Incident Specific Annex 3
Cyber Incident Response

Coordinating Agency

West Virginia Division of Homeland Security and Emergency Management (WVDHSEM)

Primary Supporting Agencies

WV Office of Technology (WVOT)
WV Intelligence/Fusion Center (WVI/FC)

Support Agencies and Organizations

West Virginia Department of Military Affairs and Public Safety (WVDMAPS)/West Virginia National Guard J2 (WVNG J2)
U. S. Department of Homeland Security (DHS)
Federal Emergency Management Agency (FEMA)
National Guard Bureau (NGB)

Purpose

This annex discusses policies, organizational structure, actions, and responsibilities for a coordinated, multidisciplinary, broad-based approach to prepare for, respond to, and recover from cyber-related incidents impacting critical state processes and infrastructure.

Scope

A. This annex describes the framework for West Virginia cyber incident response coordination among State departments and agencies and, upon request, county, local, and private-sector entities. The Cyber Incident Annex is built primarily upon the National Cyberspace Security Response System (NCSRS), described in the National Strategy to Secure Cyberspace. The NCSRS is a public-private architecture that provides mechanisms for rapid identification, information exchange, response, and remediation to mitigate the damage caused by malicious cyberspace activity.

B. This framework may be utilized in any incident with cyber-related issues, including significant cyber threats and disruptions; crippling cyber-attacks against the internet or critical infrastructure information systems; technological emergencies; or declared disasters.

C. This annex describes the specialized application of the West Virginia Emergency Operations Plan (WVEOP) to cyber-related incidents. Cyber-related incidents may result in activation of both Emergency Support Function (ESF) 2 Communications and this incident specific annex.

D. When processes in both annexes are activated, WVDHSEM and WVOT will continue their responsibilities under this annex and also fulfill their responsibilities as described in ESF 2 Communications.

Policies

A. This annex is intended to be consistent with the WVEOP, the National Response Framework (NRF), and the National Incident Management System (NIMS).

B. All agencies assigned responsibilities within this annex will develop and maintain the necessary plans, standard operating procedures, mutual aid agreements, and model contracts to successfully accomplish their tasks.

C. This annex applies to all threats or acts of cyber terrorism and/or cyber disruptions within the state that require a coordinated response.

D. This annex will be activated as a precautionary measure to respond to a potential cyber incident.

E. WVDHSEM is responsible for the development and maintenance of this annex. This should occur at minimum once every two years.

Situation

A. There have been an increasing number of cyber incidents occurring and it is imperative that a plan is in place for local, State, Federal government agencies and private industry to recover from a cyber-attack and/or disruptive incident.

B. West Virginia's critical infrastructures and key resources consist of, but are not limited to, the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials and postal and shipping. Cyberspace is the nervous system of these infrastructures-the control system of our State and country.

C. Cyberspace is comprised of hundreds of thousands of interconnected computers, servers, routers, switches and network cables that make our critical infrastructure work. Thus, the healthy functioning of cyberspace is essential to our economy and security. The threat of a cyber-related attack that could affect the state's infrastructure, computer systems, communications capabilities, economic security and other critical assets cannot be minimized or ignored in today's computer-dependent world.

D. 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 West Virginia.

E. The State of West Virginia's critical infrastructure and key resources depend on properly functioning cyber and communication equipment to perform their functions and maintain a standard of living for the citizens in West Virginia. Damage to these systems could create great hardship and civil unrest.

F. Cyber incidents may occur with little or no warning and may involve a variety of tactics which could affect critical state infrastructure and key resource sites. 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.

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

H. Telecommunications and information technology within the State of West Virginia depends on commercial, dedicated and fiber-optic telephone lines, satellite- based communications systems, internet, and interoperable radio resources.

Planning Assumptions

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

B. WVDHSEM will provide emergency information and warnings through the Emergency Alert System (EAS) network. The National Oceanographic and Atmospheric Administration (NOAA) Weather Radio service will provide weather related updates.

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

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

E. 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.

F. All state agencies will notify WVOT and WVOT will notify WVDHSEM in the event of a suspected cybersecurity incident affecting their department/agency.

Organizational Structure

A. The WVDHSEM Director, or designee, will provide general guidance for emergency operations, including the response to cyber incidents, in coordination with WVOT. During periods of a heightened cyber terrorist threat(s) or after an incident has occurred the State of West Virginia State Emergency Operations Center (WVSEOC) will be activated, per the State of West Virginia Standard Operating Procedures (SOPs).

B. The WVDHSEM Director, or designee, will facilitate the cyber terrorist incident response activities of the state departments and agencies to provide policy guidance in support of the incident commander. During terrorist incidents, the director will normally carry out those responsibilities from the WVSEOC.

C. If the state's resources are insufficient or inappropriate 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/Unified Command or the WVSEOC.

Concept of Operations

A. General

1. A cyber-related incident may take many forms: an organized cyber-attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to Critical Infrastructure or Key Resources (CI/KR).

2. Large-scale cyber incidents may overwhelm government and private-sector resources by disrupting the Internet and/or taxing 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.

3. The State Government plays a significant role in managing intergovernmental and, where appropriate, public-private coordination in response to significant cyber-incidents.

   a. State Government responsibilities include:

      1) Distributing indications and warning of potential threats, incidents, and attacks;

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

3) Analyzing cyber vulnerabilities, exploits, and attack methodologies;

4) Providing technical assistance;

5) Conducting investigations, forensics analysis, and prosecution;

6) Attributing the source of cyber-attacks;

7) Defending against the attack.

8) Leading recovery efforts.

B. Activation

1. Pre-Incident

   State departments and agencies maintain computer incident response capabilities that can rapidly respond to cyber incidents on their networks, including events of prolonged duration.

2. Notification and Activation Procedures

   Procedures in this annex are implemented when it is determined that a cyber-related incident is imminent or underway. Notification of WVDHSEM is made through established communications channels that exist between the State Government, nongovernmental entities, and the public. Responses to a cyber-related incident could well require activation of a number of ESFs and other Support Annexes, based on the nature of the threat.

3. Initial Actions

   WVDHSEM, WVOT, and other State/Federal agencies as appropriate work closely together to coordinate the response during a cyber-incident or attack, identify those responsible, and otherwise respond appropriately.

C. Ongoing Actions

WVDHSEM or WVOT coordinates technical and other assistance with and/or to other State or Federal agencies for response to major failures of critical information systems.

Agency Responsibilities Matrix

Supporting Agency	Acronym	Responsibilities
West Virginia Division of Homeland Security and Emergency Management	WVDHSEM	• Coordinate WVSEOC staffing and functioning. • Coordinate Resource Management and Coordination through ESF 2. • Coordinate Communications and Information Technology. • Coordinate Emergency Public Information. • Coordinate with local, State and Federal departments and agencies. • Coordinate Comprehensive emergency planning. • Identify cyber related critical infrastructure/key resources. • Ensure that necessary changes and revisions to this Annex are prepared, coordinated, approved and distributed. • Assist law local and federal law enforcement with cyber related investigations and data analysis. (WVI/FC)
WV Office of Technology	WVOT	• Monitor the state network at all times for suspicious cyber activity. • Coordinate Information Technology damage and assessment. • Act as a liaison to Federal entities such as MS-ISAC, US-CERT, and US Department of Homeland Security in the event of a large scale cyber- incident. • Disseminate cyber related information via multiple means. • 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. • Coordinate cyber training and education of state sectors. • Support and communicate with state agencies and school systems experiencing a cyber-incident on their respective network. • Assist local, State, and Federal law enforcement with cyber related investigations and data analysis. • Establish and maintain a continuity of operations plan for reestablishing access to hosted services following a disaster. • Report any suspicious activity to the WVDHSEM when the state network is significantly threatened by a cyber-incident.
West Virginia Department of Military Affairs and Public Safety	WVDMAPS	• Support the lead agency in response to a cyber-incident. • Maintain law and order. (WVSP) • Criminal investigation. (WVSP) • Protect critical infrastructure.

		• Support communications and information technology. • In coordination with DHSEM and WVOT, provide overall direction of cyber terrorist incident response activities.Advise and assist the state emergency response effort • Leverage Army and Air personnel expertise via a cyber-liaison response capability. • Provide response augmentation in accordance with proper legal authority.

Authorities & References

Authorities

The Enhancement of Non-Federal Cyber Security, The Homeland Security Act (Section 223 of P.L. 107-276)

Homeland Security Presidential Directive-5 (HSPD-5)

Homeland Security Presidential Directive-7 (HSPD-7)

Federal Information Security Management Act (FISMA)

Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications

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 National Security Telecommunications and Information Systems

Executive Order 12333: United States Intelligence Activities, as amended

References

National Strategy to Secure Cyberspace

The West Virginia Office of Technology Cyber Incident Response Plan

*EMAP Standard*s

4.4.3 – Emergency Operations Plan

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	PAGE/CHANGE	CHANGE MADE BY (SIGNATURE)
1	5/1/2017	IS 3-8, (Record of Changes Added)	
2	5/1/2017	IS 3-8, EMAP Standard Added, (4.4.3 – Emergency Operations Plan)	