



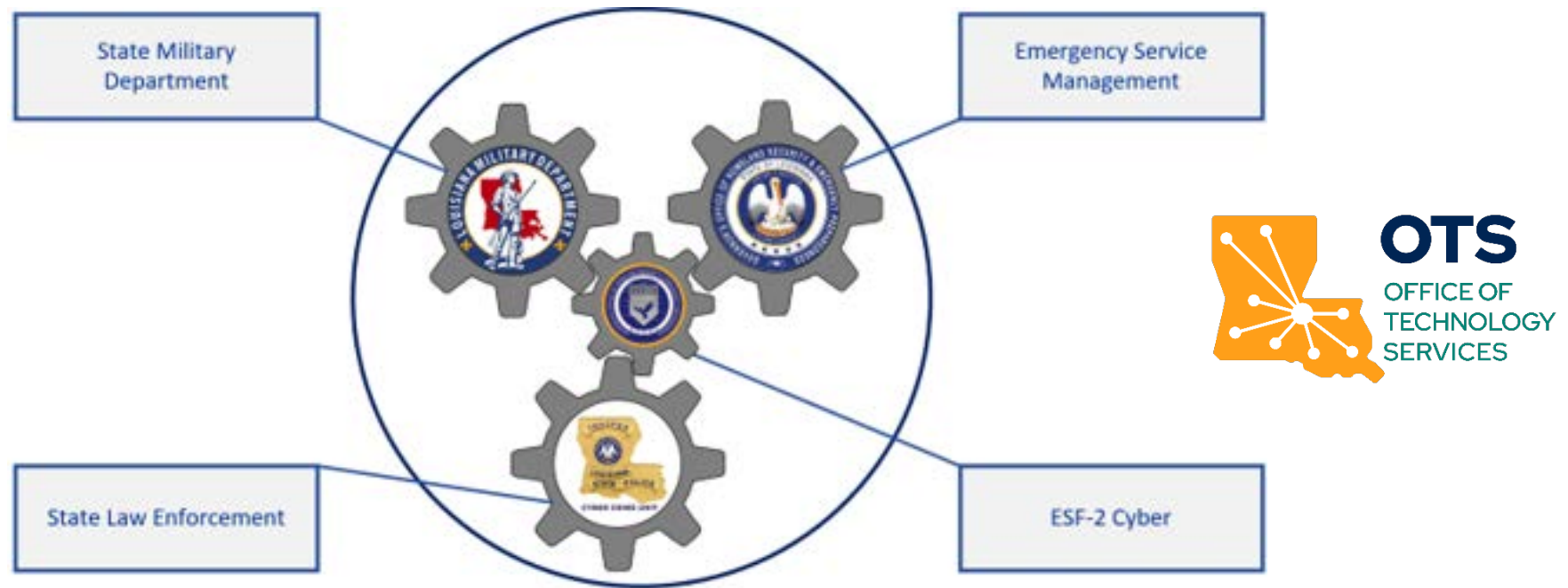
# GOHSEP ESF-2 Cyber

## Cyber and Emerging Threats (CET)



# WHO?

- ESF- 2 Cyber is a multi-agency collaboration of Louisiana's previous cybersecurity investments



## What?

- Office of Cyber Readiness (OCR)
- Cyber Threat Analysis Center (CTAC)
  - ▶ Security Operations Center
  - ▶ Intelligence Section
- Incident Response Team (IRT)

## Why?

Mission: Protect Critical Infrastructure and Key Resources (CIKR)



April 2, 2025



# Education (K-12) Cyber Intel

## CTAC K-12 Cyber Threat Brief 10.07.26

K–12 school systems remain attractive targets because cyber incidents can simultaneously disrupt instruction, payroll, student services, transportation, communications, and physical-safety operations. Recent events highlight two major concerns: ransomware or network intrusions that force districts offline, and third-party education vendors whose compromise can expose student, staff, or health information across multiple districts. Schools should confirm whether they use the affected Frontline products, review vendor notifications, require multifactor authentication for privileged and vendor accounts, and maintain offline procedures for attendance, medical information, parent communications, and payroll. Districts should also coordinate cyber incident plans with law enforcement and emergency personnel because swatting and cyber disruptions can quickly become physical-safety events.

### **Executive Summary**

Louisiana school systems should focus on operational continuity as well as data protection. Districts should know how they will take attendance, reach parents, access medical information, pay employees, and operate safely when core networks or cloud platforms are unavailable.

**CTAC ASSESSMENT:** The most immediate risk is not limited to one product or attack group. Schools face concentrated exposure through shared vendors, privileged accounts, internet-facing services, and operational dependence on a small number of interconnected platforms.



# Cyber Threat Analysis Center

## Security Operations Center

- ▶ No cost Managed Detection and Response (MDR) services through Security Operations Center (SOC) services
- ▶ Ramping up efforts to protect CIKR by serving as a central hub for threat intelligence analysis, network monitoring, and response across the state.
- ▶ Monitors and identifies emerging cyber threats, tracks trends, and transforms threat intelligence into actionable insights



## Office of Cyber Readiness

- Offer a no-cost service that provides agencies with a comprehensive cyber hygiene assessment
- Using a suite of advanced tools, OCR conducts an assessment on the external attack surface as well as an internal “Domain Health Check” (assessing an entity’s AD environment compared to Microsoft best practices).
- The initiative is designed to help organizations better understand their exposure to cyber threats and take proactive steps to safeguard sensitive data and digital infrastructure.

## Incident Response Team

- A rapid deployment unit specifically designed to assist public and private CIKR agencies that have been compromised by cyber threats, ensuring swift and effective recovery
- The priority is to support agencies in crisis and get them back online safely in a secure posture
- Every agency/organization needs to prepare for a cyber incident by having a Cyber Incident Management Response Plan (CIMRP) – templates available

## Enduring Support

- **Support & Escalation Procedures**
- **Standard Support (Mon–Fri, 0700–1730):** Submit a ticket for all planned system changes and normal requests.
- **After-Hours Support:** Submit a ticket, then send an alert via the SIGNAL chat/text app.
- **Critical Emergencies (Systems Down):** Call the ESF2 Cyber after-hours line directly for a response within 15 minutes to 2 hours.
- **Escalation:** Contact ESF2 Cyber leadership if you do not receive a timely response.



# Future Projects and Initiatives

- **Email Subscription Service – Coming Soon**
  - Threat Intelligence
  - LCAP updates
  - Alerts and Bulletins
  - Grants and Compliance
- **Information Security Training – Coming Soon**
  - Cyber Security Training available to your staffs
  - Assign a training coordinator for your agency and sign up your team members
- **Workshops – Coming Soon**
  - In person training for specific topics
  - Example: Incident Response Playbook

## How?

- For more information and to request LCAP services, please scan the QR Code, or click on the following link,  
<https://forms.office.com/g/YzD8n1xjEq>
- Please report all cyber incidents to the Louisiana State Analytical and Fusion Exchange at 1-800-434-8007
- Visit <https://getagameplan.org/make-a-plan/cybersecurity-plan/>.





## Contacts

### **GOHSEP ESF-2 Cyber**

### **Cyber and Emerging Threats**

- **COL Stephen Durel – Director, Cybersecurity**
  - ▶ [Stephen.Durel@la.gov](mailto:Stephen.Durel@la.gov)
- **Darren Delrie – Services Manager**
  - ▶ [Darren.Delrie@la.gov](mailto:Darren.Delrie@la.gov)
- **Nick Cutrera – Operations Manager**
  - ▶ [Nick.Cutrera@la.gov](mailto:Nick.Cutrera@la.gov)
- **[ESF2.Cyber@la.gov](mailto:ESF2.Cyber@la.gov)**