Board of Homeland Security
Strategic Plan
2022 - 2027

This page intentional blank

Approval and Implementation

Transmitted herewith is the Homeland Security 2022 – 2027 Strategic Plan as approved and adopted this _6th_ day of _October_, 2021 by the Board of Homeland Security. This plan supersedes any/all previous Homeland Security Strategic Plan documents promulgated by the State of Georgia for this purpose.

Secretary
Georgia Board of Homeland Security

10/6/2021

Date

Executive Summary

Terrorist organizations remain committed to death, destruction, and the disruption within our borders. These groups are targeting our families, our businesses, and our way of life. Protecting the State of Georgia from this campaign of terror requires teamwork. Only through collaborative efforts can we reduce our vulnerabilities and defend against future attacks. Through strategic planning, training, and exercising, our collective preparedness is enhanced. Should a domestic, transnational, or international terrorism organization launch an attack in Georgia, our response and recovery must be seamless.

Our statewide homeland security strategic goals are to:

- Strengthen intelligence and information sharing system for the detection and prevention of threats to public safety and welfare.

- Increase use of technology to create a more resilient state.

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

- Reduce the vulnerability of critical infrastructure or key resources to cyber related incidents or attacks through a systematic approach to cyber security protection programs.

- Enhance the response to a disaster, attack, or event through the development of multiagency response teams using the finite resources of the government.

- Promote citizen preparedness through effective preparedness planning, volunteer opportunities, and awareness programs.

- Strengthen infrastructure, structural, human, and economic recovery capabilities.

Our strategic goals and objectives are based on a foundation of shared values of freedom; community health and safety; economic prosperity and quality of life; security of people, infrastructure, and the environment; continuous improvement; financial stewardship and accountability; and an all-citizen and all-state focus in every aspect of executing out plan.

The State of Georgia Board of Homeland Security is pleased to present the Homeland Security 2022 – 2027 Strategic Plan. The Strategic Plan provides a framework for Georgia's continuing progress toward developing and maintaining the capabilities to prevent, protect, respond, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies through well-prepared citizens, responders, and community leaders who are coordinated across disciplines and jurisdictional boundaries.

Table of Contents

Record of Change

Change #	Date	Part Affected	Date Posted	Who Posted

Record of Distribution

Plan #	Office/Department	Representative	Signature
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

1.0 Introduction

1.1 Purpose

The Georgia Emergency Management and Homeland Security Agency coordinates the development and implementation of the 2022 – 2027 Strategic Plan including planning, development, and coordination of statewide policies developed in support of public and private organizations responsible for preventing terrorism, raising awareness, reducing vulnerabilities, responding to, and recovering from terrorist acts.

The Board of Homeland Security 2022 – 2027 Strategic Plan is a living document requiring an annual critical review to remain relevant to a changing environment. The Plan serves as a tool for state, county, and local organizations to use when spending federal grant funds, by assisting these agencies in prioritizing the cost effective use of Georgia's capabilities, ensuring that the state is optimally using its resources. Everyone in Georgia has a role to play in homeland security – from individual citizens to our federal partners.

National guidelines were used during the development of the 2022 – 2027 Strategic Plan. This guidance was developed as a direct result of presidential directives, aimed at creating a secure nation integrated at all levels in its preparedness. Homeland Security Presidential Directive Eight (HSPD-8) outlines a comprehensive process to prepare states in the event of a significant hazard that would require the ability to mobilize all resources across the country, not just independent providers at the federal, state, and local levels.

In creating the 2022 – 2027 Strategic Plan, the Board of Homeland Security recognized the importance of instituting an inclusive planning process to ensure comprehensive input was received from across the state. Georgia Emergency Management and Homeland Security Agency made recommendations for revisions and implementing the objectives and steps, in support of the continued development of sustainable, risk-based, and all-hazard preparedness capabilities for the state.

The 2022 – 2027 Strategic Plan was developed to protect all Georgians. Our citizens are key to ensuring the security of the state. Citizens are encouraged to educate themselves about personal preparedness and volunteer their services to help government agencies and non-governmental organizations achieve the homeland security goals and objectives that will make Georgia a more secure and resilient state.

1.2 Authority

The Homeland Security 2022 – 2027 Strategic Plan is based on the authority of the State Government of Georgia, specifically that portion of the Official Code of Georgia, Title 38, Chapter 3, Articles 1 through 3 and is compliant with the National Incident Management System and supports the National Response Framework.

1.3 Mission Areas

Georgia continues to improve its preparedness by updating plans, filling identified gaps, and ensuring that all stakeholders are properly trained and exercised in the four primary preparedness mission areas:

➢ **Prevention** – Actions to avoid an incident or to intervene or stop an incident from occurring.

➢ **Protection** – Actions to reduce the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks, major disasters, and other emergencies.

➢ **Response** – Activities that address the short-term, direct effects of an incident.

➢ **Recovery** – Activities that include the development, coordination, and execution of human, economic, and infrastructure restoration plans.

This 2022 – 2027 Strategic Plan encompasses these mission areas through six goals, divided among the four missions. These goals provide the basic framework to develop and sustain homeland security capabilities in Georgia.

Prevention:
Goal 1: Strengthen intelligence and information sharing system for the detection and prevention of threats to public safety and welfare.

Goal 2: Increase the use of technology to create a more resilient state.

Protection:
Goal 1: Reduce risk to statewide infrastructure by adopting a coordinated approach between cities, counties, and state government.

Response
Goal 1: Enhance the response to a disaster, attack, or event through the development of multiagency response teams using the finite resources of the government.

Goal 2: Promote citizen preparedness through effective preparedness planning, volunteer opportunities, and awareness programs.

Recovery
Goal 1: Strengthen infrastructure, structural, human, and economic recovery capabilities.

1.4 General Definitions and Acronyms

Catastrophic Disaster - Any natural or manmade incident, including terrorism, which results in extraordinary levels of mass casualties, damage, or disruption that severely affects the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to local, state, tribal, territorial, insular area, and private sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.

Community Recovery – A process that begins within the first month following disaster that focuses on community and economic redevelopment. The process includes widespread community involvement in identifying and completing projects intended to rebuild communities and make them stronger than they were prior to disaster.

Critical Infrastructure - Those systems and facilities in both the public and private sector that are essential to the Nation's security, public health and safety, economic vitality, and way of life. The Nation's infrastructure is composed of 16 primary sectors such as water, transportation, communications, dams, energy and emergency services to name a few. Although infrastructure systems are defined and may operate independently; there are many interdependencies between the 16 sectors and their associated systems and facilities that need to be considered in making a community, state or region whole following a major disaster.

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

Intermediate Recovery - Phase of recovery which involves returning individuals, families, critical infrastructure and essential government or commercial services to a functional, if not pre-disaster, state. Such activities are often characterized by temporary actions that provide a bridge to permanent measures.

Long-term Recovery - Phase of recovery that may continue for months or years and addresses complete redevelopment and revitalization of the impacted area, rebuilding or relocating damaged or destroyed social, economic, natural and built environments and a move to self-sufficiency, sustainability and resilience.

Major Disaster - As defined by the Stafford Act, any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake,

volcanic eruption, landslide, mudslide, snowstorm, or drought) or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this act to supplement the efforts and available resources of local, state governments and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Mitigation - Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. Mitigation capabilities include, but are not limited to, community-wide risk reduction projects; efforts to improve the resilience of critical infrastructure and key resource lifelines; risk reduction for specific vulnerabilities from natural hazards or acts of terrorism; and initiatives to reduce future risks after a disaster has occurred.

Natural Resources - Land, fish, wildlife, biota and water. Water means salt and fresh water, surface and ground water used for drinking, irrigation, aquaculture and recreational purposes, as well as in its capacity as fish and wildlife habitat.

Nonprofit- An incorporated organization which exists for educational or charitable reasons, and from which its shareholders or trustees do not benefit financially. Any money earned must be retained by the organization, and used for its own expenses, operations, and programs. Many nonprofit organizations also seek tax exempt status, and may also be exempt from local taxes including sales taxes or property taxes. Also called not-for-profit organization.

Nongovernmental Organization - A nongovernmental entity that serves the interests of its members, individuals, or institutions and is not for private benefit. Nongovernmental organizations may include faith-based and community-based organizations.

Reconstruction – The long-term process of rebuilding a community's destroyed or damaged housing stock, commercial and industrial buildings, public facilities, and other structures.

Recovery – Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources.

Redevelopment – Usually used to refer to rebuilding the community's economic activity after a disaster. It is different from economic recovery in that it goes beyond the process

of merely restoring disrupted economic activity to the creation of new economic opportunities and enterprises in the aftermath of the recovery period, particularly including those that arise as by-products or direct outcomes of the disaster itself.

Resilience - Ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.

Risk - 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

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.

Response - Those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Sustainability - Meeting the needs of the present without compromising the ability of future generations to meet their own needs.

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

Whole Community - A focus on enabling the participation in national preparedness activities of a wider range of players from the private and nonprofit sectors, including nongovernmental organizations and the general public, in conjunction with the participation of Federal, state, and local governmental partners in order to foster better coordination and working relationships. Used interchangeably with "all-of-Nation."

ACRONYMS

CIKR – Critical Infrastructure and Key Resources
CR – Community Recovery
EOP – Emergency Operations Plan
ESF – Emergency Support Function
GEMA/HS – Georgia Emergency Management and Homeland Security Agency
GEOP – Georgia Emergency Operations Plan
NDRF – National Disaster Recovery Framework
NRF – National Response Framework
PCII -- Protected Critical Infrastructure Information
SOC – State Operations Center

2.0 Prevention Goals and Objectives

2.1 Prevention Goal 1: Strengthen intelligence and information sharing system for the detection of threats impacting the state of Georgia.

Georgia's intelligence system is comprised of the interconnected personnel, policies, processes, technologies, equipment, facilities, training, and capabilities implemented to sustain the intelligence cycle within the State. The intelligence cycle is the systematic process through which raw information is transformed into meaningful and useful data that can aid in the detection, prevention, and mitigation of threats to public safety. The intelligence cycle includes the following phases:

1. **Evaluation:** The evaluation, or feedback, phase of the intelligence cycle is both the first and last step of an ongoing process. Evaluation involves defining those questions, or *intelligence requirements*, to which intelligence is expected to contribute, prioritizing those requirements, and assessing the efficacy of the personnel, policies, processes, technologies, equipment, facilities, and training used to meet them.

2. **Collection:** Once requirements, priorities, and needs have been established, intelligence is collected. The collection phase involves detection of information, recognition of the information as useful and relevant, initial documentation, and submission of the information for actualization.

3. **Analysis:** Collection produces information which must undergo further processing and exploitation before it can be regarded as intelligence and typically involves developing derivative data from limited initial information. More particularly, analysis involves determining the probable credibility, reliability, relevance, timeliness, and impact of information using all available resources to fully identify and vet the persons, places, facts, and circumstances associated with the raw data.

4. **Dissemination**: Dissemination refers to the actualization of intelligence; the process of moving intelligence from producers to consumers or stakeholders.

Intelligence is defined as data that has been evaluated and determined to be relevant to the identification of individuals who, or organizations which, are reasonably suspected of involvement in criminal activity, such as terrorism. Similarly, a Suspicious Activity Report (SAR) is official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity, such as school violence. Since threats and acts of violence to and within the state of Georgia generally constitute criminal or suspicious activity, timely and collaborative sharing of relevant criminal intelligence information among affected stakeholders is vital to the detection and prevention of threats to public safety throughout Georgia. Georgia's intelligence systems are highly technical and specialized entities that are governed by both state and federal law and influenced by agency policy, as well as national standards, initiatives, and best

practices recommended by several advisory organizations. These information and intelligence analysis policies, practices, and procedures are layered within established technological, interpersonal, and technical capabilities to ensure timely and accurate information sharing while establishing safeguards to protect the constitutional rights and civil liberties of all people. Therefore, strengthening a collaborative statewide system for criminal intelligence and threat information by leveraging state law enforcement and other government assets to enhance the intelligence cycle in support of local, county, and federal threat-mitigation efforts is essential to the continuity and efficacy of the State's capability to detect and prevent threats impacting Georgia.

Objectives Prevention Goal 1:

1. Develop and implement enhancements to a statewide Suspicious Activity Reporting mobile application. (3-6 months)

2. Enhance existing programs to gather intelligence to identify, assess, and prioritize threats to Georgia and our citizens. (3-6 months)

3. Coordinate with public safety, emergency management, educational, and private sector entities throughout the state to increase awareness of the National Suspicious Activity Reporting Initiative and the State's suspicious activity reporting mobile application through the implementation of updated training and public messaging. (6-60 months)

4. Identify and assess the intelligence capabilities and needs of municipal and county law enforcement agencies located throughout Georgia. (12-60 months)

5. Identify existing legal and physical barriers to, and limitations on, information sharing and develop legislative recommendations to address any issues or concerns. (3-6 months)

6. Assess the technology, personnel, equipment, facilities, and funding needed to enhance of the State's capability to identify, collect, analyze, and disseminate information relative to existing or emerging threats and develop an associated budgetary and legislative sustainment plan. (6-18 months)

7. Address recruitment and retention of intelligence analysts employed by state, county, and local law enforcement agencies by accrediting existing analyst certification training program requirements via the Georgia Peace Officer Standards and Training Council. (6-18 months)

8. Develop statewide intelligence collection standards, requirements, and policies. (18-36 months)

9. Creation of a statewide intelligence center designed to meet the intelligence needs of public safety, emergency management, educational, and private sector entities within Georgia. (18-60 months)

2.2 Prevention Goal 2: Increase use of technology and cyber-security programs to create a more resilient state.

A cyber-resilience framework is a crucial component of modern-day governments. Despite the growing security risks in a remote working world, many organizations are still unprepared. In 2019, just 49% of enterprise leaders felt confident about their organization's ability to detect a cybersecurity threat; let alone contain it. Cybersecurity is about reacting. Cyber Resilience is about anticipating. This framework highlights the critical and continual actions required to achieve Cyber Resilience.

Developing cyber-resilience does not come down to having the perfect incident response tools. More often than not, cybersecurity systems do not fail because of a technology issue but fail because of actions by users of the systems.

Cyber-resilience is the measure of the ability to continue with working as normal while attempting to prevent, detect, control and recover from threats against its data and IT infrastructure. Without a strong cybersecurity framework, organizations are open to attacks, where a bad actor could gain access to networks, infrastructure or personal computer devices, and destroy or steal sensitive data.

What Is a Cyber Resilience Framework?
The standard cyber-resilience framework is made up of six key pillars:

1. **Identify** critical assets, systems and data. The enterprise must understand the resources that support all critical functions within a business context.
2. **Protect** critical infrastructure services. In this step, the enterprise installs first-line security programs that will limit or contain the impact of any potential threat.
3. **Detect** strange events and suspected data breaches or data leaks before major damage occurs. This step demands constant security monitoring.

4. **Respond** to a detected security breach or failure. This function involves an end-to-end incident response plan to ensure business runs as usual in the face of a cyberattack.
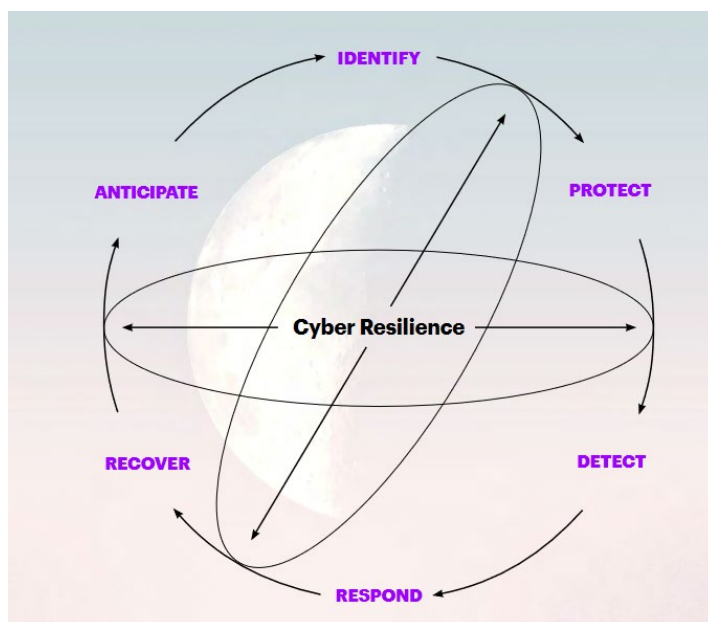
5. **Recover** to restore any affected infrastructure, capabilities or services that were compromised during a cybersecurity incident. This step focuses on making a timely return to normal efforts.
6. **Anticipate** to foresee threat actor's actions in advance to be able to implement protective means, placing pre-emptive threat intelligence gathering at the core of cyber-security.

Objectives Prevention Goal 2:

1. **Cyber Response Readiness / Cyber-Incident Escalation Paths**: Develop and defined escalation paths based on incident impact. Escalate cyber-incidents to the most appropriate management level, with inclusion of local, national, and international agencies. (6-18 months)

2. **Strategic Threat Intelligence / Peer Monitoring Capabilities:** Anticipating future threats—including using and evaluating peer-monitoring feeds within and outside the security team. With an "extremely competent" ranking, respondents suggest their organizations are using the specific "business" context to enrich reporting in threat feeds. Facilitate regularly communicate peer-monitoring to the business and IT organizations, with the overall process continually of reviewing and improving. (12-36 months)

3. **Resilience Readiness / Cyber-Incident Recovery Extreme:** Ensure organizations, both public and private with critical infrastructures and key resources have integrated cybersecurity recovery plan into Business Continuity and Disaster Recovery strategies, with the plan updated based on environmental changes. (6-60 months)

4. **Creation of Emergency Support Function 17 Cyber Security:** In the event of a significant cybersecurity incident, ESF 17 would provide a centralized entity for responding to a cyber-incident that affects the State of Georgia. ESF 17 provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts. Additionally, ESF 17 ensures appropriate coordination and inclusion of necessary state, federal and local agencies and private industry, In order to minimize the impact of a cyber-security incident. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations and potentially could impact public health, safety, or critical infrastructure. (6-36 months)

2.3 Protection Goal 1: Reduce risk to statewide infrastructure by adopting a coordinated approach between cities, counties, and state government.

Critical infrastructure is the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of our nation and state, its economy, and the public's health and safety. There are essential steps to identifying and protecting critical infrastructure and key resources, 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, man-made, and technological events. Critical infrastructure and key resources 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.

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. Presidential Policy Directive 21 identifies the 16 critical infrastructure sectors as:

1. Dam Sector: supplies basic water maintenance and controls water services in the United States, including hydroelectric power, city and industrial water supplies, agricultural water systems, silt and surge control, stream route for inland mass transportation, modern waste administration, and recreation services.

2. Financial Services Sector: aims to protect our country's most vital source of economic vitality.

3. Energy Services Sector: powers the U.S. economy of the 21st century. Without a steady energy supply, the wellbeing and welfare of citizens are undermined, and the U.S. economy cannot work.

4. Nuclear Reactors, Materials, and Waste Sector: includes the nuclear infrastructure and power reactors that provide electricity to millions of Americans as well as the medical isotopes used to treat cancer.

5. Food and Agricultural Sector: nearly completely privately owned and is comprised of an expected 2.1 million farms, 935,000 restaurants, and more than 200,000 enlisted food manufacturing, processing, and storage facilities. This division represents approximately one-fifth of the country's economic activity.

6. Water and Wastewater Systems Sector: potable drinking water is essential for ensuring the general wellbeing for all humankind. Treated wastewater is indispensable for avoiding sickness. In this way, ensuring the supply of drinking water and the administration of wastewater treatment is essential to our Nation's economy.

7. Healthcare and Public Health Sector: ensures health and safety for all citizens. The benefits from this sector are mostly private which requires a coordinated effort and data sharing between the general population and private divisions.

8. Emergency Services Sector: a community of millions of highly-skilled, trained emergency personnel, along with the physical and cybersecurity resources, providing a wide range of preparedness and recovery services during both day-to-day operations and incident response.

9. Transportation Systems Sector: transportation framework rapidly, securely, and safely moves individuals and products through the nation and abroad.

10. Chemical Sector: an essential segment of the U.S. economy that produces, stores, uses and transports potentially hazardous chemicals.

11. Communications Sector: a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems. A fundamental part of the economy.

12. Information Technology Sector: key to the country's security, economy, and general wellbeing as organizations, governments, the scholarly community, and private residents are progressively reliant upon.

13. Defense Industrial Base Sector: the overall modern complex that empowers innovative work and the upkeep of military weapons frameworks, subsystems, and segments or parts, to meet U.S. military requirements.

14. Critical Manufacturing Sector: vital to a thriving economy and includes manufacturers of metals, machinery, automotive and transportation equipment and electrical equipment producers.

15. Government Facilities Sector: incorporates a wide array of buildings that are owned or rented by elected, state, neighborhood, and tribal governments.

16. Commercial Facilities Sector: incorporates many different organizations that attract individuals for shopping, business, entertainment, or hospitality, most of which are privately owned.

Objectives Protection Goal 1:

1. Develop a selection methodology for the identification and protection of critical infrastructure and key resource facilities located within the State to ensure an integrated system of resilient sectors. (6 months)

2. Record existing and undocumented information related to critical infrastructure security such as GPS locations, owner and current contact information, sector, systems, networks, and functions in the Infrastructure Protection (IP) gateway. (6-12 months)

3. 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. (12 months)

4. Assess risks, threats and vulnerabilities at identified facilities. (18-60 months)

5. Develop and implement protective and resiliency programs for infrastructure facilities. (24-36 months)

6. Improve education facilities safety by developing prevention and protection programs. (12-60 months)

7. 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)

2.4 Response Goal 1: Enhance the response to a disaster, attack, or event through the development of multiagency response teams using the finite resources of the government.

The spread of rapidly evolving and innovative technology, equipment, techniques, and knowledge presents new and emerging dangers for homeland security in the years ahead. Terrorists remain intent on acquiring weapons of mass destruction (WMD) capabilities, and rogue nations and nonstate actors are aggressively working to develop, acquire, and modernize WMD that they could use against the Homeland. Meanwhile, biological and chemical materials and technologies with dual use capabilities are more accessible throughout the global market. Due to the proliferation of such information and technologies, rogue nations and non-state actors have more opportunities to develop, acquire, and use WMD more than ever before. Georgia continues to strengthen and integrate its detection and counter-measure capabilities to address this profound risk to Georgia. Similarly, the proliferation of unmanned aircraft systems, artificial intelligence, and biotechnology increase opportunities for threat actors to acquire and use these capabilities against Georgia.

Following the September 11, 2001, attacks against the United States, Georgia expanded and developed both State and local assets to respond to any future attacks focused on Georgia. Efforts focused on explosive detection canine teams, explosive technicians, search and rescue teams (SAR), law enforcement chemical, biological, nuclear, radiological, and explosive teams (CBNRE), hazmat teams, and special weapons and tactic teams (SWAT), all with a focus on a timely response to requests for assistance. The locations and numbers of these assets was based on funding, geographic location, and support from local governments. Overtime, the missions of each of these assets has grown as the funding stream and local involvement has decreased. While still highly effective, the time to reassess the staffing, equipping, training, and locations of these assets is at hand.

Response Goal 1 Objectives:

1. Evaluate current team assignments, duties, training needs, equipment needs, and response capabilities. (6-12 months)

2. Evaluate teams geographic location to determine if assets are positioned for the most effective and robust response to an incident. (6-12 months)

3. Ensure the limited fund sources are being used effectively to provide for the most effective and robust response to an incident. (1-60 months)

4. Using data from the evaluation process; determine if teams or equipment should be remain as, expanded, consolidate, deactivated, or redeployed. (12 -36 months)

5. Evaluate and enhance unmanned aerial systems detection systems. (6-60 months)

6. Evaluate and enhance state-wide voice and data communications network used by public safety for response to manmade or natural events. (24-36 months)

2.5 Response Goal 2: Promote citizen preparedness through effective preparedness planning, volunteer opportunities, and awareness programs.

Research on preparedness shows people who believe themselves "prepared" for disasters often are not as prepared as they think. Forty percent of survey respondents did not have household plans, eighty percent had not conducted home evacuation drills, and nearly sixty percent did not know their community's evacuation routes.

Nearly twenty percent of survey respondents reported having a disability that would affect their capacity to respond to an emergency situation, but shockingly only one out of four of them had made arrangements specific to their disability to help them respond safely in the event of an emergency.

Our nation's emergency managers, firefighters, law enforcement officers, paramedics, and other emergency responders do an incredible job of keeping us safe, but they cannot do it alone. We must all embrace our individual responsibility to be prepared and in doing so, we contribute to the safety and security of the nation as well.

Individuals must take seriously the responsibility of being prepared to survive for three days on their own, to create evacuation and shelter plans for themselves and their families, and to get out of harm's way when necessary. Citizens must be engaged and educated about what they should expect from their government during emergencies as well as what the government expects from them in the form of advance preparation and responsible action. Community safety and personal preparedness is vital to the overall preparedness of Georgia, and its ability to withstand and recover from natural disasters, man-made emergencies, economic downturns, and terrorist attacks.

Community Preparedness Principles

- **Collaboration**: Government must collaborate with community leaders from all sectors for effective planning and capacity building.

- **Integration**: Non-governmental assets and resources must be fully integrated in government plans, preparations, and disaster response.

- **Personal/Organizational Preparedness**: Everyone must be fully aware, trained, and practiced on how to prevent, protect, mitigate, prepare for, and respond to all threats and hazards.

- **Volunteer Service**: Citizen activism and volunteer service provides ongoing support for community safety and critical surge capacity in response and recovery.

Community Preparedness Model

Response Goal 2 Objectives:

1. **Assessment of needs and capabilities**. State and local jurisdictions develop a community awareness, training, and preparedness process for determining the strengths and weaknesses of current emergency response planning; model community asset inventory to identify the human and material resources available or missing; guidelines for assigning response, recovery, and reconstruction responsibilities; a model emergency response exercise guide; and recovery and reconstruction planning guidelines, checklists, and model plans. The guide can then use by business and industry, schools, hospitals, correctional facilities, and neighborhood organizations. (6-60 months)

2. **Training:** Develop and enhance interdisciplinary, multijurisdictional training to encourages mutual understanding and lay the foundation for cooperation in emergencies. Educate the public on safety, help citizens take an active role in protecting themselves from harm, and teach citizens what to do in the event of a crisis. (12-36 months)

3. **Improving coordination and communication.** There is no substitute for pre-disaster planning and practice. When a disaster strikes, it is essential that government, business and industry, and volunteer groups have tested the plans

and procedures that will guide them. Develop and enhance communications programs for the coordination of preparedness training through the use of social media, web based training programs, and in-person training. (3-36 months)

4. **Management of volunteers and donated resources.** Recent major disasters demonstrated both the importance of volunteer resources and the potential for logistic nightmares. Spontaneous volunteers are invaluable in emergency response. In the first hours after an earthquake, tornado, or wildfire, bystanders make the majority of rescues, and volunteers and local citizens are often active in cleaning up. Yet the convergence of people and goods on a disaster area presents a challenge to emergency management officials — to use resources where they are most needed while restricting those that would be in the way. Ensure Response, recovery, and reconstruction plans incorporate systems for managing donated resources and training for coordination of spontaneous volunteers. Expand volunteer and donation management programs. (12-48 months)

2.6 Recovery Goal 1: Strengthen infrastructure, structural, human, and economic recovery capabilities.

Recovery begins with pre-disaster preparedness and includes a wide range of planning activities. The ability of a community to accelerate the recovery process begins with its efforts in pre-disaster preparedness, mitigation and recovery capacity building. These efforts result in a resilient community with an improved ability to withstand, respond to and recover from disasters. Timely decisions in response to disaster impacts can significantly reduce recovery time and cost. A key element of the recovery process is that the impacted community assumes the leadership in developing recovery priorities and activities that are realistic, well-planned and clearly communicated. Recovery encompasses more than the restoration of a community's physical structures to its pre-disaster conditions. Of equal importance is providing a continuum of care to meet the needs of the affected community members who have experienced the hardships of financial, emotional or physical impacts as well as positioning the community to meet the needs of the future.

The recovery process is best described as a sequence of interdependent and often concurrent activities that progressively advance a community toward a successful recovery. However, decisions made and priorities set early in the recovery process by a community will have a cascading effect on the nature and speed of the recovery progress.

Recovery Goal 1 Objectives

1. **Pre-Disaster Recovery Planning:** The speed and success of recovery can be greatly enhanced by establishment of the process and protocols prior to a disaster for coordinated post-disaster recovery planning and implementation. All stakeholders should be involved to ensure a coordinated and comprehensive planning process, and develop relationships that increase post-disaster collaboration and unified decision making. Development and enhancement of plans to identify State, locally-generated tools and resources, pre-disaster, that will serve to support and sustain disaster mitigation and recovery efforts. (3-18 months)

2. **Partnerships and Inclusiveness:** Partnerships and collaboration across groups, sectors and governments promote a successful recovery process. Partnerships and inclusiveness are vital for ensuring that all voices are heard from all parties involved in disaster recovery and that all available resources are brought to the table. This is especially critical at the community level where nongovernmental partners in the private and nonprofit sectors play a critical role in meeting local needs. Inclusiveness in the recovery process includes individuals with disabilities and others with access and functional needs, advocates of children, seniors and members of underserved populations. Sensitivity and respect for social and cultural diversity must be maintained at all times. Develop and enhance community partnerships and collaboration groups to ensure a recovery efforts are achieved in a timely manner. (12-48 months)

3. **Resilience and Sustainability:** A successful recovery process promotes practices that minimize the community's risk to all hazards and strengthens its ability to withstand and recover from future disasters, which constitutes a community's resiliency. A successful recovery process engages in a rigorous assessment and understanding of risks and vulnerabilities that might endanger the community or pose additional recovery challenges. Resilience incorporates hazard mitigation and land use planning strategies; critical infrastructure, environmental and cultural resource protection; and sustainability practices to reconstruct the built environment, and revitalize the economic, social and natural environments. Develop and promote the implementation of the National Infrastructure Protection Plan (NIPP) risk management framework to enhance the resilience and protection of critical infrastructure against the effects of future disasters. (12-60 months)

3.0 Plan Maintenance and Revision

3.1 Evaluation

GEMA/HS conducts all exercises within the structure provided by the Homeland Security Exercise Evaluation Program (HSEEP). ESFs will participate in all exercise activities when applicable and will follow the HSEEP process to include active participation in planning and evaluation meetings, workshops, and conferences.

GEMA/HS systematically coordinates and conducts event debriefings and compiles After Action Reports for any incident that calls for the activation of all or any portion of the GEOP. Necessary ESFs shall participate in this process when applicable. After Action Reports will document areas for improvement, resource shortfalls, and corrective action planning requirements which will be incorporated into subsequent updates to the GEOP, Annexes, or ESF SOGs, when applicable.

3.2 Maintenance and Revision

GEMA/HS is the agency responsible for publishing the GEMA/HS Plans Standardization and Maintenance Policy. The Deputy Director of Homeland Security oversees the update and maintenance of the 2022-2027 Strategic Plan as directed by the Board of Homeland Security. Appropriate officials in state agencies should recommend changes at any time and provide information periodically as to changes of personnel and available resources.

A full review and rewrite of the Board of Homeland Security 2022 to 2027 Strategic Plan will be conducted five years after being published or as otherwise determined by the Board.