# Cyber Incident Reporting
## *A message for reporting in CT*

Cyber incidents can have serious consequences. The theft of government, private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to entities and individuals engaged in government, personal or commercial online transactions. Such risks are increasingly faced by government entities, businesses, consumers, and all other users of the Internet.

The State of Connecticut Department of Emergency Services and Public Protection/Division of Emergency Management and Homeland Security (CT DESPP/DEMHS) has developed a Cyber Disruption Response Plan (CDRP) which describes the framework for state cyber incident response coordination among state agencies, federal, local, and tribal governments, and public and private sector entities (https://portal.ct.gov/-/media/DEMHS/_docs/Cyber-Disruption-Response-Plan-Signed-Oct-2018.pdf?la=en). The plan establishes a state 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 in the state or on the state computer network, the CDTF may be activated in order 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.

When supporting affected entities, various local, state, and federal agencies, as well as private sector resources, can work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use the combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains how, what, and when to report a cyber incident to the State of Connecticut.

## *How to Report Cyber Incidents:*

Municipalities, tribal nations or private sector entities experiencing a significant cyber incident (see Table 2 on page 2 for description of reportable incidents) may report it to the State at:

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

Located within DEMHS, CTIC is the state's intelligence fusion center, made up of local, state, and federal law enforcement and other public safety professionals. The CCIU is the unit of the CT State Police devoted to investigating cyber crimes. **Once notified, CTIC will make all appropriate notifications as outlined in Table 1 on page 2.**
State agencies experiencing a significant cyber incident (see Table 2 on page 2 for description of reportable incidents) must report it to the CT Department of Administrative Services/Bureau of Enterprise Technology (DAS/BEST) as well as to their agency Information Technology Unit.

Once informed of an incident, local, state and federal agencies, and the private sector as appropriate, will work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy, civil rights, and civil liberties.

## *What to Report:*

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information includes: name and contact information (phone number, email address); location of the incident; description of the incident; how and when the incident was initially detected; who or what has been potentially or actually affected; what response actions have already been taken; and who has been notified.

## *When to Report:*

The charts below, taken from the CDRP, outline the potential threat levels of a cyber security incident, with recommendations on when an incident should be reported and recommended communications flow. Entities should also contact their trusted partners as appropriate, which may include 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)

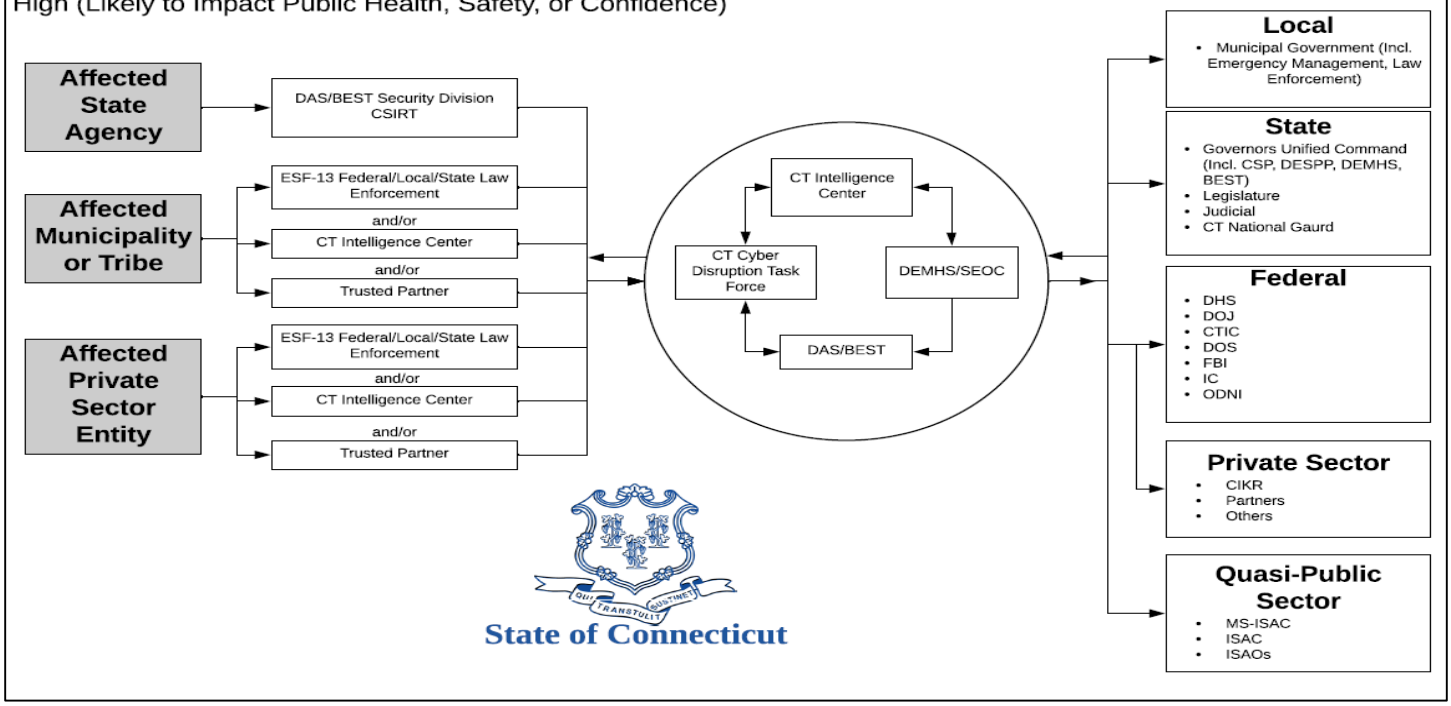


Table 2: Connecticut Cyber Security Threat Matrix

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 |