount that supplement what otherwise happens in school to help their child make more educational progress.

Families of students with eligible disabilities can use the on-line accounts to obtain goods and services up to a specific dollar amount that supplement what otherwise happens in school to help their child make more educational progress.



FAQ

Frequently Asked Questions



FAQ

Preguntas Frecuentes



How the Accounts Work

Information and Resources about how SSES accounts work. Coming Soon



## ESC 14 Special Education Liaisons

**Liaisons will support you with the required LEA activities in the DMS process.**

### **How can ESC Liaisons support you?**

Assist Local Education Agencies in developing multidisciplinary teams to help ensure a broad representation reflective of the LEA size and demographic.

Assist Local Education Agencies with annual completion of the Self-Assessment, including familiarization with the TEA developed rubric, drafting justification statements, and accessing the Ascend Platform.

Assist Local Education Agencies with the development of their Strategic Support Plan (SSP) as part of the Texas commitment to continuous improvement that focuses on improving outcomes for students with disabilities.

Assist Local Education Agencies in gathering necessary student documentation and preparing for desk reviews and on-site reviews.

Participate alongside the Local Education Agency in phone calls and on-site visits with TEA.

Connect districts with resources and specialists to support ongoing continuous improvement.

### **Contacts:**

Cody Martin,  
[cmartin@esc14.net](mailto:cmartin@esc14.net)  
325-675-8653

Patty Garcia,  
[pgarcia@esc14.net](mailto:pgarcia@esc14.net)  
325-675-7022



**LIAISONS RECEIVE DIRECT AND ONGOING TRAINING FROM TEA  
REVIEW AND SUPPORT TEAM REGARDING THE LEA  
ACTIVITIES WITHIN DIFFERENTIATED MONITORING AND SUPPORT.**

**WEDNESDAY, DECEMBER 2  
9:00 A.M.- 12:00 P.M.**

Face-to-Face and Distance Learning options!



# CAUTION!

SECONDARY BRAINS  
UNDER CONSTRUCTION

Join a group of educators across the state as we learn strategies, specifically for secondary students, to work within our already busy schedule that focuses and promotes healthy relationships between peers, a willingness to learn, and an increase in self-control!

Click [HERE](#) to register

Contact: Angi Thomas  
[athomas@esc14.net](mailto:athomas@esc14.net) or (325) 675-8676



# 34th Annual Gathering of Professionals

## The Neuropsychology of Trauma-Informed Schools

with Dr. Elaine Fletcher-Janzen

Wednesday, December 9th  
8:30am-3:30pm  
Shelhamer (South Campus)

\$25 fee due at registration - Lunch included

- See PTTStop for more information - Join in-person or via zoom -

Register by 12/2 - Session #109055



# Autism Extravaganza

## March 1, 2021

### Guest speaker:

# PAULA KLUTH

Save  
the  
Date

9am - 3:30pm  
Beltway Park Church North Campus  
Registration open in January @ [www.esc14.net](http://www.esc14.net)



follow the R14Autism  
FB page for updates

