CLARION COUNTY
CYBER INCIDENT PLAN

1. PURPOSE

A. To provide guidance to County departments/agencies, municipalities, schools, health care facilities, Clarion University and business/industries, for the protection of persons and property in the event of a cyber incident.

B. There may be national, Commonwealth or local cyber incidents impacting critical processes or economic activities that are significant enough to prompt Federal, Commonwealth or local agencies, or the private sector to act.

C. In some cyber incidents, Federal, Commonwealth and local response activities will be operating concurrently requiring coordination and mutual support.

D. Cyber incidents may require Commonwealth coordination and possible disaster emergency declaration by the Governor.

2. SITUATION AND ASSUMPTIONS

A. Situation

1). Cyber incidents are not bound by County borders and may lack an easily identifiable signature. Cyber incidents alone or in combination with other events will present new and unique challenges to Clarion County intelligence/information sharing, law enforcement and emergency management organizations.

2). A cyber incident may take many forms: ransomware, Email-phishing, an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber-consequences, a data destruction malware, supervisory control and data acquisition attack, or other incidents capable of causing extensive damage or disruption to public or private critical infrastructure or key assets.

3). Critical infrastructures and key resources which support the sustainment of public health and safety are of primary importance in determining response priorities.

4). Potential impacts from a significant cyber incident may quickly overwhelm local capabilities to respond to the incident. Public and private sector collaboration and prioritization of efforts may be necessary to address critical needs.

5). Cybercrime, including computer intrusions or attacks, fraud, identity theft, transmission of malicious code, password trafficking, theft of payment card or information, or other financial payment information or funds.

B. Assumptions

1). In the current risk environment, cyber incidents occur every day, often cascading across Federal, Commonwealth, local and private sector systems. Not every cyber incident requires national or Commonwealth coordinated prevention, protection, mitigation, response or recovery activities.

2). Approximately 85% of all critical infrastructure in the United States is privately owned. Owners and operators play a critical role in protecting their systems, information and data. Public and private sector cyber security efforts are designed to encourage these owners and operators to follow industry best practices, utilize the most up-to-date and advanced cyber security software and protection methods and provide all employees with cyber security awareness training.

3). The Federal and Commonwealth governments will play a significant role in managing intergovernmental prevention, protection, mitigation, response and recovery activities; and where appropriate, public-private response coordination to a cyber incident. These responsibilities include, but are not limited to the following:

a). Providing indications and warnings of potential threats, vulnerabilities, and reports of incidents and attacks;

b). Information sharing both inside and outside the government, including best practices, investigative information, coordination of incident response and mitigation;

c). Providing technical assistance;

d). Conducting investigative, forensics and prosecution; and

e). Providing active defense against the attack (i.e. firewalls, email spam defense, vulnerability scans [inside and outside of the network]).

3. CONCEPT OF OPERATIONS

A. General

1). Local cyber prevention, protection and mitigation activities involve investigating and **reporting** on the extent of cyber intrusions while response activities are occurring. These activities may provide Commonwealth and local response and recovery personnel with critical information concerning the projected impact and consequences, both seen and unforeseen, of a cyber incident. Information sharing between Commonwealth and local stakeholders is essential to ensure the effective management of a cyber incident and shall be considered an incident priority during a cyber event.

2). Rapid identification, information exchange, investigation, and coordinated response and remediation are critical in management of impacts from a local significant cyber incident.

3). Clarion County EMA is responsible for coordinating local response, recovery and mitigation efforts as they relate to impacts of an emergency or disaster.

B. Commonwealth Cyber Threat Advisory Levels

1). To facilitate communication of its preparedness posture, the Commonwealth of Pennsylvania utilizes Commonwealth Cyber Threat Advisory Levels. The current Commonwealth Cyber Threat Advisory Level is determined by the Office of

Administrations Chief Security Officer or designee in collaboration with PSP and can be found at **www.cybersecurity.pa.gov**.

2). Commonwealth Cyber Threat Advisory Levels communicate the current level of malicious cyber activity and reflect the potential for or actual damage from a cyber threat. The indicator consists of 5 levels:

a). **LOW** – indicates a low-level risk. No unusual activity exists beyond the normal concern for hacking activities, known viruses or other malicious activity. This is an advisory level baseline.

b). **GUARDED** – indicates a moderate risk of malicious cyber activity. The potential exists for malicious cyber activities that could compromise public and private sectors essential systems and/or diminish critical services, but no known exploits have been identified.

c). **ELEVATED** - indicates a significant risk of malicious cyber activity which has the potential to compromise essential systems and/or diminishes critical services. At this level within the Commonwealth, there are known vulnerabilities that are being exploited that can result in moderate level of damage or disruption. The potential for significant impact is a growing concern.

d). **HIGH** - indicates a high risk of increased malicious cyber activity which successfully targets or compromises core infrastructure causing multiple service outages or system compromises. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption within the Commonwealth is high.

e). **SEVERE** - indicates a severe risk of malicious cyber activity resulting in wide-spread outages and/or significantly destructive compromise to systems with no known remedy or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or wide spread level of damage or disruption of critical infrastructure assets within the Commonwealth.

4. **ORGANIZATION AND RESPONSIBILITIES**

A. Organization

Clarion County Department of Public Safety is the lead agency for the County.

B. Responsibilities

1). Pennsylvania Emergency Management Agency (PEMA)

a). Provide direction and coordination from either the Commonwealth Watch and Warning Center (CWWC) in Harrisburg or a mobile State Coordinating Center.

b). Coordinate the response of other Commonwealth departments and

agencies.

c). Coordinate requests for any unmet needs received from the various entities involved with a cyber incident, planning requested through the County Department of Public Safety.

d). Provide necessary communications support.

2). Pennsylvania State Police (PSP)

PSP shall be the lead entity responsible for coordinating Commonwealth law enforcement investigations, evidence collection and criminal forensic analysis.

3). Clarion County Department of Public Safety (DPS)

a). Provide coordination for planning and response with the appropriate State and county departments and agencies.

b). Coordinates response with municipalities, schools, University, health care facilities and business/industries.

c). Provide timely situation reports to the Commonwealth Watch and Warning Center during the emergency.

d). Reports incidents and any unmet needs to PEMA.

4). Local Law Enforcement agencies

Take reports on cyber incidents and forward to PSP or appropriate federal agencies as per Cyber Incident Reporting.

5). Law Enforcement agencies, municipalities, schools, University, health care facilities and business/industries

a). Maintain security software on computer systems and backup data offsite.

b). **Notifies Clarion County DPS of cyber incidents.**

c). Maintain up to date firewall and email spam software on all systems.

d). Ensure current cyber security training for all staff.

e). Provide coordination for planning and response with the Clarion County DPS.

f). Provide timely situation reports to the Clarion County DPS during the emergency.

g). Reports any unmet needs to Clarion County DPS.

5. ADMINISTRATION AND LOGISTICS

The County Emergency Management Agency is responsible for developing and maintaining the cyber incident plan.

6. AUTHORITY AND REFERENCES

A. Authority

Emergency Management Services Code, 35 PA C.S., 7101 et. seq.

B. References

1). Commonwealth of Pennsylvania, Emergency Operations Plan

2). Commonwealth of Pennsylvania, Emergency Operations Plan, Cyber Incident Annex

3). Clarion County Emergency Operations Plan

7. DEFINITION OF TERMS

A. Cyber incident – An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For this plan, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

B. Significant cyber incident – A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

8. EXERCISES AND TRAINING

See Clarion County EOP

9. PLAN MAINTENANCE AND DISTRIBUTION

See Clarion County EOP