State of Connecticut

Cyber Disruption Response Plan

April 2024

CYBER DISRUPTION RESPONSE PLAN

Approved by: _____ Date: 5/2/2024

Mark Raymond, Chief Information Officer, CT DAS/BITS

Approved by: _____ Date: 5/6/24

Justin Hickey, Acting Chief Information Security Officer, CT DAS/BITS

Approved by: _____ Date: 5/6/24

Brenda Bergeron, Deputy Commissioner, CT DESPP/DEMHS

Approved by: _____ Date: 5/7/24

Ronnell A. Higgins, Commissioner, CT DESPP

RECORD OF REVISIONS

Revision Number	Date	Page/Section Changed	Changed By
1	July 2018	Initial plan developed	Brenda Bergeron
2	Dec 2022	Review and update the entire plan	Sheri DeVaux
3	November 2023	Operational Revisions and Correction of Typographical Errors	Brenda Bergeron
4	April 2024	Update individual and unit names and complete operational revisions	Brenda Bergeron and Quentin Battisti

Table of Contents

I. Summary

A. Purpose

This Cyber Disruption Response Plan (CDRP or the Plan) is designed to provide a framework for how the State of Connecticut will respond to cyber-attacks, and to highlight the resources and responsibilities for individual agencies. The State's response will vary depending on the resources which are available or are needed by the targeted entity and the potential impact caused by the cyber-incident. Even cyber-incidents with the potential to have a significant impact on public health, safety, or critical operations may be entirely managed by the targeted organization using their own resources or with the assistance of third-party vendors. While they may not need the State's help in responding to and recovering from the cyber incident, the sharing of threat intelligence is still of great value.

Cyber-attacks may take many forms:

- Destructive attacks, such as ransomware;
- Malware attempting to steal sensitive information;
- An uncontrolled exploit, such as a worm;
- Denial-of-Services, which interrupt operations;
- Website defacements;
- Malware that steals computing resources to mine cryptocurrency;
- And even physical attacks and natural disasters which impact cyber operations.

Many cyber incidents start with an alert from an employee or a security tool that something is not working correctly or there was potentially malicious activity. Organizations should have a Cyber Incident Response Plan as part of their overall incident response plans. A Cyber Incident Response Plan template is available on the State of Connecticut's Cybersecurity Resource page, https://portal.ct.gov/connecticut-cybersecurity-resource-page. It is recommended that that all entities have an up-to-date Incident Response Plan along with current Continuity of Operations Plans to manage escalating incidents. Under that plan, it is the job of the affected entity's cyber security team to triage these alerts and differentiate between the false positives and the alerts that need to be investigated further.

Once it is confirmed, or highly suspected, that there is malicious activity on a network, organizations should start working through their incident response plans.

Cyber incidents have the potential to overwhelm or disable government resources at the local level and potentially at the state level as well. Collaboration between the private sector and all levels of government is essential for preventing and responding to cyber-attacks. Furthermore, Cyber incidents often have cascading effects, as many organizations and networks are reliant on their partners, third party vendors, and the supply chain. Cyber incidents affecting the private sector can have an adverse effect on the government and vice versa. They can lead to disruptions in critical infrastructure, significant financial losses, and/or the theft of highly sensitive data.

B. Scope and Identification of ESF 17 State Cyber Disruption Task Force

This Plan describes the framework for state cyber incident response coordination among state agencies, federal, local, and tribal governments, and public and private sector entities with critical computer information systems or cyber response assets or capabilities. The framework may be utilized in any emergency with cyber-related issues, including significant cyber threats, disruptions, and cyber-attacks against state computer networks, critical infrastructure, or information systems. As part of the framework for a serious cyber response, an ESF 17 Cyber Disruption Task Force (CDTF) has been established. The Plan also includes an outline of the CDTF's roles and responsibilities in the coordination of rapid identification, information exchange, response, and remediation to mitigate the damage caused by either a deliberate or unintentional disruption of cyber activity. It is anticipated that every lead and supporting state agency will have at least one member on the CDTF, and federal, private sector and local members as appropriate. The CDTF may be activated upon the direction of the Governor, DESPP Commissioner or Deputy Commissioner in charge of DEMHS, State Chief Information Officer, State Chief Information Security Officer, or State Emergency Management Director. The State's Chief Information Officer or his/her designee will lead the CDTF. See Connecticut General Statutes Title 28 and State Response Framework.

This plan is part of the ESF 17 annex to the State Response Framework (SRF). Under the National Incident Management System (NIMS), Connecticut has established a Cyber Emergency Support Function, ESF 17. Cyber-related incidents may also result in the activation of Emergency Support Function (ESF) 2--Communications, ESF 5—Emergency Management, ESF 12-- Energy and Utilities, and multiple other ESFs as appropriate. Adherence to NIMS is in accordance with the Governor's Executive Order 34.

The ESF 17 CDTF is a task force of subject-matter experts specifically charged with the responsibility for preparedness, detection, alert, response, and recovery planning and implementation activities associated with potentially catastrophic cyber incidents that may affect the State of Connecticut. In addition to the CDTF, there is a statewide Cyber

Security Committee which operates as the ESF 17 "blue sky" working group, sharing information on a regular basis regarding emerging or continuing cyber threats. The Cyber Security Committee is co-chaired by the State Chief Information Officer and the Deputy Commissioner of DESPP responsible for DEMHS. At the local level, each of the five DEMHS Regional Emergency Planning Teams (REPTs) has an ESF 17 municipal working group with a lead.

Leaders of the ESF 17 CDTF Policy Group include but may not be limited to:

- DAS BITS State Chief Information Officer (lead)
- State Cyber Information Security Officer
- DESPP Deputy Commissioner, Division of Emergency Management and Homeland Security (DEMHS)
- State Emergency Management Director, CT DEMHS
- CT Intelligence Center (CTIC) Director or Manager
- CT State Police Computer Crimes Unit
- CT Military Department/CT National Guard
- Federal and State Law Enforcement
- Federal Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA).

Each entity may delegate or designate one or more individuals to serve on or advise the CDTF.

See Appendix F for Emergency Management Actions.

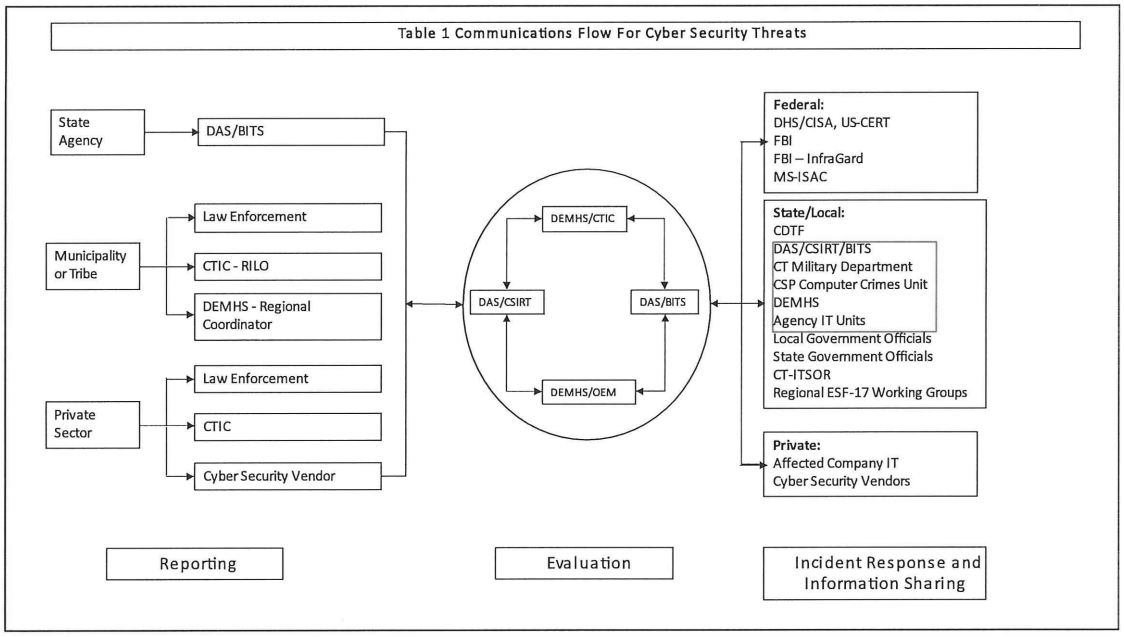
C. Initial Triage of a Cyber-Incident/Quick Reference Guide

The CT Cyber Disruption Response Plan (CT-CDRP or CDRP) is a comprehensive plan for dealing with a significant cyber incident. For a **quick reference** in the event of an imminent emergency situation, please refer to Table 1 and Table 2 (following). These provide a description of the communications flow for reporting and responding to a cyber incident, as well as the levels of disruption and appropriate response actions.

Initial Triage of a cyber incident is the responsibility of the affected organization. For State of Connecticut agencies, this falls under the Department of Administrative Services, Bureau of Information Technology Solutions (DAS/BITS) and the Chief Information Security Officer (CISO) for Connecticut. For municipalities and other public organizations, the responsibility falls under the senior executive leader, and for private organizations

under the senior executive responsible for the organization or its designee responsible for Information Technology (IT). In all cases, the affected organization should execute its Cyber Incident Response Plan, and contact the Connecticut Intelligence Center (CTIC), the State's intelligence fusion center, which will work with the affected organization to report the incident to any other appropriate officials.

D. Reporting a Cyber Incident—



Private Sector and Municipalities - All cyber incidents, especially ones that pose a moderate, high, or severe threat, [1] should be reported to local law enforcement and the Connecticut Intelligence Center (CTIC) as soon as possible. Reports may come from a government or private sector entity, or from a third-party vendor. The timely reporting of cyber incidents will greatly increase the state's ability to respond to a large-scale cyber incident. Reports can be submitted via email to ctic@ct.gov or by phone at 860-706-5500. Initial reports should include the following information:

- The location of the incident (including all affected entities)
- How and when the incident was initially detected
- A brief description of the incident
- Response actions that have already been taken

[1] For the purpose of this document, a moderate, high, or severe threat is defined as having the potential to affect public health, safety, national security, or disrupt critical systems.

- Who has already been notified (local law enforcement, Federal Bureau of Investigation, Department of Homeland Security, CTIC, etc.)
- A point of contact (name, title, phone number, email address)

Upon receipt of a cyber incident, CTIC will work to collect additional intelligence and then share the initial report with appropriate entities, which may include the FBI, DHS, CISA, DAS/BITS, and/or Connecticut State Police (CSP). The rapid sharing of information will allow each of those partners to query their databases for relevant intelligence and potentially identify resources that might be available to respond to the incident.

State Agencies - All cyber incidents affecting State Agencies should be immediately reported to the DAS/BITS Centralized Computer Security Incident Response Team (CSIRT) by contacting the Service desk at 860-622-2300. Further Incident Response information can be found on the BITS Intranet Site.

https://ctgovexec.sharepoint.com/sites/BITSSecurityRiskAndCompliance

E. Escalation of Incident Response

In the case where the affected entity's senior leadership determine that its available incident response capabilities are exhausted, or there is a potential impact on public health, safety, or critical operations, the senior leadership should have its emergency management director reach out to the DEMHS regional coordinator for additional assistance [this may include activating the State Response Framework (SRF), which in turn may include activation (partial or full) of the State Emergency Operations Center]. That will allow the State of Connecticut and its governmental and private sector partners to support incident response. The State of Connecticut's primary incident response capability is the Connecticut National Guard's Defense Cyber Operations Element, for immediate on-site incident response.

State of CT agencies and commissions should follow the procedure outlined in the Department of Administrative Services, IT Security Division, Incident Response Plan.

F. Concept of Coordination

Coordination is essential to cyber security and disruption response. As described above, the State has established a Cyber Security Committee as an ESF 17 working group of the DESPP/DEMHS Emergency Management and Homeland Security Advisory Council. This "blue sky" working group shares current information and issues related to cyber security, and includes federal, state, tribal, local, and private sector partners. This working group is primarily a policy and information-exchange group meeting under non-emergency conditions.

A second group, the ESF 17 CDTF, is a smaller, mission-centric task force designed to act quickly and in a coordinated manner to respond to a large (large in effect or large in geographical area) cyber disruption occurring in the state. The CDTF may be activated

to assist in coordinating a cyber response, including assisting in coordinating any investigation related to cyber- crimes if requested.

A cyber incident may occur without notice or may rapidly escalate. It is essential to follow the existing structure of the SRF and this plan and to act quickly to share information and communicate with subject matter experts and affected entities and communities.

DAS/BITS will act as the lead state technical agency for the cyber-related incident response component of a broader emergency unless or until the event becomes an Incident of National Significance. If the incident involves a state agency, DAS/BITS leadership will designate an Incident Commander. If the incident does not involve a state agency, the ESF-17 CDTF may function as a Unified Command or Multi Agency Policy Group.

As outlined in the State Response Framework, DESPP/ DEMHS serves as the coordination point for state response, following the National Incident Management System Multi Agency Coordination. DAS/ BITS, working with CTIC, Connecticut's Intelligence Fusion Center, will be the focal point for cyber incident information involving state computer networks. The CTIC may also work with federal and local partners, the State Cyber Security Committee/Working Group, and the DESPP Chief Information Security Officer (CISO), to collect, analyze, and disseminate cyber incident information. The CTIC may refer an incident for investigation by the DESPP/CSP Cyber Crimes Investigations Unit. The DESPP/CSP may also conduct interagency training and cross-coordination among local, state, and federal law enforcement as part of its cyber-crimes planning.

DAS/BITS responds to state agency cyber incidents by activating its Cyber Incident Response Plan and convening its Centralized Computer Security Incident Response Team (CSIRT). The DAS/BITS Security Division serves as the CSIRT. In addition, state agencies may have Information Technology Security Officers, and/or develop Security Operations Centers, who work in coordination with appropriate partners, which may include CSIRT and/or the CT Intelligence Center (CTIC).

Upon detection of an impending threat or significant event in the state or on the state computer network, the CDTF may be activated in order to determine appropriate actions to respond to and mitigate damage. The CT DESPP/DEMHS Emergency Management Director will work with the Office of the Governor, DESPP Commissioner, DESPP Deputy Commissioner for DEMHS, and State Chief Information Officer to determine whether the State Emergency Operations Center (EOC) should be partially or fully activated along with appropriate ESFs as needed. Depending on availability of infrastructure and the nature of the incident, communication with affected agencies and entities can take place using any available means. Communications may include situation status, prevention and mitigation measures, instructions for cleaning, requests

to disconnect infected machines, updates on the general health of the network, and other information.

The state's priorities remain those of protecting lives, property (physical and technological), and the environment. A component of these priorities is protection, restoration, and continuity of the state's business operations.

During a cyber incident affecting a state computer system, the CDTF will report information to the DAS/BITS Centralized Computer Security Incident Response Team (CSIRT), which will share the information with the Multi State – Information Sharing and Analysis Center (MS-ISAC), CTIC and the CISA U.S. Computer Emergency Readiness Team (US-CERT). The CDTF may also consult with the State Information Technology Officers Roundtable (ITSOR), Connecticut National Guard, the InfraGard Connecticut chapter (a Federal Bureau of Investigation (FBI)-sponsored group of public and private organizations), and/or, depending on the security requirements of the incident, the Information Systems Security Association, which shares information related to cyber and physical security or other entities as needed.

Following the SRF, the CDTF will work as needed with Department of Defense resources through the State EOC to coordinate response activities and facilitate information sharing between the State EOC and military installations and systems within the State of Connecticut. It is critical that Department of Defense operations within the State of Connecticut be kept informed and assets leveraged throughout a cyber disruption. The CT National Guard Cyber Operational Element may be called upon to assist in response to or recovery from a cyber disruption in the State.

Communications flow and information sharing are essential to a positive cyber disruption response. Table 1, above, provides a communications flow chart in a cyber incident that is likely to have an impact to public health, safety or confidence (See Table 2 Threat Matrix):

G. Cyber Security Threat Levels and Anticipated Response

Table 2 provides the Cyber Security Threat Levels identified for Connecticut, with potential impacts and general anticipated response activity. The determination of a particular threat level will be made by the State Chief Information Security Officer (CISO), in consultation with the DAS CSIRT, or, if a Level 3 or higher, with the ESF-17 CDTF:

Table 2: The Connecticut Cyber Security Threat Matrix consists of five distinct threat levels which are affected by internal and/or external cyber security events. The matrix provides general guidance for communications and anticipated response activities for each threat level.

Threat Level	Description	Potential Impact	Communication Activity	Anticipated Response Activity
Emergency	Poses an imminent threat to the provision of wide-scale critical infrastructure services	Wide spread outages, and/or destructive compromise to systems with no known remedy, or one or more critical infrastructure sectors debilitated	SEOC coordinates all communications CTDF activated	SEOC. Governor's Unified Command activated and is represented in the SEOC
Severe	Likely to result in a significant impact to public health or safety	Core infrastructure targeted or compromised causing multiple service outages, multiple system compromises or critical infrastructure compromises	Notify and activate by phone or otherwise the CDTF Notify DAS/BITS Security Division	Voluntary resource collaboration among CDTF members Info sharing Communications and messaging Possible SEOC activation
High	Likely to result in a demonstrable impact to public health, safety, or confidence	Compromised systems or diminished services	Notify CDTF Notify DAS/BITS Security Division	Real time collaboration via phone and email as required. Activity can be conducted remotely
Medium	May affect public health, safety, or confidence	Potential for malicious cyber activities, no known exploits, identified or known exploits identified but no significant impact has occurred	Contact CTIC, share with one or more agencies within the CDTF who will share with additional CDTF agencies and partners as appropriate	Information only. No follow up activity required. No real time collaboration
Low	Unlikely to affect public health, safety, or confidence	Normal concern for known hacking activities, known viruses, or other malicious activity	None required	None expected

1. Cyber Disruption Response Escalation Paths

This section provides the following information for each threat level:

- Level definition—a brief description of what each security level means;
- Escalation criteria—description of the variables that are in place for the alert level to change (De-escalation occurs when the situation has returned to the next previous level);
- Potential impact—how the level affects state agencies, the private sector, municipalities, tribes, and the public;
- Communications procedures and action steps—how the knowledgeable party communicates with the ESF-17 CDTF, the CTIC, or other response partners in order to inform affected individuals and organizations of the threat;

It is important to note that these threat levels are based on the risk an event poses and the impact it has, particularly on the state government enterprise. Incidents may require the DAS/BITS CSIRT or the ESF-17 CDTF to skip levels, and/or to address an intervening threat before returning to the originating level after that threat has been mitigated.

a) Cyber Security Threat Level 1—Low

- Definition and potential impact: Insignificant or no malicious activity has been identified. Examples include but are not limited to:
  - Credible warnings of increased probes or scans in a State network;
  - Infection by known low risk malware;
  - Other like incidents;
  - Normal activity with low level of impact.
- Communication procedures: Besides day-to-day operational communications, no additional or special communication procedures are required.

Escalation Criteria: A threat may move to MEDIUM if the state CISO, CIO or equivalent has determined that the following conditions are in place: the threat is limited to one agency, application or website, and/or; the risk of threat is low and can be easily remediated without a long-term impact to state, tribal, municipal or private sector entities or to CT residents.

b) Cyber Security Threat Level 2—Medium

- Definition and potential impact: This is the first active threat level in the cyber security threat matrix. Level 2 means that malicious activity has been identified on state, municipal, tribal, and/or private sector networks with minor impact. There is no threat to mission critical applications or resources. The threat is easily identified and can be remediated during normal working hours.

Examples include but are not limited to:

  - Change in normal activity with minor impact to IT operations;
  - A vulnerability is being exploited and there has been minor impact;
  - Infection by malware with potential to spread quickly;
  - Compromise of non-critical system(s) that did not result in loss of sensitive data;
  - A distributed denial of service attack with minor impact.

- Communication Procedures and Action Steps: All IT resources are still operational. Communications will proceed as usual, with notifications to CTIC and DAS/BEST Security Division/CSIRT and other partners as appropriate. Email will be used to provide any alerts, status reports, updates and ancillary information to critical infrastructure owners and operators. Landlines and cell phones will be used for any clarification purposes and to address questions about remediation efforts.

Escalation Criteria: In order to raise the threat level to HIGH, the threat must involve one or more agencies, entities or critical infrastructure sectors, critical applications, or websites, and/or; the risk of the threat has been determined to have significant impact(s) to state, tribal, municipal, or private sector IT or other operations.

c) Cyber Security Threat 3—High

- Definition and potential impact: Malicious activity has been identified in (state, municipal, tribal or private sector) networks with a moderate level of damage or disruption. There may be multiple web defacements; attackers may have gained administrative privileges on compromised systems, which may include access to sensitive information; issue may be remediated in one to three business days, and may require that critical applications or services be taken offline while the issue is resolved. Continuity of Operations/Continuity of Government Plans (COOP/COG) may need to be activated.

  Examples include but are not limited to:
  - An exploit for a vulnerability that has a moderate level of damage;
  - Compromise of secure or critical system(s);
  - Compromise of systems containing sensitive information or non-sensitive information;
  - More than one agency or entity affected in the network with moderate level of impact;
  - Infected by malware spreading quickly throughout the Internet with moderate impact;
  - A distributed denial of service attack with moderate impact.
- Communication Procedures and Action Steps : A Level 3-High situation means that some IT critical resources have been affected by a cyber security event or that multiple agencies have had significant security breaches. At this level, the following communications methods may be utilized:
  - If the threat occurs to the state IT system, ESF-17 CDTF will be convened by the state CIO via email, telephone, cell phone or messenger and the Team will start making preparations to enact the State Cyber Incident Response Plan;
  - ESF-17 or CIO will notify MS-ISAC via a secure portal, email or telephone. ESF-17 may also request assistance from MS-ISAC with remediating the issue;

- ESF-17, through CTIC or other means, will notify CT ITSOR and provide it with updates or remediation information;
- ESF 17 CDTF member may recommend to DESPP/DEMHS that the State Emergency Operations Center (SEOC) be activated to coordinate incident action planning, resource requests, joint information communications, etc..,
- Email will be used to communicate alerts, status reports, updates and ancillary information;
- Telecommunications such as landlines and cell phones will be used for clarification purposes and to address questions about remediation efforts.
- If the threat occurs to a municipal, tribal, or private sector IT system, and an ESF 17 CDTF team member is contacted and/or state resources are requested from one or more ESF 17 CDTF team member, the ESF 17 CDRF members will confer with each other as needed to assist as possible and to maintain situational awareness.

Escalation Criteria: To raise the state (municipal, tribal, or private sector) threat to SEVERE, the threat must have the potential to affect multiple agencies or entities and/or could require the state, other governmental entity, or infrastructure critical to public health and safey to shut down the IT infrastructure for five to ten business days to restore normal operations.

d) Cyber Security Threat 4—Severe

- Definition and potential impact: Confirmed cyber attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised state or other government IT resources and are using them to propagate the attack or to spread misinformation. Impacts to municipal, tribal or private sector infrastructure and operations will be monitored following the SRF, and requests for mutual aid will be received through the DEMHS Regional Coordinators for consideration by the ESF 17 CDTF or the SEOC, including coordinating assistance to contain or address the cyber disruption.

  Malicious activity has been identified in (state, municipal, tribal or private sector) networks with a major level of damage or disruption. Examples include but are not limited to:
  - Malicious activity affecting core infrastructure;
  - A vulnerability is being exploited and there has been major impact;

- Data exposed with major impact;
- Multiple system compromises or compromises of critical infrastructure;
- Attackers have gained administrative privileges on compromised systems in multiple locations;
- Multiple damaging or disruptive malware infections;
- Mission critical application failures but no imminent impact on the health, safety, or economic security of the state;
- A distributed denial of service attack with major impact.

- Communications Procedures and Action Steps: At Level 4—Severe, the state's IT critical resources have been severely affected by a cyber security event that has caused IT service to be offline/unreliable for an extended period of time. This event may affect telecommunications and may cause incident responders to use alternate forms of communication. In addition to steps that have been identified in the previous levels, the following may occur:
  - The ESF-17 CDTF will be notified via email if available, cell phone or messenger, will activate the Incident Response Plan, and will recommend an SEOC activation.
  - For a state network severe event, DESPP/DEMHS will recommend an SEOC activation in order to coordinate incident action planning, resource requests, joint information communications, among other actions under the National Incident Management System and the State Response Framework:
  - If the threat occurs to a municipal, tribal, or private sector IT system, and a DEMHS Regional Coordinator or an ESF 17 CDTF team member is contacted and/or state resources are requested from one or more ESF 17 CDTF team member, the ESF 17 CDRF members will confer with each other as needed to assist as possible and to maintain situational awareness. A recommendation may be made to activate the SEOC if the situation warrants state action;
  - Members of the ESF-17 CDTF will be stationed at the SEOC to ensure continued communications and subject matter expertise;
  - The ESF-17 CDTF will work with the SEOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
  - The ESF-17 CDTF will notify the MS-ISAC and request assistance if necessary.
  - Email will be used if available to communicate alerts, status reports, updates, and ancillary information.

- Pursuant to the SRF, a WebEOC incident may be opened and WebEOC used to provide situational awareness, process requests for assistance, etc…
- Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
- Messengers—Depending on the nature of the event, the state may use messengers to communicate information between incident responders, the ESF-17 CDTF, and the SEOC.

Escalation Criteria: To raise the threat level to EMERGENCY, the threat has affected multiple agencies or entities and has required or could require the state, other governmental entity, or infrastructure critical to public health and safety to shut down its IT infrastructure for six or more business days to restore normal operations.

e) Cyber Security Threat Level 5—Emergency

- Definition and Potential Impact: Unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks have an impact at the national, state, and local levels. Impacts to municipal, tribal or private sector infrastructure and operations will be monitored following the SRF, and requests for mutual aid will be received through the DEMHS Regional Coordinators for consideration by the ESF 17 CDTF or the SEOC, including coordinating assistance to contain or address the cyber disruption.

  Malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but are not limited to:
  - Malicious activity resulting in widespread outages and/or complete network failures;
  - Data exposure with severe impact;
  - Significantly destructive compromises to systems, or disruptive activity with no known remedy;
  - Mission critical application failures with imminent or demonstrated impact on the health, safety, or economic security of the state;
  - Compromise or loss of administrative controls of critical system;
  - Loss of critical Supervisory Control and Data Acquisition (SCADA) system(s).
- Communications Procedures and Action Steps: At Level 5—Emergency, the state's (or other) critical IT resources are rendered inoperable by a cyber security attack that will take weeks to recover.

Such an event will have a widespread effect on IT communications and necessitate the need for alternate forms of communication (e.g., satellite, radios, messengers). In addition to steps that have been identified in the previous levels, the following may occur:

- SEOC—The SEOC will be activated, and following the SRF, the Governor's Unified Command will meet there.
- If the threat occurs to a municipal, tribal, or private sector IT system, and an ESF 17 CDTF team member is contacted and/or state resources are requested from one or more ESF 17 CDTF team member, the ESF 17 CDRF members will confer with each other as needed to assist as possible and to maintain situational awareness. A recommendation will be made to activate the SEOC if the situation warrants state action;
- The SEOC will coordinate incident action planning, resource requests, joint information communications, among other actions under the National Incident Management System and the State Response Framework:
- Members of the ESF-17 CDTF will be stationed at the SEOC to ensure continued communications and subject matter expertise
- The ESF-17 CDTF will work with the SEOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
- The ESF-17 CDTF will notify the MS-ISAC and request assistance to remediate the issues.
- Pursuant to the SRF, a WebEOC incident will be opened and WebEOC used to provide situational awareness, process requests for assistance, etc…
- Telecommunications may become unreliable making it necessary for incident responders and first responders alike to use alternate forms of communication;
- Messengers—Depending on the nature of the event, the state may use messengers to communicate information between incident responders, the ESF-17 CDTF, and the State EOC.

H. Agency Roles and Responsibilities (see Appendix A for more complete list of Primary and Secondary Agencies under ESF 17)

When a cyber disruption occurs within the State of CT with potential widespread impacts on public safety or business and government continuity, DEMHS will be the lead coordinating agency and may take the following initial actions:

The Emergency Management Unit of DEMHS will:

- Recommend to the Governor partial or full activation of the State Emergency Operations Center (SEOC) or alternate SEOC if necessary to coordinate response and recovery activities;
- Activate the ESF 17 Cyber Disruption Task Force (CDTF) which will coordinate with the affected parties for resource and assistance requests;
- Work with other agencies to engage the CT National Guard Joint Cyber Team for on-site response;
- Activate of agency liaisons and additional ESF Task Forces to further support the incident;
- Follow the State Response Framework procedures for all-hazards response, including;
    - Coordinate briefings for the Governor and his/her Unified Command as to the proposed action plan and determine resources available;
    - Work with ESF 2 partners to establish and maintain emergency communications with affected entities and geographic areas;
    - Coordinate with the Office of the Governor, DAS BITS, and other partners to provide joint, consistent public messaging, briefings to state and local officials, and the private sector;
- If the effects of the cyber disruption warrant, on behalf of the Governor, prepare an Presidential Emergency and/or Major Disaster Declaration request and, once signed by the Governor, submit to the Federal Emergency Management Agency (FEMA) to leverage federal funds and resources;
- Coordinate the provision of additional assistance through the Federal government, the Emergency Management Assistance Compact or other interstate mutual-aid agreements.

The Connecticut Intelligence Center (CTIC) of DEMHS will:

- Coordinate intelligence collection and information sharing between the private sector and all levels of government (local, state, and federal);
- Coordinate technical support and recommendations to the victim(s) based on current threat intelligence;
- Maintain communication with the National Fusion Center Association Cyber Intelligence Network, the Northeast Regional Intelligence Group and similar organizations
- Monitor Suspicious Activity Reports and share with appropriate agencies.
- Conduct monitoring, analysis, and dissemination of information related to the cyber incident.

Division of Connecticut State Police

CSP will:

- Collect evidence which could be used in a criminal investigation by the Cyber Crimes Investigation unit (CCIU) or another law enforcement agency;
- Collaborate with CTIC on the collection of criminal intelligence;
- Work with other law enforcement partners to protect evidence, crime scenes, and investigate any potential crime.

Division of Statewide Emergency Telecommunications (DSET)

DSET will:

- Notify and work with all of the State's Public Safety Answering Points (PSAPs) depending on the type of disruption;
- Coordinate the ESF 2 Communications Task Force at the SEOC.

Connecticut Military Department/Connecticut National Guard

In addition to responsibilities outlined in the SRF, in a cyber-incident, the Connecticut National Guard's Joint Cyber Team's duties may include incident response functions, including assessment and remediation functions, reporting, coordination with federal, state, and local elements. CT Military/CTNG may also act as a conduit for other military resources or actions.

Department of Administrative Services (DAS) Bureau of Information Technology Solutions (BITS)

When a cyber-incident occurs within the State of CT's network, DAS/BITS may take the following initial actions:

- Stand up the DAS BITS Centralized Computer Security Incident Response Team (CSIRT), and/or DAS Incident Management Team (IMT) ;
- Conduct an initial assessment of affected systems/networks and develop an action plan to remediate and/or restore services;
- Follow the State Response Framework procedures for all-hazards response;
- Brief appropriate State of CT officials as to the proposed action plan and determine resources available;
- Communicate with appropriate ESF 17 Task Force leads and the SEOC if activated, or the State Emergency Management Director or his designee, to provide situational awareness where required;
- Communicate with appropriate ESF 17 Task Force leads and the SEOC if activated or the State Emergency Management Director or his designee, for resource and assistance requests;
- Facilitate communication of cyber-security related information to the state CTIC, MS-ISAC and to U.S. Department of Homeland Security/US-CERT;

DAS/BITS will also serve as the ESF 17 Technical lead of the CDTF for a large-scale event.

Department of Energy and Environmental Protection (DEEP)/Public Utility Regulatory Authority (PURA)

In addition to responsibilities outlined in the SRF, in a cyber-incident, DEEP/PURA duties include, but may not be limited to:

- Follow the State Response Framework procedures for all-hazards response;
- Follow Emergency Support Function #12 – All Hazards Energy and Utilities Annex;

- Serve as the Primary State Agency technical expert for public utility operations, including briefing appropriate State of CT officials as to the technical issues related to the situation;
    - As required support ESF 17 Task Force leads and the SEOC if activated, or the State Emergency Management Director or his designee, to provide situational awareness and expertise on public utility matters.
    - Participate in briefings for the Governor and his/her Unified Command as to the proposed action plan and how it relates to public utility operations.
- As needed Facilitate communications between ISO-NE and SEOC and state officials for responding to regional ISO-NE operating procedure (OP) No. 4, OP No. 7 and other required OPs.
- Monitor impacts of ISO-NE OPs on state and local level and facilitate communications and state and local response efforts.

CT Education Network

CEN will make reasonable efforts to provide network-based services in support of business continuity for any CEN member during a crisis.

To declare a crisis, the CEN member may contact CEN, via their member services liaison, Director, or the CEN service desk. Upon declaration, CEN will coordinate with the liaison/designate to initiate the process of aiding. CEN will attempt to offer network-based services that are deemed helpful and (1) do not unduly affect the normal operation of CEN services (2) do not conflict with agreements that CEN may have with other contractors or providers (3) do not conflict with agreements or services with other CEN members.

CEN, by request of the member in crisis, may assist as an intermediary as needed and may make efforts to contact other member institutions. Recognizing a situation as a crisis, any response or non-response shall be at the sole discretion of the CEN.

- The Member continuity policy can be reviewed at https://ctedunet.net/wp-content/uploads/sites/2510/2021/12/2019-07-02_CEN_Policy_Member_Contuinuity68.pdf

I. Additional Support

Cyber Operating Centers and private vendors/contractors may have significant responsibility for and/or involvement with cyber-related issues on behalf of

state/municipal/private sector agencies/entities. Their responsibilities include those outlined in any applicable contracts with the agencies or entities, and may also include; those outlined in this plan and the State Response Framework, and; those found within state or federal law, regulation, or policy.

II. Plan Development and Maintenance

DEMHS will ensure that this Cyber Disruption Response Plan is reviewed and updated on a regular basis. DEMHS representatives and other participating agencies will participate in after-action reviews and follow up on Plan improvements and other corrective actions following exercises and actual events.

Appendix A – State ESF 17 Agencies and Federal Resources

State Primary Agencies:

- Department of Administrative Services (DAS) [Technical]
    - Bureau of Information Technology Solutions (BITS)
- Department of Emergency Services and Public Protection (DESPP) /Division of Emergency Management and Homeland Security (DEMHS) [Coordinating]
    - Emergency Management
    - CT Intelligence Center (CTIC)

State Support Agencies: Include but are not limited to:

- DESPP Division of CT State Police (CSP)
    - CSP Cyber Crimes Investigation Unit (evidence collection and analysis, responsible for potential prosecutions)
- DESPP Division of Statewide Emergency Telecommunications
- DESPP Division of Scientific Services
- DESPP Division of Fire Prevention and Control
- CT Military Department (Army/Air National Guard Joint Cyber Team)
- University of Connecticut
- CT Education Network (CEN)
- Connecticut State Colleges and Universities
- Department of Energy and Environmental Protection (DEEP)
    - Public Utility Regulatory Authority (PURA)

Federal Resources

The federal government has a variety of resources it can provide through several different agencies to aid victims of cyber-attacks. These resources include incident response and analysis capabilities along with information sharing coordination. Furthermore, the federal government conducts criminal investigations, and the United States Intelligence Community plays a significant role in combatting malicious cyber actors abroad.

Federal Department of Homeland Security/Cybersecurity and Infrastructure Security Agency (CISA)

CISA provides services and resources to State, Local, Tribal and Territorial (SLTT) stakeholders to reduce risk and improve organizational resiliency. Reduction of risk and prevention of security incidents remains the primary mission of CISA, but when security incidents impact an SLTT entity, CISA Region 1 provides local support though coordination with

both law enforcement and other federal entities to facilitate the successful resolution of the incident.

Short of a national level security event, assistance is provided by regionally assigned Cybersecurity and Physical Security personnel that can support formal reporting of the incident to national authorities, coordination of state entities with federal counterparts and potentially consultation and advice on methods and considerations to speed recovery and restoration of services.

Further information is available at:

- Infrastructure Security Division - https://www.cisa.gov/infrastructure-security
- Cyber Security Division - https://www.cisa.gov/cybersecurity
- CISA Region 1 - https://www.cisa.gov/region-1

MS-ISAC

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a CISA-supported collaboration with the Center for Internet Security designed to serve as the central cybersecurity resource of the nation's State, Local, Territorial, Tribal governments.

United States Coast Guard (USCG)

The USCG Cyber Operations Department consists of the Cyber Protection Team (CPT) which is a deployable unit based in Alexandria, Virginia responsible for offering cybersecurity services to the Marine Transportation System (MTS), the Cybersecurity Operations Center (CSOC), and the Maritime Cyber Readiness Branch (MCRB) which focuses on cybersecurity in the commercial maritime transportation community. Their mission is to support enhance the resiliency of MTS Critical Infrastructure against cyber disruption through consistent proactive engagements with public and private industry organizations.

Further information is available at:

- https://www.dco.uscg.mil/Our-Organization/CGCYBER/
- https://www.dco.uscg.mil/Our-Organization/CGCYBER/Maritime-Cyber-Readiness-Branch/

United States Secret Service (USSS)

The Secret Service is a law enforcement agency that investigates criminal matters related to financial systems, which includes cyber-attacks.

Further information is available at:

- https://www.secretservice.gov/investigation/cyber

DHS Office of Intelligence and Analysis (I&A)

Office of Intelligence and Analysis' (I&A) mission is to equip the Department of Homeland Security and its partners with timely intelligence and information needed to keep the homeland safe, secure, and resilient. I&A is a member of the Intelligence Community (IC) and is authorized to access, receive, and analyze law enforcement information, intelligence information, and other information from Federal, state, and local government agencies, and private sector entities, and to disseminate such information to those partners

Further information is available at:

- https://www.dhs.gov/office-intelligence-and-analysis

Federal Bureau of Investigations (FBI)

The FBI has responsibility for investigating federal violations involving a range of cyber incidents perpetrated by criminals, nation-states, terrorists, or hacktivists. The FBI leverages agents, analysts, and computer scientists within its fifty-six field offices in the U.S. and Puerto Rico to conduct investigations into incidents including, but not limited to, business email compromises, ransomware, data breaches, financial account compromise and theft, and distributed denial of service attacks.

Cyber incidents affecting the State of Connecticut are the responsibility of the Cyber squad (CY-1) in the FBI's New Haven Field Office, located at 600 State Street, New Haven, Connecticut 06511, (203) 777-6311. That squad is one component of the FBI-led Connecticut Cyber Task Force, which, at present, is comprised of investigators from several federal, state, and local agencies.

Reporting: Although telephonic and in-person reporting are welcome, victims of cybercrimes are generally encouraged to report an incident to the FBI's Internet Crime Complaint Center. Timely reporting is critical in any cyber incident, particularly those involving the theft of money and IC3 has specialized teams whose function is to track and freeze-stolen funds so they can be returned to the defrauded victim.

The FBI values its various partnerships, whether that is with other federal, state, local and tribal agencies, private corporations, non-profit/community organizations, or academic institutions. In regard to private companies, the FBI's InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. There are currently 79 InfraGard chapters, including one in Connecticut.

Further information is available at:

- https://www.ic3.gov/
- https://www.fbi.gov/contact-us/field-offices
- https://www.infragard-ct.org

Appendix B - References

- US-CERT Reporting System

  https://forms.us-cert.gov/report/

- Federal Cyber Reporting Guidelines

  http://www.us-cert.gov/federal/reportingRequirements.html

- DHS/US-CERT Cyber Security Alert Bulletin

  http://www.us-cert.gov/cas/alerts/

- DHS/US-CERT Technical Cyber Security Alert Bulletin

  http://www.us-cert.gov/cas/techalerts/

- FEMA Cyber Terrorism Defense Initiative

  http://www.cyberterrorismcenter.org/

- US Coast Guard Sector Long Island Sound Cyber Incident Response Concept of Operations (April 2018 draft)

- National Council of Information Sharing and Analysis Centers: www.nationalisacs.org/

- National Cyber Awareness System: www.us-cert.gov/ncas

- The State of Connecticut General Assembly :http://www.cga.ct.gov

Appendix C - Authorities

1. **State (Selected):**
   - Connecticut General Statutes (CGS) Titles 28 and 29, including Conn. Gen. Stat. Section 28-1a(b) which makes DESPP/DEMHS responsible for coordinating state homeland security, including protocols and standards for the use of intelligence information and Conn. Gen. Stat. Section 28-5(b), which requires, among other things, the preparation of a comprehensive plan and program for the civil preparedness of the state, to be followed by state and local government agencies and others.
   - CGS 36a-701b—requires notification of breach of security re computerized data containing personal information to the person affected and to the Office of Attorney General, generally no later than 90 days
   - CGS 52-570b Action for Computer-Related Offenses
   - CGS 53a-250 Computer Crimes Definitions
   - CGS 53a-251 Computer Crime
     - (b) Unauthorized Access to Computer System
     - (c)Theft of Computer Services
     - (d) Interruption of Computer Services
     - (e) Misuse of Computer System Information
     - (f) Destruction of Computer Equipment
   - CGS 53a-252 to 53a-258 Degrees of Computer Crimes
   - CGS 53a-259 Value of Property or Computer Services
   - CGS 53a-260 Location of Offense
   - CGS 53a-261 Jurisdiction
   - CGS Section 53a-301 Computer Crime in Furtherance of Terrorist Purposes. This law makes it a class B felony if a person commits a computer crime or unauthorized use of a computer or computer network with intent to intimidate or coerce the civilian population or a unit of government. When the crime is directed against a public safety agency, the law imposes a five year mandatory minimum sentence (CGS § 53a-301).

2. **Federal (Selected):**
   - FEMA December 2017, *Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage*
   - National Cyber Incident Response Plan, DHS, December 2016
   - *Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers* --Bureau of Justice Assistance, Department of Justice, May 2015

- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)
- Homeland Security Presidential Directive-5 (HSPD-5): Management of Domestic Incidents (2003)
- Homeland Security Presidential Directive-7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection (revoked in part by Presidential Policy Directive 21)
- Department of Homeland Security National Infrastructure Protection Plan 2013 (NIPP)
- NIST Special Publication 800-55 Revision 1, Security Measurement (2008)
- NIST Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide (2012)
- The Enhancement of Non-Federal Cyber Security, The Homeland Security Act (Section 223 of P.L. 107-276) (2002)
- Federal Information Security Management Act (FISMA) (2002)
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- The Defense Production Act of 1950, as amended
- National Security Act of 1947, as amended
- National Security Directive 42: National Policy for the Security of Nation Security Telecommunications and Information Systems (1992)
- National Strategy to Secure Cyberspace (2003)
- Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunication (1984)
- Executive Order 2008-10, Executive Order Mitigating Cyber Security Threats

Appendix D – Common Acronyms, Abbreviations and Terms

CDRP - Connecticut Cyber Disruption Response Plan

CDTF – ESF 17 Cyber Disruption Task Force

CEN—CT Education Network

CIKR - Critical Infrastructure and Key Resources

CISA—Federal Cybersecurity and Infrastructure Security Agency

CISO-Chief Information Security Officer

CIO - Chief Information Officer

COOP - Continuity of Operations Plan

CSIRT - DAS/BITS Centralized Computer Security Incident Response Team

CSP - Connecticut State Police, a division of DESPP

CT - Connecticut

CTIC - Connecticut Intelligence Center, the state's designated fusion center, and part of DEMHS

DAS/BITS - CT Department of Administrative Services/Bureau of Technology Solutions

DESPP - CT Department of Emergency Services and Public Protection

DEMHS - CT Division of Emergency Management and Homeland Security, a division of DESPP

DHS I&A - U.S. Department of Homeland Security Office of Intelligence and Analysis

ESF - Emergency Support Function is a group of government and private-sector entities that provide the support, resources, program implementation, and services that are most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims and communities return to normal, when feasible, following domestic incidents.

ESF 17 – Cyber Emergency Support Function under the CT State Response Framework and Local Emergency Operations Plans

IAP - Incident Action Plan

ICS - Incident Command System

ISO New England - is an independent, non-profit electricity Regional Transmission Organization

IT - Information Technology

ITSOR - CT State Agency Information Technology Security Officers Roundtable

MS-ISAC - Multi State Information Sharing and Analysis Center

NASCIO - National Association of State Chief Information Officers

NCC - Network Control Center

NESEC - Northeast States Emergency Consortium

NESPAC - New England State Police Administrators Conference

NIMS - National Incident Management System

PSAP - Public Safety Answering Point

SEOC - State Emergency Operations Center

SOC - Security Operations Center

SRF - CT State Response Framework

US-CERT - U.S. Computer Emergency Readiness Team

USSS—U.S. Secret Service

WebEOC - An internet-based system that enables local and state agencies and private sector partners to share up-to-date emergency management information about a variety of situations and conditions.

Appendix E – Cyber Disruption Response Policy (ESF-17)

Cyber Disruption Response Policy

Policy Owner	DESPP/DEMHS
Policy Approver(s)	Mark Raymond DAS/BITS, Brenda Bergeron DESPP/DEMHS
Related Procedures	*Incident Response Procedure, Incident Response Runbooks*
Effective Date	

Purpose

The purpose of this policy is to ensure the State of Connecticut's Cyber Disruption response capabilities have a maintained quality and integrity. The response will be determined by the magnitude of the threat presented by incidents. Without a Cyber Disruption response capability, the potential exists that if a Cyber Disruption incident occurs the magnitude of harm associated with the incident could be significantly greater than if the incident were addressed and responded to in a timely manner.

Scope

The Cyber Disruption Response Policy applies to all information systems and information system components of the State of Connecticut and specifically, may include;

- State of Connecticut Enterprise Network
- Municipalities
- Critical Infrastructure Companies
- Tribal Nations

Policy Statements

Requirements:

- All ESF members are required to submit a valid Non-Disclosure Agreement annually.
- Cyber disruption response plans will be reviewed and, where applicable, revised on an annual basis. Review will be based on the documented results of previously conducted tests or live executions of the Cyber disruption response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.
- Create a response task force to lead efforts during a cyber disruption.

- The task force responsibilities include creating and maintaining an Annex to:

  - Identify Cyber Disruption response (IR) roles.
  - Identify Cyber Disruption response responsibilities.
  - Define testing methodologies and tests. Include the following capabilities:
  - Execute tests. Tests can come in different forms:
  - Perform an After-Action Review and develop an improvement plan.

- Operate the Cyber Disruption response capability.
  - Categorize incidents according to established standards to establish appropriate subsequent processes.
  - Analyze discovered threats:
  - Recommend methods to contain threats to minimize impact and maintain operations:
  - Recommend methods to eradicate contained threats and recover to normal operations:
  - Perform post-recovery tasks.

- To facilitate incident response operations, responsibility for incident handling operations will be assigned to ESF-17. In the event that an incident occurs, and the magnitude meets *(what Threat Level)*, the members of this team will be charged with executing the Cyber Disruption Response plan under the State Response Framework. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations as outline in the State Agency Training and Exercise Program.

- Cyber disruption response should be tested annual using tabletop exercises, simulation tests, or through the use of a full-scale test. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. An After-Action Review will be performed, and an Improvement Plan documented and shared with key stakeholders.

Appendix F--Emergency Management Actions

A. Prevention and Mitigation Activities

Agencies and organizations conduct the following activities on an ongoing basis:

- Monitor computer network systems for unauthorized activity;
- Attempt to ensure network protection and defense systems are correctly patched and up to date;
- Consider risk assessments to determine broad implications from ongoing cyber activity within computer networks and identify network vulnerabilities;
- Monitor events, and share and collect information among or between: State Cyber Security Committee/Working Group; Connecticut Intelligence Center (CTIC); CT State Agency Information Technology Security Officers Roundtable (ITSOR), and/or; CDTF members that may indicate the development of a regional catastrophic cyber incident;
- Develop, maintain, update, and exercise an Agency Continuity of Operations Plan (COOP), including (1) identifying critical functions that could or would be affected by a cyber incident and (2) pre-planning for how these functions will continue to be performed while cyber capabilities are not available;
- DEMHS, including CTIC and Emergency Management, the DESPP CISO, the CSP Cyber Crime Investigations Unit, the DAS/BEST IT Security Unit and the federal CISA, will collaborate with government and private sector entities throughout Connecticut to provide regular operational and information security briefings. Regular cyber threat briefings will be provided at large venue meetings, conferences, exercises, and other government and private sector settings as requested and appropriate to ensure continual education of current threat picture, cyber response framework, and mitigation strategies;
- Ensure that DAS/BEST maintains updated contact information for agency security liaisons and IT managers, including off-hours contact information;
- Ensure that individuals with responsibilities that include identifying, responding to, investigating, or recovering from a cyber incident receive ongoing training and have opportunities to continue their education in the discipline.

B. Preparedness Activities

Activities to prepare for response to a cyber incident include but are not limited to:

- Identify and resolve legal issues relating to response and recovery from a cyber incident;
- Stay abreast of trends in cyber security prevention, preparedness, response, recovery, and mitigation;
- Identify threats and vulnerabilities to the entity's or agency's network and IT systems/applications, including to the State network and systems/applications;
- Identify mitigation measures (e.g. plans, procedures, hardening measures, etc.) for threats and vulnerabilities;

- Develop redundant communications means and methodologies to enable intra- and extra-jurisdictional transactions;
- Develop plans and procedures to address specific disruptions, including COOP planning described above;
- Develop cyber threat related training and exercises to be held on a regular basis and/or integrate cyber issues into existing training and exercises;
- Communicate with other jurisdictional CDTF representatives to exchange best practices and information pertinent to preparing for catastrophic cyber-related incidents.

C. General Response Activities

Response activities in a cyber disruption include but are not limited to:

- Conduct or cooperate with investigative duties including scene security, interviewing, investigation, computer forensic analysis, reporting, and prosecution support (ESF 13 coordination, which may include DESPP/CSP Cyber Crimes Investigation Unit, local ESF 17 and cyber crimes task forces, and federal law enforcement partners);
- Request activation of the SRF and the State Emergency Operations Center (SEOC) to support the coordination of activities;
- Monitor events, and share and collect information among or between regional EOCs and/or CDTFs that may indicate the development of a regional catastrophic cyber incident, using procedures established in the SRF (e.g., use of WebEOC by state, local, nongovernmental agencies to provide situational awareness, track response to requests for assistance);
- Provide situational awareness and subject-matter expertise and recommend solutions for the SEOC during a response, including:
- Physical presence of one or more CDTF members at the SEOC to assist Governor's Unified Command and SEOC Command Staff, including Operations, in understanding and managing resources to respond to technical and operational issues regarding cyber-related resources and networks;
- Physical presence of one or more CDTF members at the SEOC to assist Governor's Unified Command, including SEOC Planning Section, in the development of priorities and objectives of a long-term response to a catastrophic incident. Objectives and activities become the key elements of an action plan for a determined operational period, set out for the Incident/Unified Commander in an Incident Action Plan (IAP) or Regional Incident Action Plan (RIAP).
- Provide CDTF representatives for other jurisdictions with situational awareness and assistance during a catastrophic event as necessary and possible.
- Share early warning information with all CDTF members, including with CTIC, for federal and regional distribution. Ensure that notifications to MS-ISAC, US-CERT, Fusion Center Cyber Intelligence Network, and NCCIC take place in

order to mitigate other potential threats and assess the attacks or incident's reach.

- Coordinate IT-related intra- and inter-jurisdictional response activities.
- Coordinate with Governor's Unified Command/Multi-Agency Policy Group, SEOC Command staff and state Emergency Support Functions (ESFs), including ESF- 2 (Communications), ESF-3 (Public Works, Critical Infrastructure), ESF-5, (Emergency Management), ESF-7 (Resource Support/Private Sector Coordination), ESF-12 (Energy and Utilities), ESF-13 (Law Enforcement) and ESF 17 (cyber) liaisons to procure critical cyber-related resources via all possible avenues, including the Federal government, and existing interstate and international mutual aid agreements.