EMERGENCY SUPPORT FUNCTION 20 – CYBERSECURITY ANNEX

PRIMARY AGENCIES: Florida Digital Services (FL[DS]) – Department of Management Services (Lead), Cyber Crime Office & Office of Statewide Intelligence – Florida Department of Law Enforcement, Florida Division of Emergency Management

SUPPORT AGENCIES AND ENTITIES: Florida Department of Military Affairs, Florida Department of Economic Opportunity.

FEDERAL PARTNERS: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, Multi-State Sharing and Analysis Center, Federal Bureau of Investigation, National Cybersecurity and Communications Integration Center

I. INTRODUCTION

A. PURPOSE

Emergency Support Function 20 (ESF-20) – Cybersecurity is established for FL[DS] to provide consultation and support to State Emergency Response Team (SERT) and the State Emergency Operations Center (SEOC) for cybersecurity incident monitoring and response during SEOC activation. Events requiring FL[DS] consultation and support includes, but is not limited to:

- A cybersecurity incident or an event caused by a cybersecurity incident.
- An event creates the potential for cybersecurity incidents.

ESF-20 will integrate cybersecurity personnel from support agencies and entities to provide awareness and technical expertise to the SERT during SEOC activations. SEOC activation is determined in accordance with the State Comprehensive Management Plan, incorporated by Rule 27P-2.002, F.A.C. The following definitions apply to the ESF 20 – Cybersecurity Annex.

Florida Statute defines cybersecurity to mean the protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of data, information, and information technology resources s. (282.0041(8), F.S.). .

An incident is defined as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.(*See* 44 U.S.C. § 3552(b)(2).) For purposes of this annex, a cybersecurity incident may include but is not limited to a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

B. SCOPE

The scope of this functional annex is to establish ESF-20 – Cybersecurity as an operational emergency support function within the SEOC. This annex assigns roles and responsibilities among primary and support agencies, describes the operational

priorities of the ESF, and sets policies and procedures for the coordination of state, federal, and private entities as it relates to a cybersecurity incident. Nothing in this annex supersedes the procedures established in the main body of the State Comprehensive Emergency Management Plan unless the supersession is specifically stated in this annex.

C. OBJECTIVES

The standing objectives of ESF-20 – Cybersecurity are to:

1. Provide support to SERT for monitoring and coordinating cybersecurity incident response for state, federal, and private sector partners impacted or potentially impacted by a cybersecurity incident that requires the activation of the SEOC.

2. Provide support and coordinate cybersecurity incident response with SERT Command in the event the SEOC is compromised by a cybersecurity incident.

3. Support and coordinate situational awareness and information sharing among primary and support agencies identified within this annex relating to cybersecurity incidents.

4. Advise SERT on potential impacts to cybersecurity infrastructure in the event of a non-cyber specific event.

II. ORGANIZATION

ESF-20 is a partnership of multiple state agencies and offices with the support and guidance from federal partners. The primary entities are those that are responsible for maintaining the ESF, establishing performance goals in coordination with the SERT Chief, and coordinating with support entities needed for ESF staffing for cybersecurity incident response.

A. PRIMARY AGENCIES

1. Florida Digital Service, within the Florida Department of Management Services. The Florida Digital Service will serve as the ESF lead.

2. Cyber Crime Office, an office within the Florida Department of Law Enforcement.

3. Office of Statewide Intelligence, an office within the Florida Department of Law Enforcement

4. Florida Division of Emergency Management, an agency within the Executive Office of the Governor.

B. SUPPORT AGENCIES AND ENTITIES

The following agencies are considered support entities. They will be included in situational awareness and coordination activities:

1. Florida Department of Military Affairs

2. Florida Department of Economic Opportunity

In the event of a cybersecurity incident, ESF-20 may request assistance from other state agencies for cybersecurity and information technology resources. If a state of emergency has been declared and a State Coordinating Officer (SCO) appointed, the SCO may mission tasks agencies to provide resource support.

Requesting State Agency Support

In the event of a cybersecurity incident, ESF-20 may request assistance from other state agencies for cybersecurity and information technology resources. In addition, the ESF Lead has authority to request staff augmentation for ESF-20 from all State agencies that have cybersecurity staff. In the event that additional staffing is required but cannot be sourced from state agencies, the ESF-20 Lead should elevate the need to the SERT Chief to consider mission tasking state agencies to provide support, or to explore the use of contracting staff. If a state of emergency has been declared and a State Coordinating Officer (SCO) appointed, the SCO may mission tasks agencies to provide resource support.

C. Federal Partners

The following federal entities are considered partners of ESF-20. ESF-20 will coordinate to provide and receive situational awareness, best practices, and be made aware of coordination opportunities with other states.

1. US Cybersecurity and Infrastructure Security Agency

2. Department of Homeland Security

3. Multi-State Sharing and Analysis Center

4. Federal Bureau of Investigation

5. National Cybersecurity and Communications Integration Center

In the event the SEOC is activated in response to a cybersecurity incident, ESF-20, through the SERT Chief, may request a liaison from the above and other federal entities to provide representation at the SEOC.

D. Roles and Responsibilities

Primary Agencies

Florida Digital Services

- Serve as ESF-20 Lead within the SEOC.
- Coordinate overall response and recovery of a cybersecurity incident.

- Manage requests for resources required to address impacts of a cybersecurity incident.
- Coordinate activities and information between the SERT and other ESF-20 partners.
- Coordinate with FDLE to assess of the vulnerability of computer networks, telecommunications systems, radio, and internet services used for routine and emergency operations during a cybersecurity incident.
- Provide stand-by contractor support for response to a cybersecurity incident.
- Oversee ESF development and training in coordination with FDEM.

Florida Division of Emergency Management

- Provide at least one liaison to staff ESF-20.
- Coordinate with FDEM Bureaus for emergency management trainings and exercises.
- Ensure situational awareness from the SEOC is provided to ESF-20 in event ESF-20 is not activated.
- Provide subject matter expertise on FDEM managed systems, including WebEOC, AlertFlorida, Salesforce, and other applicable systems.

Florida Department of Law Enforcement

- Provide at least one liaison to staff ESF-20.
- Coordinate sharing of law enforcement sensitive information to and from ESF-16 and the Florida Fusion Center.
- Ensure ESF-20 staff and SERT Command Staff are provided appropriate briefings on cybersecurity incidents that are or may impact emergency management functions.

FDLE Office of Statewide Intelligence

- Coordinate and prepare information for dissemination to government and/or critical infrastructure partners as required and/or appropriate with ESF-20 partners.
- Collect and analyze law enforcement information following the incident's conclusion.
- Coordinate notification process and information flow to response partners and NCCIC.

FDLE Cybercrime Office

- Serve as lead point of contact for ESF-20 on law enforcement sensitive information.

SUPPORT AGENCIES AND ENTITIES

Florida Department of Military Affairs

- Integrate into ESF-20's information sharing structure.
- Provide a liaison to ESF-20 if requested by the ESF-20 lead or SERT Chief.
- Collect, analyze, and share cybersecurity threat and vulnerability information with appropriate agencies/entities on affected state, local, and private sector critical infrastructures if available and appropriate.
- Provide awareness on available FLNG incident response and recovery resources such as information assurance, applications, and network operations personnel, for affected state, local, and private sector partners.

Florida Department of Economic Opportunity

- Integrate into ESF-20's information sharing structure.

- Provide a liaison to ESF-20 if requested by the ESF-20 lead or SERT Chief.
- Assess the commercial and economic impacts of cybersecurity incidents.
- Coordinate with ESF-14 on targeting messaging for private sector partners.
- Coordinate with ESF-20 to determine approved information sharing guidelines for the Virtual Business EOC.

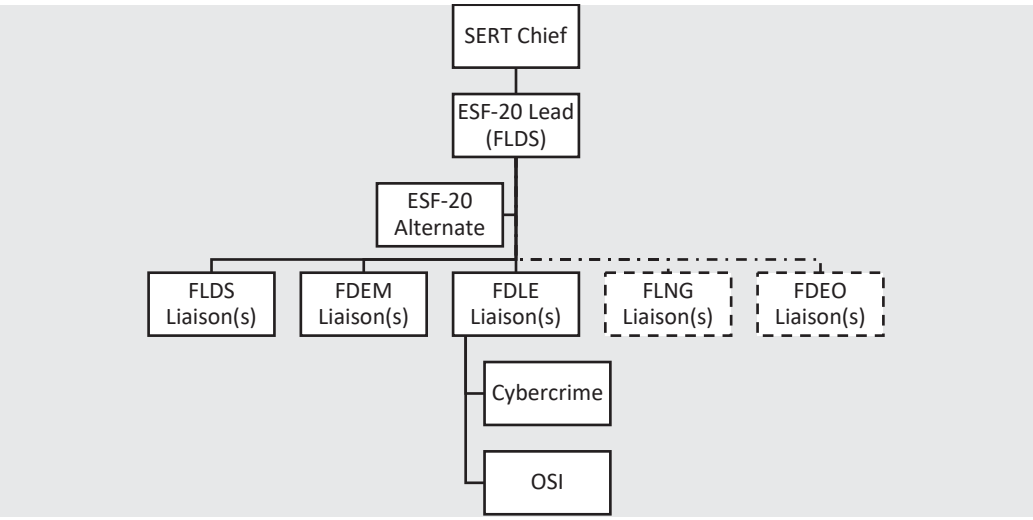
E. COMMAND AND CONTROL

ESF-20 adopts the core command and control structure as described in the Base Plan of the CEMP. Specifically, ESF-20 reports directly to the SERT Chief or his/her designee. The State Chief Information Officer (housed within FL[DS]), or their designee, will serve as ESF-20 Lead. The ESF-20 Lead will appoint an alternate to serve as a deputy for ESF-20 functions. This ESF-20 Alternate Lead will be a staff member of FL[DS].

FL[DS], FDEM, and FDLE will appoint one or more designated staff to serve as liaisons within ESF-20. The individuals appointed are expected to be located physically in the SEOC to attend all meetings and to coordinate with the ESF-20 Lead and the SERT, as well as provide information to and from the FDEM emergency coordination officer or designee.

As part of the command and control structure, ESF-20 will coordinate with the Florida National Guard (FLNG), and FL Department of Economic Opportunity Emergency Coordinating Officer (FDEO ECO) or their designee to provide situational awareness as appropriate.

Organizational Chart



III. CONCEPT OF OPERATIONS

A. PREPAREDNESS ACTIVITIES

ESF-20 does not supplant the roles and responsibilities of any existing cybersecurity preparedness entities at the local, state, or federal level. Rather, the preparedness goal of ESF-20 is to ensure there is coordination and advocacy for cybersecurity as it relates to emergency management and consequence identification.

Information Sharing and Situational Awareness

The primary preparedness function of ESF-20 is to establish and enforce a cybersecurity information sharing protocol between the FL[DS], FDLE, and FDEM. This ensures that the primary cybersecurity partners are able to monitor ongoing threats that could cascade into requiring either a state response or enhanced monitoring of the SEOC. Nothing in this annex should be considered to override existing rules as it relates to cybersecurity and law enforcement sensitive information sharing. This annex also does not change the federal reporting requirements of any state agency.

Information on cybersecurity incidents received by ESF-20 will be shared with both the Florida Fusion Center and the State Watch Office. If the incident involves a disruption at a critical infrastructure facility that impacts its ability to perform mission critical functions, the State Watch Office will provide situational awareness to the appropriate ESF and county partners.

Information on cybersecurity incidents received by either the State Watch Office or the Florida Fusion Center will be shared with each other, as well as with ESF-20. While some information will be considered law enforcement sensitive and exempt from sharing, at minimum, the following information should be shared:

1. Facility / Entity Name and Address
2. Mission Critical Functions of Facility
3. Extent of Disruption
4. Estimated Restoration
5. Extent of State Involvement in Response if any

Training and Exercises

Annually, ESF-20 will assess the current capabilities of the ESF and SEOC as it relates to an emergency management response to a cybersecurity incident in line with FDEM's Integrated Preparedness Plan. As part of this assessment, ESF-20 shall identify gaps and recommend potential trainings and exercises to the SERT Chief and FDEM's State Training Officer.

ESF-20 should participate in SEOC exercises, as requested, and is encouraged to participate in other exercises to maintain awareness of other ESFs and SEOC functions.

B. ALERT AND NOTIFICATION

Utilizing the information sharing structures established in the Preparedness phase, ESF-20 will receive information regarding cybersecurity incidents throughout the state.

Upon reviewing notifications, ESF-20 will determine the need to advise the SERT Chief and FDEM on the recommendation to increase the SEOC activation level. ESF-20 will utilize the information below to determine the need to recommend further action.

Cybersecurity Incident Severity Schema

The United States Federal Cybersecurity Centers, in coordination with departments and agencies with a cybersecurity or cybersecurity operations mission, adopted a common schema for describing the severity of cybersecurity incidents affecting the homeland, U.S. capabilities, or U.S. interests. The schema establishes a common framework for evaluating and assessing cybersecurity incidents to ensure that all departments and agencies have a common view of the:

- The severity of a given incident;
- The urgency required for responding to a given incident;
- The seniority level necessary for coordinating response efforts; and
- The level of investment required of response efforts.

The table below depicts several key elements of the schema.

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

Observed Actions	Intended Consequence[1]
Effect	Cause physical consequence
	Damage computer and networking hardware
Presence	Corrupt or destroy data
	Deny availability to a key system or service
Engagement	Steal sensitive information
	Commit a financial crime
Preparation	Nuisance DoS or defacement

Community Lifeline Impacts as a Trigger

In conjunction with the Cybersecurity Incident Severity Schema, ESF-20 will utilize impacts to Community Lifelines to determine the need to recommend SEOC action.

Utilizing Community Lifelines as a guide will allow ESF-20 to focus on the consequence of the cybersecurity incident. In principle, if a cybersecurity incident inhibits the capabilities of a jurisdiction or entity to the extent that a Community Lifeline is disrupted anywhere in the state, then ESF-20 should elevate the incident to the SEOC and ensure other ESFs are notified.

The table below lists the Community Lifelines, their subcomponents, and what SERT ESFs are involved with those subcomponents. ESF-20 should consult with the applicable Lifeline ESFs to determine the recommendation for SEOC actions.

Community Lifeline	Subcomponent	ESFs Involved
Safety and Security	Law Enforcement	ESF 16
	Fire Service	ESF 4/9
	Search and Rescue	ESF 4/9
	Government Service	ESF 7
	Community Safety	ESF 4/9, 16
Food, Water, Shelter	Food	ESF 6, 11, 15, 18
	Water	ESF 6, 11, 15, 18
	Shelter	ESF 6, 18
	Agriculture	ESF 17
Health and Medical	Medical Care	ESF 8
	Public Health	ESF 8
	Patient Movement	ESF 4/9, 8
	Medical Supply Chain	ESF 7, 8
	Fatality Management	ESF 8, 16
Energy	Power Grid	ESF 12
	Fuel	ESF 19
Communications	Infrastructure	ESF 2
	Response Communications	ESF 2, 4/9, 16
	Alerts and Warning	ESF 2, 5, 14 16
	Finance	ESF 18
	911 and Dispatch	ESF 2, 4/9, 16
Transportation	Highway and Roadways	ESF 1/3
	Mass Transit	ESF 1/3
	Railway	ESF 1/3
	Aviation	ESF 1/3
	Maritime	ESF 1/3, 19
Hazardous Materials	Facilities	ESF 10
	HazMat	ESF 8, 10
	Pollutants	ESF 8, 10
	Contaminants	ESF 8, 10

Alert and Notification for Non-Cybersecurity Events

ESF-20 adheres to the alert and notification procedures as described in the Base Plan of the CEMP as it relates to non-cybersecurity specific events. ESF-20 will on occasion receive situational awareness from FDEM on other events and may be asked to activate into the SEOC. This request will come from either the SERT Chief or by an automated message from FDEM's mass notification system.

C. MOBILIZATION

Upon the decision to activate, ESF-20 will be notified either directly by the SERT Chief, or via an automated message from FDEM's mass notification system. This notice will include a report time. The mobilization time will vary based on the event and can be as short as one hour for a no-notice event.

Physical Staffing of the SEOC

When activated, ESF-20 will be expected to staff at least one ESF-20 member on the SEOC floor at a desk specified by the Operations Section. This staff will serve as the primary point of contact between ESF-20 and the rest of the SERT. During a cybersecurity specific incident, ESF-20 may be required to provide additional staffing on the SEOC floor, to include 24-hour staffing. During a non-cybersecurity specific event, ESF-20 Lead will work with the SERT Chief to determine a reasonable staffing plan for the ESF.

Virtual Staffing of the SEOC

Recognizing that ESF-20 members have specialized equipment and resources at home agencies, it is anticipated that ESF-20 will have a remote footprint of activated staff. These staff are still required to coordinate with the ESF-20 Lead to ensure there is a unified effort. The SEOC utilizes web conferencing and team collaboration software that can be utilized by ESF-20 to maintain coordination among the team. The SERT Chief retains the right to direct that remote staff relocate physically to the SEOC should the event require it.

The ESF-20 Lead is required to keep a roster of remote staff by day. Remote staff are required to keep track of hours worked for the SEOC and be prepared to provide to the SEOC.

D. EXECUTION

Cybersecurity Specific Event

During a cybersecurity specific incident, ESF-20 will have the following standing orders:

1. Staff the SEOC and serve as part of the Unified Command Group providing subject matter expertise on cybersecurity-specific information.

2. Provide technical coordination with impacted entities and provide operational guidance to SEOC based on impacted entity reports.
3. Coordinate with federal and state agencies and entities involved in the cybersecurity law enforcement and response mission and provide relevant updates to the SEOC.
4. Provide regular updates to the SERT Planning Section for publishing in situation reports.

Scope of Activities

Once activated for a cybersecurity specific incident, it is not the mission of ESF-20 to respond directly to the cybersecurity incident, rather it is to assist the SEOC in response. The primary goal of ESF-20 is to assist the SERT Command staff to comprehend the actual, likely, and potential impacts of the cybersecurity incident. Leveraging partnerships both in and out of the SEOC, ESF-20 will attempt to provide the SERT information on the extent of service disruption or data breach, the estimated restoration time, core partners, and potential cascading impacts. This information will allow the SERT to direct its efforts to minimize the negative impact of the incident.

Information Sharing

ESF-20 will be expected to regularly share information with SERT Partners, to include state government, county emergency management, private sector partners, and the general public. The specific details shared with each stakeholder will vary due to the sensitivity of the information, and the SERT expects ESF-20, in coordination with ESF-14 (External Affairs) to determine the level provided to each partner. ESF-20 will also work directly with ESF-14 to assist in creating public messaging and executive talking points for public dissemination. If a Joint Information Center (JIC) is established, ESF-14 may request a dedicated subject matter expertise in cybersecurity to be embedded with the JIC for public information generation purposes.

Coordination with Federal Partners

ESF-20 shall directly coordinate with the appropriate federal entities as it relates to a cybersecurity incident. In consultation with ESF-20 and the SCO, the SERT Chief will request a liaison from the Cybersecurity and Infrastructure Security Agency (CISA) for any incident that requires a SEOC response. The CISA Liaison will embed with ESF-20 for information sharing and technical expertise.

Non-Cybersecurity Event

ESF-20 will initially activate for Non-Cybersecurity events to ensure they are in briefed on the current circumstance and to determine if there is a potential for a cascading impact that could result in a cybersecurity incident. Once the assessment is completed, the ESF-20 Lead will discuss with the SERT Chief regarding ongoing staffing needs.

During an SEOC activation that does not involve a cybersecurity incident, ESF-20 may be requested by FDEM to assist with monitoring system security and providing

enhanced guidance on cybersecurity practices relevant to the SEOC. In general, it is anticipated that this request will be for a specific and limited timeframe to augment a temporary limitation.

E. DEMOBILIZATION

The ESF-20 Lead shall monitor ongoing staffing needs and coordinate with the SERT Chief on the need for ESF-20 activation. The SERT Chief retains the discretion to demobilize ESF-20 from the SEOC. Once the notice to demobilize is given to the ESF-20 Lead, the lead will notify the other members.

Prior to demobilization, all ESF-20 staff are expected to provide any after-action comments to the Planning Section Chief as designated by the SERT Chief.

F. RECOVERY

After a response shifts to the recovery phase, ESF-20 is expected to remain engaged for the purpose of providing subject matter expertise to FDEM Recovery Bureau Staff as they coordinate with federal entities on reimbursement for operational expenses. In the event that a Joint Field Office or other Recovery Office is opened that requires a cybersecurity subject matter expert, ESF-20 will coordinate the staffing of that expert.

ESF-20 will ensure that all time worked, and all operational costs are provided to FDEM Recovery staff upon request.

IV. ADMINISTRATION

ESF-20 adheres to the administration procedures outlined in the Base Plan of the State CEMP with no variation.

V. REFERENCES AND AUTHORITIES

- Section 282.0051 Florida Statutes
- Section 282.318 Florida Statutes
- Section 815.06 Florida Statutes
- Presidential Policy Directive 41, United States Cyber Incident Coordination
- National Association of State Chief Information Officers Cyber Disruption Response Planning Guide
- Department of Homeland Security 2020 National Preparedness Report
- Framework for Improving Critical Infrastructure Cybersecurity, 2018

- Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 2013
- National Cyber Incident Response Plan, 2016
- National Security Strategy, 2017