Cyber Incident Reporting
A guide for CT partners

The State of Connecticut's Department of Emergency Services and Public Protection / Division of Emergency Management and Homeland Security (CT DESPP/DEMHS) and the Connecticut Intelligence Center (CTIC) are providing this document as a guide for reporting cyber incidents within the state. A cyber incident can be reported at various stages; however, those that involve the transferring of money are time sensitive. Notifying CTIC is critical to the state's ability to combat cyber actors and understand threats. When reported, this information will be used to brief task force members, to identify and share trends, and disseminate products that can help defend against further attacks.

What to Report: To identify the cyber trends in Connecticut and across the country, CTIC requests that all cyber incidents, even unsuccessful attempts, are reported to CTIC. Helpful information includes: name and contact information (phone number, email address); location of the incident (affected agency); brief description of the incident (ransomware, spear phishing, etc.); how and when the incident was initially detected; the extent of the incident (what data was possibly affected); what response actions have already been taken; and who has been notified (local law enforcement, FBI, CTIC, etc.).

When to Report: Cyber incidents, especially those involving the transference of money, should be reported to the appropriate authorities *as soon as possible*. If a cyber incident is reported within 48 hours, it will greatly increase the state's ability to assist. However, agencies are encouraged to report all cyber incidents to CTIC, no matter the timing.

If the cyber incident involves the direct transference of money: It is essential for information to be submitted to the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) as soon as possible. The faster these incidents are reported to IC3, the greater probability any money that was transferred can be recovered. After incident information has been reported to IC3, contact your local Law Enforcement Agency (LEA) and CTIC. If you have any questions regarding cyber incident reporting and the communications flow, please refer to Table 1 on page 2.

Internet Crime Complaint Center (IC3)	https://www.ic3.gov

If the cyber incident does not involve the transference of money: The affected agency should first notify their local LEA, then CTIC. This allows the local LEA to collect initial information and assign a case number, while also providing CTIC the opportunity to simultaneously share the reported issue with all its partners. Municipalities, tribal nations, or private sector entities can report cyber incidents to the state at:

Connecticut Intelligence Center (CTIC)	**Cyber Crimes Investigation Unit (CCIU)**
Email: ctic.cyber@ct.gov Phone:(860) 706-5500	Email: cybercrime@ct.gov Phone:(860) 685-8450

State of Connecticut's Cyber Disruption Response Plan (CDRP): CT DESPP/DEMHS developed the CDRP, which describes the framework for cyber incident response coordination among state agencies, federal/local/tribal governments, and public and private sector entities (https://portal.ct.gov/-/media/DEMHS/_docs/Plans-and-Publications/EHSP0006-Cyber-Disruption-Response-Plan-2018.pdf?la=en). This plan establishes the state's Cyber Disruption Task Force (CDTF), which is a group of subject matter experts from various disciplines involved in cyber preparedness, detection, alert, response, and recovery planning and implementation activities. Upon detection of an impending threat or significant event within the state or on the state's computer network, the CDTF may be activated to determine appropriate actions to respond to, mitigate, and investigate damage. If an event overwhelms a local community or is widespread, the State Emergency Operations Center (SEOC) may be opened to coordinate a unified response.

Cyber Incident Reporting
A guide for CT partners

Taken from the CDRP, Table 1 outlines the communications flow for reporting cyber incidents, and Table 2 provides the Cyber Security Threat Matrix. Once notified, CTIC will make all appropriate notifications to its partners as outlined in Table 1 below. State agencies experiencing a significant cyber event *must* report it to the CT Department of Administrative Services/Bureau of Enterprise Technology (CT DAS/BEST) and to their Information Technology Unit. Entities should also contact their trusted partners as appropriate (e.g. cyber insurance providers, legal counsel, etc.).

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

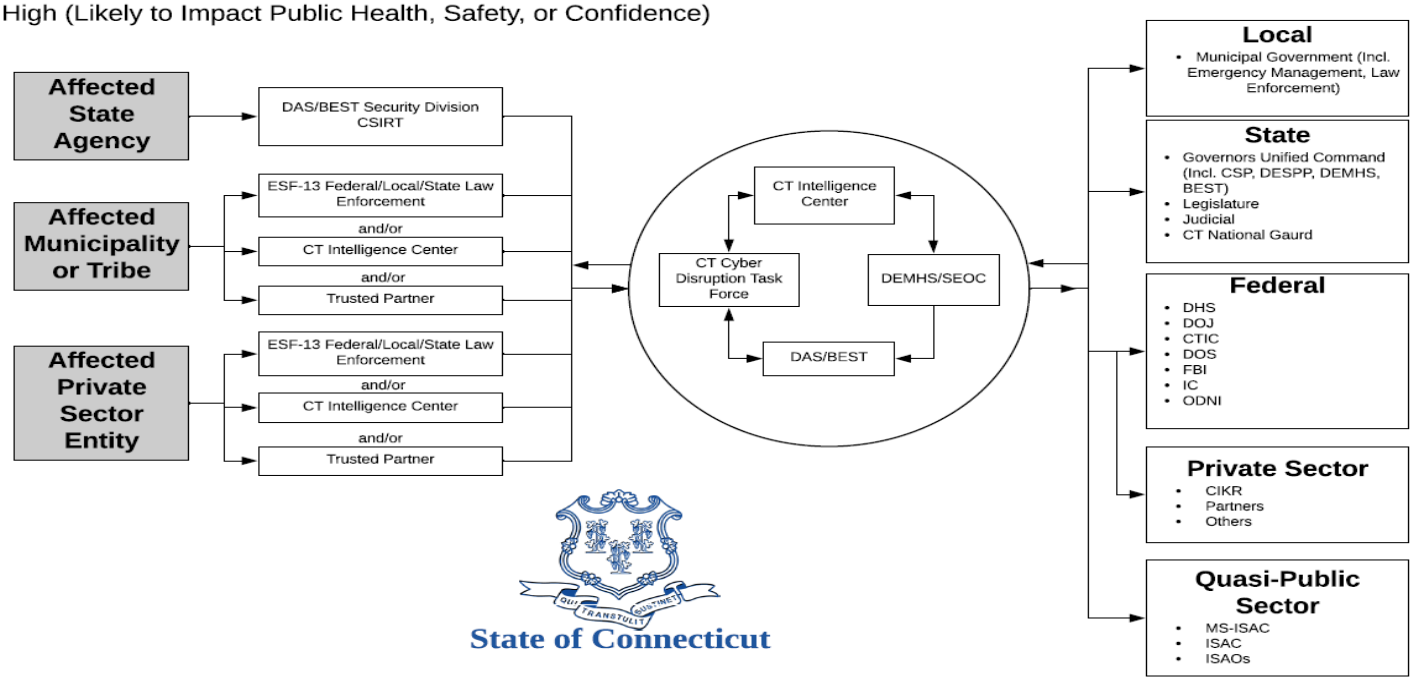

Table 2: Connecticut Cyber Security Threat Matrix

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