State of Connecticut

Cyber Disruption Response Plan

August, 2018

CYBER DISRUPTION RESPONSE PLAN

Approved by:______________________________ Date: 10/17/2018

Mark Raymond, CIO
State of CT/DAS

Approved by:______________________________ Date: 10/17/18

William Hackett, Deputy Commissioner, CT DESPP/DEMHS
State Emergency Management Director

Approved by:______________________________ Date: As of: Aug 31, 2018

Dora B. Schriro, Commissioner
State of CT/DESPP/DEMHS

RECORD OF REVISIONS

Revision Number	Date	Page/Section Changed	Changed By
1			
2			

Table of Contents

State Primary Agencies:

- Department of Administrative Services (DAS) [Technical]
  - Bureau of Enterprise Technology (BEST)
- Department of Emergency Services and Public Protection (DESPP) [Coordinating]
  - Division of Emergency Management and Homeland Security (DEMHS)

State Support Agencies: Include but are not limited to:

- CT Chief Cybersecurity Risk Officer
- DESPP Division of CT State Police (CSP)
  - CSP Cyber Crimes Investigation Unit (evidence collection and analysis, responsible for potential prosecutions)
- DESPP Division of Scientific Services
- DESPP Connecticut Intelligence Center (CTIC)
- DESPP CT Fire Prevention and Control Commission
- CT Military Department (Army/Air National Guard, Defensive Cyber Operational Element)
- University of Connecticut
- Connecticut State Colleges and Universities
- Department of Energy and Environmental Protection (DEEP)
  - Public Utility Regulatory Authority (PURA)

External/Private Sector Support: Cyber Operating Centers and private vendors/contractors that have significant responsibility for and/or involvement with cyber-related issues on behalf of state agency(ies). May include but not be limited to:

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Infragard (see also FBI below)
- National Consortium of Fusion Centers
- Verizon
- Qwest
- Level 3
- AT&T
- Northern Crossroads
- Sprint
- Frontier
- T-Mobile
- Fibertech (Nutmeg Network, including Public Safety Data Network)
- G4S (State Microwave System, Network Control Center)

Federal Support:

- Federal Bureau of Investigations/Infragard
- FBI Cyber Task Force
- United States Department of Homeland Security, including:
  - United States Secret Service
  - Cyber-terrorism Defense Initiative
  - National Security Integration Center
  - National Cyber Security and Communications Integration Center
  - Security/Information Analysis and Infrastructure
  - United States Computer Emergency Readiness Team (US-CERT)
  - State Liaison Officer, FEMA Region 1

Local Support: DEMHS Regional Emergency Planning Teams, including ESF2 (communications), ESF 5 (emergency management), ESF 12 (energy and utilities), ESF 13 (law enforcement), as well as local cyber/computer/electronic communications crimes task forces.

I. 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 on page 14 and Table 2 on page 18. 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.

II. Introduction

A. Purpose

The CT Cyber Disruption Response Plan (CT-CDRP or CDRP) was developed in recognition of the increasing dependence on Information Technology (IT)/computer-based systems and the knowledge that disruptions to some systems may have profound and detrimental effects on public safety, critical infrastructure, and business and industry. Should there be a significant cyber incident within the State or affecting the State, the purpose of this plan and others is to provide the framework for emergency management of response and recovery, recognizing that the effects of a long term cyber failure, whether caused by attack, error, or natural disaster, will require flexibility, creative problem solving, and clear and coordinated messaging to the public.

The CT-CDRP is an annex to the State Response Framework (SRF), the state's all-hazards framework, which describes how the State of Connecticut and its governmental and private sector partners will work to support local governments and their residents in responding to disasters and emergencies.

DAS/BEST personnel will respond to a cyber incident related to its enterprise by activating its Incident Response Plan, but in the event of a regional catastrophic incident or an event that may cause catastrophic cascading effects, DAS/BEST and other specified IT industry professionals as necessary will integrate into the statewide Incident Command System (ICS).

The CT-CDRP outlines organizations, actions, and responsibilities for a coordinated approach to protect against, prepare for, respond to, and recover from cyber-related catastrophic incidents affecting computer information systems owned and operated by the State of Connecticut, public and private critical infrastructure systems, and private information systems critical to the state and/or national security or economy.

B. Scope

This CDRP 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. This plan provides a framework for a cyber response, including the establishment of a Cyber Disruption Task Force (CDTF) and 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, as well as the State's Chief Cyber Security Risk Officer, 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, 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 serves as an annex to the State Response Framework (SRF). Cyber-related incidents may result in the activation of Emergency Support Function (ESF) 2-- Communications, ESF 12-- Energy and Utilities, and multiple other ESFs as appropriate.

The 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.

Activities conducted pursuant to this CT-CDRP shall take place within state and local planning and incident command structures, complement existing plans and procedures, and are compliant with the National Incident Management System (NIMS), in accordance with Governor Malloy's Executive Order 34.

C. Common Abbreviations and Acronyms

The following is a list of some of the common abbreviations and acronyms used in this plan:

CDRP Connecticut Cyber Disruption Response Plan

CDTF Cyber Disruption Task Force

CI/KR Critical Infrastructure/Key Resources

CIO Chief Information Officer

CISO Chief Information Security Officer

COOP Continuity of Operations Plan

CSIRT DAS/BEST Centralized Computer Security Incident Response Team

CSP Connecticut State Police

CT Connecticut

CTIC Connecticut Intelligence Center, the state's intelligence fusion center

DAS/BEST CT Department of Administrative Services/Bureau of Enterprise Systems and Technology

DESPP/DEMHS CT Department of Emergency Services and Public Protection/Division of Emergency Management and Homeland Security

DHS IO Federal Department of Homeland Security Intelligence Officer

EOC Emergency Operations Center

ESF Emergency Support Function is a grouping of government and certain private-sector capabilities into an organizational structure to 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. The ESFs serve as the primary operational-level mechanism to provide assistance to state, local, and tribal governments or to federal departments and agencies conducting missions of primary Federal responsibility.

IAP Incident Action Plan

ICS Incident Command System

Infragard Federal Bureau of Investigation (FBI)-sponsored group of CT public and private organizations meeting on issues related to security.

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

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.

III. Related Resources

The CT-CDRP should be read and implemented in conjunction with the State Response Framework, the State Disaster Recovery Framework, and the DAS BEST Cyber Incident Response Plan, which addresses individual agency or entity response to a cyber incident. Additional references and authorities may be found in Section VII.

IV. Situation and Assumptions

Cyber incidents may take many forms:

- An organized attack;
- An uncontrolled exploit, such as a virus, worm, or Denial of Service which has a widespread impact on public safety;
- A natural disaster with significant cyber consequences;
- Other incidents causing extensive damage to critical infrastructure;
- Inadequate or improper information technology (IT) infrastructure maintenance, security, and/or design.

In addition, an incident can be a "false positive" where no actual damage or danger is present but an investigation is needed to reach that conclusion.

An act of cyber crime is defined as unlawful access of data systems, networks, computers, or telecommunications without the consent of another. Acts of cyber crime may infiltrate, illegally modify, and/or corrupt data systems and networks to prevent proper performance of these systems, thus inhibiting organizational business processes to continue. Cyber terrorism is cyber crime with a terrorist purpose. Cyber terrorism is defined as the politically motivated use of computers and information technology to cause severe disruption or widespread fear in society. See, for example, Connecticut General Statutes Section 53a-301 and 6 U.S. Code 1531. In addition, unintentional disruptions caused by natural disaster or human error can also lead to large scale disruptions of service, as demonstrated by the long term devastation caused to Puerto Rico and other islands in 2017 by Hurricanes Irma and Maria.

The results of these events can lead to the loss of mission critical information, unavailability of information systems that support private sector internet, critical infrastructure, public health, economic institutions, and other organizations that sustain and provide critical services to Connecticut residents. Cyber threats can endanger vital control systems for other infrastructure such as electricity generation, transmission, and distribution.

Information technology service providers within Connecticut play a vital role in cyber disruption response because the private sector provides the backbone for information technology systems. Federal, state, and local government computer assets are all connected in varying degrees to privately administered critical communications infrastructure providers. It is essential that these providers be integrated into the coordination and decision making processes in a Cyber Disruption Response Plan.

Private sector entities included in this Plan should have existing policies and procedures to manage a cyber disruption, and government cyber response efforts must be coordinated with the affected private sector.

In addition to the private sector, cyber incidents have the potential to overwhelm or disable government resources. The state computer network is utilized by most Connecticut government agencies that provide critical services, including those that support public safety and public health. Many local law enforcement agencies depend on the state computer network to provide and transmit current, accurate information. Technical staff within state agencies must keep up with current technologies as cyber threats change, and the training can be expensive. Redundancy must continue to be built into the state computer network, and continuity of operations plans for all state agencies must be maintained and tested.

V. Concept of Coordination

Through its Chief Cybersecurity Risk Officer, Connecticut has developed a cyber security strategy to help define the challenges and opportunities associated with maintaining a healthy cyber community in Connecticut. See Attachment 1, CT Cybersecurity Strategy, July 2017. The Strategy identifies coordination as essential to cyber security. In addition, the State has established a Cyber Security Committee as a working group of the DESPP/DEMHS Emergency Management and Homeland Security Advisory Council. This working group shares current information and issues related to cyber security, and includes federal, state, tribal, local, and private sector partners.

A coordinated response to cyber incidents will minimize the extent and length of damage. 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/BEST will act as the lead technical agency for the cyber-related incident response component of a broader emergency situation unless or until the event becomes an Incident of National Significance. 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 BEST, 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/BEST responds to cyber incidents by activating its Cyber Incident Response Plan, and convening its Centralized Computer Security Incident Response Team (CSIRT). The DAS/BEST 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 should 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.

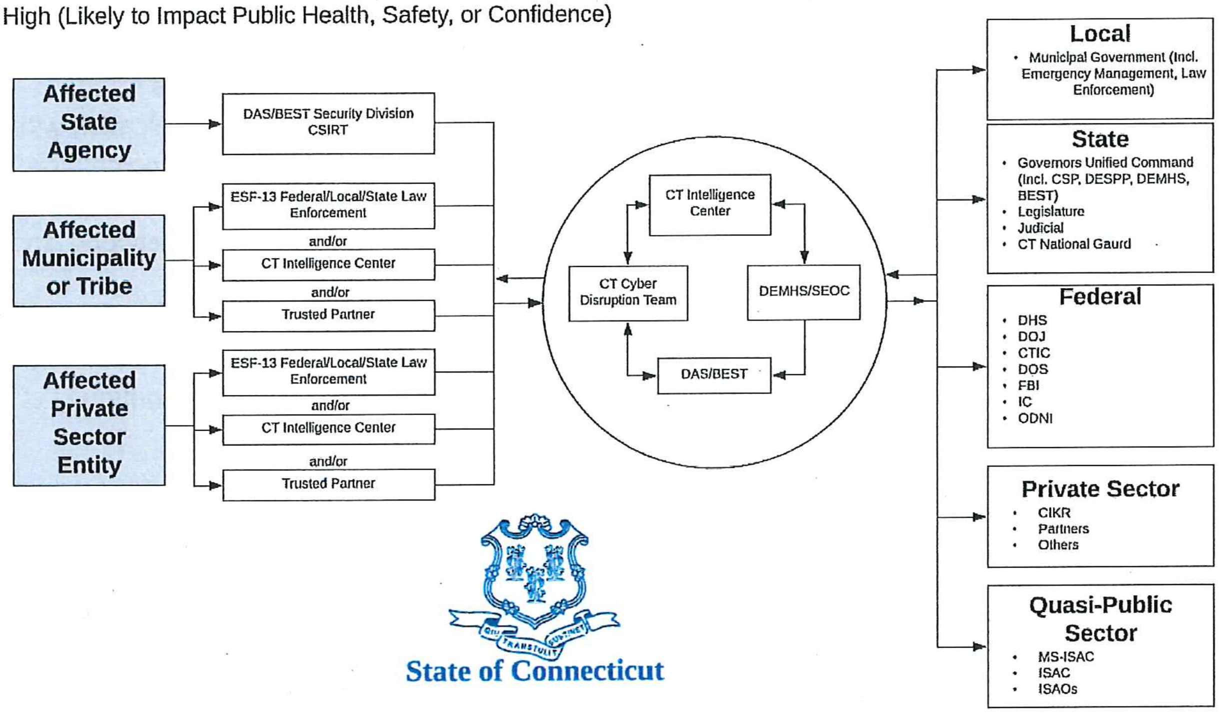
During a cyber incident affecting a state computer system, the CDTF will report information to the DAS/BEST Centralized Computer Security Incident Response Team (CSIRT), which will share the information with the Multi State – Information Sharing and Analysis Center (MS-ISAC), CTIC, DESPP CISO, and the 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 Response Team may be called upon to assist in response to or recovery from a cyber disruption in the State.

In support of the state's efforts to communicate potential or actual threats to supporting agencies, federal government, and the private sector, the Cyber Security Advisory System may be adopted, based on the Multi-State Information Sharing and Analysis Center, Cyber Alert Indicator and National Information Analysis and Infrastructure Protection Center Standards.

Communications flow and information sharing are absolutely essential to a positive cyber disruption response. Table 1, below, 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):

Table 1: Communications Flow for Cyber Security Threats at Levels Emergency, Severe or High (Likely to Impact Public Health, Safety, or Confidence)



A. Complex and Expanding Incidents

1. Regional Cyber Incidents:

Because of the nature of cyber networks and cyber terrorism, it is likely that a significant cyber terrorism incident will affect jurisdictions in addition to Connecticut, requiring coordination of mitigation and response actions across state boundaries.

At the start of any potential incident, and during the duration of any incident, all partners on the CDTF must ensure that communication with DAS/BEST and DEMHS is established in order to share situation status and manage the disruption as necessary. DAS/BEST and DEMHS must disseminate such information to all appropriate partners.

For regional incidents, information sharing to and from the CDTF or one or more of its members may occur from other mutual aid or information sharing organizations, including but not limited to:

- NESPAC (New England State Police Administrators Conference)
- NESEC (Northeast States Emergency Consortium)
- Northeast Region Fusion Centers International Emergency Management Group (New England states and Eastern Provinces of Canada)
- ISO New England
- NASCIO (National Association of State Chief Information Officers)

2. States of Emergency and National Cyber Incidents:

A cyber incident may create effects of such a nature or magnitude that (1) it requires the State to declare an emergency and/or (2) the Governor to request a Presidential emergency declaration if state and local resources are overwhelmed. Upon such a declaration, or in an incident of such enormity that the federal government declares the event an Incident of National Significance, the federal government may activate appropriate annexes to the National Response Framework including the federal Cyber Disruption Response Plan. FEMA has also released a *Power Outage Incident Annex: Managing the Cascading Impacts from a Long-Term Power Outage* (December 2017).

VI. 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;
- CTIC, in coordination with DEMHS, the DESPP CISO, the CSP Cyber Crime Investigations Unit, and the DAS/BEST IT Security Unit, will collaborate with government and private sector entities throughout Connecticut to establish annual operational and information security briefings. Regular defensive 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. Response and Recovery Actions

1. General Response Activities

CDTF response and recovery 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 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, 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) liaisons to procure critical cyber-related resources via all possible avenues, including the Federal government, and existing interstate and international mutual aid agreements.

2. 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 Officer (CIO), in consultation with the DAS CSIRT, or, if at a High, Severe or Emergency Level 3, with the CDRT:

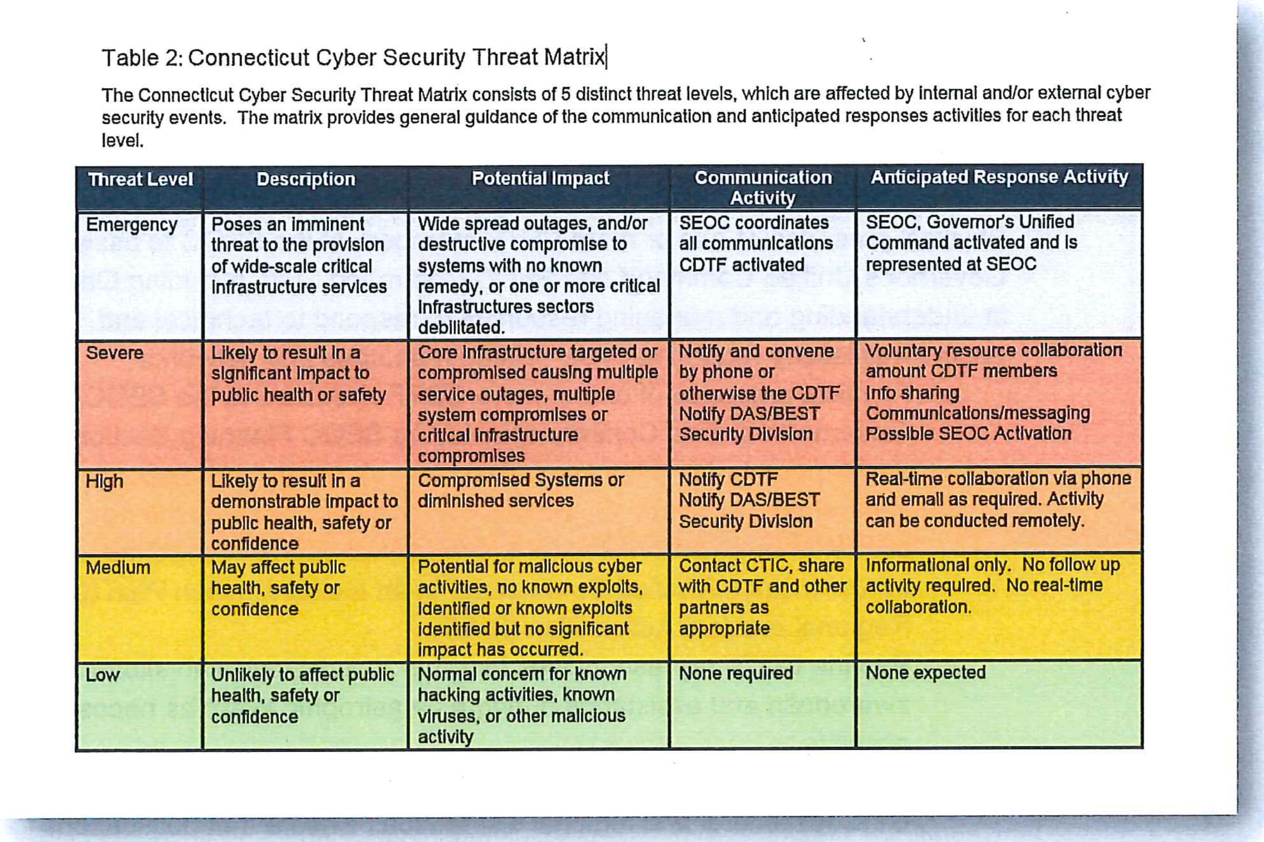


Table 2: Connecticut Cyber Security Threat Matrix

The Connecticut Cyber Security Threat Matrix consists of 5 distinct threat levels, which are affected by internal and/or external cyber security events. The matrix provides general guidance of the communication and anticipated responses 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 infrastructures sectors debilitated.	SEOC coordinates all communications CDTF activated	SEOC, Governor's Unified Command activated and is represented at 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 convene by phone or otherwise the CDTF Notify DAS/BEST Security Division	Voluntary resource collaboration amount CDTF members Info sharing Communications/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/BEST 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 CDTF and other partners as appropriate	Informational 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

3. Cyber Disruption Response Escalation and De-Escalation Paths

This section provides the following information for each threat level:

- Level definition—a brief description of what each security level means;
- Escalation/De-escalation criteria—description of the variables that are in place for the alert level to change;
- Potential impact—how the level affects state agencies, the private sector, municipalities, tribes, and the public;
- Communications procedures—how the knowledgeable party communicates with the CDRT, 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/BEST CSIRT or the CDRT 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 —LOW

- Definition: 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, municipal or private sector network;
    - Infection by known low risk malware;
    - Other like incidents;
    - Normal activity with low level of impact.
  - Actions:
    - Continue routine preventative measures;
    - Continue routine security monitoring;
    - Determine baseline of activity for the State/municipality/business—it is important to know what "normal" looks like;
    - State agencies need to contact the DAS/BEST IT Security Division, which will interface with MS-ISAC, and CTIC for information sharing and additional guidance if needed;
    - Ensure all personnel receive proper training on cyber security policies and security best practices.
- Escalation criteria: Infrastructure is operating normally and there are no known major cyber threats at this time.

CYBER SECURITY THREAT LEVEL- LOW

If a Cyber Security Threat Level LOW occurs in municipality or private sector and can be handled without negative impacts outside the municipality or business, no need to inform state CDTF. The municipality or business should notify CTIC for intelligence collection purposes, including monitoring trends.

- De-Escalation criteria: In order to return to this level, the conditions that caused the change must be remediated.
- Potential impact: No cyber-related issues should be affecting state IT resources.
- Communication procedures: Besides day-to-day operational communications, no special communication procedures are required.

b) Cyber Security Threat Level —MEDIUM

- Definition: This is the first active threat level in the cyber security threat matrix. Level MEDIUM means that malicious activity has been identified on state, municipal or private sector networks with minor impact. Examples include but are not limited to:
    - Change in normal activity with minor impact to IT operations;
    - A critical vulnerability, with the potential to cause significant damage if exploited, has been detected;
    - 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.

- Actions:
  - State agencies need to contact the DAS/BEST IT Security Division, which will interface with MS-ISAC, and CTIC for information sharing and additional guidance;
  - Continue recommended actions from previous level;
  - Agency(ies) Incident Response Plan(s) activated;
  - Identify vulnerable systems;
  - Identify vulnerable systems and implement appropriate counter-measures;
  - Identify malware on system and remediate accordingly;
  - Document data exposure with minor impact;
  - When available, test and implement patches, install anti-virus updates, and other security measures in next regular cycle;
  - Contact CTIC and Multi-State Information Sharing and Analysis Center (MS-ISAC) for information sharing and additional guidance.

- Escalation criteria: In order to raise the state agency threat level to Level MEDIUM, the state CIO or equivalent at local level or private sector must determine 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 it can be easily remediated without having a long-term impact to state, tribal, municipal, private sector, or CT residents.

CYBER SECURITY THREAT LEVEL- MEDIUM

If Cyber Security Threat Level MEDIUM occurs in municipality or private sector, and can be handled without any serious effects within the municipality or business, and without any external effects, the municipality or private sector should notify CTIC for intelligence collection purposes, including monitoring trends.

- Potential impact: At Level MEDIUM, the following conditions are in place:
  - Impact to IT services:
    - There is no threat to mission critical applications or resources;
    - The issue has been properly identified and can easily be remediated without risk of a data breach or theft of services;
    - The issue can be remediated within normal business hours;
    - The threat can be easily remediated by state agencies following normal procedures (e.g., software patches, updating virus files).
  - Special Events/Circumstances: A special event or circumstance incites hackers interested in trying to disrupt an agency's IT services or deface a website, etc…
  - Agency/business impact: IT staff will take proactive measures. Impact to IT services should be minimal since the threat has been identified and countermeasures exist for remediation.
- Communication Procedures: 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. See Table 1 Matrix. 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.

- De-Escalation criteria: To return to Level -LOW, any issues must be completely resolved and agencies must confirm that IT resources are working normally and/or the special event or circumstance has passed.

c) Cyber Security Threat —HIGH

- Definition: Malicious activity has been identified in (state/municipal/private sector) networks with a moderate level of damage or disruption. 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 affected in the (state/municipal/private sector) 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.
  - Actions:
    - Refer to Matrix in Table 1 for communications flow;
    - Continue recommended actions from previous levels;
    - Agency(ies) Incident Response Plan(s) activated Identify vulnerable systems;
    - Increase monitoring of critical systems;
    - Contact MS-ISAC Security Operations Center (SOC) for additional guidance;
    - Immediately implement appropriate counter-measures to protect vulnerable critical systems;
    - When available, test and implement patches, install anti-virus updates, and other system security measures as soon as possible;
    - Contact CT Cyber Disruption Team and CT Intelligence Center for situational awareness and information sharing regarding potential threats and outreach to other entities for prevention purposes;
    - Real time collaboration via phone and email as required;
    - Consider SEOC activation.
- Escalation criteria: In order to raise the state (municipal/private sector) or agency threat level to Level HIGH, the threat must involve two or more agencies or critical infrastructure sectors, critical applications, or websites; and/or the risk of the threat has been determined to have a significant impact to (state/municipal/private sector) IT operations.

CYBER SECURITY THREAT LEVEL- HIGH

If Cyber Security Threat Level HIGH occurs in municipality or private sector, CTIC, CDTF and DAS BEST Security Unit shall be notified of the incident.

- Potential Impact: At Level HIGH, the following conditions are in place:
  - Impact to IT Services could include:
    - There are multiple web defacements;
    - A critical vulnerability is being exploited and there has been moderate impact;
    - Attackers have gained administrative privileges on compromised systems;
    - Critical applications or resources have been affected;
    - Compromise of secure or critical system(s) containing sensitive information;
    - Compromise of critical system(s) containing non-sensitive information, if appropriate;
    - IT services may be interrupted by denial of service attacks;
    - The issue can be remediated within one to three business days and may require that critical application or services be taken offline until the issue can be remediated.
  - Continuity of Operations Plan(s)/Continuity of Government Plan(s) (COOP/COG) may have to be initiated to address the damages from the cyber-attack.
  - Remediation Effort: The threat can be remediated by (state/municipal/private sector) agencies installing software patches, updating anti-virus files, or denying network access to specific IPs or IP ranges.
  - Agency Impact
    - Agency IT staff will work with municipal/private sector Subject Matter Experts (SMEs) or DAS/BEST and the CDRT to install software patches, update anti-virus files, or deny network access to specific IPs or IP ranges;
    - Agency(ies) Incident Response Plan(s) activated;
    - If state is affected, DAS/BEST and the CDRT will work with the Governor's Office/Unified Command and the Attorney General to address any ramifications, including political or legal issues that may arise from the incident.
  - CDRT will work with the SEOC, if activated, or DESPP/DEMHS to address any communication or facility needs required by the agency to address the incident.

- Communication Procedures: A Level HIGH situation means that some of the (state/municipal/private sector) 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:
  - Refer to Matrix in Table 1 for communications flow, which includes:
  - CDRT 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 and this CDRP;
  - CDRT or CIO will ensure that MS-ISAC is notified. CDRT may also request assistance from MS-ISAC with remediating the issue;
  - CDRT, through CTIC or other means, will notify CT ITSOR and provide it with updates or remediation information;
  - 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.
- De-Escalation Criteria: To return to Level MEDIUM or below, the incident must pass the criteria defined within that section.

d) Cyber Security Threat—SEVERE

Level SEVERE signifies confirmed cyber attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised (state/municipal/private sector) IT resources and are using them to propagate the attack or to spread misinformation.

- Definition: Malicious activity has been identified in (state/municipal/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.
  - Actions:
    - Refer to Matrix in Table 1 for communications flow;
    - Continue recommended actions from previous levels;
    - Agency(ies) Incident Response Plan(s) activated;
    - Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, and system log files for unusual activity;

    - Consider limiting or shutting down less critical connections to external networks such as the Internet;
    - Consider isolating less mission critical internal networks to contain or limit the potential of an incident;
    - Fax, phone (where available) or state radio network in lieu of email and other forms of electronic communication;
    - When available, test and implement patches, anti-virus updates, and other measures immediately;
    - SEOC activation based on conditions, following the State Response Framework. Voluntary resource collaboration among CDRT members, technical information sharing and resource deployment, including mutual aid if needed. May include financial considerations.
- Escalation: To raise the state (municipal/private sector) or agency threat level to Level SEVERE, the threat must have the potential to affect multiple agencies and/or could require the state to shut down the IT infrastructure for five to ten business days to restore normal business operations.

CYBER SECURITY THREAT LEVEL- SEVERE

If Cyber Security Threat Level SEVERE occurs in municipality or private sector, CDTF and DAS BEST Security Unit must be notified of the incident as soon as possible. CTIC shall be informed as part of the response process.

- Potential Impact:
  - Impact to IT Services
    - A critical vulnerability is being exploited and there has been a significant impact;
    - Telecommunications may be interrupted causing agencies to use alternate forms of communication;
    - Email communications may be disrupted or untrusted, making it necessary for agencies affected by the event to use alternate forms of communications;
    - CDRT may have to be relocated to the SEOC for command and control purposes;
    - Agency IT Operations may have to be relocated to the SEOC for command and control purposes;
    - COOP/COG may have to be implemented to restore IT operations and/or to address damages from the cyber-attack;
    - Normal grid supplied power may become unreliable/unavailable for extended periods of time and considerations of emergency backup power are being prioritized;
    - Multiple damaging or disruptive virus attacks; and/or multiple denial of service attacks against critical infrastructure services;

        - The threat can only be remediated by restoring the applications and systems to an operational state by rebuilding equipment, restoring critical systems or applications to a previous date before the attacks occurred.

    - Agency Impact
        - Agency IT staff will work with DAS/BEST and CDRT to restore equipment, systems, and applications to an operational state;
        - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues that may arise from the incident.

    - Municipal/Private Sector Impact
        - Impacts to municipal and 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 at the SEOC, including assistance to contain or address the cyber disruption.

- <u>Communications Procedures:</u> At Level SEVERE, the (state/municipal/private sector) 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.
    - The CDRT will be notified via email if available, cell phone or messenger, will activate the Incident Response Plan, and will recommend a State EOC activation.
    - The CDRT will work with the SEOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
    - CDRT or CIO will ensure that MS-ISAC is notified, 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 among incident responders, the CDRT, and the State EOC.
- <u>De-Escalation Criteria</u>: To return to Level HIGH or below, the incident must pass the escalation criteria identified within that section.

e) Cyber Security Threat Level—EMERGENCY

At Level- EMERGENCY, 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.

- Definition: Malicious activity has been identified with a catastrophic level of damage or disruption. Examples include but are not limited to:
  - Malicious activity results 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).
  - Actions:
    - Continue recommended actions from previous levels;
    - Shut down connections to the Internet and external business partners until appropriate corrective actions are taken;
    - CDRT ensures that potential threats are disseminated and outreach for prevention purposes is made to other entities;
    - CDRT contacts appropriate law enforcement partners to pursue enforcement actions through investigation and criminal prosecution;
    - Isolate internal networks to contain or limit the damage or disruption.

- Escalation: To raise the threat level to Level EMERGENCY, the following conditions must be in place: The threat has affected multiple agencies and/or could require the state to shut down the IT infrastructure for six to thirty business days to restore normal business operations.

CYBER SECURITY THREAT LEVEL- EMERGENCY

If Cyber Security Threat Level EMERGENCY occurs in municipality or private sector, CDTF and DAS BEST Security Unit must be notified of the incident as soon as possible. CTIC will be informed as part of the response process.

- Potential Impact:
  - Impact to IT Services:
    - Telecommunications are unavailable making it necessary to use alternate forms of communication;
    - The power grid is unreliable causing agencies to rely on backup generators or uninterrupted power supply (UPS);

        - Buildings have been damaged or destroyed rendering IT resources inoperable;
        - CDRT must relocate to SEOC for command and control purposes;
        - Agency(ies) Incident Response Plan(s) activated;
        - COOP/COG must be implemented to restore IT operations and/or to address damages from the cyber-attack;
        - Data centers have to be restored or relocated to alternate facilities;
        - The issues raised by the incident will take over six business days to remediate and critical applications and services will be offline until the issues are resolved;
        - The threat can only be remediated by restoring the applications systems, and facilities to an operational state by rebuilding equipment or restoring critical systems or applications to a previous date before the attacks occurred.
    - Agency Impact
        - Agency IT staff will work with DAS/BEST and CDRT to restore equipment, systems, and applications to an operational state;
        - Agencies will work with the Governor's Unified Command and Attorney General to address any ramifications, including political and legal issues, which may arise from the incident.
- Communications Procedures: At Level --EMERGENCY, the state/municipal/private sector critical IT resources are rendered inoperable by a cyber security attack that will take weeks to recover. Such an event will affect IT communications and necessitate the need for alternate forms of communication (e.g., satellite, radios, messengers)
    - SEOC—The SEOC will be activated, and following the SRF, the Governor's Unified Command will meet there.
    - The CDRT will work with the SEOC to establish temporary communications for recovery personnel, including issuing radios to responders assisting in the recovery process.
    - CDRT or CIO will ensure that MS-ISAC is notified, and request assistance if necessary.
    - 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 CDRT, and the State EOC.
- De-Escalation Criteria: To return to Level SEVERE or below, the incident must pass the escalation criteria identified within each section.

VII. Responsibilities

A. Agency Roles and Responsibilities

1. Department of Administrative Services/Bureau of Enterprise Systems and Technology

DAS/BEST has an Ops Center that functions 24/7. Through this center's analysts, subject matter experts and leadership are contacted based on the requirement of a situation/incident. Staff members are on call 24/7 from the various divisions within BEST. When a cyber disruption occurs within the State of CT's network, DAS/BEST may take the following initial actions:

- Activate all or part of the CDTF, in consultation with other members; CIO to lead the CDTF;
- Stand up the DAS BEST Centralized Computer Security Incident Response Team (CSIRT), and/or DAS Incident Management Team (IMT) (if state network);
- Conduct an initial assessment of affected systems/networks and develop an action plan to remediate and/or restore services (if state network);
- 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 Task Force leads and the SEOC if activated, or the State Emergency Management Director or his designee, to provide situational awareness;
- Communicate with appropriate ESF Task Force leads and the SEOC if activated or the State Emergency Management Director or his designee, for resource and assistance requests;
- Coordinate all IT personnel and resources in the response effort;
- Facilitate communication of cyber-security related information to the state CTIC and to U.S. Department of Homeland Security/US-CERT;
- Facilitate IT continuity of operations/continuity of government for state agencies.
- When a cyber disruption occurs within the State of CT and the CDTF is activated, but whether the State of CT network is affected is not immediately known, DAS BEST may take the following initial actions:
  - Activate all or part of the CDTF, in consultation with other members, and lead the CDTF;
  - Determine the scope of the disruption and if State of CT's networks/systems are affected;
  - Ensure that State of CT's networks are protected;
  - Participate in the sharing of information regarding the disruption including possible steps to restore services and protect systems;
  - Determine areas where resources are available to lend assistance;
  - Follow the State Response Framework procedures for all-hazards response;
  - Serve as the Primary State Agency technical expert, including briefing appropriate State of CT officials as to the technical issues related to the situation;

- Assist the appropriate ESF Task Force leads and the SEOC if activated or the State Emergency Management Director or his designee, including but not limited to, coordinating response to resource and assistance requests.

2. Department of Emergency Services and Public Protection/Division of Emergency Management and Homeland Security

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:

- Activate all or part of the CDTF, in consultation with other members, and participate in the CDTF;
- Follow the State Response Framework procedures for all-hazards response;
- Engage DAS/BEST as a technical specialist within the Multi-Agency Coordination (MAC);
- If indicated, recommend to Governor activation of the SEOC to coordinate response and recovery;
- Coordinate support for CDTF and ESF activities and response resources as needed.
- Working with CDTF partners, develop an action plan to remediate and/or restore services;
- DEMHS will coordinate briefings for the Governor and his/her Unified Command as to the proposed action plan and determine resources available;
- ESF Task Force leads and the SEOC will brief or provide situation reports for dissemination to affected government or business entities for situational awareness;
- ESF Task Force leads and the SEOC will coordinate with affected parties for resource and assistance requests;
- As the threat develops, and following the SRF, DEMHS may take the following protective and coordination actions as deemed necessary:
- Partial or full activation of State Emergency Operations Center (SEOC) or alternate SEOC if necessary to coordinate response and recovery activities;
- As necessary, activation of Agency liaisons and ESF Task Forces;
- Establish and maintain emergency communications with affected entities and geographic areas;
- Prepare and disseminate public information news releases in coordination with the Office of the Governor, DAS BEST, and other partners;
- Assess the situation and develop an initial plan of action with CDTF partners;
- Coordinate briefing of local, state, and Federal officials on the situation;
- Coordinate receiving requests for assistance and mobilizing resources to provide assistance to affected areas;
- Support ongoing operations in affected areas;

- 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 or interstate mutual-aid agreements.

3. Department of Emergency Services and Public Protection/Connecticut State Police and DESPP IT

The DESPP Chief Information Security Officer (CISO) serves as a cybersecurity advisor to both the DESPP Commissioner and Connecticut's Homeland Security Advisor (HSA). When a cyber disruption occurs within the Public Safety Data Network or associated systems, the DESPP CISO, CSP and/or DESPP IT may take the following initial actions:

- Recommend activation of the CDTF;
- Conduct an initial assessment of affected systems/networks and develop an action plan to remediate and/or restore services;
- Brief appropriate senior state officials as to the proposed action plan and determine resources available;
- Communicate with appropriate ESF Task Force leads and the SEOC if activated, and the State Emergency Management Director or his designee, to provide situational awareness;
- Communicate with appropriate ESF Task Force leads and the SEOC if activated and the State Emergency Management Director or his designee, for resource and assistance requests.
- When a cyber disruption occurs within the State of CT and the CDTF is activated but the effect on the Public Safety Data Network is not yet known, the DESPP CISO, CSP and/or DESPP IT will take the following initial actions:
- Participate in the CDTF;
- Determine the scope of the disruption to see if the Public Safety Data Network or other key public safety communications network is affected;
- Depending on the disruption, ensure the Public Safety Data Network is protected;
- Participate in the sharing of information regarding the disruption including possible steps to restore services and protect systems;
- Assist as requested in the criminal investigation of the incident, including possible involvement of the CSP Cyber Crimes Investigations Unit;
- Determine areas where resources are available to lend assistance.
- Report incident to DAS/BEST IT Security Division.

4. CT Intelligence Center

In addition to responsibilities outlined in the SRF, in a cyber incident, DESPP CT Intelligence Center duties may include:

- Communications roles as indicated in the Table 1 Matrix, p.11
- Coordinate information sharing with DAS/BEST IT Security Division and DESPP CISO

- The following as outlined in the *Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers* (2015):
    - Strategic Analysis – assess national security and public safety issues as it pertains to Cyber threats to create an overall sense of current trends, tactics, patterns, and emerging risks and threats.
    - Technical Analysis – provide information to support local analysis and investigations with specialized information from numerous sources. Technical information is shared laterally across all participating partners as cyber issues make themselves known.
    - Intrastate Coordination – CTIC will maintain and foster a clear communication channel between the National Fusion Center Association Cyber Intelligence Network, Northeast Regional Intelligence Group, and regional participating cyber programs. This is to ensure the sharing of information and intelligence is enabled across all SME's in the region.
    - Suspicious Activity and Intelligence Reporting – CTIC will make appropriate notifications to agencies depending on the nature of the information.
    - Alerts, Warnings, and Notifications – CTIC will create alerts, warnings, and notifications as necessary.
    - Coordination with Response and Recovery Personnel –
    - Monitor Data Sources – MSISAC, NFCA CIN, NCCIC, USCERT and other sources
    - Regional and Statewide Exercises
    - Regional Outreach – cyber threat

5. DESPP Division of Scientific Services

In addition to responsibilities outlined in the SRF, in a cyber incident, DESPP Division of Scientific Services duties may include investigative activities associated with both the CSP computer crime investigative unit as well as the forensic computer crime unit.

6. DESPP Division of Statewide Emergency Telecommunications

In addition to responsibilities outlined in the SRF, in a cyber incident, DESPP Division of Statewide Emergency Telecommunications duties may include:

- Notification of the Network Control Center (NCC) at the DESPP Message Center of the event. This notification may set in motion messaging to and from the State's Public Safety Answering Points (PSAPs) depending on the type of disruption. The outbound messaging may take the form of telephone calls or emergency notification system alerts, and the NCC could field inbound questions from the PSAPs;

- Notification of the NG911 account manager at AT&T;
- Notification of the AT&T Resolution Center.

7. DESPP CT Commission on Fire Prevention and Control

CT Commission on Fire Prevention and Control duties includes responsibilities outlined in the SRF, and any other ESF-4 fire service duties assigned by the CDTF as appropriate to a cyber incident.

8. CT Chief Cybersecurity Risk Officer

In a cyber incident, the CT Chief Cyber Security Risk Officer's duties may include but not be limited to: identifying critical partners, and helping to coordinate communications by and between them; providing guidance on priorities; staffing or leading a task force as requested, and; assisting with messaging.

9. CT Military Department (Army/Air National Guard)

In addition to responsibilities outlined in the SRF, in a cyber incident, CT Military Department's Defensive Cyber Operational Element (DCOE) Team's duties may include incident response functions, including assessment and remediation functions, reporting, and coordination with federal, state, and local elements.

10. 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:

- Participate in the CDTF as requested;
- 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 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.

- Assist the appropriate ESF Task Force leads and the SEOC if activated or the State Emergency Management Director or his designee, including but not limited to, coordinating response to resource and assistance requests for matters pertaining 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.

B. External 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. The vendors/contractors outlined in the External/Private Support section have a relationship/contract with the State as of the date of this plan. Their responsibilities include: those that are outlined in any applicable contracts with the agencies or entities; those outlined in this plan and the State Response Framework, and; those found within state or federal law, regulation, or policy.

C. Federal Support

Unity of Governmental Effort. Various government entities possess different roles, responsibilities, authorities, and capabilities that can all be brought to bear on cyber incidents. These entities must coordinate to achieve optimal results. The first federal agency to become aware of a cyber incident will rapidly notify other relevant federal agencies to facilitate a unified federal response and ensure that the right combination of agencies responds to a particular incident.

1. Federal Bureau of Investigations/Infragard:

- FBI Field Office Cyber Task Forces: http://www.fbi.gov/contact-us/field
- Internet Crime Complaint Center (IC3): http://www.ic3.gov
- https://www.ingragard.org

2. United States Department of Homeland Security, including:

- United States Coast Guard: The USCG Sector Commander has a direct role in the federal government response to a cyber incident. The Captain of the Port, Long Island Sound (COTP LIS), will respond to a reported cyber threat or cyber incident to ensure the safety and security of COTP ports, waterways, coastal areas, waterfront facilities, vessels, and their associated activities.
- United States Secret Service
  - http://www.secretservice.gov/contact/field-offices
- Cyber-terrorism Defense Initiative
- National Security Integration Center
- National Cyber Security and Communications Integration Center
  - NCCIC: 888-282-0870 or NCCIC@hq.dhs.gov
- Security/Information Analysis and Infrastructure
- United States Computer Emergency Readiness Team (US-CERT)
  - http://www.us-cert.gov
- State Liaison Officer, FEMA Region 1

3. DHS Intelligence Officer Roles for Connecticut Cyber Disruption Response Plan:

In support of the State of Connecticut (CT) the U.S. Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) has assigned an Intelligence Officer (IO) with departmental and national intelligence authorities to CTIC. As a member of the U.S. DHS and the U.S. Intelligence Community (USIC), the DHS IO is the senior intelligence official for DHS I&A residing at CTIC. The DHS IO is responsible for collecting, reporting, analyzing, and disseminating intelligence information that fuses unique state and local information with USIC information to answer USIC intelligence requirements and/or a DHS / CTIC key intelligence questions. During a cyber incident, the DHS IO will respond as follows:

- DHS IO will receive notification of cyber incident from CTIC and / or other stakeholder(s).
- DHS IO receives the Indicators of Compromise (IOCs) from CTIC and processes the IOCs to determine a federal response.
- DHS IO will share information with stakeholder partners and classified data with cleared stakeholder partners involved with the incident.
- When a reported cyber information meets a collection requirement, the DHS IO will draft a raw and unevaluated information report.
- DHS IO will provide the State of CT with any USIC feedback or DHS HQ offer(s) of mitigation assistance or related intelligence information.
- Information not meeting a USIC or DHS requirement will be referred back to CTIC and reported through the appropriate CTIC information sharing groups.

VIII. Plan Development and Maintenance

DESPP/DEMHS, DAS BEST, and the other members of the CDTF will work together to ensure that this Cyber Disruption Response Plan is reviewed and updated on a regular basis. CDTF members 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.

A. 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

B. 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

IX. Attachments

1. CT Cybersecurity Strategy, July 2017

2. CT Cyber Incident Response Plan Template, December 2017 (FOUO)

3. CT Cybersecurity Action Plan, May 3, 2018