BOARD OF HOMELAND SECURITY

WEDNESDAY, JUNE 5, 2019
1:30 TO 2:30 PM
GEMA/HS HEADQUARTERS
TRAINING ROOM

BOARD MEETING MINUTES

Board Members Present:
Homer Bryson, Vice Chairperson
Philip Peacock, Secretary
Vic Reynolds
Chris Carr
Kathleen Toomey
Richard Woods
Gary Black
Kyle Sapp
Bill Cowsert
Alan Powell
Erika Shields

Board Members Absent:
Col. Mark McDonough
Thomas Carden
Mark Williams
Russell McMurry
Calvin Rhodes

Representatives Present:
Col. Marc Belscamper
Col. Thomas Barnard
Larry Barnes
David Allen

The Board of Homeland Security held the board meeting on June 5, 2019 at the Georgia Emergency Management and Homeland Security Agency (GEMA/HS) Headquarters in Atlanta, Georgia. A List of Attendees, the Agenda, and the Meeting Presentation are attached hereto and made official parts of these minutes as Attachments #1, #2, and #3. Director Homer Bryson called the meeting to order at 1:31 PM.

All board members are present except Col. Mark McDonough with the Department of Public Safety, Adjutant General Thomas Carden with the Department of Defense, Commissioner Mark Williams with the Department of Natural Resources, Commissioner Russell McMurry with the Department of Transportation, and Calvin Rhodes with the Georgia Technology Authority.

Vice Chairperson Homer Bryson welcomed everyone to the GEMA/HS Headquarters in Atlanta, Georgia.

Roll Call

Approval of the Minutes:
Vice Chairperson Homer Bryson presented the minutes of the April 3, 2019 meeting for discussion and approval. Attorney General Chris Carr made a motion to approve the minutes. Representative Alan Powell seconded the motion. The motion passed unanimously.

Old Business:
Vice Chairperson Homer Bryson announced the Georgia Department of Education has created an Office of School Safety and Climate. Dr. Garry McGiboney will be heading up this effort as the Deputy Superintendent. Superintendent Richard Woods expressed his excitement for the new program.

Harlan Proveaux with GEMA/HS announced that the agency was awarded the 2019 Homeland Security grant funds. Funding decreased by $750,000 this year. Harlan Proveaux presented a draft of the Board of Homeland Security Strategic Plan for 2020 to 2025. He asked the board members to review the document and provide feedback. Schedule for 2019 meetings is provided in each binder. Today's board meeting is about the Critical Infrastructure and Key Resources (CIKR).

New Business:
a) Critical Infrastructure and Key Resources Overview
Warren Shepard with GEMA/HS presented an overview of CIKR in the State of Georgia. Critical Infrastructure are those "systems and assets, whether physical or virtual, so vital to the United States or Georgia that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Consequence is the effect of an event, incident, or occurrence. Key Resources are public and privately controlled resources essential to minimal operation of the economy and the government. Protected Critical Infrastructure Information (PCII) is a program designed to safeguard sensitive infrastructure information voluntarily shared with the government for homeland security purposes. PCII is a key part of efforts designed to protect the Nation's critical infrastructure from cyber-attacks. Resilience is the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Risk Management is the process of identifying, analyzing, and communicating risks and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood (a function of threats and vulnerabilities) and the associated consequences. Threat is the natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability is the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

In Georgia there are several things that are at risk: Metropolitan Area, Nuclear Power Plants, Airports, Agriculture, Ports, Tourism, Sporting Events, Energy, Transportation, and Schools. Evolving threats to critical infrastructure are extreme weather, accidents or technical failures, cyber threats, acts of terrorism, and pandemics. There are sixteen critical infrastructure sectors

whose assets, systems, and networks, whether physical or vital, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Identifying CIKR is intended to support collaborative planning efforts and provide necessary information for steady-state risk management and to support incident management during response, recovery efforts. There are essential steps to identifying and protecting critical infrastructure, which may include; conducting risk assessments and prioritizing assets, understanding the interdependencies of key infrastructure, analyzing cross-sector cascading effects, and coordinating with private and public sectors to improve protection and resiliency. Threats to critical infrastructure should be assessed in the context of natural, manmade, and technological events. CIKR are physical and cyber-based systems that are essential to the operations of the economy and government. Risks should be determined based on those threats, including the likelihood of occurrence and the impact these threats would have on the immediate infrastructure and on interdependent systems and facilities. Failure of one part of the system will affect the system and create cascading affects throughout. Disruption in any part of the cross-sector supply chain may have a direct impact on the local, regional, or state economic stability. Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences. Maintain situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure. Provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure. Conduct comprehensive assessments of critical infrastructure. Map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies. Risk Management model has the elements of critical infrastructure, which are physical, cyber, and human. First step is to Set Goals and Objectives, then Identify Infrastructure, Assess and Analyze Risk, Implement Risk Management Activities, and Measure the Effectiveness. While this is happening, they will constantly reevaluate and change it as needed.

The mission of the CIKR Unit is to facilitate the protection of life and property against manmade incidents by directing the State's efforts in the areas of prevention, preparedness, mitigation, response, and recovery. A combination of programs are implemented and managed by CIKR to achieve the goals established by the Unit work together to accomplish the mission. These include CIKR Protection, Security, and Resiliency, Training and Exercises, and Information Sharing. The Infrastructure Protection Gateway (IP Gateway) serves as the single interface through which homeland security partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis. CIKR uses IP Gateway, various data collection, analysis, response tools, infrastructure protection tools, and datasets by leveraging a single user registration, management, and authentication process. CIKR conducts surveys and assessments of various critical infrastructure and key resource locations throughout the State. Each facility is provided with a detailed summary and comparison product called a DashBoard for their use. The Infrastructure Assessment Tool (IST) is used to

conduct assessments on critical infrastructure and key resources. Once a facility has agreed to an assessment and completed the PCII Statement, the basic date is load in to IP Gateway based on the Sector. During an onsite assessment, the IST is used to gather security reliance data. This dynamic assessment tool has 28 sections in which between 500 and 1,700 data points are collected.

The PMI is a quantitative value using a 0 to 100 scale as an aggregate measure of the following five operational dimensions of protection, as they relate to the security posture. Physical Security refers to measures and features that protect a facility and its buildings. Security Management refers to plans and procedure that a facility has in place to deal with security issues. Security Force refers to a designated group of employees or contractors with security duties. Information Sharing refers to the exchange of hazard and threat information with private industry, local, State and Federal agencies. Security Activity History/Background refers to previous vulnerability assessments and new protective measures that a facility may have implemented to improve its security posture.

The Resilience Measures Index (RMI) is a quantitative value using 0 to 100 scale is an aggregate measure of the following four operational dimensions of resilience, as they relate to the resilience posture. Preparedness refers to activities that a facility has taken to define its hazard environment. Mitigation Measures refers to activities a facility has taken prior to an event to reduce the severity or consequences of a hazard or incident. Response Capabilities refers to immediate and ongoing activities, tasks, programs, and systems developed or undertaken to manage the adverse effect of an event. Recovery Mechanisms refer to activities and programs a facility has in place to help return conditions to a level that is acceptable for operations. The CIKR Unit completed thirty-two assessments, participated in eighteen infrastructure assessments with the U.S. Department of Homeland Security, Port exercise in Savannah, GA, DHS Secure Video Conferences, FEMA Region IV Super Bowl Planning, DHS Super Bowl Planning, School Food Defense Project, Election Secure Briefings, Oversite Georgia Body Recover Canine Team Program, Oversight Law Enforcement CBRN Teams, Oversight HazMat Teams, Oversight Ago Terrorism, Submitted 215 special events to DHS for Special Event Assessment Rating review and assignment in 2018 to 2019, and suspicious person training at the National Golf Course in Augusta, GA.

Warren Shepard reviewed the draft of the Board of Homeland Security 2020 to 2025 Strategic Plan. Proposed Protection Goal 3 is to reduce risk to statewide infrastructure by adopting a coordinated approach between cities, counties, and state government. The project start date is August 1, 2019. Identify the state agency for each critical infrastructure sector from August 2019 to February 2020. Develop a selection methodology of CIKR facilities in the State from August 2019 to February 2020. Collect documents related to critical infrastructure security from February 2020 to August 2020. Create, develop, and implement training standards for critical infrastructure assessment officers from August 2019 to February 2020. Assess risks, threats, and vulnerabilities at identified facilities from February 2020 to August 2025. Develop and implement protective and resiliency programs from August 2021 to August 2022. Improve

education facilities safety by developing prevention and protection programs from August 2020 to August 2025. Coordinate cyber security in the State from August 2022 to August 2025.

Harlan Proveaux with GEMA/HS asked for feedback on the objectives and timeline for the strategic plan. The next two meetings will be focused on Information Gathering and Sharing from the Georgia Bureau of Investigation (GBI).

Adjournment:
There being no further business to be brought before the Board, Vice Chairperson Homer Bryson adjourned the meeting at 2:45 PM.

Official Attachments:

1. List of Attendees
2. Agenda
3. Meeting Presentation

BOARD OF HOMELAND SECURITY

WEDNESDAY, JUNE 5, 2019
1:30 TO 2:30 PM
GEMA/HS HEADQUARTERS
TRAINING ROOM

BOARD MEETING ATTENDEES

Board Members:
Homer Bryson, Vice Chairperson
Philip Peacock, Secretary
Vic Reynolds
Chris Carr
Kathleen Toomey
Richard Woods
Gary Black
Kyle Sapp
Bill Cowsert
Alan Powell
Erika Shields

Representatives:
Col. Marc Belscamper
Col. Thomas Barnard
Larry Barnes
David Allen

Others Attending:
Scott Dutton
Joey Greene
Gary Kelley
Scott Minarcine
Michael Nix
Tina Piper
Harlan Proveaux
Tommy Ratchford
Ashley Seay
Mark Sexton
Warren Shepard
Cody Whitlock
Ferron Yi

Board of Homeland Security Meeting

AGENDA

June 5, 2019
1:30 - 2:30 P.M.
GEMA/HS Headquarters
Training Room
Atlanta, GA

Agenda Topic	**Speaker**
Call to Order	Homer Bryson, Director GEMA/HS
Roll Call	
Approval of Minutes from April 3, 2019	
Old Business	
New Business **a)** Critical Infrastructure/Key Resource Overview	Harlan Proveaux, Deputy Director GEMA/HS Warren Shepard, Manager CI/KR GEMA/HS
Adjournment	

Georgia Emergency Management & Homeland Security Agency

Critical Infrastructure and Key Resources Overview

Warren Shepard
CIKR Unit Manager

What is ?

- **Critical Infrastructure**: those "systems and assets, whether physical or virtual, so vital to the United States or Georgia that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
- **Consequence:** the effect of an event, incident, or occurrence.
- **Key Resources**: publicly and privately controlled resources essential to minimal operation of the economy and the government.
- **PCII:** Protected Critical Infrastructure Information (PCII) program is designed to safeguard sensitive infrastructure information voluntarily shared with the government for homeland security purposes. PCII is a key part of efforts designed to protect the Nation's critical infrastructure from cyber-attacks

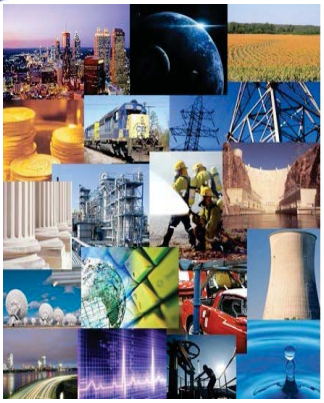
What is ?

- **Resilience**: the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions to include the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience.
- **Risk Management**: the process of identifying, analyzing, and communicating risks and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.
- **Risk**: potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences.

What is ?

- **Threat:** the natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- **Vulnerability**: the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

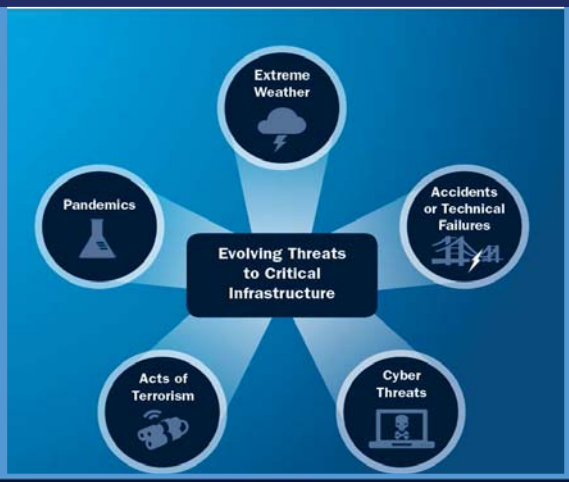
At Risk In Georgia



- Metropolitan Area
- Nuclear Power Plants
- Airports
- Agricultural
- Ports
- Tourism
- Sporting Events
- Energy
- Transportation
- Schools

UNCLASSIFIED

Risks to Georgia



UNCLASSIFIED

What are the Critical Infrastructure Sectors?

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Communications
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems Sector
- Water and Wastewater Systems

DHS DOD DOE DOT DAG/DHHS DHHS EPA

UNCLASSIFIED

Georgia CIKR by Sector

- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Communications
- Transportation Systems Sector
- Water and Wastewater Systems

UNCLASSIFIED

What and Why

Identifying CIKR is intended to support collaborative planning efforts and provide necessary information for steady-state risk management and to support incident management during response/recovery efforts. The creation of a CIKR Plan ensures emergency management agencies have an understanding of the critical infrastructure and key resources, in order to make multi-disciplinary, multi-resource, and multi-tiered informed decisions regarding preparedness, incident response and recovery.

It also assures emergency management can rapidly identify, assess and efficiently allocate resources that will sustain the community and enhance response and recovery efforts.

There are essential steps to identifying and protecting critical infrastructure, which may include; conducting risk assessments and prioritizing assets, understanding the interdependencies of key infrastructure, analyzing cross-sector cascading effects, and coordinating with private and public sectors to improve protection and resiliency.

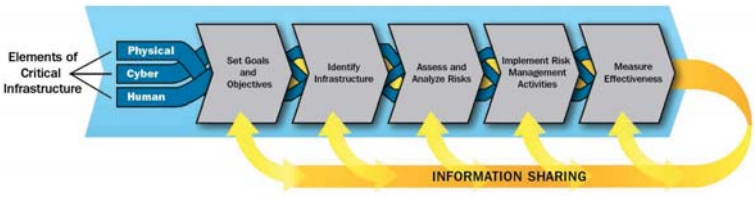
What and Why

- Threats to critical infrastructure should be assessed in the context of natural, man-made, and technological events. CIKR are physical and cyber-based systems that are essential to the operations of the economy and government.
- Risks should be determined based on those threats, including the likelihood of occurrence and the impact these threats would have on the immediate infrastructure and on interdependent systems and facilities. Critical infrastructure is not a distinct collection of physical entities. Instead, it is an interconnected system of systems, each part relying on and affecting the operations of other parts of the system, also known as a cascading impact.
- Failure of one part of the system will affect the system and create cascading effects throughout. Disruption in any part of the cross-sector supply chain may have a direct impact on the local, regional or state economic stability and the inability to provide vital life-line services.

What and Why

- Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences
- Maintain situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure
- Provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure
- Conduct comprehensive assessments of critical infrastructure
- Map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies

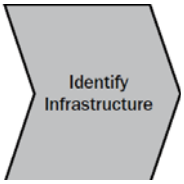
Critical Infrastructure Risk Management



Set Infrastructure Goals and Objectives

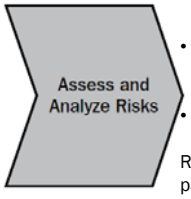
Establish a set of broad goals for critical infrastructure security and resilience. These goals are supported by objectives and priorities and serve as targets for collaborative planning by government and the private sector.

Identify Infrastructure



To manage critical infrastructure risk effectively, partners must identify the assets, systems, and networks that are essential to their continued operation, considering associated dependencies and interdependencies. Critical infrastructure partners view criticality differently, based on their unique situations, operating models, and associated risks.

Assess and Analyze Risks



Critical infrastructure risks can be assessed in terms of the following:

- Threat – natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- Vulnerability – physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence – effect of an event, incident, or occurrence.

Risk assessments are conducted by many critical infrastructure partners to inform their own decision making, using a broad range of methodologies. These assessments allow critical infrastructure community leaders to understand the most likely and severe incidents that could affect their operations and communities and use this information to support planning and resource allocation in a coordinated manner.

Implement Risk Management Activities

Decision makers prioritize activities to manage critical infrastructure risk based on the criticality of the affected infrastructure, the costs of such activities, and the potential for risk reduction. Some risk management activities address multiple aspects of risk, while others are more targeted to address specific threats, vulnerabilities, or potential consequences. These activities can be divided into the following approaches: Identify, Deter, Detect, Disrupt, and Prepare .

Measure Effectiveness

Measure Effectiveness

The critical infrastructure community evaluates the effectiveness of risk management efforts within sectors and at the State, local, and regional levels by developing metrics for both direct and indirect indicator measurement.

Critical Infrastructure and Key Resources Unit

The mission of the Critical Infrastructure and Key Resources Unit (CIKR) is to facilitate the protection of life and property against manmade incidents by directing the State's efforts in the areas of prevention, preparedness, mitigation, response, and recovery. A combination of programs are implemented and managed by CIKR to achieve the goals established by the Unit work together to accomplish the mission.

These include:

- CIKR Protection, Security and Resiliency
- Training and Exercises
- Information Sharing

The Infrastructure Protection Gateway (IP Gateway) serves as the single interface through which homeland security partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis. This, in turn, enables homeland security partners to quickly identify relevant vulnerability and consequence data in support of event planning, incident preparedness, and response efforts.

Critical Infrastructure and Key Resources Unit

CIKR uses IP Gateway, various data collection, analysis, and response tools to infrastructure protection tools and datasets by leveraging a single user registration, management, and authentication process.

Highlights of the IP Gateway include the ability to access:

- A selection of physical and cyber vulnerability assessment and security survey capabilities.
- A suite of critical infrastructure information, including assessments, analytical products and reports.
- Integrated data visualization and mapping applications to support complex data analysis.
- An array of tools to support critical infrastructure planning and analysis, including a robust data search capability.

CIKR conducts surveys and assessments of various critical infrastructure and key resource locations throughout the State. Each facility is provided with a detailed summary and comparison product called a DashBoard for their use.

Infrastructure Assessment Tool (IST)

The Infrastructure Assessment Tool (IST) is used to conduct assessments on critical infrastructure and key resources. Once a facility has agreed to an assessment and completed the PCII Statement, the basic date is load in to IP Gateway based on it Sector.

During an onsite assessment the IST is used to gather security and reliance data. This dynamic assessment tool has 28 sections in which between 500 and 1,700 data points are collected. Upon submission, two Dashboard products are generated. The facility is compared to like facility within the same Sector.

Overview Protective Measures Index (PMI)

Protective Measures Index (PMI)
The PMI is a quantitative value using a 0-100 scale is an aggregate measure of the following five operational dimensions of protection, as they relate to the security posture :

Physical Security refers to measures and features that protect a facility and its buildings, perimeter, and occupants.

Security Management refers to plans and procedure that a facility has in place to deal with security issues.

Security Force refers to a designated group of employees or contractors with security duties.

Information Sharing refers to the exchange of hazard and threat information with private industry and local, State, and Federal agencies.

Security Activity History/Background refers to previous vulnerability assessments and new protective measures that a facility may have implemented to improve its security posture.

Overview Resilience Measures Index (RMI)

Resilience Measures Index (RMI)
The RMI is a quantitative value using a 0-100 scale is an aggregate measure of the following four operational dimensions of resilience, as they relate to the resilience posture:

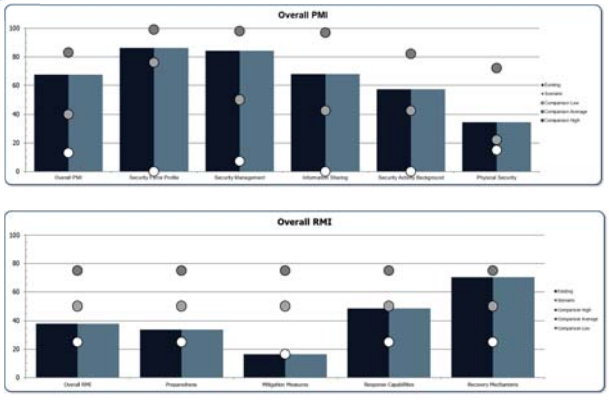
Preparedness refers activities that a facility has taken to define its hazard environment.

Mitigation Measures refers to activities a facility has taken prior to an event to reduce the severity or consequences of a hazard or incident.

Response Capabilities refers to immediate and ongoing activities, task, programs, and systems developed or undertaken to manage the adverse effect of an event.

Recovery Mechanisms refer to activities and programs a facility has in pace to help return conditions to a level that is acceptable for operations.

PMI / RMI Overall Graph



Protective Measures Dashboard

Example Protective Measures Dashboard

Critical Infrastructure and Key Resources Unit

- Completed 32 Critical Infrastructure Assessments
- Participated in 18 Infrastructure Assessments with US DHS
- Port of Savannah Exercise
- DHS Secure Video Conferences
- FEMA Region IV Super Bowl Planning
- DHS Super Bowl Planning
- School Food Defense Project
- Election Secure Briefings
- Oversite Georgia Body Recover Canine Team Program
- Oversight Law Enforcement CBRN Teams
- Oversight HazMat Teams
- Oversight Agro Terrorism
- Submitted 215 Special Events to DHS for Special Event Assessment Rating review and assignment in 2018-19
- Suspicious Person Training Augusta National Golf Course

Proposed 2020 – 2025 Strategic Plan

Board of Homeland Security
2020 – 2025 Strategic Plan

Proposed Protection Goal 3

Reduce risk to statewide infrastructure by adopting a coordinated approach between cities, counties, and state government.

Objectives:

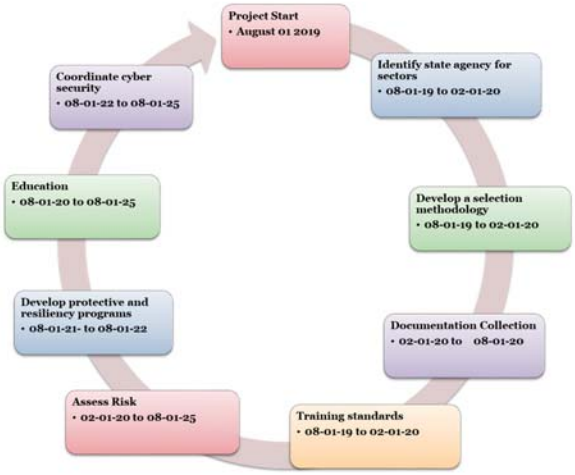
1. Identify the appropriate state agency best equipped to coordinate the safety and security of each of the critical infrastructure sectors, to ensure the state's finite resources are used efficiently as possible. (6 months)
2. Develop a selection methodology for the identification of critical infrastructure and key resource facilities located within the State to ensure an integrated system of resilient sectors. (6 months)
3. Record existing and undocumented information related to critical infrastructure security (GPS locations, owner and current contact information, sector, systems, networks, and functions in the Infrastructure Protection (IP) gateway. (6-12 months)
4. Create, develop, and implement training requirements for critical infrastructure assessment officers to ensure the assessments and analyses are being conducted in a uniform and standard method throughout the State. (6 months)

Proposed Protection Goal 3

Reduce risk to statewide infrastructure by adopting a coordinated approach between cities, counties, and state government.

Objectives:

5. Assess risks, threats and vulnerabilities at identified facilities. (18 – 60 months)
6. Develop and implement protective and resiliency programs for infrastructures facilities. (24-36 months)
7. Improve education facilities safety by developing prevention and protection programs. (12-60 months)
8. Coordinate cyber security in the State among the government, public, and private sectors to ensure information systems are protected and resilient to cyber threats and to ensure incident response capabilities exist to rapidly contain and remediate attacks. (36 months)


Project Start
• August 01 2019
Identify state agency for sectors
• 08-01-19 to 02-01-20
Develop a selection methodology
• 08-01-19 to 02-01-20
Documentation Collection
• 02-01-20 to 08-01-20
Training standards
• 08-01-19 to 02-01-20
Assess Risk
• 02-01-20 to 08-01-25
Develop protective and resiliency programs
• 08-01-21- to 08-01-22
Education
• 08-01-20 to 08-01-25
Coordinate cyber security
• 08-01-22 to 08-01-25

Questions?