State of Connecticut

Cyber Disruption Response Plan

December 2022

CYBER DISRUPTION RESPONSE PLAN

Approved by: _____ Date: 1/10/2023

Jeff Brown, Chief Information Security Officer, CT DAS/BITS

Approved by: _____ Date: 1/11/203

Mark Raymond, Chief Information Officer, CT DAS/BITS

Approved by: _____ Date: 1-11-2023

Brenda Bergeron, Deputy Commissioner, CT DESPP/DEMHS

Approved by: _____ Date: 1.11.2023

James Rovella, 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

Table of Contents

I. Summary

A. Purpose

This 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 states response will vary depending on the resources 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 can 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 States 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. It is the job of the affected entities 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. (An 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).

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 the theft of highly sensitive data.

B. Initial Triage of a Cyber-Incident

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 their 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) to report the incident to appropriate officials. .

C. 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 Task Force:

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

1. 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 ESF-17, 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 ESF-17 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: 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 special communication procedures are required.

b) Cyber Security Threat Level 2—Medium

- Definition: This is the first active threat level in the cyber security threat matrix. Level 2 means that malicious activity has been identified on state networks with minor impact. 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: 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.

c) Cyber Security Threat 3—High

- Definition: Malicious activity has been identified in (state) 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) 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: A Level 3-High situation means that some of the state's 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:
    - ESF-17 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;
    - 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.

d) Cyber Security Threat 4—Severe

Level 4-Severe signifies confirmed cyber attacks are disrupting federal, state, and local government communications; and/or unknown exploits have compromised state IT resources and are using them to propagate the attack or to spread misinformation.

- Definition: Malicious activity has been identified in (state) 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: 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.
  - The ESF-17 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 ESF-17 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 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, and the State EOC.

e) Cyber Security Threat Level 5—Emergency

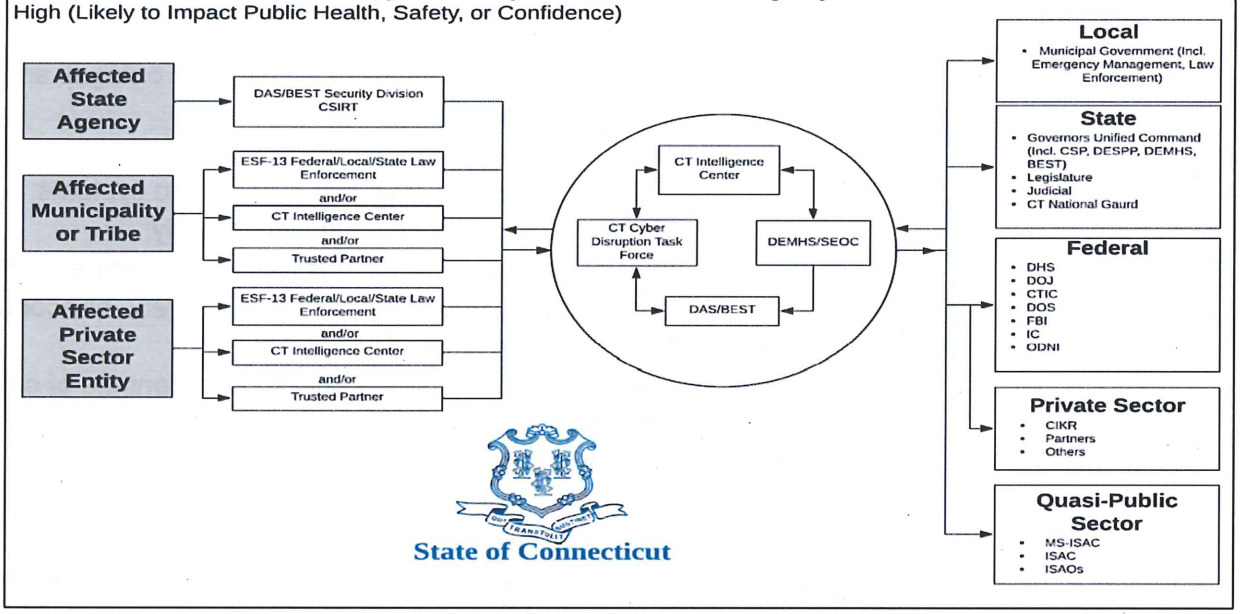
At Level 5—Emergency, unknown vulnerabilities are being exploited causing widespread damage and disrupting critical IT infrastructure and assets. These attacks have an impact at the national, state, and local levels.

- 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).
- Communications Procedures: At Level 5—Emergency, the state's 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 ESF-17 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 will notify the MS-ISAC and request assistance to remediate the issues.
  - 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, and the State EOC.

D. Reporting a Cyber Incident

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



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. 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
- What response actions have already been taken
- Who has already been notified (local law enforcement, Federal Bureau of Investigation, Department of Homeland Security, CTIC, etc.)

[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.

- 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 FBI, DHS, CISA, USSS, and 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 ITSecurity SecOps team 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. Agency Roles and Responsibilities

1. Department of Emergency Services and Public Protection (DESPP)

When a cyber-incident occurs within the State of Connecticut with potential to affect public health, safety, national security, or disrupt critical systems, the Division of Emergency Management and Homeland Security (DEMHS) will be the lead coordinating agency. The various Divisions within DESPP may take the following actions:

- 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 Task Force which will coordinate with the affected parties for resource and assistance requests;
- Activate of agency liaisons and additional ESF Task Forces to further support the incident;
- Establish and maintain emergency communications with affected entities and geographic areas;
- Coordinate information sharing and briefings between the private sector and all levels of government (local, state, and federal) using the Connecticut Intelligence Center (CTIC);
- Provide technical support and recommendations to the victim based on current threat intelligence using the Connecticut Intelligence Center (CTIC);
- Collect evidence which could be used in a criminal investigation by the Connecticut State Police (CSP) Cyber Crimes Investigation unit (CCIU) or another law enforcement agency;
- Work with partners to develop an action plan to remediate and/or restore services and brief the Governor and his/her Unified Command as to the proposed action plan and determine resources available;
- Engage the Connecticut National Guard for on-site incident response;
- Have the Division of Statewide Emergency Telecommunications (DSET) notify and work with all of the State's Public Safety Answering Points (PSAPs) depending on the type of disruption;
- Prepare and disseminate public information news releases in coordination with the Office of the Governor and other partners;
- On behalf of the Governor, prepare a 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;
- And coordinate the provision of additional assistance through the Federal government or interstate mutual-aid agreements.

2. Connecticut National Guard

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

3. 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;

4. 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.

5. 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

G. 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. The resources outlined in the Appendix A have a relationship/contract or are associated with the State as of the date of this plan.

Their responsibilities include those 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.

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 and 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.

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

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

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

CIKR - Critical Infrastructure and Key Resources

CIO - Chief Information Officer

COOP - Continuity of Operations Plan

CSIRT - DAS/BITS Centralized Computer Security Incident Response Team

CSP - Connecticut State Police

CT - Connecticut

CTIC - Connecticut Intelligence Center, the state's designated fusion center

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

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

SEOC - State Emergency Operations Center

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.

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

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.