6 December 2018 Meeting Minutes
Louisiana Cybersecurity Commission

- Meeting commenced at 10:00 a.m. CST -

- Roll-call was taken and the following commissioners were in attendance:

  Co-Chair, Major General Glenn Curtis – Louisiana Army National Guard;
  Chairman Craig Spohn – Cyber Innovation Center
  William Bradley (retired), Century Link;
  Kevin Reeves, Superintendent of Louisiana State Police
  Mark Northrup, CLECO Utility Company
  Dickie Howze, Division of Administration
  Jeffrey Moulton, Stephenson Disaster Management Institute;
  Dr. Leslie Guice, President of Louisiana Tech University;
  Sonya Wiley – Emergency Operations Center Director, Rapides Parish
  Paul Rainwater
  Casey Tingle, Gov.'s Office of Homeland Security and Emergency Preparedness;
  Ramesh Kolluru, University of Louisiana at Lafayette (by Proxy);
  Michael Dunaway, University of Louisiana at Lafayette;
  Edward Flynn, Louisiana Chemical Association;
  Yenumula Reddy, Professor at Grambling State University;
  Kyle Ardoin, Louisiana Secretary of State (by Proxy);
  and
  Frances Gladden, Cox Communications.

- Hard copy materials were distributed to the commissioners and associate personnel in attendance. Electronic copies were previously emailed.

- Chairman Spohn gave introductory remarks.

- Dr. Hal Moore – Chief Technology Officer, NORAD USNORTHCOM J8 was introduced by Commissioner Moulton as a guest speaker.

  - Dr. Moore remarked about the war against cybercrimes and the sense of urgency. His department is attacked over 100 times a day, some with nation-state involvement.

- HUNT 101 – Hunt incident response team (HIRT)→ if there is a cyber-attack that exceeds the state's response capabilities, next group to call is HIRT with DHS. HIRT is part of the NCCIC and proactively hunts for malicious cyber activity in public and private sector organizations and critical infrastructure.

- There are steps to get assistance from HIRT:

    - Onsite activities take 7-21 days, so it is not a quick fix, will need to rely on back-up infrastructure.

- Dr. Moore discussed the attack on Colorado's Dept. of Transportation → this was a nation-state attack that attacked both CO Agencies and FBI, DHS, and other federal agencies.

    - Ransom-ware was placed on messaging and light control systems for the entire state. There was a request for assistance made by the state to NORTHCOM. NORTHCOM brought in Title 10 personnel from cyber command, which did not have the expertise required. Accordingly, CA guard members with expertise were brought on Title 10 orders to assist with the ransom-ware attack.

    - A cloud service provider was used by CDOT, but attached to the virtual server, which was open. The virtual server was created on Feb 18, but compromised on Feb 20, 2 days later. The attack was called "Sam sam." The issue was that the virtual server connection was unsecure even though the cloud was secure. CO was able to isolate their system to operate during recovery.

    - MG Curtis commented about arranging fly-away teams to bring requisite personnel to incident response sites under Title 32 and Title 10.

- COL Donnelly and Chairman Spohn introduced minutes from 13 September. There was Motion and a second to adopt minutes from previous meetings. The motion passed without opposition.

- MG Curtis:
    - Legislative Report Update from the Legislative Subcommittee by MAJ Anderson, who discussed the conditionally approved items from the Governor's office (namely LCC-001 and LCC-007).
    - General Curtis-are preparing sponsors for each of the bills.
- The Two Items for Conditional Approval were:
    - Cyber trespass Action 14:73.11
        - Proposed 3 solutions: 1) Could this be included in current trespass with significant revisions; 2) Could amend computer tampering legislation to include trespass; or 3) keep trespass a separate action.
- Concurrent resolution to develop non-financial incentives. This issue was resolved.
- Gen Curtis suggested taking these three options to the governor's office. Wanted to present this to commission for comments about these three options. Commission agreed to put forth the three options regarding cyber trespass to the Governor's office
- **Committee Reports were provided by the following Commissioners:**
- Commissioner Mark Northrup: Cyber risk, assets, and capabilities assessment: Need to understand the State's risk and assets and start from a foundational standpoint. Next recommendation is to foster collaboration in the state to help build the cyber strategy in the state.
    - Recommendations are split into four imperatives that were designed to grant greater authority to GOHSEP to launch statewide initiative for gathering information (both public and private) for cybersecurity information. Also want to launch a statewide initiative to develop a threat matrix of threat, vulnerabilities, and consequences; as well as initiative to partner and contribute (between private and public

sectors) in the ID and inventorying of current cyber capabilities of the 16 major critical infrastructure sectors.

- There was a discussion on how to mark and categorize levels of authority to access of classifications of sensitive information.

- Commissioner Flynn commented that it will be extremely important to have a well-developed operational plan to appeal to varying industries with different economic imperatives and critical assets.

- ESF 17 Report by Commissioner Moulton:

  - Top Recommendations:

    - Adopt an ESF 17 Annex into State Emergency Operations Plant.

      - Chairman Spohn asked if there is an inventory of cyber assets and personnel with expertise. The answer is there is not presently a catalog, but Dr. Dunaway explained that this is a process that will begin soon.

    - Define what is a state cyber incident → defined as "an incident that has been initiated by malicious cyber actor and has a direct impact or potential direct impact on the physical environment and/or results in a sustained economic disruption that includes a likely impact on the public health and welfare (Level 4 Cyber incident as defined by the National Cyber Incident Response Team) or imminent threat to loss of life.

    - Adopt a decision matrix and workflow matrix for deployment of cyber resources to assist requesting entities that experience a cyber incident.

    - Present a State Cyber Support Matrix for a Parish, Political Subdivision and Tribal Territories and a separate matrix for state cyber support to private sector entities

- Final recommendation is for a Tabletop Exercise → testing the annex and response
- MG Curtis asked for a vote to adopt ESF 17 Imperatives. Chairman Spohn wishes to have additional time to consider expanding to more than malicious cyber actors to ensure that a state cyber incident is more broadly defined.
- MAJ Anderson asked if there would be a reason the Governor would not want to issue a declaration of an emergency. Alberto Depuy commented there may be a concern with conflating a virtual versus a physical threat. Issue of adopting a definition of a state incident will be considered until next commission meeting.

- Information Sharing and Integration Committee by Dr. Kolluru's Proxy, Arun Lakhotia
  - Need to develop Threat Models for Pure Cyber Attack and Cyber Physical Attack
  - Significant Asset is LA_SAFE- Louisiana's Fusion Center, the Louisiana State Analytical and Fusion Exchange Center. Additional Assets:
    - Louisiana Guard
    - LANG's Cyber Protection Teams
    - Louisiana Business Emergency Operations (LABEOC)
    - Future Asset: Small Business Cybersecurity Operations Center
  - Recommendations:
    - Expand LA-SAFE- make this strong assets stronger
    - Create ISAOs and convince state partners to share information and adopted CISA into state legislation

- Dr. Guice for the Workforce Development, Education, and Public Outreach Key findings Outreach Committee
    - Focused on 3 goals to create 2 imperatives to mobilize public and private resources and transform, elevate and sustain the learning environment
    - Identified issues were the workforce gap, need to sustain educational efforts, but need to create lifelong educational and training and public awareness. This is a short term and a long term problem.
    - 4 recommendations for the committee:
        - Cybersecurity Educational Initiative with funding commitment from the state
        - Formation of regional alliance, which are in essence, already shaped up
        - Launch an effort to recruit cybersecurity workers from underutilized and underrepresented populations such as veterans
        - Strengthen k-12 school programs for cybersecurity curriculums
    - Suggests an Education Management Council to oversee imperatives that engages educational leaders. The LCC will also oversee the Education Management Council.
    - Regional Alliances will require a coordinated approach to uniting public and private partners in each region of the state. These will also require commitments from major universities
    - Requesting funding from the state for recruitment and retention of teachers and K-12 pathways. Will also need cyber infrastructure and staff. Need program development of summer camps and certifications.

- Suggestion by Chairman Spohn to define regions, potentially 5 regions. No opposition to committee imperatives

- Commissioner Dunaway for the Economic Development Committee:

  - Mission is to enhance cybersecurity in the private sector for a secure and resilient economic. Noted that cybersecurity is the "new normal" for business operations

  - Findings divided into two categories: 1) Develop a cybersecurity program with private entities and get them to help design it; and 2) develop programs to enhance cybersecurity awareness and capacity of individual businesses and organization. Want to establish a voluntary certification program on cybersecurity.

  - Top recommendations: 1) establish an enduring state-wide program for cybersecurity as a long-term investment strategy; 2) Important training and education in cybersecurity for business at the regional, local, and entity levels and be designed with input from the business community; and 3) Endorse or adopt the NIST cybersecurity framework and the Baldridge Cybersecurity Excellence Builder Program as a the foundation of a statewide program.

  - Recommendation to establish a state award for cybersecurity.

  - Chairman Spohn asked how we explain standard of NIST framework to the public --How do we educate the public?

- Scott Meyers – Proxy for Secretary Ardoin for the Election Security Committee:

  - 3 Priority Recommendations: 1) Work with clerks and registrars to get them to join the election ISACs and deploy assets from the ISAC such as sensors; 2) Perform a state-wide tabletop exercise to include all areas of state government and the private industry; and 3) conduct and analyze physical security assessments and improvements, especially at voting

machine warehouses and individual clerk offices. It is recommended to work with DHS.

- Law Enforcement Committee by Commissioner Reeves and Devin King:
  - Key Findings: 1) shortage of skilled personnel; 2) lack of logging standards, which creates a gap in intelligence. Need a single repository for information; and 3) lack of resources, training.

    Solutions: 1) institute of statewide network of security liaisons and regional teams that provide basic training to other personnel and incident response; and 2) expand cyber capabilities by acquiring more staff and technology with and through the fusion center and develop a state-wide a statewide digital forensics lab, as well as develop malware and cryptography analysis lab.

- Commission's Way Ahead by COL Donnelly → NGA has a national cyber submit that will occur in Shreveport from 14-16 May 2019
  - Dec 14, 2019 – NGA 2019 Summit Planning Conference Call
  - December 15, 2019 – EOY Commission Report submitted to the Governor
- MG Curtis committed that the executive summary of the LCC is close to completion and will be sent to the commissioners in the following week. MG Curtis and Chairman Spohn thanked everyone for their contributions to the commission and hope everyone can attend the NGA's National Cyber Summit.
- Meeting concluded at 12:26 p.m.