ESF-2 Cyber/LCAP

Capabilities

Cyber Program Restructuring

- **Task:** The GOHSEP Director identified a need to restructure the State Cyber Program (SCP) into a clear, concise initiative that not only follows, but is also supported by federal/state statutory, regulatory and advisory requirements.

- **Purpose (Center of Gravity):** The intent is to use the National Response Framework (NRF) and Louisiana Disaster Act as the baseline to facilitate a cyber program that has the ability to prepare for, respond to, recover from, mitigate and then prevent future adverse cyber attacks in the State of Louisiana.

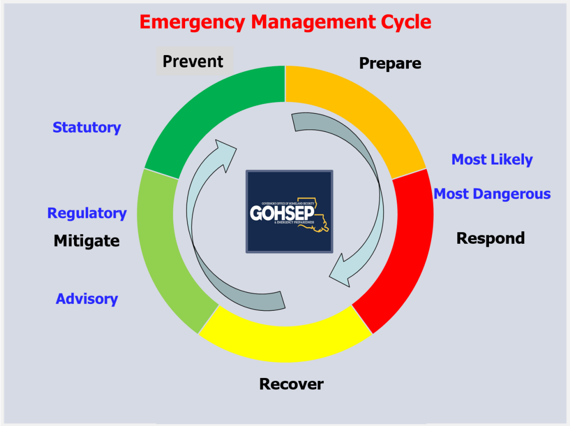
- **Issue:** Cyber attacks became prevalent in the past five years, forcing Louisiana to respond as a state with local and parish agencies also responding respectively. The need for a response facilitated the current status of the Cyber Program. The key issue is that the program never evolved to fully embrace the emergency management cycle and has remained in a response mode. From a operational standpoint the Cyber Team (comprised of LANG, OTS, LSP & GOHSEP) responded effectively; however, the executive leaders at GOHSEP never developed a strategic plan with a vision and mission that each agency could use with common statutory (legal), regulatory (policy) and advisory (SOPs) methods. The cyber tasking and methods varied depending upon the individual agency legal interpretations, policy guidelines and internal SOPs. There also was no standard method of After Action Reviews (AAR) or template used, creating a void in lessons learned.

- **Discussion:** The vision of GOHSEP is to serve as an extension of the Office of the Governor and provide sound leadership during crisis events while also enhancing the day-to-day state agency programs servicing Louisiana residents, businesses and organizations. The mission of GOHSEP is to utilize three priorities to save lives, protect property and maintain infrastructure. GOHSEP will use this vision and mission to do several things. First and most importantly, GOHSEP will correctly place the SCP in compliance with the NRF by aligning it under ESF-2 Cyber. Secondly, GOHSEP and OTS have agreed to a strategic partnership where the administrative, logistical and operational structure will now fall under the GOHSEP purview. GOHSEP has a relationship with all ESFs and is the primary agency in ESF-5 Emergency Management. As the concept develops, GOHSEP has adjusted the State Emergency Operations Plan (SEOP) to reflect the mission alignment, administrative, logistical and operational correctly and accurately. The GOHSEP Assistant Director - Security and Interoperability (AD-SI) will serve as the executive leader of the SCP. The AD-SI already has a similar statewide mission, as the Chair of the Statewide Interoperability Executive Committee. This program manages the Louisiana Wireless Information Network (LWIN). The program utilizes secure 700 mhz radio communications to facilitate 13Mil push to talk actions from over 122k radios in all 64 parishes every month. It should be noted that 70% of the 122k users are from local jurisdictions. First responder communications is one of the major success stories of how a program evolves and consistently saves lives, protect property and maintain infrastructure. GOHSEP will use the lessons learned in the SIEC & LWIN evolution and apply them to ESF-2 Cyber, which will grow and enhance state cyber capabilities.

Cyber Program Restructuring

- **Concept of Operation:** The Strategic Action Plan (SAP) is designed to talk concepts only and deliberately will not address specifics due to operational and security concerns in the cyber arena. The SEOP lists the ESF-2 Cyber Annex and is considered to be a regulatory document, meaning it is policy related. The SOPs will be held internal to agencies performing the cyber mission in each stage of the emergency management cycle. They are listed in order of mission receipt and mission priority:

• GOHSEP HQ: ESF-5 Emergency Management	Prepare, Respond, Recover, Mitigate, Prevent
• LANG J3-6: ESF-2 Cyber Co-Lead/Quick Reaction Force	Prepare, Respond, Recover
• GOHSEP SI: ESF-2 Cyber Co-Lead	Mitigate, Prevent, Prepare, Respond, Recover
• LSP: ESF-2 Cyber Co-Lead	Prepare, Respond, Recover
• OTS: ESF-2 Cyber State Agency Support	Respond, Recover (State Agencies Only)



- **Recommendation:** GOHSEP will utilize the statutory NRF & the Louisiana Disaster Act, the regulatory SIEC & LWIN lessons learned & SEOP ESF-2 Cyber Annex in conjunction with advisory internal SOPs to maximize federal and state funding in a comprehensive cyber program. In clear terms, the SCP will evolve into a proactive homeland security and emergency preparedness platform!

Incident Response 2019-Present

- Cyber Incident Response Services
  - Coordination of Identification and Classification of Incident in partnership with Louisiana State Police Cyber Crimes Unit
  - Incident Response Management
    - Containment
    - Eradication
    - Recovery & Remediation
- Agencies assisted 2019-Present
  - Total – 170+ public and private Critical Infrastructure and Key Resources (CIKR)

GOVERNOR'S OFFICE OF HOMELAND SECURITY
GOHSEP
& EMERGENCY PREPAREDNESS

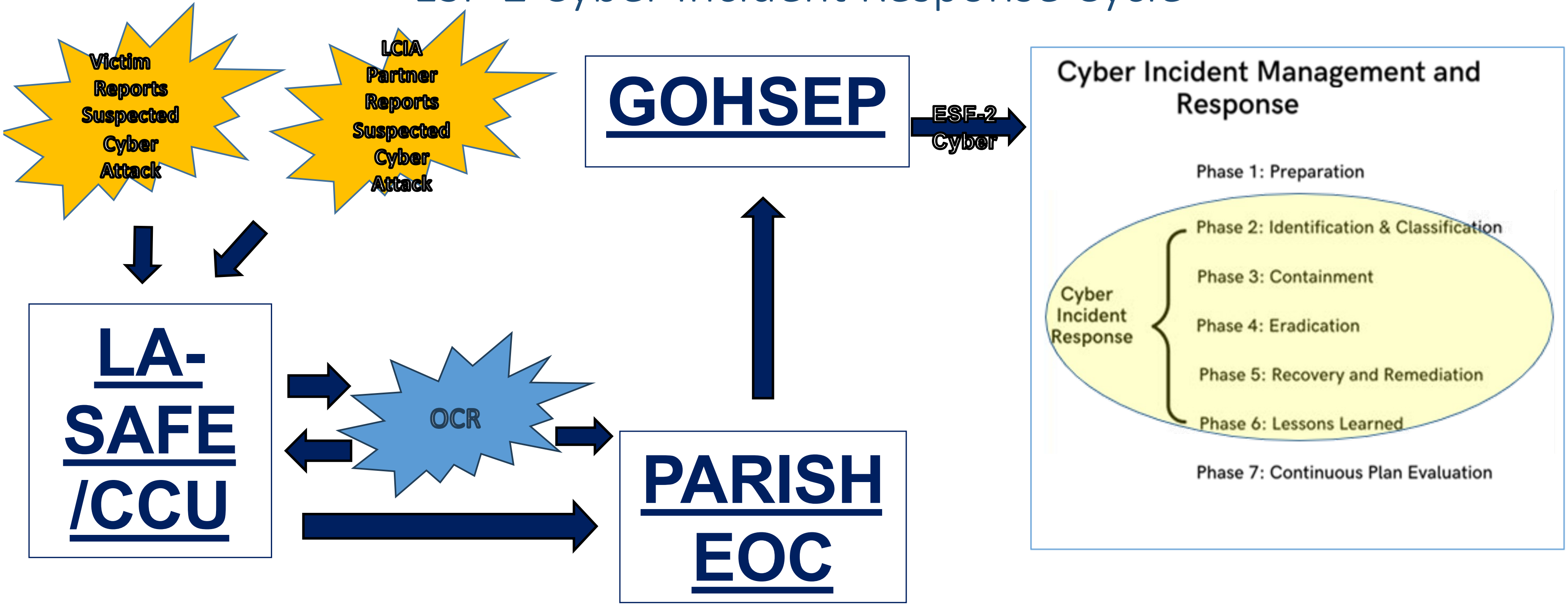
UNCLASSIFIED

INITIAL ATTACKS WERE TO LA PARISH SCHOOL BOARD SYSTEMS

LOUISIANA

PREVENT PREPARE RESPOND RECOVER MITIGATE

ESF-2 Cyber Incident Response Cycle



Victim Reports Suspected Cyber Attack

LCIA Partner Reports Suspected Cyber Attack

GOHSEP

ESF-2 Cyber

LA-SAFE /CCU

OCR

PARISH EOC

Cyber Incident Management and Response

Phase 1: Preparation

Cyber Incident Response

Phase 2: Identification & Classification

Phase 3: Containment

Phase 4: Eradication

Phase 5: Recovery and Remediation

Phase 6: Lessons Learned

Phase 7: Continuous Plan Evaluation

Contact Louisiana State Analytical and Fusion Exchange (LA-SAFE): **1-800-434-8007** LaFusion.Center@la.gov.

LA Cyber Assurance Program

- Cyber Assessment Program – Office of Cyber Readiness – LANG/LMD
  - No Cost vulnerability assessments for State and Local Agencies
  - Status: 78 - Assessed, 6 – In progress
  - Critical Vulnerabilities Identified to Date: 74
- Cyber Threat Analysis Center
  - 24/7 monitoring, analysis, and response to cybersecurity threats, events, and incidents for State and Local Agencies
  - Status: Evaluating tools to pilot with first 10 CIKR entities
- Deployment of Endpoint Detection and Response (EDR) Software
  - One year EDR software license at no cost to State and Local Agencies
  - Status: Deployed – 199 Entities w/108,000+ Endpoints
  - Malware Blocked Last 90 Days: 3,039

Training/Exercises/Outreach

- Completed - 6
  - Louisiana Board of Regents – 2
  - Louisiana Association of Computer Using Educators – 2
  - Louisiana Municipal Association – 1
  - Louisiana Supreme Court – 1
  - Entergy – 1
  - Louisiana Offshore Oil Port – 1

- Planning - ?
  - Louisiana Board of Regents - ?
- Perpetual -
  - GOHSEP UL Academy
    - Cybersecurity – 2
    - Artificial Intelligence – Planning
  - Cyber Awareness Month
    - October

GOHSEP Points of Contact

- LCAP@la.gov – Louisiana Cyber Assurance Program/ESF-2 Cyber general inquiries/Cyber Incident Management and Response Plans
- ctac.intel@esf2.la.gov – Cyber Threat Analysis Center STIX/TAXI and SOC services
- lmd-ocr-conf@esf2.la.gov – Office of Cyber Readiness Cyber Hygiene Assessments

GOVERNOR'S OFFICE OF HOMELAND SECURITY
GOHSEP
& EMERGENCY PREPAREDNESS
LOUISIANA
PREVENT
PREPARE
RESPOND
RECOVER
MITIGATE

Questions?