6/13/2016

INCIDENT ANNEX 5
CYBER ANNEX

LEADS: Department of Information and Innovation (DII)
Division of Emergency Management and Homeland Security (DEMHS)

SUPPORT: STATE AND FEDERAL AGENCIES

Vermont State Police
    Vermont Intelligence Center
Vermont Criminal Justice Services-Office of Technology Management
Vermont National Guard (VTNG)
Vermont Attorney General's Office
US Department of Homeland Security
    Multi-State Information Sharing and Analysis Center (MS-ISAC)
    United States Computer Emergency Readiness Team (US-CERT)
US Federal Bureau of Investigation (FBI)
US Secret Service (USSS)

I. INTRODUCTION

The purpose and scope of the Cyber Annex is to create an emergency action plan in response to a significant intrusion into the State or private sector cyber environments. There has been an increasing number of cyber incidents nation and worldwide; and it is imperative that a plan is in place for local, state, federal government agencies and private industry to warn of, respond to, and recover from a disruptive cyber incident.

Vermont's critical infrastructure consists of the physical and cyber assets of public and private institutions across 16 sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information technology, communications, energy, nuclear, transportation, finance, dams, chemicals, commercial facilities, and critical manufacturing Cyberspace is the nervous system of these highly interdependent infrastructure sectors, the control system of our state and country.

Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet or taxing/penetrating critical infrastructure information systems. Complications from disruptions of this magnitude may threaten lives, property, the economy, and national security. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage caused by this type of malicious cyberspace activity.

II. SITUATION AND ASSUMPTIONS

A. SITUATION

1. Cyberspace is comprised of hundreds of thousands of interconnected computers, servers, routers, switches and network cables that allow our critical infrastructure,

to include our State government, to operate. Thus, the healthy functioning of cyberspace is essential to our economy and state security. The threat of a cyber-related attack that could affect a state's infrastructure, computer systems, communications capabilities, economic security and other critical assets cannot be minimized or ignored in today's computer-dependent world.

2. Cyber threats are an increasingly unpredictable, dangerous, and proliferating hazard to state, local, and tribal governments, as well as private industry. Every day, networks are under attack across the state from a variety of sources, using myriad methods, all of which are growing in sophistication. In most cases, governments, industry, and operators of critical infrastructure are able to contain these threats and need no additional assistance.

3. Vermont shares several key infrastructure connections within the United States and Canada. No single agency at the local, state, or federal level possesses the authority and expertise to act unilaterally on the issues that could arise while responding to an act of cyber terrorism or other cyber incident in the State of Vermont.

4. The State of Vermont's critical infrastructure depends on properly functioning information technology to perform its functions and maintain a standard of living for the citizens of Vermont. Damage to these systems could create great hardship and civil unrest.

5. Cyber incidents may occur with little or no warning and may involve a variety of tactics, techniques and procedures which could affect critical state infrastructure. Likewise, a cyber incident could rapidly overwhelm the ability of local, state and federal agencies to respond to natural disasters as well as acts of terrorism.

6. Telecommunications and information technology services and activities are essential to providing direction and control for emergency operations and response activities, to providing emergency information, warnings and guidance to the general public, and communicating with all levels of government, where necessary.

7. Telecommunications and information technology within the State of Vermont depends on commercial, dedicated and fiber-optic telephone lines, a satellite-based communications system, internet, and limited radio resources.

8. A significant cyber incident is defined in this annex as an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture. State-level coordination of significant cyber incidents is triggered when the State Emergency Operations Center (SEOC) activates after receiving a request for assistance related to the incident. At that point, the significant cyber incident will be monitored and coordinated through the SEOC under the guidance of the Cyber Unified Coordination Group (UCG), which is described below. The Governor may proclaim a state of emergency under RCW 43.06.010(12) and/or order the

National Guard into active state service under RCW 38.08.040 in response to the incident.

9. Public Law 93-288 provides the authority for the Federal Government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property.

B. ASSUMPTIONS

1. Some redundant telecommunications and information technology services will survive the effects of an emergency or disaster.

2. Vermont Division of Emergency Management and Homeland Security will provide emergency information and warnings through the Emergency Alert System (EAS) network, and VTAlert.

3. Some people will ignore, not hear or not understand warnings of impending dangers broadcasted over radio and television or sounded by local siren systems.

4. Volunteer emergency communications resources will maintain the capability to respond and continue service through the disaster period.

5. Federal, state, local and private sector agencies will work together on cyber related issues and response to lessen the effects of a cyber-related incident and/or terrorist act.

6. All state agencies will notify the Department of Information and Innovation in the event of a cybersecurity incident affecting their Department/Agencies' IT systems.

7. Most cyber events will not result in SEOC activation.

III. MISSION

This annex provides guidance to ensure the preparedness, mitigation, response and recovery of information technology systems before, during and after an act of cyber terrorism and/or cyber disruption within both the State IT enterprise, and those of private owner-operators of Vermont critical infrastructure.

IV. CONCEPT OF OPERATIONS

1. This Annex applies to all threats or acts of cyber terrorism and/or cyber disruptions within the state that require a coordinated multi-agency response.

2. This Annex may be activated as a precautionary measure to respond to a validated warning of a high impact-high probability cyber incident or, absent sufficient warning, as a direct response to an actual cyber incident.

3. The principles of the National Incident Management System (NIMS) and Incident Command System (ICS) as applied to the SEOC will guide organizational structure and response/recovery. It is expected that local, state and federal resources, and private sector owner-operators may need to establish an incident command structure for certain cyber incidents.

4. This Annex applies to all state agencies. DEMHS activates State Support Function 2 (SSF2) as part of the SEOP when a significant impact to the communications and/or information technology infrastructure is expected or has occurred. When activated, SSF2 provides communications and information technology support to the impacted area, as well as internally to the SEOC and those agencies needed for emergency response in affected areas. SSF2 support is scalable to meet the specific needs of each incident, and response resources draw from a matrix of personnel from supporting agencies.

5. If the state's resources are insufficient to deal with an emergency situation, a request will be made for assistance from other jurisdictions pursuant to mutual aid agreements or from organized volunteer groups. Mutual aid personnel and volunteers will normally work under the immediate control of their own supervisors according to their Mutual Aid Agreement or Memorandum of Understanding. All response agencies are expected to conform to the general guidance provided by the senior decision-makers and carry out mission assignments directed by the Incident Commander or SEOC Manager.

6. The Director of DEMHS or designee is responsible for the maintenance of the Cyber Annex and for ensuring that necessary changes and revisions to the Annex are prepared, coordinated, approved and distributed.

7. The State of Vermont Cyber Response Assessment Board (CRAB) will coordinate the response to any significant cyber event affecting State or Private Sector technologies which meets thresholds of significance. This team will possess the required resources, authorities, and execution responsibilities that do not reside in one department, agency, organization, or company within the State. The CRAB consists of four permanent members: (1) DEMHS; (2) Director, Vermont Intelligence Center (VIC); (3) Department of Information and Innovation (DII) Chief Information Security Officer (CISO), and (4) the National Guard Director of Military Support (DOMS), augmented by other agencies as determined by the group. If a permanent member of the CRAB is unavailable for the incident, a designee may attend in his/her stead.

a. CRAB members will use their own authorities to assist response activities and are responsible for understanding and communicating the full range of capabilities that their organizations bring to bear.
b. Any of the permanent members may convene the CRAB, to be held virtually or physically, in response to an identified threat or hostile cyber activity.
c. CRAB notification will be determined through a dialogue between the DEMHS Watch Officer and the VIC, and will use the following criteria to inform the decision to notify:
    i. Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) intrusion or attack, such that system control is lost within Water/Wastewater, Energy, Dam, Nuclear, Chemical, Health Care, or Transportation sectors.
    ii. Compromise of State IT enterprise resulting in: life safety issues, or data breach involving Personally Identifiable Information (PII) or Protected Health Information (PHI)
    iii. Compromise of sensitive Defense Industrial information
    iv. Compromise of State ISPs

d. Each department and agency involved in a significant cyber incident shall be responsible for ensuring the availability of its representative to the CRAB. CRAB representatives should have familiarity with both emergency and incident management processes, as well as have a deep understanding of cyber threat and response issues.

e. During a significant cyber incident, the CRAB will provide guidance to leaders in the SEOC, if activated.

f. CRAB, during its deliberations, will use the Escalation and Notification Matrix below to assist in determining the level of severity of the cyber event as well as the recommended organizational responses.

8. A graphic decision process flow aid (Figure 1) is provided at the end of this document.

Escalation and Notification Matrix [1]		
Functional Impact Categories		**Notification Requirements**
Category	**Definition**	
None	No effect to the organization's ability to provide all services to all users	*Primary Contact: Name, Phone, Email* *Alt. Contact: Name, Phone, Email* *Provide Situation Report within: X (hours, minutes)*
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	
Medium	Organization has lost the ability to provide a critical service to a subset of system users	
	Organization is no longer able to provide some critical services to any users	
	Information Impact Categories	**Notification Requirements**
Category	**Definition**	
None	No information was exfiltrated, changed, deleted, or otherwise compromised	
	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated	
	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	
	Sensitive or proprietary information was changed or deleted	

V. Roles and Responsibilities

A. General

Most departments/agencies of government have emergency functions in addition to their normal day to day duties. The emergency functions they are assigned usually parallel or complement normal functions. Each department/agency is responsible for developing and maintaining its own cyber monitoring and impact assessment procedures.

The following is the assignment of primary emergency functions to departments and agencies or any other concerned organization whether political or private, profit or nonprofit, necessary to carry out this emergency plan. Assignment of support emergency functions to certain agencies is also included.

B. Lead Agencies

Vermont Department of Information and Innovation

A. Participate as Permanent Member of the CRAB.

B. Coordinate the execution of this Annex.

C. Coordinate statewide Information Technology damage and assessment.

D. Act as a liaison to Federal entities such as MS-ISAC, US-CERT, FBI, and US Department of Homeland Security in the event of a large scale cyber-incident, involving the state enterprise.

E. Disseminate cyber related threat, response, and recovery information

concerning cyber events targeting the State IT enterprise via multiple means.

F. In the case of a cyber event targeting the State enterprise, identify the cause of a cyber incident, isolate the risk, when appropriate, remove the problem from a system and prepare the system for recovery, and determine when the system can safely be restored to service.

G. Coordinate cyber training and education of state agencies.

H. Support and communicate with state agencies experiencing a cyber incident on their respective network.

I. Assist local, state, and federal law enforcement with cyber related investigations and data analysis.

J. Establish and maintain a continuity of operations plan for reestablishing access to hosted services following a disaster.

K. Report any suspicious activity to the Vermont Intelligence Center when the state network is significantly threatened by a cyber incident.

Vermont Division of Emergency Management and Homeland Security

A. Participate as Permanent Member of the CRAB.

B. Coordinate cyber response resource management.

C. Coordinate Emergency Public Information.

D. Coordinate with local, state and federal departments and agencies.

E. Identify cyber related critical infrastructure.

F. Ensure that necessary changes and revisions to this Annex are prepared, coordinated, approved and distributed.

G. Coordinate SEOC staffing and operations.

H. Ensure the SEOC, when activated, acts as a Multi-agency Coordination Center (MACC). For an event affecting the State IT enterprise and which meets criteria for an SEOC activation, SSF-2 (DII) and SSF-5 (DEMHS) will jointly act as EOC managers and conduct decision-making activities collaboratively. If the cyber attack is focused on private sector critical infrastructure the technical expertise will come from the VTNG Cyber Advisor Teams (CAT). NG CAT teams will be activated iaw with SEOC SOP and the VT NG Cyber Annex. Further refinement of the EOC organizational structure for the response will occur within the CRAB deliberations.

C. Support Agencies

Law enforcement agencies (refer to SSF 13, Annex M)

A. Support of the lead agency in response to a cyber incident.

B. Maintenance of law and order due to social repercussions as a result of

the cyber event.

C. Intelligence gathering and warning dissemination (Vermont Intelligence Center).

D. Direct criminal investigation of a cyber event or coordination with Federal LE investigatory assets.

E. Support communications and information technology.

F. In coordination with DEMHS and DII, support of cyber terrorist incident response activities.

G. Provide information for private sector entities following a cyber-incident.

H. Assist local and federal LE with cyber-related investigations and data analysis.

The Vermont Intelligence Center (VIC)

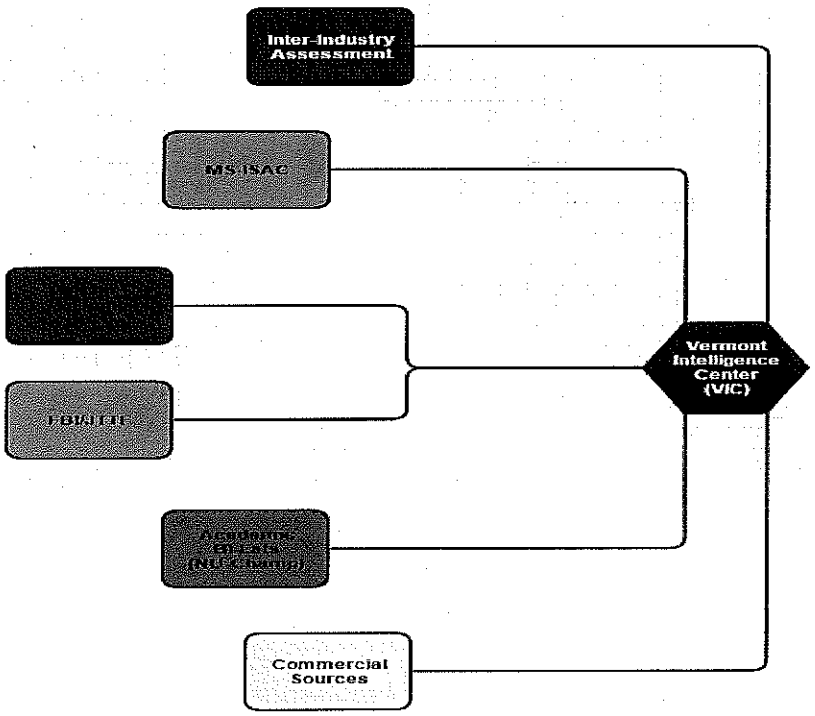
A. Participate as Permanent Member of the CRAB.

B. Intelligence gathering via existing cooperative networks of State, Federal, Academic, and Private Sector contacts. See image below.

C. Specific event assessment and acting as nexus of notification from private sector critical infrastructure partners.

D. Warning dissemination to DII and/or relevant CI sector partners

E. Acting as the single LE reporting nexus for all private owner-operators of State critical infrastructure who suffer a cyber attack.



The Attorney General's Office shall:

A. Provide legal advice to the involved agencies.

B. If necessary, prosecute responsible individuals.

Vermont National Guard

1. National Guard resources are available to support the spectrum of domestic operations, as may be directed by the Governor of Vermont through the Vermont National Guard Adjutant General. National Guard response will be as authorized by Vermont State Statute and in accordance with the State Emergency Operations Plan (SEOP).
2. When local and state resources are exceeded (both governmental and private sector), those unmet resource requirements will be requested by the DEMHS Watch Officer (or to the State of Vermont EOC, if activated) to the VTNG.
3. The Vermont National Guard, through its Director of Military Support (DOMS) will validate, approve and coordinate the mission with the DEMHS and the Director of Operations for Military Support (or designated representative).
4. For a cyber-response mission request, and once assessed and vetted through the Guard's Judge Advocate General, the Vermont National Guard will advise and assist the state emergency response effort by participating in the CRAB and by leveraging its Cyber Assistance Team (CAT), as defined by the VTNG Cyber Annex.

Norwich University (NU) Global Cyber Threat Observatory

The mission of the NU Global Cyber Threat Observatory is to monitor, evaluate, analyze and publish global cyber threat data in collaboration with public, private and academic partners around the world and to provide, where possible, advanced early warning of emerging cyber threats. NU's Threat Observatory is a key input into the VIC's cyber-fusion analytic processes.

U.S. Secret Service (USSS)

The Secret Service has primary jurisdiction to investigate financial crimes, which include counterfeiting of U.S. currency or other U.S. Government obligations; forgery or theft of U.S. Treasury checks, bonds or other securities; credit card fraud; telecommunications fraud; computer fraud, identify fraud and certain other crimes affecting federally insured financial institutions. All credible cyber threat or warning information provided by USSS and related to the Financial Services Sector will be provided to the VIC.

U.S. Federal Bureau of Investigation

FBI cyber threat, response and recovery information within the State of Vermont is covered by the Burlington, Vermont Resident Agency (RA) , which falls under

the direction of its Albany, NY, Headquarter Office.

The FBI's Cyber Division contains the Computer Intrusion Section which provides operational resources and expertise for the investigation of a cyber event, which threatens or impacts critical infrastructure; and

Computer Analysis Response Team (CART), which provides quality technical investigative capabilities, forensic services, testimony and support to the FBI and other law enforcement agencies.

U.S. Attorney's Office, District of Vermont

The US Attorney's Office (USAO) is responsible for prosecuting cyber crimes which meet or exceed a dollar amount threshold of $5,000.00. Each situation would be reviewed by the United States Attorney for a prosecutorial decision. If it is determined that the incident did not reach the threshold level but was extremely disruptive to the vendor, state, etc., consideration would be given toward the message it would send to the public if Federal charges were brought against anyone committing such acts. All interaction with the USAO will be coordinated through the FBI RA.

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Homeland Security Presidential Directive 7 tasked the DHS with the establishment of Information Sharing and Analysis Centers to facilitate cross-sector communication for all sectors of critical infrastructure.

MS-ISAC provides communication with the other states and with the other ISACs. There are ISACs for the following sectors:

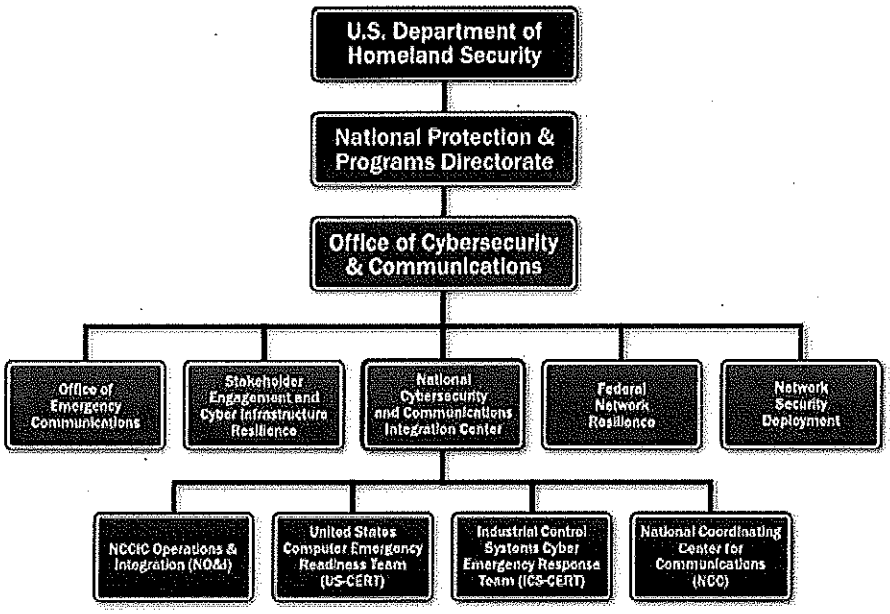
- Multi-State – State Governments (and by extension, local governments)
- Financial Sector
- Food and Agriculture Sector
- Telecommunications Sector
- Information Technology Sector
- Water and Wastewater Sector
- Health Care Sector
- Surface Transportation (Railroads and public transportation) Sector
- Energy (electricity, oil, and gas) Sector
- Chemical Sector
- Emergency Services

Some of the services provided by the MS-ISAC are:

- Development of common alert and reporting procedures.
- Collection, analysis, and dissemination of cyber incident data.
- Collect and relay cyber threat information.
- Provide trending and other analysis for cyber security planning.
- Coordinate with other ISACs on the analysis of cross sector threats.
- Conference calls when major events are in progress, or when new threats emerge.

The Department of Homeland Security (DHS)

When cyber incidents occur, the Department of Homeland Security (DHS) can provide assistance to impacted entities, analyze the potential impact across critical infrastructure, investigate those responsible in conjunction with law enforcement partners, and coordinate the national response to significant cyber incidents. The Department works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.



DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24/7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement.

- **NCCIC's United States Computer Emergency Readiness Team (US-CERT)** brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners.
- **NCCIC's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

- **NCCIC's National Cybersecurity Assessment and Technical Services (NCATS)** offers cybersecurity scanning and testing services that can identify vulnerabilities within networks and provide risk analysis reports with actionable remediation recommendations. These services provide proactive mitigation to exploitable risks and include network (wired and wireless) mapping and system characterization; vulnerability scanning and validation; threat identification and evaluation; social engineering, application, database, and operating system configuration review; and incident response testing.
- **NCCIC's National Coordinating Center for Communications (NCC)** leads and coordinates the initiation, restoration, and reconstitution of national security and emergency preparedness telecommunications services and/or facilities under all conditions.

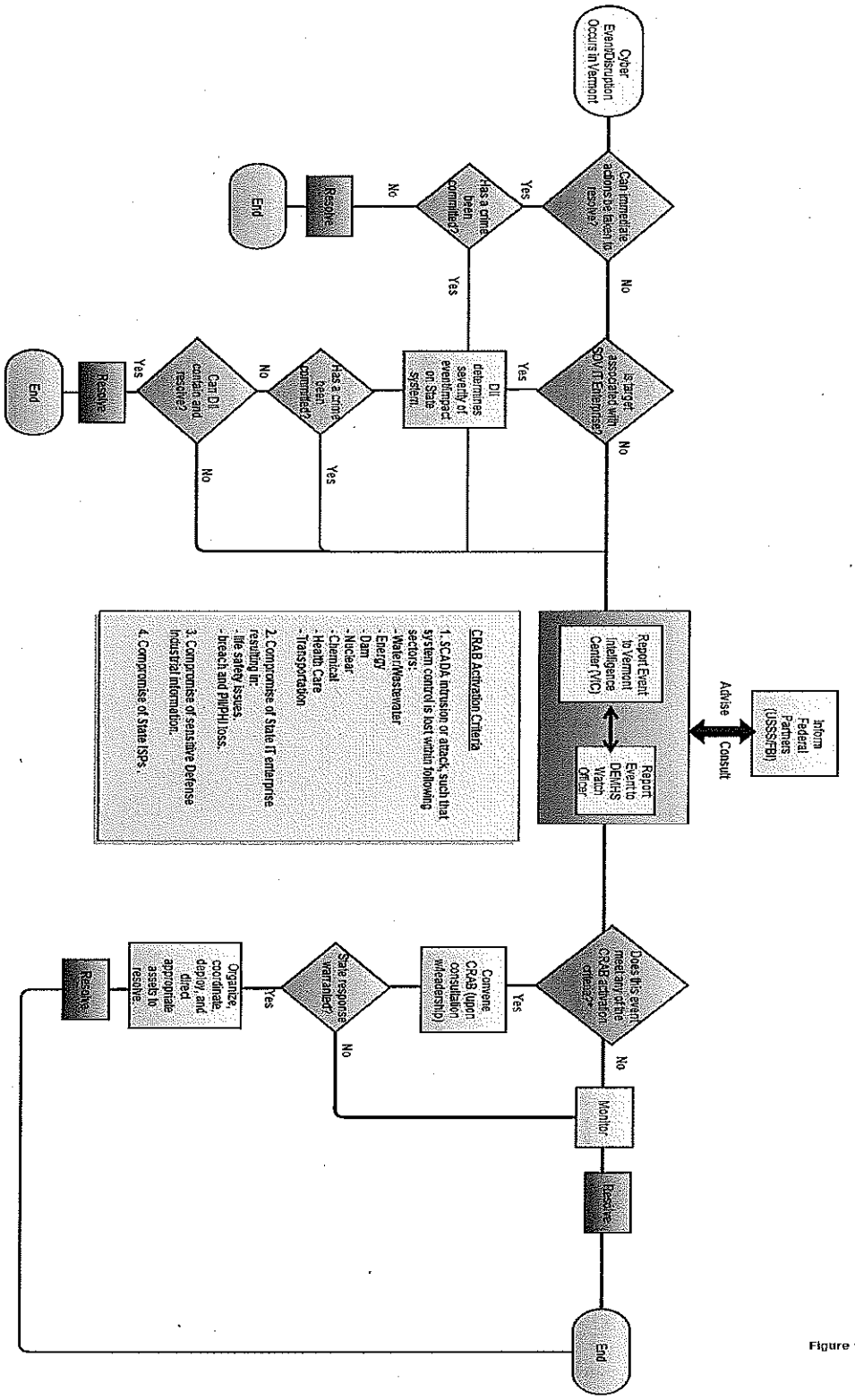

Cyber Event/Disruption Occurs in Vermont
Can immediate actions be taken to resolve?
Yes
No
Has a crime been committed?
Yes
No
Respond
End
Is danger associated with SOV IT Enterprise?
Yes
No
DII determines severity of event/impact on State System.
Has a crime been committed?
Yes
No
Can DII contain and resolve?
Yes
No
Resolve
End
Report Event to Vermont Intelligence Center (VIC)
Report Event to DEMHS Watch Officer
Advise
Consult
Inform Federal Partners (USSS/FBI)
CRAB Activation Criteria
1. SCADA intrusion or attack such that system control is lost within following sectors:
- Water/Wastewater
- Energy
- Dam
- Nuclear
- Chemical
- Health Care
- Transportation
2. Compromise of State IT enterprise resulting in:
- life safety issues,
- breach and PII/PHI loss.
3. Compromise of sensitive Defense Industrial Information.
4. Compromise of State ISPs.
Does this event meet any of the CRAB activation criteria?
Yes
No
Convene CRAB (upon consultation w/leadership)
State response warranted?
Yes
No
Organize, coordinate, deploy, and direct appropriate assets to resolve.
Resolve
Monitor
Resolve
End

Figure 1