NATIONAL GOVERNORS ASSOCIATION

Addressing Energy Cybersecurity through State Cyber Governance Bodies

June 7, 2021

The call will begin shortly

NATIONAL GOVERNORS ASSOCIATION

Addressing Energy Cybersecurity through State Cyber Governance Bodies

June 7, 2021

Housekeeping

General:

- This call will be recorded.
- Slides and a recording will be distributed afterwards.
- Participants are muted upon entry.

Questions:

- Feel free to unmute yourself!
- Please submit questions into the chat box or question box
- “Raise your hand” and I will ask you to unmute
- Please chat or email mrogotzke@nga.org with any technical questions

Agenda

I. Energy Cybersecurity Governance Bodies Overview

- **Dan Lauf**, Energy Program Director, NGA

II. Louisiana Cybersecurity Commission

- **Dr. Ramesh Kolluru**, Commissioner, Louisiana Cybersecurity Commission & Vice President for Research, Innovation and Economic Development & Professor, School of Computing and Informatics, UL Lafayette

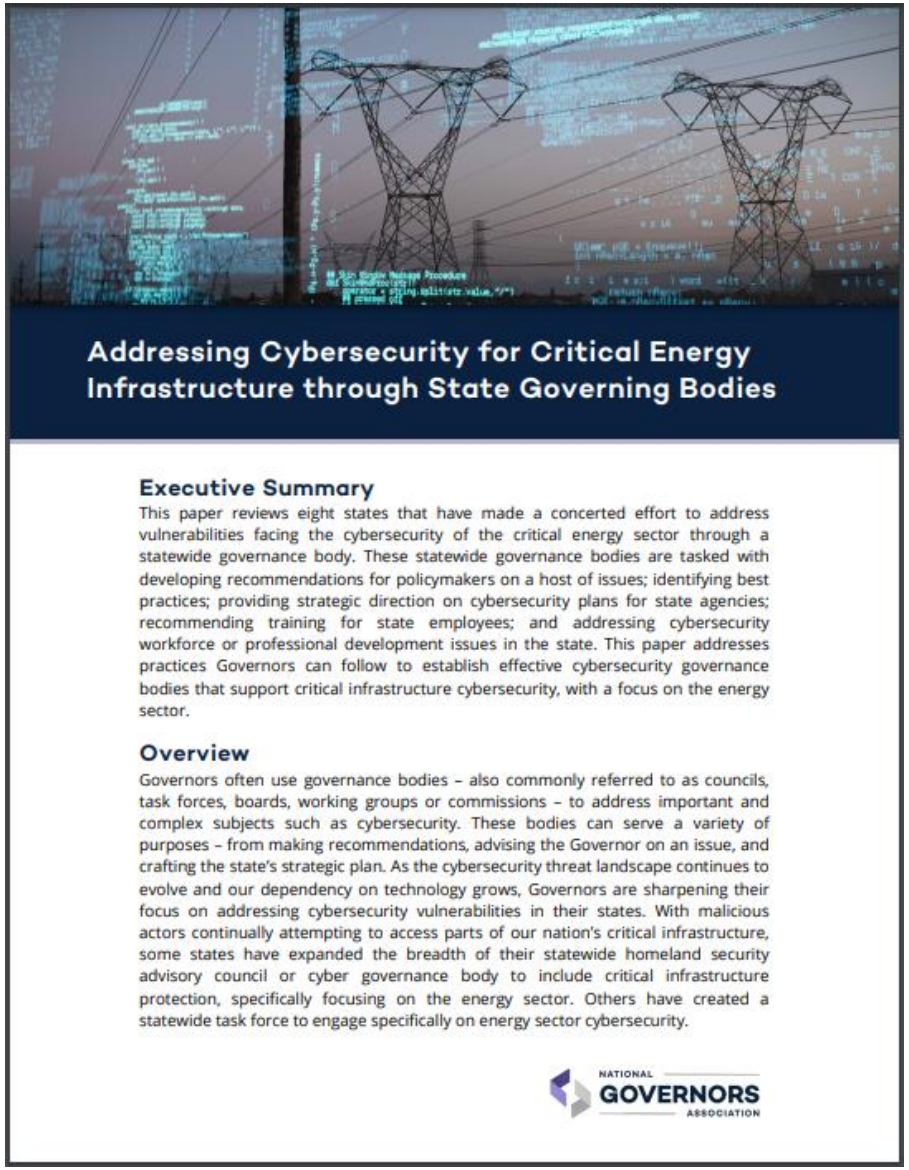
III. Indiana ECC Energy Committee

- **Bob Richhart**, Chief Technology Officer, Hoosier Energy and Co-chair of the Indiana Energy Committee
- **Danielle McGrath**, President, Indiana Energy Association

IV. Audience Q & A

NGA's Energy Cybersecurity Projects

- **On-Demand Technical Assistance**
  - Contact **Dan Lauf** (dlauf@nga.org) or **John Guerriero** (jguerriero@nga.org) with any requests
- **Energy Cybersecurity Information Sharing**
  - **Energy Sector Cybersecurity Partnerships and Information Sharing Whitepaper –** coming June 2021
- **Coordination, Messaging, and Incident Response**
  - **State Role in GridEx VI –** Pre-exercise coordination for November 2021 exercise
  - **Energy Cybersecurity Threat Briefings for States –** Process memo and pilots
  - **Ongoing Coordination with Energy Sectors –** Including with the ESCC, ONG-SCC, and EGCC
- **Energy Supply Chain Cybersecurity**
  - **Experts Roundtable on Securing the Distribution Grid and Supply Chain –** Dates to be announced
- **State Energy Cybersecurity Governance**
  - **Addressing Cybersecurity for Critical Energy Infrastructure through State Governing Bodies**



New Report:

Addressing Cybersecurity for critical Energy infrastructure through State Governing Bodies

Sponsored by U.S. DOE, Office of Cybersecurity, Energy Security, and Emergency Response

[Download the report here]

LOUISIANA CYBERSECURITY COMMISSION

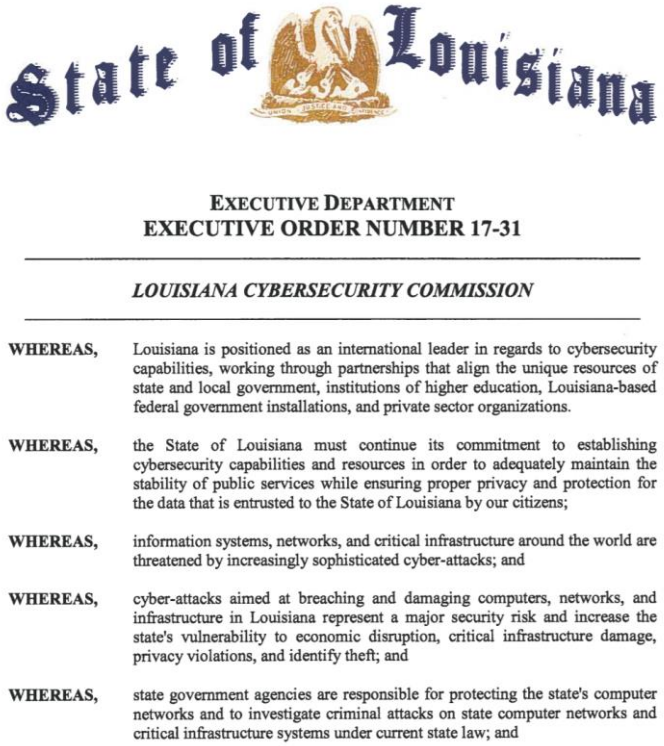
ADDRESSING ENERGY CYBERSECURITY THROUGH STATE CYBER GOVERNANCE BODIES

June 7, 2021

Ramesh Kolluru, Ph.D.

VP for Research, Innovation and Economic Development
Professor, School of Computing and Informatics
University of Louisiana at Lafayette

LOUISIANA CYBERSECURITY COMMISSION



State of Louisiana

EXECUTIVE DEPARTMENT
EXECUTIVE ORDER NUMBER 17-31

LOUISIANA CYBERSECURITY COMMISSION

WHEREAS, Louisiana is positioned as an international leader in regards to cybersecurity capabilities, working through partnerships that align the unique resources of state and local government, institutions of higher education, Louisiana-based federal government installations, and private sector organizations.

WHEREAS, the State of Louisiana must continue its commitment to establishing cybersecurity capabilities and resources in order to adequately maintain the stability of public services while ensuring proper privacy and protection for the data that is entrusted to the State of Louisiana by our citizens;

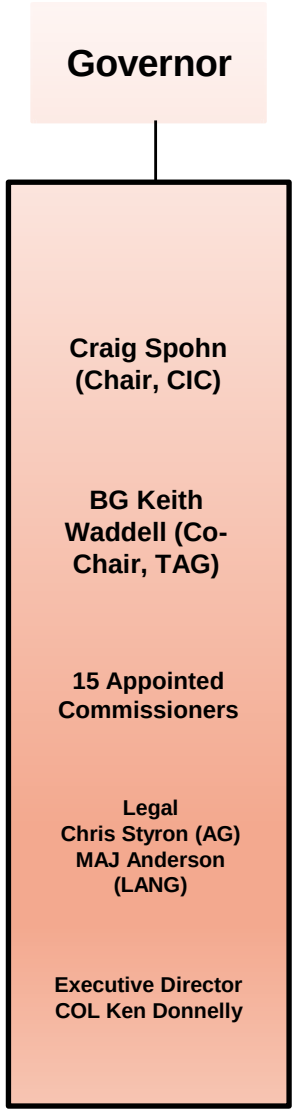
WHEREAS, information systems, networks, and critical infrastructure around the world are threatened by increasingly sophisticated cyber-attacks; and

WHEREAS, cyber-attacks aimed at breaching and damaging computers, networks, and infrastructure in Louisiana represent a major security risk and increase the state's vulnerability to economic disruption, critical infrastructure damage, privacy violations, and identify theft; and

WHEREAS, state government agencies are responsible for protecting the state's computer networks and to investigate criminal attacks on state computer networks and critical infrastructure systems under current state law; and

- Executive Order **JBE 17-31** Published on **December 7, 2017**
- Establishes a **15 person** Cyber Commission
- The goals of the Commission include, but are not limited to:
  1. Identify, prioritize, and mitigate Louisiana's cyber risk
  2. Promote cybersecurity awareness and recommend best practices for the security of all of Louisiana's cyber ecosystem
  3. Promote actions, including legislative, administrative, and regulatory, where appropriate, to enhance cybersecurity in Louisiana
  4. Grow Louisiana's cybersecurity workforce and educate the public/private sectors about cybersecurity
  5. Enhance Louisiana cyber emergency preparedness and response capabilities
  6. Monitor, understand, and share cyber threat information
  7. Build comprehensive digital forensics and cyber investigative capability
  8. Identify, prioritize, acquire, and establish funding mechanisms to enhance Louisiana's cybersecurity efforts
  9. Facilitate economic development by promoting a cyber-safe Louisiana for businesses and consumers.

LOUISIANA CYBERSECURITY COMMISSION



DEC 2017

- **Governor John Bel Edwards established the Louisiana Cybersecurity Commission -** a statewide partnership comprised of key stakeholders, subject matter experts, and cybersecurity professionals from Louisiana's public sector, private industry, academia, and law enforcement.

2018

- **Established 8 Standing Committees**.
- Focus on cybersecurity-related Legislative Bills
- Conducted a comprehensive study and completed a baseline assessment of the state's Cyber Ecosystem.
- Developed Priority Recommendations\Imperatives\Initiatives for Implementation.

2019

- Added 2 New Commissioners – Now at 17
- **Completed the State's first Strategic Plan and Action Plan (2017-2021).**
- **NGA Facilitated Workshop (Critical Infrastructure) and developed the 1st ever Critical Infrastructure Plan.**
- Established the state's very first **Cyber Coordination Center** at the Water Campus in Baton Rouge, to enhance cyber information sharing. **Currently working with the Public Service Commission to add utility organizations.**

2020

- Cyber commission focused on cybersecurity-related Legislative Bills
- State Police established a Louisiana Cybersecurity Alliance Group
- A law passed requiring Managed Service Providers (MSP) contracting with the state to provide notice of cyber incidents and ransomware to the Fusion Center.
- The Louisiana Cybersecurity Talent Initiative to fund degree and certificate programs in cybersecurity.
- A resolution passed establishing an Emergency Response Fund for cyber to support resource requirements for response to SLTT cyber-attacks happening around the state.

LOUISIANA CYBERSECURITY COMMISSION

2019 - Critical Infrastructure (NGA facilitated workshop)

- **Competitive process**: Louisiana's proposal was selected by the National Governors Association (NGA) to receive technical assistance from national cybersecurity professionals and leading experts.
- This support led to the development of Louisiana's Critical Infrastructure Cybersecurity Strategic Plan, led by Commissioners Dr. Ramesh Kolluru and Mr. Mark Northrup, with support from Dr. Arun Lakhotia.
- We now have a **Critical Infrastructure Cybersecurity Resiliency Plan** for Louisiana's private and public sector critical infrastructure assets.

LCC - 7 Standing Committees*, *Formally Adopted on 25 Mar 2021

Critical Infrastructure + Information Sharing
Chair: Ramesh Kolluru (UL); Co-Chair: Arun Lakhotia (UL)

Emergency Preparedness (ESF 17)
Chair: Jeffrey Moulton (STC); Co-Chair: Brian Landry (LCA)

Workforce and Economic Development, Education, and Public Outreach
Chair: Dr. Les Guice (LA Tech); Co-Chair: Brad Lambert (LED)

Legislation and Funding
Chair: BG Keith Waddell (LANG); Co-Chair: Craig Spohn (CIC)

Election Security
Chair: Kyle Ardoin (Secretary of State); Co-Chair: Brad Harris (SoS)

Law Enforcement, Prosecution and Digital Forensics
Chair: Lamar Davis (LSP); Co-Chair: Devin King (LSP)

Maritime Industry
Chair: April Danos; Co-Chair: Not Designated

LOUISIANA CYBERSECURITY COMMISSION

Louisiana's Critical Infrastructure Cybersecurity Resiliency Plan

- Framework for Improving Critical Infrastructure Cybersecurity (CI).
  - Cyber systems and critical infrastructure assets are vital to Louisiana and the USA. Their disruption or destruction would have a debilitating impact on our homeland security, economic vitality, public health, and our way of life.
  - Louisiana's natural gas, oil, petrochemical and transportation industries play a critical role in fueling America with reliable energy, chemicals, commodities, and food supply.

- Prior to the establishment of the Cyber Commission and the NGA facilitated workshop.
  - There was no coordinated and systematic effort by the State of Louisiana to work with private sector critical infrastructure owners and operators in preparing for, responding to, and recovering from a cyber event or attack.
  - There was no focus on assessing and addressing Louisiana's CI cybersecurity risks.
  - Convened private sector partners from across all Louisiana CI sectors including the energy sector.
  - Plan addresses Priority Sectors of CI including the Oil and Gas, Petrochemical and Energy sectors (ENTERGY, CLECO, SWEPCO).
  - Enhances Information Sharing and Collaboration – leveraging the work of Louisiana Business Emergency Operations Center (LA BEOC) and research on public-private partnerships.

LA BEOC
LOUISIANA BUSINESS EMERGENCY OPERATIONS CENTER

- Proposed plan (3 Primary Goals)
  - Assessing cybersecurity posture of Louisiana's public and private sector CI and establishing risk-informed priorities;
  - Enhancing trust and creating memoranda of understanding with private sector stakeholders; and,
  - Creating and exercising the Louisiana Critical Infrastructure Cybersecurity Plan.

LOUISIANA CYBERSECURITY COMMISSION

Asset Protection and Cyber-Incident Response

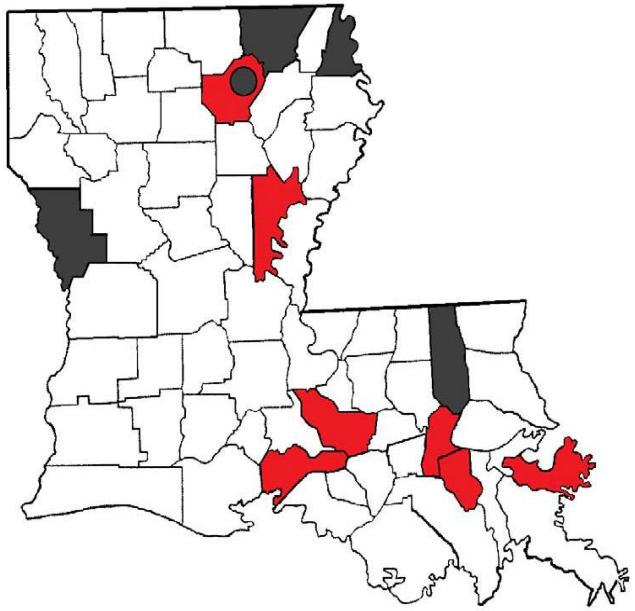
- ESF-17 – Cyber Incident Response Annex was added to the State's Emergency Operation Plan in 2019.
- Louisiana's ESF-17 team consists of leaders from the Office of Technology Services, the Governor's Office of Homeland Security, Louisiana State Police, and the Louisiana National Guard. Federal Partners (DHS, FBI, USSS). Also, other cybersecurity experts from across SLTT, academia and the private sector.
    - Conducts Training Exercises with CI Organizations inside a Cyber Range.
    - ESF-17 and the Louisiana National Guard's cyber protection teams, the Federal Bureau of Investigation and the Department of Homeland Security, held a four-day training seminar with Louisiana power supplier CLECO, as a part of the States annual disaster relief exercise in 2017.
- 2019 - Governor John Bel Edwards declared a statewide cyber security emergency after a malware attack on three public school districts in North Louisiana.

LOUISIANA CYBERSECURITY COMMISSION

Attacks against LA Parish School Board Systems

Incident Response Timeline

- **23 July – Reports of multiple ransomware attacks**
- Activated Emergency Support Function-17 (ESF-17)
- **24 July – Gov. Edwards state-wide Emergency Declaration**
- **24 July – LANG and state agencies respond at affected entities**
- 24 July – 13 Sep – Identification, Containment, Eradication, Recovery
- 13 August – Schools start on-time!



Response Numbers

5	Parishes Affected	95	Guard Activated
54	Schools Affected	30K	Students Served
7	Infections Prevented	10K+	Systems Recovered

UNCLASSIFIED

Legend
Compromised | Prevented

LOUISIANA CYBERSECURITY COMMISSION

Way Ahead for the Critical Infrastructure and Information Sharing Committee

Successfully finished the NGA Workshop and presented the completed plan to the Cyber Commission and the State.

- Recommended to State leaders that Louisiana immediately establish a Risk Management Framework to develop a Critical Infrastructure Cybersecurity Plan.
- Included the plan in the State's Strategic Plan for Cybersecurity.

The proposed plan was broken down into three distinct phases that would follow a very structured methodology:

Phase 1: Collect information related to critical infrastructures in Louisiana across the 16 critical infrastructure (CI) sectors and map those assets.

Phase 2: Evaluate cyber-readiness of these CI assets and analyze them for disruption consequences – including cross-sector interdependencies, and cascading effects.

Phase 3: Identify known vulnerabilities and adopt the DHS State Prioritization Guidebook to evaluate risk-based prioritization potential and need.

2019:

Members of the LCC, Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP), and other State, Local, Tribal and Territorial (SLTT) level partners, private sector and industry organizations, have **completed Phase 1 of the Plan**.

2020:

COVID Pandemic and State Emergencies (Hurricanes, Floods) presented challenges. Spin off the ***Maritime Sector Committee***.

2021:

Begin focusing attention of Phases 2 and 3 of the plan. Next in line: ***Healthcare Sector***; possibly ***Energy Sector Committee***?

LOUISIANA CYBERSECURITY COMMISSION

Hurricane Laura mangled transmission towers in Southeast Louisiana and shut the Energy System down.

Faced a complete rebuild of the transmission and distribution systems that support its power grid.

Also, impacted the production of OIL.

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a **single compromised password**.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a **virtual private network** account.

Louisiana's ESF-17 reached out to CISA to offer assistance.

State Energy officials (including energy emergency coordinators) continue to conduct coordination calls with CISA and DOE's CESER office.

Use this crisis as an opportunity to enhance our focus on cybersecurity within the *State Energy Plan*

Louisiana's Energy Critical Infrastructure Cybersecurity

LOUISIANA CYBERSECURITY COMMISSION

QUESTIONS

Indiana Executive Council on Cybersecurity – Energy Committee

NGA WEBINAR – JUNE 7

Governor Holcomb’s Executive Order

MISSION

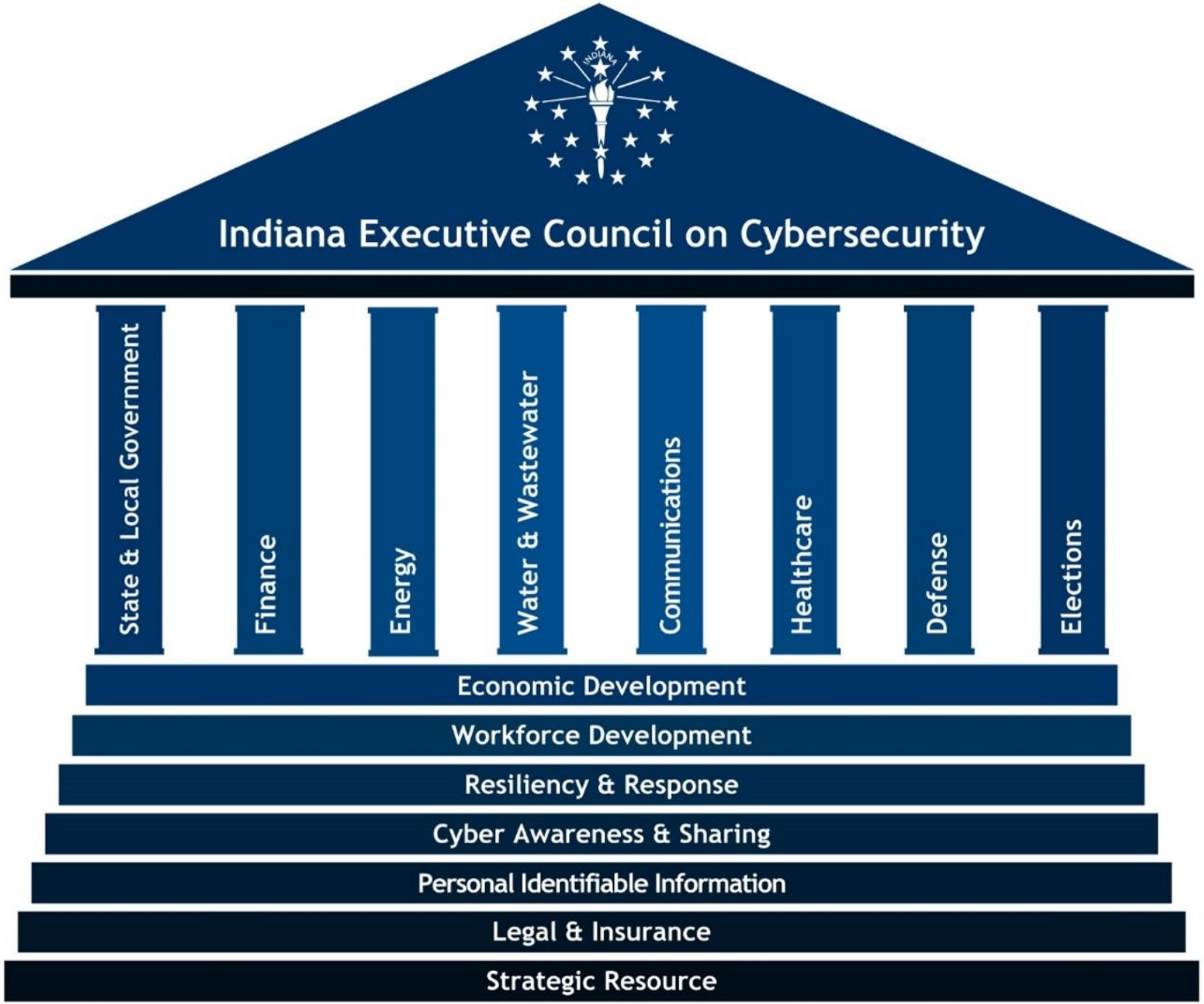
In order to protect the security and economy of the State, it is appropriate and necessary for state government to establish and lead a statewide, collaborative effort involving government, private-sector, military, research, and academic stakeholders to enhance Indiana's cybersecurity.

DIRECTIVES (PER EXECUTIVE ORDER)

- Establish an effective governing structure and strategic direction
- Formalize strategic cybersecurity partnerships across the public and private sectors
- Strengthen best practices to protect information technology infrastructure
- Build and maintain robust statewide cyber incident response capabilities

DIRECTIVES (PER EXECUTIVE ORDER)

- Establish processes, technology, and facilities to improve cybersecurity statewide
- Leverage business and economic opportunities related to information, critical infrastructure, and network security
- Ensure a robust workforce and talent pipeline in fields involving cybersecurity


Indiana Executive Council on Cybersecurity
State & Local Government
Finance
Energy
Water & Wastewater
Communications
Healthcare
Defense
Elections
Economic Development
Workforce Development
Resiliency & Response
Cyber Awareness & Sharing
Personal Identifiable Information
Legal & Insurance
Strategic Resource

COUNCIL IN REVIEW

- More than 250 members
- 15 teams; 1 Council
- Complete Plans with Four Areas (including Energy)
  - Research
  - Planning
  - Implementation
  - Evaluation

Energy Committee

CHAIR: DANIELLE MCGRATH, PRESIDENT, INDIANA ENERGY REC
CO-CHAIR: ROBERT I. RICHHART, CTO, HOOSIER ENERGY

Deliverable #1: Critical Infrastructure Information

- **Objective 1:** IECC Energy Committee will provide current definitions and review of potential policy changes to protect critical infrastructure information while maintaining public access and freedom of information by July 2018.
  - Complete: 100%

Deliverable #2: Training

- **Objective 1:** IECC Energy Committee will provide the IECC Workforce Development Committee the needs of the energy sector as well as examples to consider as Indiana cybersecurity training and apprenticeship programs are being developed by July 2018.
  - Complete: 100%

Deliverable #3: Contacts

- **Objective 1:** Over eighty-five percent of Indiana electric and natural gas utilities provided the Indiana Utility Regulatory Commission's Emergency Support Function lead on behalf of Indiana Department of Homeland Security a cybersecurity contact by June 2018.
  - Complete: 100%

- **Objective 2:** The Indiana Utility Regulatory Commission's Emergency Support Function lead will maintain the cyber contact list on behalf of the Indiana Department of Homeland Security Emergency Operations Center annually.
  - Complete: 100%

Deliverable #4: Coordinate with Others

- **Objective 1:** IECC Energy Committee will coordinate with other committees and working groups as needed to effectively complete the State Cybersecurity Strategic Plan by September 2018.
  - Complete: 100%

- **Objective 2:** IECC Energy Committee will share information with Energy ISAC regarding Indiana's new cyber sharing resources starting no later than December 2018.
  - Complete: 100%

Deliverable #5: Metrics

- **Objective 1**: IECC Energy Committee will provide the utility energy industry an annual survey that will assess cybersecurity planning, preparedness and recovery posture by June 2018. A summary of the results from all those who were surveyed was sent to the IECC.
  - Complete: 100%

- **Objective 2:** Eighty percent of all utilities will complete annual survey by July 2018. The actual result was one hundred percent participation with all responses received prior to June 2018.
  - Complete: 100%

2021 Plan Outline

- **Deliverable:** Critical Infrastructure Information (CII)
  - **Objective 1:** IECC Energy Committee will provide a review of the July 2018 definitions .
  - **Objective 2:** IECC Energy Committee will review potential state policy changes to protect critical infrastructure information while maintaining public access and freedom of information.

- **Deliverable:** Training
  - **Objective 1:** Develop a survey to determine whether there are new training needs specific to the energy industry following the Pandemic.
  - **Objective 2:** Identify and recommend opportunities at the state, vocational or higher education level.

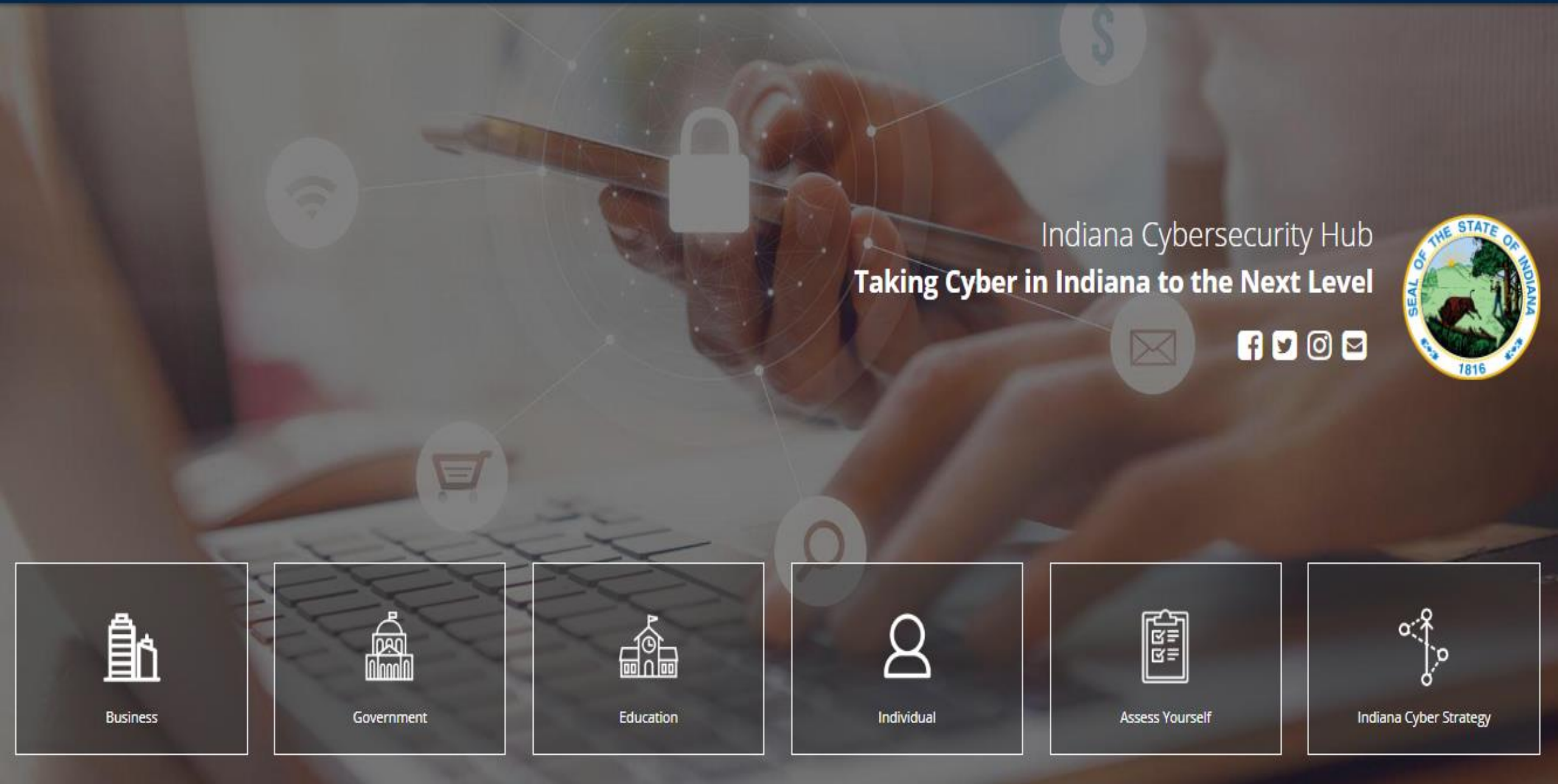
2021 Plan Outline

- **Deliverable:** IURC Cybersecurity Forum
  - **Objective 1:** Host a cybersecurity forum for small natural gas utilities to share industry information and best practices.

- **Deliverable:** Resource Guide
  - **Objective 1:** Define emerging technology and supply chain issues related to the grid.
  - **Objective 2:** Determine whether best practices and information are widely available.
  - **Objective 3:** Develop an industry specific resource guide.

2021 Plan Outline

- **Deliverable: Workplace IT**
  - **Objective 1:** Develop a survey to identify challenges in the workplace for the energy sector.
  - **Objective 2:** Identify issues stemming from the work-from-home environment.
  - **Objective 3:** Share best practices and coordinate with other sectors as needed.



Indiana Cybersecurity Hub

Taking Cyber in Indiana to the Next Level

Business

Government

Education

Individual

Assess Yourself

Indiana Cyber Strategy

INDIANA CYBER HUB

- Report a cyber crime
- Sector-specific information
- Strategic Plan
- Events
- Training
- And More….

www.in.gov/cyber

IECC Contact Information:
Chetrice L. Mosley-Romero
Cybersecurity Program Director
Cell: (317) 607-3178
Email: RomeroCLM@iot.in.gov

Audience Q & A

- Please submit questions into the chat box
- Unmute yourself
- Please chat or email Matt Rogotzke (mrogotzke@nga.org) with any technical questions

Contact

John Guerriero
Cybersecurity Program Director - Acting
Jguerriero@nga.org

Dan Lauf
Energy Program Director
dlauf@nga.org