A logo with yellow and red text

Description automatically generated

EMERGENCY SUPPORT FUNCTION - CYBERSECURITY

|  |  |  |
| --- | --- | --- |
|  | **Primary Agency:** | Local Information Technology/Operational Technology  Local Office of Emergency Management  Local Law Enforcement |
| **Support Agencies:** | Local Office of Economic Opportunity  Federal Bureau of Investigation  Cybersecurity and Information Security Agency  Florida Center for Cybersecurity  Florida Department of Military Affairs  Florida Department of Economic Opportunity |
| **I.** | **INTRODUCTION** |  |

The purpose of Cybersecurity Emergency Support Function (ESF) is to provide the state provisions for cybersecurity support before, during, and after an emergency/disaster situation.

The Cybersecurity ESF will coordinate cybersecurity resources (equipment, services, best practices, and personnel) that may be available from a variety of sources (i.e., State agencies, voluntary groups, county agencies, the cybersecurity industry, federal government agencies, and the United States security agencies) before, during or after the activation of the Emergency Operations Center (EOC) for a cybersecurity incident.

The Local Office of Emergency Management serves as the primary agency for Cybersecurity **ESF consequence management activities** and , as such, will provide coordination activities to support primary and supporting agencies for cybersecurity incidents.

# CONCEPT OF OPERATIONS

## General

Under the leadership of the OEM, Information Technology/Operational Technology (IT/OT) representatives will lead the response and recovery of a cyber-attack, and the primary and support agencies will staff the EOC when appropriate. The role of the primary agency will be to focus on coordination and ensure the management of combined agency efforts.

## Organization

## Operational Objectives

* + 1. Preparedness – AWARENESS, COMMUNICATION, TRAINING, RESOURCE SHARING
       1. Access to the Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), or Disaster Recovery (DR) Plan in strategic locations via a physical copy, thumb drive, or other means. Online versions may not be accessible during a cyber-attack.
       2. Consult county legal counsel on the steps to declare a local state of emergency to support a cyber incident for logistical needs.
       3. Consult local legal counsel to represent local government related to cyber insurance policy providers.
       4. Identify communications facilities, equipment, and personnel located in and outside the affected area that could be made available to support response and recovery efforts.
       5. Assess the need for and obtain telecommunications industry support as required.
       6. Assess needs to pre-stage communications assets for rapid deployment into the affected area.
       7. Alert and/or contact all support agencies of Cybersecurity ESF and appropriate reporting as specified by Florida Statute.
       8. Assure configuration of the War Room and Vendor Room with computers, dedicated phone lines, printers, etc. for activation as necessary.
       9. Develop scheduling for Cybersecurity ESF dedicated staff, War Room staff, and Technical Support staff as necessary.
    2. Response COMMUNICATION, EXPEDIENCY, BEST PRACTICES
       1. Identify the actual and planned actions and resources needed to support cybersecurity practices to restore services.
       2. Identify planned activity to support restoration of services that would enable impacted services.
       3. Determine what assets are available and nearest to the affected area(s) by each Cybersecurity ESF support agency and the time frame in deploying those assets.
       4. Identify communications facilities, equipment and personnel located nearest to the affected area(s) that could be made available to support recovery efforts.
       5. Coordinate the acquisition of equipment, personnel, and resources to establish temporary functional capabilities within the affected area or system.
       6. Prioritize the deployment of services based on available resources and critical needs.
       7. Accumulate damage information obtained from assessment teams (i.e., Field Support Team), the cybersecurity industry, the local county emergency operations centers, and other city/county/State agencies and report that information through the Plans Section daily.
       8. Provide specific support to the personnel outside of the EOC for full office capability at any forward assignment, including telephone, data, Internet Access, and Intranet Access,

etc.

* + - 1. Coordinate support to all governmental, quasi-governmental, and volunteer agencies impacted by cybersecurity events as required.
    1. Recovery
       1. Assess communications assets available to support a recovery. Other volunteer and local agencies with communications assets may be requested to contribute assets to the response effort. Industrial resources may also be considered for availability and effectiveness. Also, availability, operational condition, and duration of need must be considered. The logistical requirements necessary to obtain critical equipment will also be evaluated.
       2. Plan and prepare the notification systems to support the establishment of Logistical Staging Areas for necessary agencies.
       3. Review, categorize, and compare damage or impacted information obtained from all the assessment teams, cybersecurity industry, local county EOCs, and other city/county/state agencies with industry and local government sources to ensure that specific problems are clearly understood and agreed upon.
       4. Generate in a timely manner, information to be included in EOC briefings, situation reports, action plans, internal and external state agency management and/or communications industry reports.
       5. Assign and schedule sufficient personnel to cover an activation of the EOC for an extended period.
       6. Prepare and process reports using established procedures, focusing specific attention on the production of after-action reports.
       7. Maintain appropriate records of work schedules and costs incurred by Cyber-attack.
       8. Maintain appropriate tracking records of deployed equipment during event for billing and equipment retrieval.
       9. Seek information concerning the projected date the EOC will deactivate.
    2. Operations
       1. Assess the need for and obtain cybersecurity industry support as required.
       2. Prioritize the deployment of services based on available resources and critical needs.
       3. Work to resolve all conflicts regarding cybersecurity resources.
       4. Obtain information from all internally impacted departments on systems that have rendered their work inoperable.
       5. Maintain all activities on WebEOC as necessary (i.e. communications request, response, recovery, reports.)
       6. Prepare and process reports using established procedures focusing specific attention on the production of after-action reports that will be crucial for future review of Cybersecurity ESF activities and procedures.
       7. Coordinate communications support to all governmental, quasi-governmental, and volunteer agencies as required.
       8. Coordinate Cybersecurity ESF needs and time frames with the Local IT/OT responders, Office Emergency Management (OEM), and Local Law Enforcement.
    3. Mitigation

Cybersecurity ESF provides feedback to all local agencies participating involved in the cyber response, including voluntary organizations.

## Direction and Control

* + 1. The Director of Emergency Management provides support for the Cybersecurity ESF response. The Director or their Designee will manage and control the EOC to include mutual aid, Area Command, contracts for goods and services, and recovery and mitigation activities.

1. Field Support (RECON) Team: Field Support Team members from Cybersecurity ESF supporting agencies keep in contact with the EOC staff by cellular telephone, satellite phone, laptop, etc.
2. Field Operations: Agencies of Cybersecurity ESF may serve the OEM in Field Operations to perform any necessary response or recovery activities.

# RESPONSIBILITIES

## Primary Agency – Local Information Technology/Operational Technology (IT/OT)

Information Technology/Operational Technology (IT/OT) serves as the primary agency for cybersecurity response. OEM will coordinate EOC activities and manage Cybersecurity ESF activities with the other agencies.

**Primary Agency – Local Office of Emergency Management**

The Local Office of Emergency Management serves as the primary agency for Cybersecurity ESF consequence management activities and, as such, will provide coordination activities to support primary and supporting agencies for cybersecurity incidents.

**Primary Agency – Local law enforcement**

Local Law Enforcement serves as the primary agency for investigating cybersecurity incidents. OEM will provide coordination activities to support primary and supporting agencies for cybersecurity incidents.

## Support Agencies

The Florida Digital Service Department (FLDS) coordinates with other state agencies and communications entities that support cybersecurity incident response and recovery efforts for Cybersecurity ESF.

1. **Local Office of Economic Opportunity** – Coordinates economic response to assist with recovery.
2. **Federal Bureau of Investigation (FBI)** – Conduct appropriate law enforcement and national security investigative activity, like collecting evidence and gathering intelligence; Mitigate the immediate threat; Identify disruption activities; and facilitate information sharing and operational coordination with asset response personnel.
3. **Cybersecurity and Information Security Agency (CISA)** – Activates to the municipality affected as needed should the level of severity of cybersecurity incident require it, as specified by FDLE and FLDS
4. **Florida Center for Cybersecurity (CyberFL)** – serves in an advisory capacity to support affected municipalities with additional training and resources, vulnerability assessments as required, and assistance with after-action reports.
5. **Florida Department of Military Affairs** – provides National Guard cyber unit activation as needed for specific level of severity of cybersecurity incident, as specified by FDLE and FLDS
6. **Florida Department of Economic Opportunity (FDEO)**
7. **FINANCIAL MANAGEMENT**

Per State Statute 282.3186, municipalities experiencing a ransomware incident may not pay or otherwise comply with a ransom demand. All requests for cybersecurity incident services must originate through the SEOC WebEOC system. Once entered into WebEOC and tasked, Cybersecurity ESF will initiate action.

# REFERENCES AND AUTHORITIES

All references and authorities are available in the Florida Digital Service (FLDS) ESF 20 Library, as well as through guidance from House Bill 7055 and Florida State Statutes 282.3185.