COUNCIL OF GOVERNORS

Cybersecurity Working Group

Focus Area 2 | Resource Materials

COUNCIL OF GOVERNORS

Cybersecurity Working Group

Detailed Narrative

COUNCIL OF GOVERNORS

Cybersecurity Working Group

STATE CYBER ASSET ALIGNMENT AND ORGANIZATION
EXECUTIVE SUMMARY – FOCUS AREA 2

MISSION: Advise SLTT on aligning existing cybersecurity assets to maximize potential federal resources.

SYNOPSIS: States must identify and organize their own cybersecurity resources to address cyber incidents and protect their citizens. This focus area advises States on aligning their own, existing cybersecurity resources to maximize utility of federal support through a five-step process.

The Department of Defense (DoD), Cybersecurity and Infrastructure Security Agency (CISA), and other federal agencies are often unable to provide direct assistance for cyber incidents affecting states and local governments. CISA and federal law enforcement agencies can support states through CISA's cybersecurity field personnel, CISA's "Shields Up!" campaign, and by disseminating imminent threat warnings to vulnerable networks via the Multi-State Information Sharing Analysis Center (MS-ISAC). However, to maximize the utility of these resources, each state must first establish its own cyber emergency response framework.

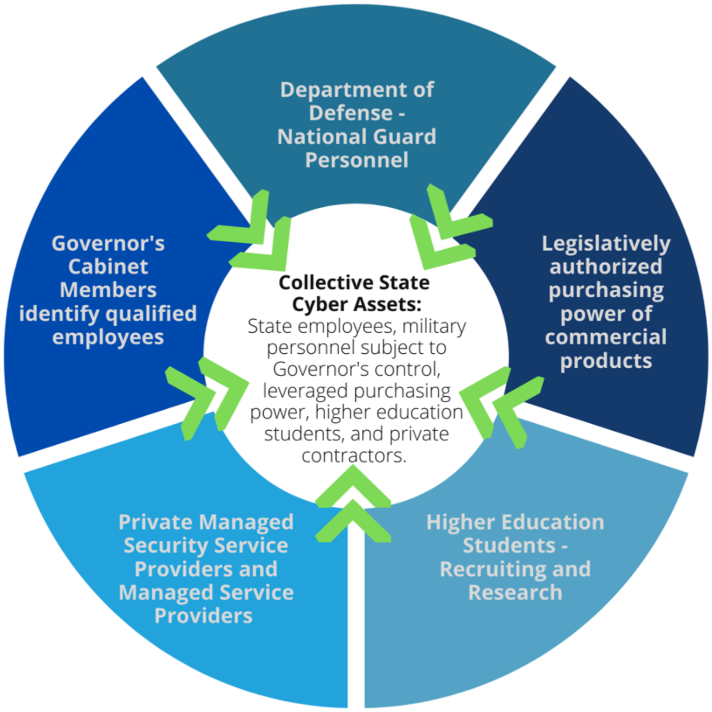
AUTHORS: This is a joint project created by Wyoming and Louisiana, with support from Governors Homeland Security Offices, CISA, and Federal Emergency Management Agency (FEMA).

SOURCES:

- National Defense Authorization Act for Fiscal Year 2022.
- DoD Directive 3025.18; DTM 17-007; 31 U.S.C. §1535.
- 6 U.S.C. §2234, passed into law as part of Public Law 117-58, Section 70602, Subtitle C.
- "A National Solution: Rethinking the Employment of Air National Guard Title 32 Status Citizen-Airmen to Defend the Nation's Cyberspace Infrastructure," Brigade General McKinney, Maurice (14 February 2013).
- Multi-State Information Sharing Analysis Center.
- 6 U.S.C. §124h.
- Fusion Center Guidelines: *Developing and Sharing Information and Intelligence in a New Era*
- *Considerations for Fusion Center and Emergency Operations Center Coordination,* Comprehensive Preparedness Guide, Federal Emergency Management Agency (May 2010).
- *Guide for All-Hazard Emergency Operations Planning,* State and Local Guide (SLG)101.

STATE CYBERSECURITY RESOURCES ALIGNMENT 5 STEPS

STEP 1: INVENTORY CURRENT CYBER RESOURCES


Department of Defense - National Guard Personnel
Legislatively authorized purchasing power of commercial products
Higher Education Students - Recruiting and Research
Private Managed Security Service Providers and Managed Service Providers
Governor's Cabinet Members identify qualified employees
Collective State Cyber Assets:
State employees, military personnel subject to Governor's control, leveraged purchasing power, higher education students, and private contractors.

Existing State Employees: Identify state employees and their respective skillsets related to the field of cybersecurity.

- Each of the Governor's Cabinet members identify members of his/her information technology departments through managers and supervisors.
- Given privacy and employment protection concerns individual to each state, Cabinet members can advertise an application internal to its employees to join (and be trained via State costs) a cyber task force for the State.
- Applications or appointments should be solicited on a permissive basis, with each employee consenting (in writing) to submit his/her resume and grant access to performance reviews.
- To assist with identifying individuals potentially interested in applying to the State's cyber task force, DHS can send each State Security Officer (often Fusion Center Director) a list of individuals with DHS security clearances on request; or facilitate with assistance from your state Security Officer to start the clearance process.
  - CISA may also provide clearances for critical infrastructure partners.
- Once the individuals are identified, managers/supervisors review resumes and work performance reviews to determine interests, qualifications, and eligibility for further training.
  - Legal Consideration Factors:
    - Performance history
    - Expression of interest
    - Adherence to application requirements (written statement, consent to background check).
    - Simple background check: credit checks, drug testing, criminal record.
  - Illegal Consideration Factors:
    - Age
    - Gender
    - Family circumstances
    - Sexual orientation
    - National Origin
    - Disability

  - Advertise that state employees will receive state sponsored training through programs such as SANS Institute, Microsoft, and CompTIA to become cyber specialists.
    - State employees should recognize the opportunity to increase their market value with the additional skillsets. Therefore, consider setting minimum state employment requirements to receive training.
  - Following review of candidates, list selected individuals, categorized by agency for Governor's and Cabinet members' aware.
    - These selected candidates will become State Cyber Task Force.
    - Consider offering selected candidates additional compensation relative to the additional duties (examples: overtime pay or set stipend per incident) based on state employment rules.
    - Readjust the selected employees' job duties or schedules to avoid overburdening them with Cyber Task Force duties (without reducing salary).
    - Consider new hires for potential workforce gaps.

Existing Department of Defense Personnel:

- Identify any Department of Defense (DoD) cyber assets within the State's employment – both National Guard and Reserve Components (as individual civilian employees).
  - Inventory the National Guard for current students in computer-related fields or those with an information technology background.
    - Each State's National Guard J1/S1 (Personnel Director) can inventory Soldiers and Airmen with military occupational specialties in the information technology fields.
      - Examples:
        - Air Force: 170A (Cyber Warfare Technician), 170D (Cyber Capabilities Developer Technician), 255A (Information Systems Technician), 255N (Network Systems Technician), 255S (information Protection Technician), 1N4A (Network Intelligence Analyst), 170B/352N/1N2X1 (Communication Signals Intelligence Production, Electronic Warfare Technician, and SIGINT Analysis Technician), 1N6x1 (Electronic System Security Assessment), 3C0x1 (Information Systems Opns/Analyst), and 948B (electronic Systems Maintenance).
        - Army: FA53/24/ or 25A DCOE Team Chief- Computer Network Defense (CND)-Service Provider(SP) Manager, 25V (Combat Documentation and Production Specialist), 25Y (Information Systems Chief), 255A (Information Systems Technician), 255S (Sr. Information Services Tech, CND-SP Incident Responder), 25B (Information Technologies Specialist), 25P (Microwave Systems Operator – Maintainer), 25Q (Multichannel Transmission Systems Operator – Maintainer), 25M (Multimedia Illustrator), 25F (Network Switching Systems Operator – Maintainer), 25N (Nodal Network Systems Operator – Maintainer), 25S/25T (Satellite/Microwave Systems Chief and Maintainer), 25O (Signal Officer). 25X (Senior Signal Sergeant), 25U (Signal Support Systems Specialist), 98K (Signal Collection/Identification Analyst), 35N (Signal Intelligence Analyst) 98C/98Z (Signals Intelligence Analyst and Senior Sergeant), 254A (Signals Systems Technician), 25W/25D (Telecommunications Operator – Chief Maintainer), (CND-SP- Infrastructure Support), and 25Z (Visual Information Operations Chief).
    - If the State is home to a Defensive Cyber Operations Element (DCOE), Cyber Protection Team, Cyber Operations Squadrons, Cyber Mission Force, or Cyber National Mission Force, the Soldiers and Airmen composing these forces received training from USCYBERCOM.

        - Commanders within individual units also have knowledge of their Airmen and Soldier's educational backgrounds in cybersecurity, despite not having a cybersecurity or technology-based position within the military.
    - Any Guardsmen or Reservists without full-time positions or in college in a cybersecurity field may become candidates for full-time state employment pending the state's budgetary constraints.
    - Guardsmen should be advised of potential positions within the state to remain in cybersecurity for future employment and retention within the state.

Federal Employees:

- Identify federal personnel that reside within each respective state and can support local efforts related to cybersecurity.
    - CISA:
        - CISA Regional Personnel: CISA has ten regions, aligned to the FEMA regions. Each CISA Region has regional and state Cybersecurity Advisors (CSAs), Cyber Security Coordinators (CSCs), Protective Security Advisors (PSAs), Emergency Communications Coordinators (ECCs), and other CISA personnel. These field personnel advise and assist in training and exercising best practices to help achieve robust resilience.
    - USSS: Field Offices
        - Cyber Fraud Task Forces (CFTFs), the focal point of our cyber investigative efforts, are a partnership between the Secret Service, other law enforcement agencies, prosecutors, private industry, and academia. The strategically located CFTFs combat cybercrime through prevention, detection, mitigation, and investigation.
        - CFTFs investigate complex cyber-enabled financial crimes and can recover lost funds, including those lost to foreign adversaries, due to cyber fraud if provided 48-72 hours notice.
    - FBI: Field Offices
        - The FBI has 56 field offices (also called divisions) centrally located in major metropolitan areas across the U.S. and Puerto Rico. They are the places where we carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations.

Private Contractors:

- Identify contractors (often managed service providers and software companies) that routinely work with the state on cybersecurity issues for potential surplus labor for state cyber incidents.
    - Private contractors also represent a recruiting pool for the State, Military, and potential volunteer force for large-scale responses.
    - Cyber-related threats and compromises can originate and/or spread through MSP/MSSPs. Therefore, identifying the MSP/MSSPs and their clients may be crucial for threat containment.

Higher Education Students:

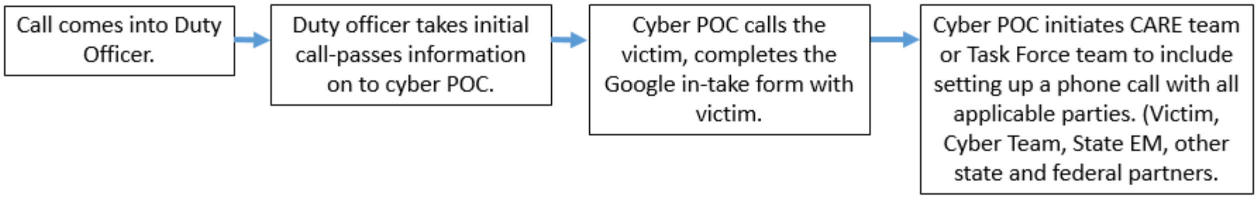
- Identify universities (public and private) or community colleges with existing or planned cybersecurity-related courses.
    - Higher education can access grant funds for cyber-related research, present recruiting opportunities (including Scholarships for Service), and/or offer collaborative opportunities for exercises.
    - Coordinate with higher education for potential recruiting events (for both military and state employment) and volunteer surplus labor during cyber incidents.
    - Higher education also helps create internships to help augment state staff for the cyber task force, state IT departments, Fusion Centers, and computer crimes teams.

State Purchasing Power (Software & Hardware):

- Identify the state agency with legislative authority to purchase information technology resources, budgetary resources, and with the greatest authority to monitor state information technology resources.
    - Balance these purchasing powers against budgetary constraints.
    - Determine the vendors contracted by the agency(ies) and re-assess the value provided by those vendors and consider mechanisms to highlight vendor competition.
        - Vendor relationships are crucial for emergency procurement, assistance and support, and collaborative concepts for future events.
        - For leverage, combined all purchases through one agency and with small group of vendors.
        - Leveraging the purchasing power can also benefit the local level (counties and municipalities) for fire walls and cyber security end user training for example.

Bring all parties together: Form the Cyber Task Force with selected and identified personnel.

- Identify the lead agency and leader of the Cyber Task Force as the team facilitators, who coordinate between the local, state, and federal partner.
- Whether it is university professors, students, state employees, DoD personnel, or private contractors willing to donate skillsets and time, the lead agency/task force bring the parties together to form the cyber incident response and leadership teams.
- The Cyber Task Force can also work to create the state's cyber response plan, training plans, exercises, as well as a phone tree, email groups, cyber intake forms, and notification processes for cyber incidents.
- An example of this would be:



Call comes into Duty Officer.

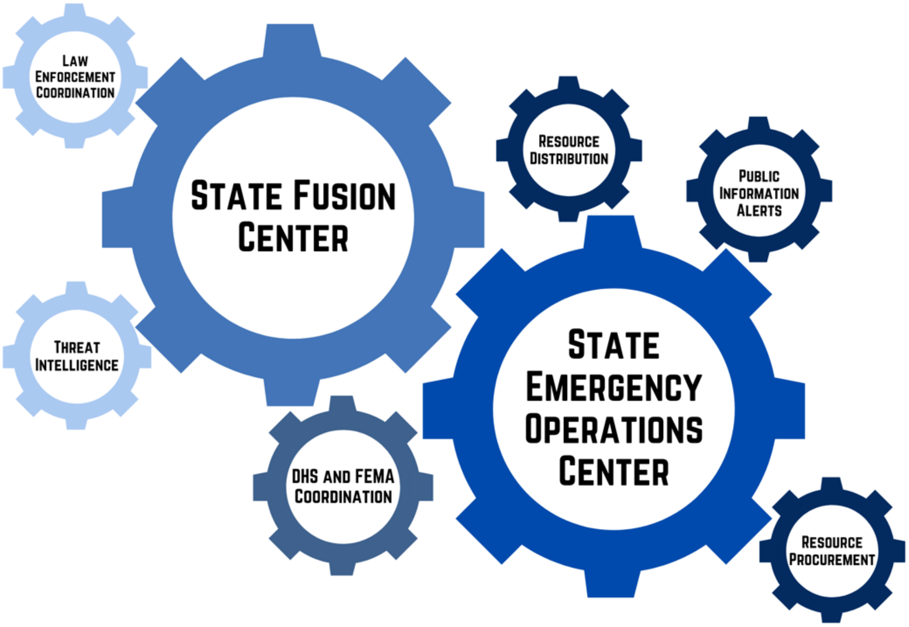
Duty officer takes initial call-passes information on to cyber POC.

Cyber POC calls the victim, completes the Google in-take form with victim.

Cyber POC initiates CARE team or Task Force team to include setting up a phone call with all applicable parties. (Victim, Cyber Team, State EM, other state and federal partners.

- Governor determines the intent and scope of the Cyber Task Force in terms of determining entities eligible to receive support (public v. quasi-public v. privately owned critical infrastructure) and scope of services provided.
- Engage local jurisdictions/counties/municipalities.
    - Example: Wyoming coordinated city, town, county, hospital IT staff and other IT staff as a local Cyber Task Force/CARE team, which meets quarterly and communicates on threats and indicators of compromise. This group is now expanding to include water/wastewater IT operators and other IT partners as well in the Critical Infrastructure Sector.

STEP 2: ENGAGE KEY STATE AGENCIES


Law Enforcement Coordination
State Fusion Center
Threat Intelligence
Resource Distribution
Public Information Alerts
State Emergency Operations Center
DHS and FEMA Coordination
Resource Procurement

State Fusion Centers:

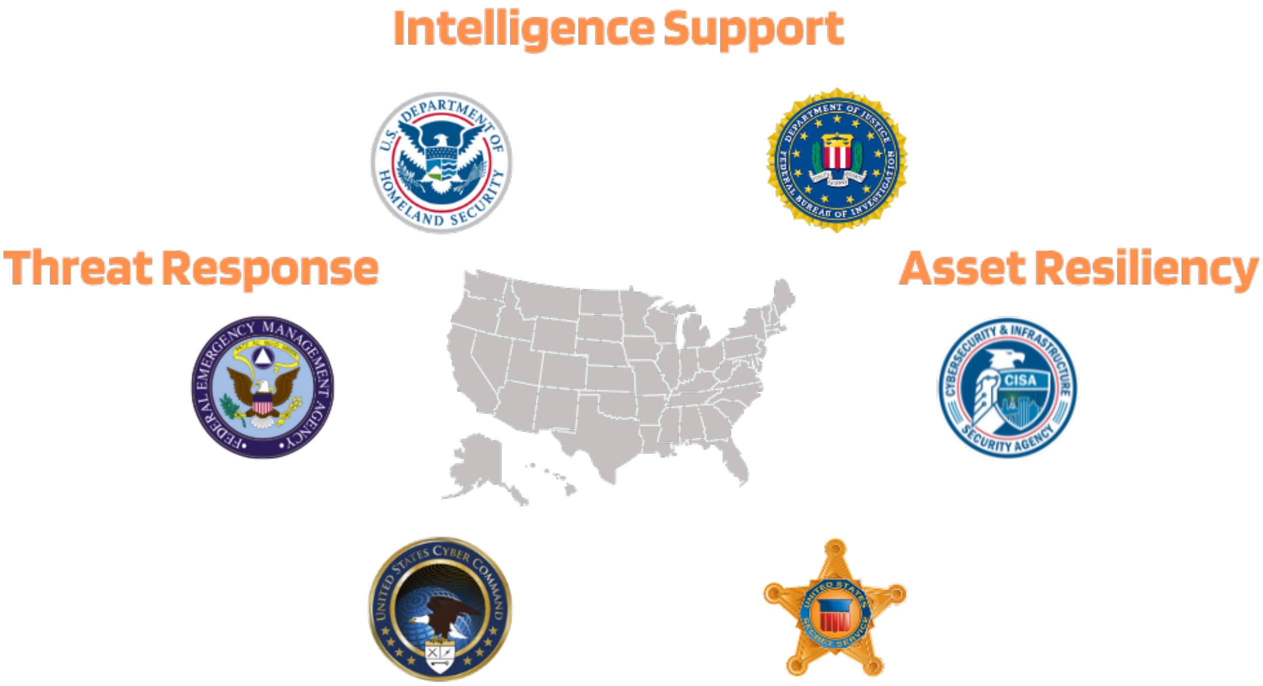
- Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering, and sharing of threat-related information between SLTT, federal and private sector partners.
- Established by the Department of Homeland Security in 6 U.S.C. §124h, Fusion Centers:
  - Review and analyze homeland security-relevant information from law enforcement agencies and other emergency response providers of State, local, and tribal government;
  - Create intelligence and other information products derived from information sources; and
- The name "Fusion" refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs.
  - Data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector—and, with analysis, can result in meaningful and actionable intelligence and information.
  - These entities coordinate with law enforcement entities, as well as receive and distribute threat intelligence (of any kind, including cyber-related information) to/from federal agencies and the Multi-State Information Sharing Analysis Center. Building a relationship with the State Fusion center and ensuring that the Fusion center is communicating cyber-related threats to State cyber leadership is key to mitigating and preventing cyber-attacks.
    - State cyber assets can become certified to research Advanced Persistent Threats (APTs) through the Fusion Center Networks.
    - State Fusion Centers can also send Requests for Information to other Fusion Centers and federal agencies for confirmation of threats or pertinent information.
    - Fusion centers can also assist with dissemination intelligence products to SLTT, emergency response agencies, appropriate Federal agencies as directed by DHS.
  - State Fusion Centers need a singular point of contact through which to share intelligence concerning cyber threat intelligence. It is *recommended* that a state official with a DHS-sponsored or DoD-sponsored security clearance be that POC.
    - Each State Fusion employs a security liaison that can assist in facilitating security clearances for relevant state employees (examples: Secretary of State's office, Homeland Security Personnel, Fusion Center Personnel, and other state personnel as appropriate) sponsored by the Protective Security Advisor (PSA) (example: Chief Information Officer/Chief Information Security Officer).
  - Potential suggestion: 24/7 Tip Reporting Line for cyber threats, to be used by the public, that feeds state agencies, the state cyber task force, and federal partners.

- As part of any campaign discussed in Step 5 – it is strongly encouraged that the public be informed about the types of information that should be reported to Fusion Centers.

State Emergency Management Operations Department/Agency:

- The lead in emergency response is the State's Emergency Management Agency, which also often serves as the State Administrative Agency for federal grant applications and FEMA aid:
  - These entities are responsible for coordinating state and local resources during a gray sky (disaster) event, enacting emergency management legislation, regulations, fund emergency management activities, mutual aid support across state lines through the Emergency Management Assistance Compact (EMAC), serve as the interface with federal agencies, develop response plans, coordinate state agency activities and activations, and assist local governments during steady state and disaster events.
  - State and local emergency managers prepare for emergencies and coordinate the activation and use of resources controlled by the State government as needed to help local governments respond to and recover from emergencies and disasters.
- In concert with a State Fusion Center, the State Emergency Management Department or Agency can also push out notifications to the public, federal agencies, and municipal entities.
  - FEMA recommends coordination between Fusion Centers and Emergency Operations Centers (EOCs) for information sharing, interstate communications between EOCs, and the synergistic enhancement of the entities' respective resources.
- Engaging the state and local emergency managers and the state and local EOCs as appropriate during any event to include cyber incidents that triggers the EOC support of the on-scene responders. This relieves the on-scene commander of external coordination and securing of additional resources (funding, manpower, intelligence, and equipment).
  - State EOCs coordinate and regularly interact with FEMA Regional Response Coordination Centers (RRCCs).
  - State EOCs are staffed and equipped to conduct prevention, protection, mitigation, response, and recovery before, during, and after any incident/event. They further coordinate resources at the state or federal level, which may include response and recovery capabilities such as mass care, evacuations, logistics, grant and finance, IPAWS (emergency public) warnings, press releases, and coordinating any assistance that has been requested of FEMA.
- Each Governor appoints a Homeland Security Advisor (HSA), often serving as the Director of the State Emergency Management Agency. These individuals have a Top-Secret Clearance along with the Governors, sponsored through DHS I&A. DHS I&A sponsors a secret-level security clearance for Fusion Center employees, which helps foster information sharing within the state.
  - Governors are respectfully advised to timely report incidents through individuals issued security clearances to the agencies that provided those clearances if there is any reliance on Secret or Top-Secret intelligence in detecting or mitigating the incident.

STEP 3: ENGAGE KEY FEDERAL PARTNERS



- **Federal Agencies with Cyber Missions:** The following federal agencies have cyber task forces with varying missions that enhance state resources: United States Secret Service (USSS), DHS/CISA, Federal Bureau of Investigation (FBI), and Multi-State Information Sharing Analysis Center (MS-ISAC).
  - Federal partners are also required to trigger certain DoD resources. Specifically, a lead federal agency is required to trigger federal funds through the DoD's Defense Support of Cyber Incident Response (DSCIR) processes:
    - Directive Type Memorandum (DTM) 17-007 (updated May 2021) authorizes DoD support of "lead federal departments and agencies for asset and threat response to cyber incidents outside the DoD Information Network (DoDIN)" with the consent of the network owner. Requests for DSCIR are evaluated by factors outlined in DoD Directive (DoDD) 3025.18, with emphasized consideration given to the impact on DoD networks, systems, and capabilities.
    - DSCIR requires another federal agency to serve as the "lead federal agency" and either make a commitment to DoD to reimburse DoD for the cost of the Servicemember's time and equipment, or DoD can waive the reimbursement requirement subject to certain conditions or when authorized by 10 U.S.C. §277(c).
    - The reimbursement from the lead federal agency is completed through an Economy Act transaction (31 U.S.C. §1535), which permits federal agencies to receive supplies or services from each other through interagency support agreements. DoDD 3025.18 utilizes the Economy Act when reimbursement is required for DSCIR.
    - Requests for DSCIR require written requests be submitted to the Executive Secretary of the Secretary of Defense.
  - CISA: Infrastructure and Investments Job Act (Public Law 117-58) established the Cyber Response and Recovery Act (CRRA), which authorized the Secretary for Homeland Security to

declare that a significant cyber incident and established the Cyber Response and Recovery Fund (CRRF).

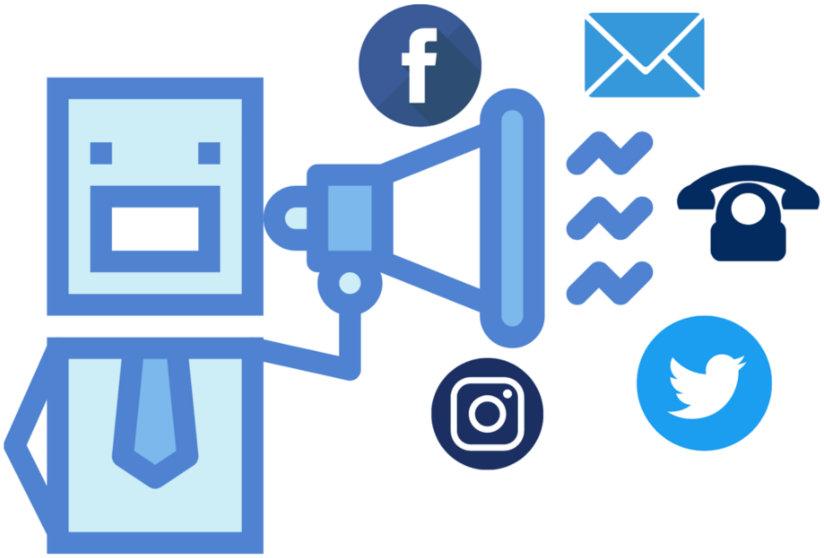
    - CRRA requires the CISA Director to coordinate asset response activities when there is a declaration. Public Law 117-58 allots $100M in multi-year money appropriated for the CRRA program.
    - Types of needs capable of triggering CRRF fund distribution are threat detection and hunting, malware analysis, analytical support, technical incident mitigation, vulnerability assessments and mitigation, and network protections.
    - In August 2021, CISA established the Joint Cyber Defense Collaborative (JCDC) to unify defensive actions and mitigate risk in advance of cyber incidents. This goal of the JCDC model—which includes the public and private sectors as well as federal and SLTT governments—is to strengthen the nation's cyber defenses through innovative collaboration, advanced preparation, and information sharing and fusion.
- USSS: On July 9, 2020, the USSS announced the creation of the Cyber Fraud Task Force, merging its Electronic Crimes Task Forces (ECTFs) and Financial Crimes Task Forces (FCTFs), which unlike its sister agencies, can recover stolen funds if notified within 48-72 hours of the event given its focus on cyber-enabled financial crimes.
- Homeland Security Investigations: employs a Cyber and Operational Technology division that oversees investigations of internet-related crimes, including child exploitation. The Cyber and Operational Technology, which houses both the HSI Innovation Lab and the Cyber Crimes Center, directly supports HSI's law enforcement and mission support programs and helps develop major advancements in technology used to combat crime through initiatives such as technical surveillance operations, cybersecurity, computer forensics, Title-III communication intercepts, and the Repository for Analytics in a Virtualized Environment (RAVEn) — HSI's next-generation platform for data analytics.
- Additional resources offered by these federal agencies include threat information sharing to mitigate/prevent events, equipment for state Fusion Centers, and collaboration on cyber-related investigations. Consistent communication between states and federal officials affords states the opportunity to receive real-time information on grants issued by various federal agencies.

STEP 4: FORM EMERGENCY SUPPORT FUNCTION FOR CYBER INCIDENT AND RESPONSE MANAGEMENT

Emergency Management Function Model

- Using the Emergency Support Functions utilized by FEMA, States (often through the Governor's Office) can create, authorize, and organize state commissions or task forces.
- ESF-2 for Communications can be expanded to include digital communication.
  - Through either the legislative or executive government process, authorize the Emergency Support Function to –
    - Perform cyber incident response and management on behalf of the state to its political subdivisions.
    - Coordinate with federal agencies for cyber threat information sharing.
    - Utilize emergency funds following surplus at end of any state fiscal year cycle.
    - Develop incident response plan (kept confidential for major state information networks and emergency response systems).
    - Recommend authorization of Governor's emergency powers (state-specific).
    - Create Emergency Management Assistance Compact (EMAC) with nearby state for mutual cyber support consistent with FEMA models – *currently an open commitment from the 2014 Joint Action Plan for State-Federal Unity of Effort on Cybersecurity.*
  - Using the inventory created in Step 1 and relationships built in Steps 2 and 3, nominate at least one lead/primary state agency (example: state military department or emergency management agency) and identify supporting state agencies, as well as contributing federal agencies.
    - The ESF is activated through the State Emergency Management Agency/Department.
  - Using state purchasing power, leverage better deals on commercial hardware and software for potential use following cyber-attacks to help rebuild networks.
  - Coordinate with federal partners to create, modify, and/or update a state-specific cyber incident response plan; compare against EMAC states for effectivity and mutual assistance.

STEP 5: CAMPAIGN TO INFORM YOUR STATE



State Public Service Campaigns

- Use the specific state's best mechanisms for information distribution to introduce the new cyber emergency support team.
- Launch individual campaigns on cyber readiness, available state resources, and mediums by which to share threat intelligence.
  - Examples:
    - Videos or stories explaining how cyber incidents can impact various state agencies and elements of critical infrastructure (as well as the potential consequences)
      - Example: https://www.dhs.gov/see-something-say-something/take-challenge
    - Stories or examples of phishing, targeted phishing, and social media fraud through reels, memes, and infographics.
- News stories, billboards, handouts, and fliers.
- Department of Transportation digital signage.
- Direct mail or inserts into utility bills.
- Targeted newsletters to 16 critical infrastructure sectors.
- Business and networking organizations (example: Business Council, Industry magazines and newsletters, Chambers of Commerce, Kiwanas, Rotary, etc.).
- Encourage all State and Local partners to become members of MS-ISAC, which performs incident response and remediation services and a 24x7x365 Security Operations Center (SOC) for threat analysis and early warning notifications along with real-time network monitoring and management.
  - Want to normalize cyber as a real emergency and target specific audiences through local networking groups to avoid audience gaps.

Federal Cyber Public Awareness Programs

- CISA: CISA and the National Cybersecurity Alliance awareness programs resources are available to launch awareness campaigns on cyber readiness, available state resources, and mediums by which to share threat intelligence.
  - CISA to work with states through the Council of Governors Cybersecurity Working Group to assist states with creating and launching informative campaigns.
    - CISA working with professional media group.
  - CISA's Awareness Partner Toolkit includes a wealth of resources–sample emails to staff, sample social media posts, and more to engage your states.
  - Cybersecurity tip sheets available via CISA and National Cybersecurity Alliance: Cybersecurity Awareness Month (October) | CISA and National Cybersecurity Alliance: Homepage (staysafeonline.org).

COUNCIL
OF GOVERNORS

Cybersecurity Working Group

Progress Card (EXAMPLE)

COUNCIL OF GOVERNORS
Cybersecurity Working Group

Cyber Asset Organization Progress Card

1 Inventory Current Cyber Assets _____/44 TOTAL POINTS

Identify Current State Employees through Cabinet Members. _____/8 PTS

Establish Cyber Force Application with Participation Incentives. _____/6 PTS

Conduct Application Process and select Cyber Task Force personnel. _____/6 PTS

Leverage unified/consolidated contract purchasing vehicles. _____/6 PTS

Identified National Guard cyber personnel for Cyber Task Force. _____/4 PTS

Coordinate with Higher Education for event, grant, and student support. _____/4 PTS

Identify local Federal Agency Offices locations for surge support. _____/2 PTS

Identify MSPs/MSSPs and IT Companies for surge support. _____/2 PTS

Bring all parties together to informally establish Cyber Task Force. _____/6 PTS

_____/12 TOTAL POINTS 2 Engage State Agencies

Establish central focal point (CFP) with State Fusion Centers for Cyber Task Force. _____/2 PTS

Ensure Fusion Center receives MS-ISAC, CISA, and other available intel products. _____/2 PTS

Establish CFP within state emergency management agency (EMA) for Cyber Task Force. _____/2 PTS

Coordinate EMA as potential communications hub for cyber events. _____/3 PTS

Identify security clearance needs with Fusion Center for Cyber Task Force personnel. _____/3 PTS

3 Engage Federal Agencies _____/10 TOTAL POINTS

Identify and engage local CISA representatives. _____/2 PTS

Identify and engage local FBI representatives. _____/2 PTS

Identify and engage local USSS Field office representatives. _____/2 PTS

Identify and engage local HSI office representatives. _____/2 PTS

Identify and engage local OHS office representatives. _____/2 PTS

_____/22 TOTAL POINTS 4 Form Emergency Support Function for Cyber

Analyze Gubernatorial powers to establish new Emergency Support Function (ESF). _____/4 PTS

Create new ESF or expand current ESF to include cyber. _____/6 PTS

Identify 1-2 lead agencies for ESF and primary supporting agencies _____/2 PTS

Create legal avenue to allocate a % of budget surplus into emergency fund for cyber. _____/4 PTS

Create or confirm authorization for Governor emergency powers to include cyber events. _____/2 PTS

Cyber ESF to create Cyber Incident Response Plan _____/4 PTS

5 Campaign to Inform the State _____/12 TOTAL POINTS

Encourage private and public critical infrastructure entities to join MS-ISAC feeds. _____/3 PTS

Identify social media platforms and other popular communication mechanisms to distribute targeted content. _____/3 PTS

Coordinate briefings at networking events and through commercial organizations. _____/3 PTS

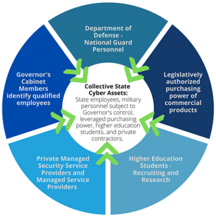
Coordinate with local CISA representatives to receive federal content for distribution. _____/3 PTS

Additional Tasks Undertaken:

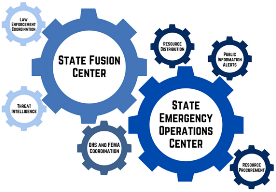
Council of Governors Cybersecurity Working Group

Cyber Asset Organization Progress notes

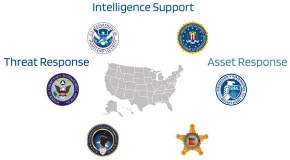
Inventory Current Cyber Assets


Department of Defense - National Guard Personnel
Legislatively authorized purchasing power of commercial products
Higher Education Students - Recruiting and Research
Private Managed Security Service Providers and Managed Service Providers
Governor's Cabinet Members identify qualified employees
Collective State Cyber Assets: State employees, military personnel subject to Governor's control, leveraged purchasing power, higher education students, and private contractors.

Engage State Agencies

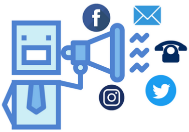

Law Enforcement Coordination
State Fusion Center
Resource Distribution
Public Information Alerts
Threat Intelligence
State Emergency Operations Center
DHS and FEMA Coordination
Resource Procurement

Engage Federal Agencies



Form Emergency Support Function for Cyber

Campaign to Inform the State



COUNCIL OF GOVERNORS

Cybersecurity Working Group

Presentation

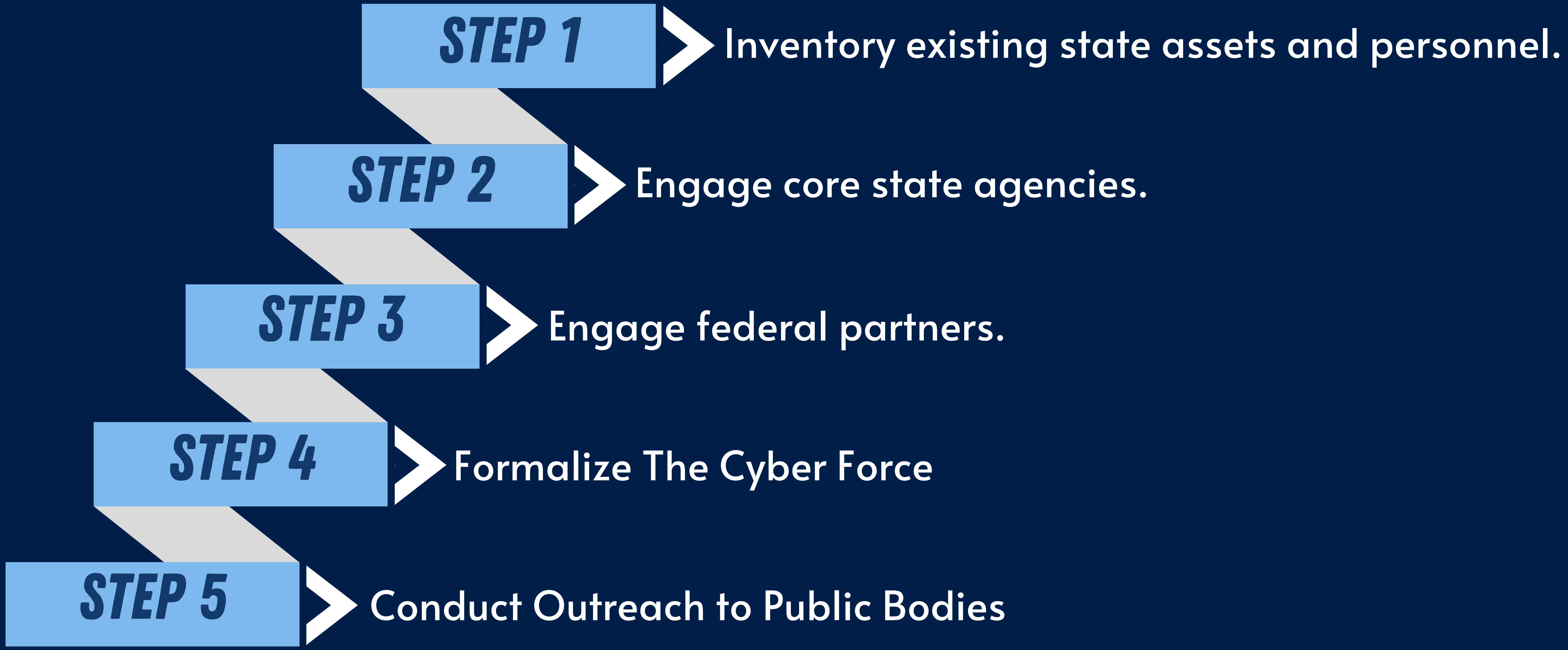
NATIONAL GOVERNORS ASSOCIATION -
COUNCIL OF GOVERNORS | 2022-2023
CYBERSECURITY WORKING GROUP

CREATING SLTT CYBER FORCES

FEBRUARY 2023

CREATING A LOCALIZED CYBER FORCE

5 steps to create a sustainable cyber force, for responses or preventative efforts, using existing resources:



STEP 1 Inventory existing state assets and personnel.

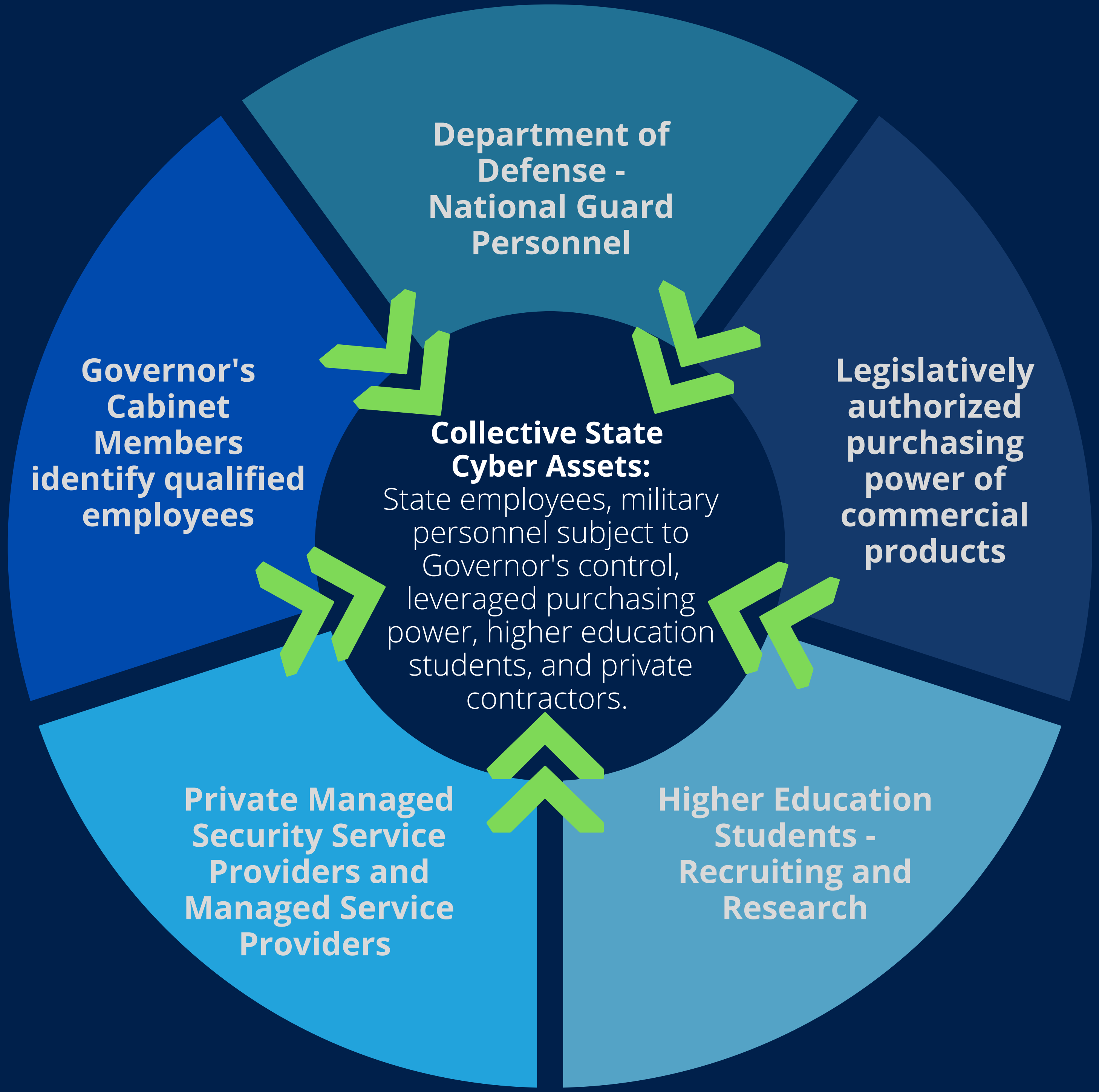
STEP 2 Engage core state agencies.

STEP 3 Engage federal partners.

STEP 4 Formalize The Cyber Force

STEP 5 Conduct Outreach to Public Bodies

STEP 1: INVENTORY

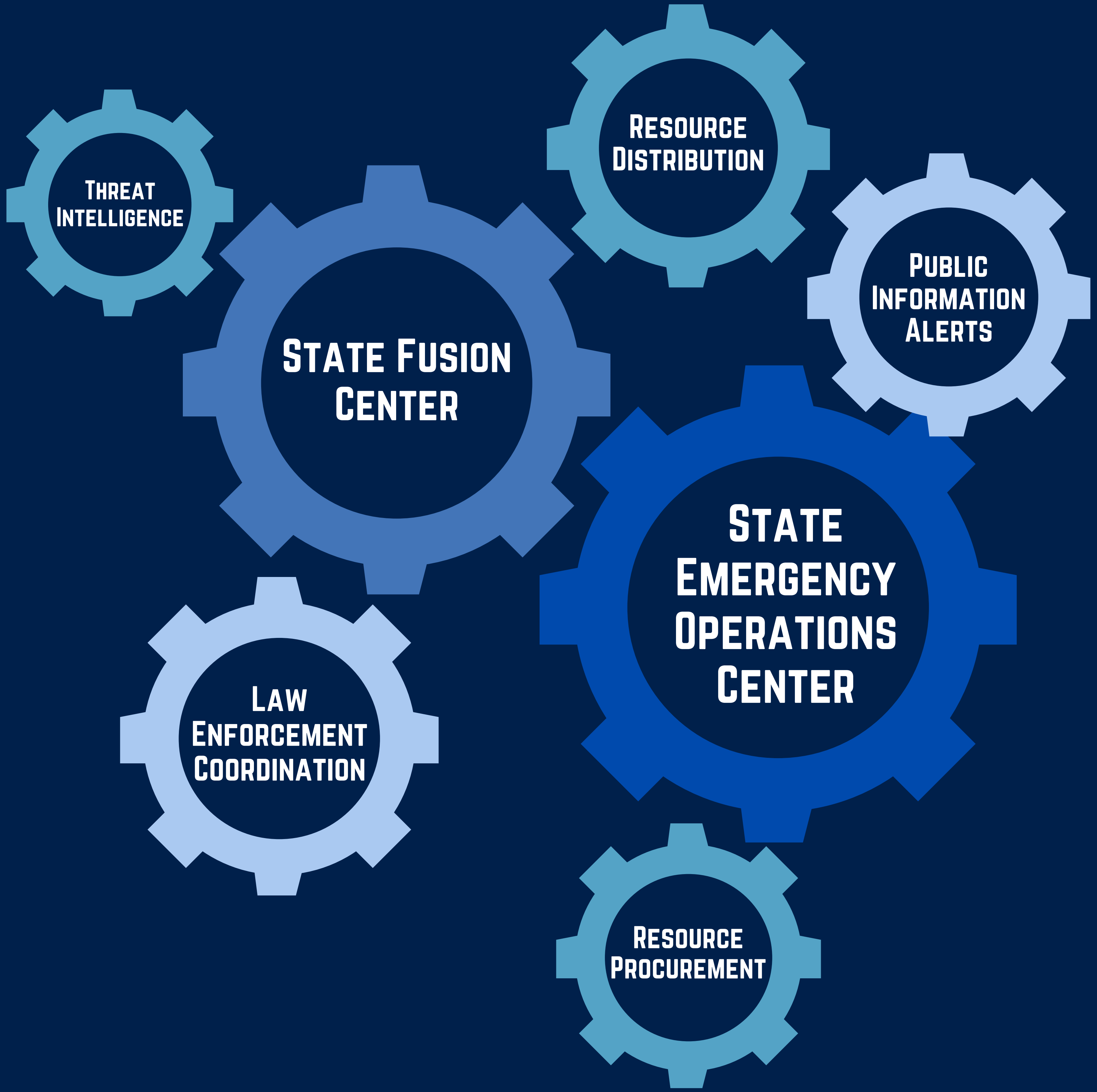

Department of Defense - National Guard Personnel
Legislatively authorized purchasing power of commercial products
Higher Education Students - Recruiting and Research
Private Managed Security Service Providers and Managed Service Providers
Governor's Cabinet Members identify qualified employees

Collective State Cyber Assets: State employees, military personnel subject to Governor's control, leveraged purchasing power, higher education students, and private contractors.

GOAL: build a "bench" of potential cyber incident responders with diversity of expertise.

- Begin by identifying who is already within the Governor’s employment with a background or interest in cybersecurity for potential reassignment or additional duties.
- Look inward to National Guard assets through unit assignments or military occupations.
- Determine which elements of government are vested with most technology purchasing power (usually the office of the Chief Information Officer).
- Identify the presence of digital forensic services within state or local law enforcement.
- Make relationships with private industry and institutions of higher education in the cybersecurity space for potential incident volunteers.

STEP 2: ENGAGE STATE AGENCIES



Threat Intelligence
Resource Distribution
Public Information Alerts
State Fusion Center
State Emergency Operations Center
Law Enforcement Coordination
Resource Procurement

GOAL: Organize all state agencies with different cybersecurity elements to consolidate talent, purchasing power, and intelligence resources.

- Concentrate on engaging the State Emergency Operations Management or the Emergency Operations Center Agency and State Fusion Centers.
- Fusion Centers act as information conduits with DHS sponsored security clearances.
- EOCs/EOMs are FEMA conduits, act as communication hub, resource control center.
- EOCs/EOMs can predict and respond to physical implications of cyber incidents.
- Fusion Center Security Liaison can facilitate clearances for key personnel.

STEP 3: ENGAGE FEDERAL PARTNERS

Intelligence Support

Threat Response

Asset Resiliency

GOAL: Build relationships with federal agencies operating in the state to facilitate the sharing of information and resources.

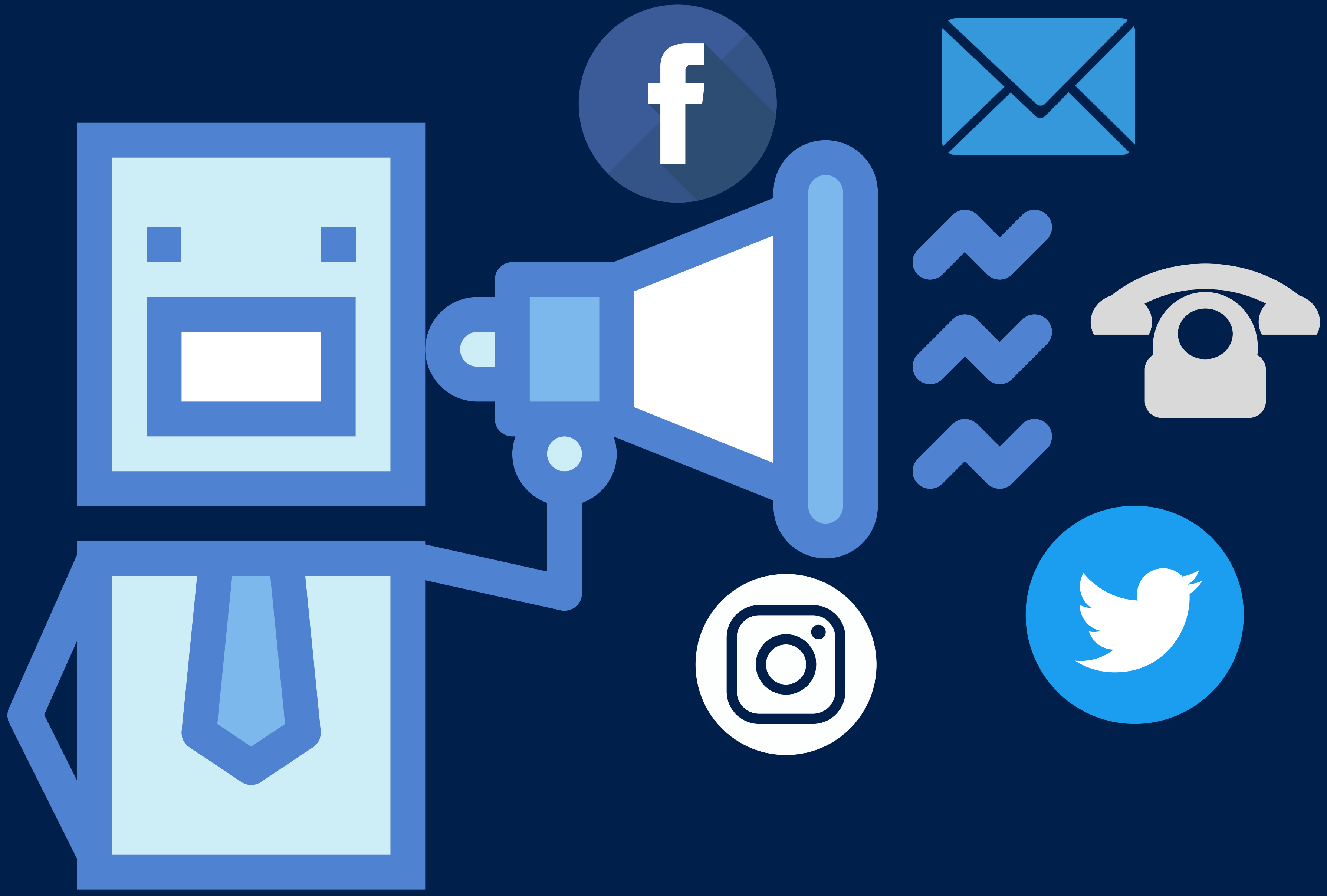
- No federal agency with capacity or the mission to respond to SLTT cyber incidents.
- SLTTs must focus on utilizing specialty skills of federal agencies.
- Concentrate on threat intelligence sharing – key to prevention and mitigation.
- Consider investigatory collaborations with state/local law enforcement that investigate cyber-related matters.
- Ensure strong professional relationship between State cyber assets and Special Agents in Charge for FBI/USSS and regional leaders within CISA and FEMA.

STEP 4: FORMALIZE THE CYBER FORCE

GOAL: Formalize and establish the cyber force through legal mechanisms (varies by state).

- Consider using the FEMA Emergency Support Functions, States can create, authorize, and organize state commissions or task forces.
  - Consider expansion of ESF-2 (Communications) to include cyber or create a new ESF.
  - ESF activated through the State Emergency Management Agency/Department.
- Through legislative or gubernatorial authority, give the new cyber force specific cyber tasking consistent with State emergency response plan.
- Use Steps 1-3 to nominate lead state agency(ies), leadership personnel, and the agency/individual responsible for coordination with federal partners to ensure information sharing.

STEP 5: INFORM PUBLIC ENTITIES



GOAL: Notify public bodies that the new cyber response is ready to assist and encourage them to call.

- Use mechanism to spread specific messages to public about the ESF or state cyber assistance capabilities through State campaigns or in coordination with federal cybersecurity campaigns.
- Options for Information Dissemination:
  - Municipal groups
  - Request prepared materials from CISA
  - Conferences (State's Annual Emergency Managers' Conference)
  - Social Media
  - Billboards
  - News stories
  - Business & networking events/organizations