Educational Technology Monthly Call

November 10, 2022

https://bit.ly/EdTech-Nov2022

Agenda

- Digital Learning Updates
- Cybersecurity
- Emergency Connectivity Fund, E-Rate, and ACP
- Important Reminders and Other Information

Suggested participants for this call:

- Chief Technology Officers
- Information Technology Staff
- E-Rate Coordinators
- Privacy Coordinators
- Digital or Virtual Learning Staff

Digital Learning Updates

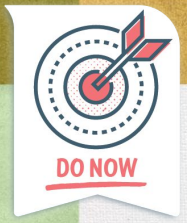
Statewide Zearn Access for Louisiana Schools K-8

The Department has partnered with Zearn to provide **Zearn School Accounts** to all public schools serving grades K-8. This opportunity will support systems' efforts to accelerate math learning and will include the following:

- **high-quality, evidence-based resources**
- **aligned professional learning**

Key actions

- Plan for implementation to begin in January.



SPED Camera Policy Submission

R.S. 17:1948 requires school systems to submit their approved policy for the installation and operation of cameras in certain classrooms to the Department by December 31 or within 60 days of receipt of funding. Since funding has been released to school systems, the Department released a submission form for LEAs to submit their policy by November 30.

Please contact specialeducation@la.gov with questions.

2022 SETDA

- The U.S. Office of Educational Technology (OET) is partnering with the State EdTech Directors Association (SETDA) to revise the National Educational Technology Plan
- OET is also focusing on the Digital Equity Education Roundtables (DEER) Initiative which provides information on closing the digital divide.

Additional 2022 SETDA Resources:

- SETDA Cybersecurity Frameworks: What K-12 Leaders Need to Know
- CoSN + SEDTA Cybersecurity Staffing Resource for K-12

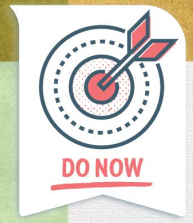
2022 National Summit on K-12 School Safety

- The National Summit on K-12 School Safety and Security was hosted by the Cybersecurity and Infrastructure Security Agency (CISA) in November. It brought federal, state, and local school leaders together to share actionable recommendations that enhance safe and supportive learning environments in kindergarten through grade 12 (K-12) schools.
- Areas of focus at the summit were: Cybersecurity, Physical Security, Emergency Planning, Capacity Building, Targeted Violence, Reporting Systems, Threat Assessment, Violence Prevention, and Online Safety.
- The 2022 National Summit on K-12 School Safety and Security Toolkit was released to support schools and school systems.

friEDTech Free Cyber Security Course for Teachers and Staff

friEDTech is currently offering their friEDTech's online cyber security course for teachers for free

Feel free to share this with teachers, staff, or any of your stakeholders who you think would benefit from this.



Reminder: Technology Contacts

- To ensure continuous and effective communication, Educational Technology is requesting updated contact information for Education Technology leaders and IT leaders for school systems.
- Submit this form to update contact information.

Contact digitallearning@la.gov with questions.

Last Reminder: Technology Readiness Tool (TRT) Data Collection

- TRT Device template is available on the Educational Technology Leaders website.
- Network and Staff Data sheet will be uploaded next week.
- Please note there is a question about a school system wide LMS.
- Device Data Sheet and Network and Staff Data sheets should be submitted by October 28th.
- Please email digitallearning@la.gov if you would like support with creating a survey regarding student home Internet access.
- Please include your school system in the file name of your submission.

Contact digitallearning@la.gov with questions.

Cybersecurity

Cyber Advisories & Alerts

Below are the Cyber Advisories and Alerts released by MS-ISAC for September/October 2022. The latest advisories and alerts are also available on the Center for Insernet Security (CIS) website here.

Alerts:

- AA22-279A : #StopRansomware: Daixin Team

Advisories:

- MS-ISAC Advisory # 2022-131: Multiple Vulnerabilities in VMware Workspace ONE Assist Could Allow for Privilege Escalation
- MS-ISAC Advisory # 2022-130: Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution
- **MS-ISAC Advisory # 2022-129**: Critical Patches Issued for Microsoft Products, November 8, 2022
  - ***Six zero-day vulnerabilities addressed in this advisory were reported by Microsoft as currently being exploited in the wild.***
    - *CVE-2022-41128 (Windows Scripting Languages Remote Code Execution)*
    - *CVE-2022-41091 (Windows Mark of the Web Security Feature Bypass Vulnerability)*
    - *CVE-2022-41073 (Windows Print Spooler Elevation of Privilege Vulnerability)*
    - *CVE-2022-41125 (Windows CNG Key Isolation Service Elevation of Privilege Vulnerability)*
    - *CVE-2022-41040 (Microsoft Exchange Server Elevation of Privilege)*
    - *CVE-2022-41082 (Microsoft Exchange Server Remote Code Execution Vulnerability)*

Cyber Advisories & Alerts

Advisories:

- MS-ISAC Advisory # 2022-128: Multiple Vulnerabilities in Google Android OS Could Allow for Privilege Escalation
- **MS-ISAC Advisory # 2022-127**: Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution
  - ***Apple is aware of a report of CVE-2022-42827 being actively exploded in the wild.***
- MS-ISAC Advisory # 2022-126: Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-125: Multiple Vulnerabilities in Mozilla Firefox and Firefox ESR Could Allow for Arbitrary Code Execution
- MS-ISAC Advisory # 2022-124: Oracle Quarterly Critical Patches Issued October 19, 2022
- MS-ISAC Advisory # 2022-123: Vulnerabilities in Aruba EdgeConnect Enterprise Orchestrator Could Allow Remote Code Execution

Cyber Security Best Practices & Mitigations

The FBI, CISA, and the MS-ISAC recommend organizations implement the following to protect against ransomware and other related malicious activities.

Preparing for Cyber Incidents

- Maintain offline backups of data, and regularly maintain backup and restoration. By instituting this practice, the organization ensures they will not be severely interrupted, and/or only have irretrievable data.
- Ensure all backup data is encrypted, immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure. Ensure your backup data is not already infected.
- Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
- Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Document and monitor external remote connections. Organizations should document approved solutions for remote management and maintenance, and immediately investigate if an unapproved solution is installed on a workstation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).

Cyber Security Best Practices & Mitigations

Identity and Access Management

- Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to comply with National Institute of Standards and Technology (NIST) standards for developing and managing password policies.
- Require multi factor authentication for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- Review domain controllers, servers, workstations, and active directories for new and/or unrecognized accounts.
- Audit user accounts with administrative privileges and configure access controls according to the principle of least privilege
- Implement time-based access for accounts set at the admin level and higher.

Cyber Security Best Practices & Mitigations

Protective Controls and Architecture

- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool. To aid in detecting the ransomware, implement a tool that logs and reports all network traffic, including lateral movement activity on a network. Endpoint detection and response (EDR) tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Install, regularly update, and enable real time detection for antivirus software on all hosts.
- Secure and closely monitor remote desktop protocol (RDP) use. Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. If RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a VPN, virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.

Cyber Security Best Practices & Mitigations

Vulnerability and Configuration Management

- Keep all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Organizations should prioritize patching of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog.
- Disable unused ports.
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.
- Disable command-line and scripting activities and permissions. Privilege escalation and lateral movement often depend on software utilities running from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally.
- Ensure devices are properly configured and that security features are enabled.
- Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
- Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.

E-Rate,
Affordable Connectivity Program
and
Emergency Connectivity Fund

E-Rate Entity Validation for 2023-24 Applications

Late November we will be sending out validation emails for preparing the State's Valid file for USAC. If you have not complete out updated District Contact Form, please do that now so that we are sure to send this information to the correct E-Rate contact in your LEA. **The Contact Form can be found here**.

This validation will include your student counts, Individual CEP percentages, group CEP percentages, NSLP numbers and ED numbers by school.

New ECF Functionality: COMADs and RIDFs

USAC will be adding ECF system functionality later this year to be able to issue Commitment Adjustments (“COMADs”) and Recoveries of Improperly Disbursed Funds (“RIDFs”). It appears that this functionality is being added to take a closer look at the actual use of internet services and devices as they were approved, or have been invoiced. To support this, applicants should note 2 specific Q&As included in USAC’s Emergency Connectivity Fund Program Newsletter for October 2022.

New ECF Functionality: COMADs and RIDFs

Q: If a service provider discovers that funded equipment and/or services are not being used, should they automatically allocate those costs from their requests for reimbursement and bill the applicant directly for this non-usage?

A: If a service provider determines that there is non-usage, we strongly encourage them to notify the school or library and provide a reasonable period of time (e.g., 30 days) to allow the school or library to reach out to the student, school staff member, or library patron to determine if the service is no longer needed. The ECF Program rules do not require the applicant and/or service provider to immediately remove the equipment/services provided to the student, school staff member, or library patron from their ECF requests for reimbursement, but do require that they take reasonable actions to monitor and track usage, which includes providing the school or library notice and time to first address the non-usage issue.

New ECF Functionality: COMADs and RIDFs

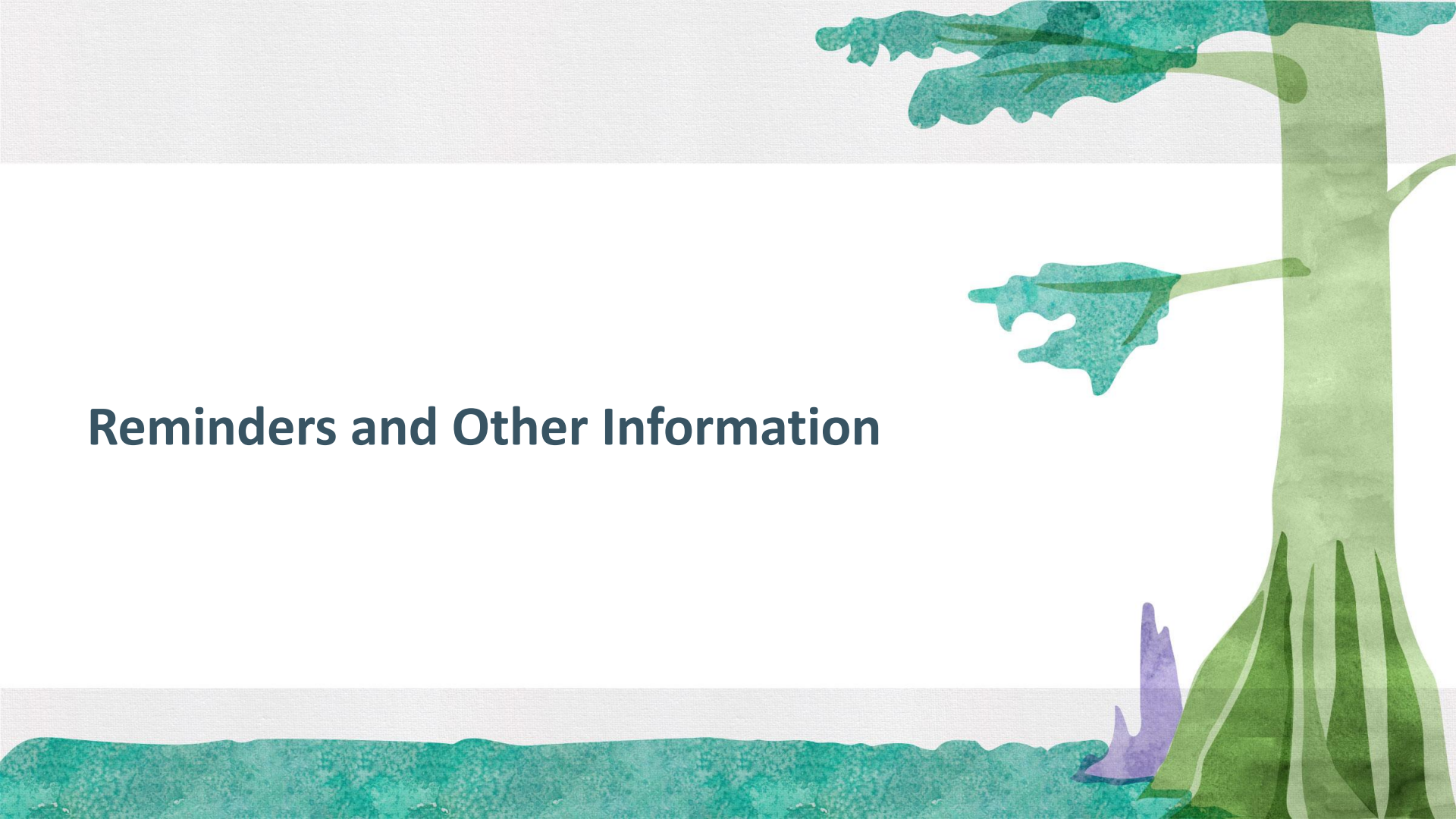
Q: Once a funding commitment decision letter has been issued, are there any additional steps that service providers using SPI invoicing should take before starting the services and/or submitting requests for reimbursement?

A: Given that only best estimates of the unmet needs were required at the application stage, service providers are reminded to work with the applicant once the funds have been committed to ensure that they are only seeking reimbursement for the actual number of students and school staff with unmet needs. While there is no requirement in the ECF Program to confirm the start of services before invoicing (like on the FCC Form 486 in the E-Rate program, for example), service providers and applicants should work together to ensure they are not requesting reimbursement for equipment and/or services that are not needed or not being used. We remind applicants and service providers that requesting extra equipment to account for anticipated damage or loss, or for warehousing, is not allowed under ECF Program rules. We also remind applicants and service providers of the one connected device and one hotspot device per student, school staff member, or library patron limit. Applicants and service providers will be responsible for returning funds if it is determined that they are not compliant with ECF Program rules.

E-Rate Important Dates and Reminders

- Upcoming Form 486 Deadlines
  - Nov. 11 - Wave 13
  - Nov. 18 - Wave 14
  - Nov. 25 - Wave 15

Reminders and Other Information



2022-2023 Education Technology Webinar and Office Hours

Slides from each meeting will be posted on the Educational Technology Leaders website. Recordings are available on request. A complete calendar of LDOE events can be found on the Louisiana Believes website.

Monthly Call Dates

November 10, 2022
December 8, 2022
January 12, 2023
February 9, 2023
March 9, 2023
April 13, 2023
May 11, 2023
June - Meet at LaCUE TLS
July - No Call

Time:	9:00 AM - 10:00 AM
Webinar Link	https://ldoe.zoom.us/j/575223228?pwd=NDNlN01SS3c0Rk4wV25aNkZhTEc2Zz09
Phone Number	1-301-715-8592
Meeting ID	Meeting ID: 575 223 228 Password: 2020-202!

Office Hours Dates

Nov - No office hours
Dec - No office hours
January 26, 2023
February 23, 2023
March 23, 2023
April 27, 2023
May - No office hours
June - Meet at LaCUE TLS
July - No office hours

Thank you for joining today's call.

Schedules, access links, and information for the Department's webinars can be found in the LDOE Weekly Newsletter and LDOE School System Support Calendar.

Helpful Links

- A+PEL PD for Educators
- LACUE
- Louisiana Believes Homepage
- School Improvement Library

Support Toolboxes

- Teacher
- System
- Principal
- Counselor
- Education Technology Staff

DEPARTMENT of EDUCATION
Louisiana Believes