

ESF 02 - Communications Annex, 2015

Table of contents

| | |
|--|----|
| I. Introduction | 3 |
| A. Purpose..... | 3 |
| B. Scope of Operations..... | 3 |
| C. Specific Authorities and References | 4 |
| II. Situation and Assumptions | 4 |
| A. Situation..... | 4 |
| B. Assumptions | 5 |
| III. Concept of Operations | 6 |
| A. General..... | 6 |
| B. Organization | 6 |
| IV. Responsibilities..... | 9 |
| A. Coordinating Agency | 9 |
| B. Support Agencies | 11 |
| C. Support Agencies Functions Table | 11 |

- Coordinating Agency :** PA Office of Administration
- Primary Agency(ies) :** PA Office of Administration
- Support Agency(ies) :** Civil Air Patrol
PA State Police
PA Department of Education
PA Department of General Services
PA Department of Military & Veterans Affairs
PA Public Utility Commission

I. Introduction

A. Purpose

1. Emergency Support Function (ESF) #2 – Communications includes those functions that in an emergency will support the restoration of the communications infrastructure, facilitate the recovery of systems and applications from cyber-attacks, and organize Commonwealth communications support to response efforts during incidents requiring a coordinated response (hereafter referred to as “incidents”).
2. ESF #2 also includes communications support to Commonwealth agencies, local governments, and first responders when their systems have been affected, and communications and information technology (IT) support to the State Emergency Operations Center (SEOC) and incident response field resources. In addition, this ESF provides for communications support and coordination among PSP, PEMA, and Public Safety Answering Points (PSAPs) throughout the Commonwealth.
3. The rapid convergence of communications and IT requires increased coordination of effort and capabilities between the communications and IT functions of Commonwealth government to facilitate ESF #2’s ability to respond to incidents of all types.

B. Scope of Operations

1. ESF #2 includes Commonwealth actions to assist industry in restoring the public communications infrastructure and to assist county and local governments with emergency communications and restoration of public safety communications systems and first responder networks. ESF #2 supports Commonwealth agencies in procuring and coordinating emergency preparedness communications services and resources.
2. ESF #2 includes communications support to the SEOC, county and municipal EOCs, and any incident response field resources.
3. ESF #2 includes communications support to emergency responders in counties when their own communications infrastructure is inoperable due to an incident.

4. ESF #2 includes addressing cyber security issues that result from or occur in conjunction with incidents. However, for incidents that are primarily cyber in nature, ESF #2 supports response as directed, with OA/OIT's Chief Information Security Officer (CISO) in the lead role. The CISO has primary responsibility for incidents within the Commonwealth network, and provides support and assistance for those outside. IT Bulletin ITB SEC024, IT Security Incident Reporting Policy, contains additional information about the Commonwealth's incident response and reporting guidelines.
5. ESF #2 includes the activation and implementation of the Commonwealth of Pennsylvania Cyber Security Incident Response Plan in the event of a significant cyber-attack, where critical systems have been subjected to moderate level of damage or disruption. The plan identifies what steps Commonwealth agencies, local governments, businesses, and citizens need to take to ensure that they are aware of the current threat level and what actions they need to take in order to be ready for a cyber-security incident that could impact the day-to-day cyber activities

C. Specific Authorities and References

Various policies, Executive Orders, and Management Directives apply to emergency response and reporting for cyber incidents and other response, including the following:

1. Executive Order 2012-05, Commonwealth Continuity of Government Commonwealth of Pennsylvania
2. Cyber Security Incident Response Plan
3. Management Directive 245.18, IT Administrator Acceptable Use, Auditing and Monitoring, Incident Notification, and Response
4. OPD SEC023B, Contingency and Continuity Planning (Operations Document).
5. ITB SECO24, Security Incident Reporting Policy (IT Bulletin)
6. FCC Rules and Regulations, 47 CFR Part 97—Amateur Radio Service and Part 95—Personal Radio Services
7. PA-STARNet Interoperability SOP (9/2010)
8. PA Statewide Essential Functions

II. Situation and Assumptions

A. Situation

1. Communications and IT 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 as necessary.

2. Communications and IT within the Commonwealth depends on commercial telephone, satellite-based communications system, a network of dedicated telephone lines, the Internet, and limited radio resources.
3. Under the provisions of Title IV—Major Disaster Assistance Programs, Section 418—Emergency Communications, Robert T. Stafford Disaster Relief and Emergency Assistance Act, the Administrator, Federal Emergency Management Agency (FEMA) Region III is authorized to establish temporary communications systems during or in anticipation of an emergency or major disaster and to make such communications available to state and local governments.
4. Three principal communications services facilitate access to the telecommunications network by national security and emergency preparedness entities in times of national emergency:
 - a. Telecommunications Service Priority (TSP): Ensures that critical and necessary phone lines are given priority restoration in the event of an emergency.
 - b. Government Emergency Telecommunications Service (GETS): Provides emergency access and priority processing in the local and long-distance segments of the Public Switched Telephone Network (PSTN).
 - c. Wireless Priority Access: Ensures that commercial mobile radio service (CMRS) providers voluntarily offer Priority Access Service (PAS) to national security and emergency preparedness personnel at the Federal, state, local, and tribal levels to help meet the national security and emergency preparedness (NS/EP) needs of the nation.
5. The Federal Communications Commission (FCC) can declare a temporary state of communications emergency when a disaster disrupts normal communications systems in a particular area. The declaration sets forth any special conditions and special rules to be observed by Amateur Radio stations during the communication emergency. Emergency management officials responsible for operations in the affected area should direct any request for declaration of a temporary state of emergency to the FCC Engineer in Charge (EIC) of the FCC Field Facility in the area.

B. Assumptions

1. Some redundant telecommunications and IT services will survive the effects of an emergency or disaster.
2. All public facilities will need to achieve and maintain high public awareness of emergency information and warnings provided by the EAS network and National Oceanographic and Atmospheric Administration (NOAA) Weather Radio service.

3. Some people will ignore, not hear, or not understand warnings of impending dangers broadcast over radio or television or sounded by local siren systems.
4. Civil Air Patrol will maintain High Frequency (HF) and Very High Frequency (VHF) radio capabilities to respond and continue communications with national, state, and local networks, and provide trained operators where necessary.
5. Volunteer emergency communications resources will maintain HF, VHF, and Ultra High Frequency (UHF) voice and data radio capabilities to respond to and continue service through the disaster period.
6. Pennsylvania State Police will provide physical security for administrative control and recovery sites; and they will ensure all Cyber Responders have been properly vetted before granting access to these facilities.
7. Private sector telecommunication companies will be able to assist with restoring critical telecommunications infrastructure and will be able to gain access to critical facilities, telecommunications
8. The PA Fusion Center facilitates cyber related communications between counties, cities, and municipalities.
9. PA Guard will be able to assist OA with reestablishing critical telecommunications infrastructure and will establishing a communications system in the event that telecommunications have been completely lost.

III. Concept of Operations

A. General

1. PEMA activates ESF #2 when a significant impairment of the communications infrastructure is expected or has occurred, or when other emergency circumstances may require increased communications capabilities. When activated, ESF #2 provides communications support to the affected area, as well as internally to the SEOC and those Commonwealth agencies needed for emergency response in affected areas. ESF #2 support is scalable to meet the specific needs of each incident, and response resources draw from a matrix of personnel and equipment available from the ESF #2 support agencies.

B. Organization

While Office of Administration is the overall coordinator of ESF #2 activities, the three primary agencies each have separate authorities and responsibilities. Accordingly, each will work within those authorities to help facilitate the overall Communications support effort.

1. Coordinating Agency
 - a. ESF Coordinator - OA

- 1) Serves as the ESF #2 Coordinator.
- 2) Coordinates with primary and support agencies to develop ESF #2 documentation, policies, and procedures.
- 3) Coordinates with primary and support agencies to provide and execute a program for training and deploying personnel to support ESF #2 operations.

b. PEMA

- 1) Through the SEOC, establishes Commonwealth priorities and coordinates Commonwealth response efforts and assistance activities. During the course of an incident response, SEOC activities and roles surge and diminish as an incident progresses.
- 2) Acts as the ESF #2 primary agency for coordination of public safety disaster emergency communications and exercises primary responsibility for coordination of the restoration of telecommunications in an incident area.
- 3) Activates ESF #2 as required by the event, including the need for state, county and local government support for tactical communications.
- 4) Receives, disseminates, and coordinates emergency communication and incident status information within Commonwealth government and externally, including serving as point of contact for information reports and issuing alerts within Commonwealth government and to the public.
- 5) Maintains a record of incident status and response, and issues reports.
- 6) Coordinates communication with public safety and emergency management agencies outside Commonwealth government, including the Federal, county, and local levels, and agencies in neighboring states.
- 7) Coordinates volunteer emergency communications resources as required to supplement other available resources.
- 8) Coordinates communication with commercial communications infrastructure and service providers.
- 9) Coordinates short-term restoration support to county and local government emergency communications in the event of a failure.
- 10) Designates personnel to support tactical communications functions.
- 11) Provides personnel to support overall ESF #2 operations.
- 12) Provides communications support to state, county, and local first responders, and in conjunction with PSP/BCIS/SNRD, provides for coordination of emergency communications with State Agencies and PSAPs using the Pennsylvania Statewide Radio Network (PA STARNet).

- 13) Monitors potential or actual communications incidents that pose a threat to communications facilities or services, and situations that create the need for extraordinary communications support.
- 14) Provides communications support, to include PEMA owned satellite-based communications systems, to field teams, other Commonwealth response or recovery facilities within the area of operation, and Commonwealth response teams.

c. PSP/BCIS/SNRD

- 1) Coordinates recovery of PA STARNet wide-area voice and data capabilities.
- 2) Monitors, recovers and supports PA STARNet interoperable communications with external systems.
- 3) Provides PA STARNet operational and performance status information to ESF #2 agencies and responders.
- 4) Provides PA STARNet network management and configuration support to ESF #2 agencies and responders.
- 5) Invokes and enforces priority status for PA STARNet use by ESF #2 agencies and responders according to established policy as necessary.
- 6) Activates recovery and alternative site plans as necessary to maintain PA STARNet operation and services.
- 7) Coordinates the restoration of public safety communications systems and first responder networks.
- 8) Coordinates with PEMA to provide and support emergency communications during incident response.
- 9) Coordinates with PEMA and support agencies to develop appropriate documentation, policies, and procedures pertinent to tactical communications functions.

d. OA/OIT

- 1) Supports recovery and use of the Commonwealth's Wide-Area Network and associated computing, network, and telecommunications systems.
- 2) Identifies and assesses any damage to IT infrastructure or disruption to IT services.
- 3) Detects any cyber-attacks, assesses damage, and coordinates response and recovery.
- 4) Coordinates recovery of Commonwealth IT resources and capabilities.
- 5) Coordinates recovery of Commonwealth telecommunications systems and services that fall under OA/OIT administrative jurisdiction.

- 6) Provides telecommunications support to PEMA for emergency alerts and for coordination of Commonwealth response.
- 7) Advises and assists Commonwealth agencies in the recovery of IT applications and databases and telecommunications facilities.
- 8) Provides IT support to field teams, other Commonwealth response or recovery facilities within the area of operation, and Commonwealth response teams.

2. Support Agencies

- a. Communications incidents and requirements are handled in accordance with the SEOP and the National Incident Management System (NIMS).
- b. Communications management is bottom-up with decisions made at the lowest level possible. Only issues requiring adjudication or additional resources are referred to the next higher management level.
- c. Agencies that provide communications assets in support of incident response control their own assets and coordinate location and use with the SEOC.
- d. Uniform emergency communications management and plans, procedures, and handbooks are to be developed and used throughout the ESF #2 operating environment.
- e. ESF #2 uses PA STARNet capabilities for wireless statewide voice and data communications within Commonwealth government and for interoperable communications with external agencies and responders. PSP/BCIS/SNRD coordinates with PEMA and leads the recovery, management, operation, and support of PA STARNet.
- f. ESF #2 supports cyber incident response when requested by OA/OIT. OA/OIT leads the coordination of cyber security issues associated with an ESF #2 response.
- g. ESF #2 coordinates tactical communications support to state, county, and local government agencies and first responders.

IV. Responsibilities

A. Coordinating Agency

1. ESF Coordinator—OA
 - a. Serves as ESF #2 Coordinator.
 - b. Identifies any non-emergency programs or funds available for application to incident response or recovery.
 - c. Coordinates recruitment of temporary employees needed by Commonwealth agencies to maintain functions and activities necessary for incident response and recovery.

- d. Activates Commonwealth Continuity of Government plans and coordinates activities under these plans with ESF #2 activities.

2. Primary Agencies

- a. PEMA: Coordinates communications support to field operations, coordinates public safety disaster communications, and operates the Commonwealth EAS.
- b. PSP/BCIS/SNRD: Coordinates with PEMA in recovery and operation of PA-STARNet, coordinates the restoration of public safety communications systems and first-responder networks, and provides support and assistance for emergency communications deployment and operation.
- c. OA/OIT: Coordinates recovery of Commonwealth network operation, telecommunications, and IT applications and databases; provides support for response to cyber incidents; and provides IT support to field operations.
 - 1) If required, the Commonwealth Information Security Office, a part of the Office of Information Technology, convenes the Pennsylvania Computer Security Incident Response Team (PA CISRT) to provide incident information and decision support, and coordinate response to cyber security issues. PA CISRT and the Enterprise Security Team (EST) provide technical and operational support to the OA/OIT CISO and ESF #2, as well as gathering and disseminating cyber security information and warnings.
 - 2) OA/OIT coordinates with local government IT representatives through the Pennsylvania Information Sharing and Analysis Center (PA ISAC) and agency Information Security Officers (ISOs) as appropriate to exchange policy and operational information necessary to respond to and recover from incidents.
 - 3) Supports Commonwealth government agencies when an incident results in cyber security issues.
 - 4) Disseminates cyber threat warning information to Commonwealth government agencies, private citizens, and business entities.
 - 5) Coordinates cyber incident preparedness, response, and recovery activities to identify, analyze, and reduce cyber threats and vulnerabilities.
 - 6) Facilitates interaction and collaboration among Commonwealth departments and agencies, and with state and local governments, the private sector, and international organizations related to cyber security and cyber incidents.
 - 7) Supports the Department of Justice, Federal Bureau of Investigation, and other law enforcement agencies in investigating and gathering of information related to cyber threats and attacks.
 - 8) Fulfills additional responsibilities as directed in the Cyber Incident Annex to prepare for, respond to, and recover from cyber incidents requiring a coordinated state response.

B. Support Agencies

1. Commonwealth Agencies
 - a. Pennsylvania State Police.
 - b. Department of Education
 - c. Department of Health
 - d. Department of Military and Veterans Affairs
 - e. Commonwealth Media Services
 - f. Public Utility Commission
2. External Support Organizations
 - a. Civil Air Patrol
 - b. National Weather Service
 - c. Volunteer Emergency Communications Resources
 - d. Commercial Communications Providers

C. Support Agencies Functions Table

| Agency | Functions |
|----------------------------------|---|
| Commonwealth Agencies: | |
| Pennsylvania State Police | <ol style="list-style-type: none"> a. Maintains access to all voice and data communications facilities that support law enforcement. b. Upon request from PEMA, assists in authentication and distribution of essential information and instructions. c. Advises and participates in decision-making in matters of law enforcement concerning the distribution of information or instructions. d. Invokes TSP for priority provisioning of new circuits or for restoration of existing circuits. e. Provides Wireless Priority Service (WPS) and GETS to key ESF #2 personnel. |

| Agency | Functions |
|--|---|
| Department of Education | Provides a statewide educational messaging system for communication and coordination with school districts. |
| Department of Military and Veterans Affairs | Operates voice and data communications systems in support of coordinating Pennsylvania National Guard incident response. |
| Public Television Network Commission | Provides a television broadcast communications system for emergency use as requested by the Governor or by PEMA in support of emergency management and incident response. |
| Public Utility Commission | <ul style="list-style-type: none"> a. Conducts surveys of telecommunications service conditions and problems. Monitors and reports completion of critical repairs. b. Collects and reports to PEMA concerning anticipated or existing telecommunications problems. c. In coordination with PEMA, develops and maintains a database for coordination of responses to telecommunications problems. d. Supplies technical advice and assistance in the emergency operations of telecommunications systems and facilities and the supply of services. e. Assists in providing essential information regarding regulated telecommunications services for priority service. f. Communicates priorities for service restoration to telecommunications providers. |
| Other Commonwealth Agencies | <p>Other agencies assist PEMA as requested in deploying agency-owned, leased, or otherwise unique communications assets to support the response effort. Each of these other Commonwealth agencies carries out the following functions:</p> <ul style="list-style-type: none"> a. Uses organizational resources to meet mission requirements before requesting ESF #2 emergency communications support through the SEOC. b. Notifies the SEOC promptly of all ESF #2 communications requirements and available assets, to eliminate the possibility of service duplications and ensure prompt provision of needed services and facilities to the proper user. c. Coordinates with ESF #2, through the SEOC, when |

| Agency | Functions |
|---|---|
| | <p>a representative of an organization at an incident location has requested regional communications resources or support.</p> <p>d. Coordinates with PEMA as necessary for any required Commonwealth-level communications support.</p> <p>e. Notifies the SEOC of any radio frequency devices being brought to an incident area.</p> <p>f. Notifies the SEOC when communications resources are to be withdrawn or discontinued.</p> <p>g. Notifies the SEOC when communications resources provided by ESF #2 are no longer required.</p> |
| External Support Organizations: | |
| Civil Air Patrol | Operates voice and data communications systems in support of military and civilian emergency services. |
| National Weather Service | Notifies the SEOC of weather watches or warnings affecting any part of Pennsylvania. |
| Volunteer Emergency Communications Resources | Resources may include Radio Amateur Civil Emergency Service (RACES), Amateur Radio Emergency Service (ARES), Military Affiliate Radio System (MARS), and Radio Emergency Associated Communications Team (REACT). These organizations supplement emergency communications systems in accord with available resources as requested by the SEOC. |
| Commercial Communications Providers | PSTN and cellular telephone provide the basic commercial methods of direction and control of emergency or disaster operations. In the event of failure of these systems, priorities for service restoration are communicated to providers. |