Emergency Support Function 17 (Cyber Security) Annex to Georgia Emergency Operations Plan

2023

Table of Contents

Table of Contents iii
Record of Change iv
Record of Distribution v
1.0 Introduction 1
1.1 Purpose 1
1.2 Scope 1
2.0 Concept of the Operation 1
2.1 General 1
2.2 Plan Activation 2
2.3 Cyber Incident Severity Classification Levels 3
2.4 SOC Activation Levels 4
3.0 Organization and Assignment of Responsibilities 4
3.1 ESF Coordinator 4
3.2 Primary Agency Assignment of Responsibilities 4
3.3 Support Agency Assignment of Responsibilities 4
4.0 Direction, Control, and Coordination 5
4.1 Information Collection and Dissemination 5
4.2 Communications and Documentation 5
4.3 Administration, Finance, and Logistics 5
5.0 Plan Evaluation, Maintenance and Revision 6
5.1 Evaluation 6
5.2 Maintenance and Revision 6
6.0 Authorities and References 7

Record of Change

Change #	Date	Part Affected	Date Posted	Who Posted
1	7/6/2023	Updated format; updated content.	7/6/2023	Jonathan Baugh

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

This Emergency Support Function (ESF) 17 Cyber Security Annex supports the Georgia Emergency Operations Plan (GEOP). This document provides guidance to the mitigation of ongoing cyber incidents impacting critical infrastructure and the information sharing of cyber incidents and threat actors. In the event of a significant cybersecurity incident, ESF-17 provides 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, to minimize the impact of a cybersecurity incident. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations and potentially could impact public health, safety, or critical infrastructure.

1.2 Scope

The scope of operations for ESF-17 includes two principal functions: the mitigation of ongoing cyber incidents impacting critical infrastructure and the information sharing of cyber vectors possibly impacting other state agencies and utilities. This Annex will be activated at the discretion of the Director of the Georgia Emergency Management and Homeland Security Agency (GEMA/HS) when there is potential for or an actual disaster situation or a planned event possibly affecting cybersecurity.

2.0 Concept of the Operation

2.1 General

Through continuous coordination, in support of potential or ongoing emergency/disaster operations in Georgia, the primary and support agencies work to ensure the following capabilities:

- ESF-17 can be partially or fully activated, depending on the demands of an incident. The full activation of ESF-17 will be decided upon by GEMA/HS.
- Not all cyber incidents will require increased activation of the Georgia State Operations Center (SOC), even if ESF-17 has been engaged. The State has resources and expertise that can be used to supplement local and private sector efforts. Federal assistance may be requested to support state and local efforts if an incident exceeds state and local capabilities. Depending on the magnitude of the incident, resources from other states or the federal government may not be available for use in Georgia for as long as 72 hours after a cyber incident is detected.

- Core members of ESF-17, the Georgia Technology Authority (GTA), Georgia Bureau of Investigation (GBI), the Georgia Department of Defense (GA DOD), and GEMA/HS, will be activated for any cyber event or incident regardless of severity at SOC Level 1 (see paragraph 6.3 of the GEOP). This core group will be responsible for initiating the process of escalating response to address the needs of the incident.
- GTA's Chief Information Security Officer (CISO) will coordinate the activities of ESF-17, as instructed by the GEMA/HS Director and Incident Commander. GTA CISO may delegate actions to a named ESF-17 Cyber Incident Response Manager (CIRM) as appropriate.
- At the discretion of GEMA/HS and GTA, ESF-17 may receive a notification or situational awareness update during a low severity incident but will not be activated beyond the core members.
- Once an incident escalates from low to medium severity, ESF-17 will be partially activated.
- During a partial activation, a small contingency of ESF-17 will implement response operations under the direction of ESF-17 leadership.
- Membership of this contingency will be determined by GEMA/HS and GTA, at the time of activation, to meet the needs of the incident response.
- Once an incident escalates from medium to high severity, ESF-17 will be fully activated.
- During a Full-Scale Activation, the SOC will be operational and complete (or near-complete) membership of ESF-17 will be utilized.
- GEMA/HS will virtually activate ESF-17 as needed, to support response activities.

2.2 Plan Activation

GEMA/HS will designate an ESF-17 CIRM to coordinate with the necessary entities within the state to organize, collaborate, implement, and maintain an adequate level of cybersecurity incident response preparedness. Additionally, the designated CIRM will lead all active incident response phases to include reporting, recovery, and lessons learned.

The CIRM shall work with the affected entity, and when applicable, ensure proper inclusion of public relations, legal, human resources staff, or law enforcement resources prior to communication with any internal or external and public entities. The CIRM shall assign an initial incident severity level using the Cyber Incident Severity Classification Levels identified in paragraph 2.3 of this document.

It is critical to accurately assess and classify the potential impact of cybersecurity incidents while also utilizing a standard terminology to effectively address an incident.

2.3 Cyber Incident Severity Classification Levels

Severity	Characteristics
1 **Severe Business Impact-High**	▪ A life-safety event/issue. ▪ Critical impact to the security of data and information systems. ▪ Affects a business/mission critical System, Service, Application System. ▪ Critical equipment/network components are substantially unavailable or seriously impacting normal business operations. ▪ Errors or an outage that affects either groups of people, or a single individual performing a business/mission critical function. ▪ High impact on the operation of the business (i.e., there is no work-around available).
2 **Major Business Impact-Medium**	▪ A department or group can still use a business-critical System, Service, Application System. ▪ Equipment or network component, some functions are not available or functioning as they should. ▪ The effect of the event is such that it does not require an immediate response.
3 **Minor Business Impact-Low**	▪ A group or individual experiences issues accessing or using a System, Service, Application System or network component or a key feature thereof, but the situation does not prohibit the execution of productive work. ▪ The event does not materially affect Customer or does not cause a substantial impact but has the potential to do so if not resolved expeditiously. ▪ The effect of the event is such that it does not require an immediate response.
4 **Minimal or No Business Impact-None**	▪ An event that may require an extended resolution time, but the individual or group has a reasonable workaround while the resolution is pending. ▪ The event does not have an adverse impact on the business operations of Customer because of the nature of the fault or the small extent of the fault and an acceptable work around is already in place. ▪ The event does not require immediate resolution.

2.4 SOC Activation Levels

The State Operations Center will activate for a Cyber Security emergency in accordance with paragraph 6.3 of the Georgia Emergency Operations Plan.

During normal activities (Level 3/GREEN: Active Monitoring), the SOC is staffed by a full-time cadre operating out of the State Warning Point and augmented with 24-hour Duty Officer coverage. This level of activation may be increased to Elevated (Level 2/YELLOW) or Full-Scale Activation (Level 1/RED) at the discretion of the Governor, the Director of GEMA/HS, or designated SOC staff. The level of activation is scalable based upon the scope of the event. The SOC remains operational throughout the response phase of an event.

3.0 Organization and Assignment of Responsibilities

3.1 ESF Coordinator

The Georgia Technology Authority will lead coordination for the ESF-17 and will assume primary responsibility for coordination amongst ESF-17 primary and support agencies.

3.2 Primary Agency Assignment of Responsibilities

Georgia Technology Authority

- Maintain an updated management and technical contact list from each agency that is updated annually.
- Maintain list of mission critical applications/services and verify on an annual basis.
  - Provide Disaster Recovery (DR) or Business Continuity (BC) assistance and support coordination that may be required from GEMA/HS or GTA.
- Maintain list of critical locations that may require connectivity and back-up power support to continue operations and provide to ESF-2 Communications Lead.
- Maintain list of GTA Liaisons/contact information; validate annually.
- Coordinate exercise of the cyber portion of the disaster response plan annually (minimum tabletop).

3.3 Support Agency Assignment of Responsibilities

Georgia Emergency Management and Homeland Security Agency

- Ensure the ESF-17 Lead (GTA) has an updated management and technical contact list from each agency that is updated annually.
- Ensure mission critical applications/services are provided to ESF-17 and verified on an annual basis.
  - Provide DR or BC assistance and support that may be required from GEMA/HS.
- Ensure critical locations are identified that may require connectivity and back-up power support to continued operations.

4.0 Direction, Control, and Coordination

4.1 Information Collection and Dissemination

ESF-17 will report all activities to the ESF-5 Situation Unit for inclusion in the development of Incident Action Plans and Situational Reports. All public information reports regarding ESF-17 activities will be coordinated with ESF-15 External Affairs.

When ESF-17 is activated, the Georgia Technology Authority, with assistance from supporting departments and agencies, assesses and responds to requests for assistance with the management and/or maintenance of information technology systems and planning or technical assistance from impacted local, state, or federal agencies or other ESFs.

In addition to the response/support personnel at the SOC, ESF-17 may provide personnel to field operations established in Georgia, including but not limited to: Joint Field Offices, Joint Information Centers, Disaster Recovery Centers, and any other incident facility established to meet operational demands for each incident requiring the activation of the GEOP.

4.2 Communications and Documentation

The GEMA/HS Planning Section has provided Standard Operating Guide (SOG) development templates and planning assistance to all ESF's listed in the GEOP. ESF-17 will strive to develop operationally ready SOGs for inclusion in the GEOP. ESF-17 will meet as necessary to develop, review, and refine SOGs that discuss specific operational processes and procedures.

4.3 Administration, Finance, and Logistics

In conjunction with ESF-7 Logistics, ESF-17 Cyber Security will develop, review, refine, and maintain lists of all resources currently available and under the control of the primary or support agencies listed in this plan. The development of these lists may be completed by several organizations and professional groups, which currently operate within this ESF. These resource lists should be compliant with the resource typing standards outlined in the National Incident Management System.

Coordination of EMAC Requests

The Emergency Management Assistance Compact (EMAC) is a national mutual aid agreement between the 50 states, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia. It is based on 13 Articles which have been enacted into state law by each state. In Georgia, EMAC is addressed in the O.C.G.A., Title 38, Chapter 3, Article 5.

States may only request assistance via EMAC when their governor has declared a state of emergency. EMAC requires that the state requesting assistance reimburse the state that provides the assistance. The Director of GEMA/HS is the EMAC Authorized Representative (AR) for the State of Georgia. The AR is tasked with the authority to commit and accept resources through EMAC partnerships. The AR may delegate this authority to the Logistics Section Chief, Deputy Logistics Section Chief, and Finance Section Chief of GEMA/HS. The GEMA/HS Logistics Section Chief is the Designated

Contact (DC) for EMAC. In the absence of the Logistics Section Chief, the agency has identified alternate Designated Contacts. The DC is commonly referred to as the EMAC Coordinator. The DC coordinates EMAC operations and prepares the official EMAC Request for Assistance (commonly referred to as the REQ-A). When completed, the REQ-A becomes a contract between the requesting and assisting states for the provision of assistance in accordance with EMAC. When the SOC is activated, the Logistics Section Mutual Aid Unit coordinates and manages EMAC missions. This unit will be initially staffed with GEMA/HS personnel but will likely be augmented by trained EMAC personnel from other states as soon as possible. This unit is also referred to as an EMAC "A" Team.

When the SOC is activated, the ESF-17 will coordinate all applicable EMAC requests with the GEMA/HS EMAC DC or the SOC Logistics Section Mutual Aid Unit. No resource (personnel or equipment) may deploy to another state via EMAC until the REQ-A has been approved and signed by the ARs of the requesting and assisting states, and they have been provided a copy of the REQ-A, have been briefed and prepared for the mission. To facilitate obtaining any assistance Georgia may need via EMAC, state ESFs should identify their shortfalls in capability and where resources may be obtained to provide this capability. This may be accomplished via informal coordination with sister agencies in other states to determine if the needed resource is available for potential deployment to Georgia, its location, and the point of contact for the resource. Such information is critical in expediting a request for assistance via EMAC. For more information on EMAC, contact the GEMA/HS EMAC Designated Contact at 404-635-7200**.**

5.0 Plan Evaluation, Maintenance and Revision

5.1 Evaluation

GEMA/HS conducts all exercises within the structure provided by the Homeland Security Exercise Evaluation Program (HSEEP). ESF-17 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. ESF-17 will 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 the GEOP, its annexes or ESF SOGs when applicable.

5.2 Maintenance and Revision

This Annex will be reviewed every two years and updated as required. In addition, the document shall be evaluated for recommended revisions and corrective measures as an integral part of the Agency Exercise or Event After Action Reports / Improvement Plans, as well as internal reviews that will follow the issuance of any Governor Executive Order or passage of legislation impacting the Agency.

6.0 Authorities and References

The authority for the Georgia Emergency Operations Plan is based on Official Code of Georgia, Title 38, Section 3, Articles 1 through 3, known as the Georgia Emergency Management Act of 1981, and is compliant with the National Incident Management System and supports the National Response Framework.

O.C.G.A. § 38-3-1, to § 38-3-10, establishes legal authority for development and maintenance of Georgia's Emergency Management Program and organization, and defines the emergency powers, authorities, and responsibilities of the Governor and Director of GEMA/HS. Moreover, the State's Emergency Services and Disaster Laws require that state and local governments develop and maintain current Emergency Operations Plans to be prepared for a variety of natural and human caused hazards. Executive Orders by the Governor supplement the laws and establish specific planning initiatives and requirements.