

Illinois Emergency Operations Plan

ESF-14 Cross Sector Business and Infrastructure

Appendix X-1 Information and Cyber Security

Illinois Emergency Management Agency and
Office of Homeland Security

September 23, 2026



Illinois Emergency Management Agency
and Office of Homeland Security



This page intentionally left blank.



State of Illinois Emergency Operations Plan (IEOP)
Emergency Support Function (ESF) ESF-14 Cross Sector Business and Infrastructure
Appendix X-1 Information and Cyber Security
Version: September 23, 2026

 State of Illinois Managed Plan Emergency Support Function (ESF) #14 Appendix X-1 Information and Cyber Security		
Title	ESF-14 Cross Sector Business and Infrastructure Appendix X-1 – Information and Cyber Security	
Managing Division/Branch	Division of Operations	Strategic Planning – Inter-Agency Strategic Planning Cell (ISPC)
Drafted/Evaluated	The ISPC, in coordination with the ESF planning group	September 2025
Evaluated Against	1. Prior version, if applicable. 2. Federal statutes and regulations. 3. State statutes and administrative codes. 4. Federal, state, and IEMA-OHS policies and directives. 5. National Preparedness Goal 6. National Response Framework 7. NRF Emergency Support Function Annexes 8. FEMA Community Lifelines 9. National Disaster Recovery Framework (NDRF) 10. IEMA-OHS policies, plans, and common definitions list. 11. Corrective actions from After-Action Reports (AARs) and real-world events where this ESF was engaged.	
Plan Type	☐ New ☒ Revised	
Branch Manager Review and Approval	Scott Gauvin, Manager of Strategic Operations and Preparedness	July 7, 2026
Senior Official Review and Approval	Theodore ‘Ted’ Berger, Director Clayton Kuetemeyer, Deputy Director Christopher Dodd, Chief of Operations Douglas Dorando, Chief Legal Counsel	September 23, 2026
Supersedes	August 2021, IEOP, Annex 22 Information and Cyber Security	



State of Illinois Emergency Operations Plan (IEOP)
Emergency Support Function (ESF) ESF-14 Cross Sector Business and Infrastructure
Appendix X-1 Information and Cyber Security
Version: September 23, 2026

State ESF-14, X-1 Coordinator	Support Agencies & Organizations
Illinois Emergency Management Agency and Office of Homeland Security (IEMA-OHS)	Illinois Emergency Management Agency and Office of Homeland Security (IEMA-OHS)
Primary State Agencies & Organizations	Illinois State Police (ISP)
Illinois Department of Innovation and Technology (DoIT)	Office of the Illinois Attorney General (OIAG)
Federal ESF-14, X-1 Coordinator	Illinois National Guard (ILNG)



Table of Contents

Record of Changes.....	4
1. Introduction.....	5
1.1. Purpose.....	5
1.2. Scope	5
1.3. Policy.....	5
1.4. Situation	6
1.5. Assumptions	6
2. Concept of Operations	7
2.1. General	7
2.2. Notification, Alert, and Warning (NAW).....	8
2.3. Activation.....	9
2.4. Communications.....	9
2.5. Resource Management	9
2.6. Reporting Requirements	9
2.7. Organization	10
3. Roles and Responsibilities	10
3.1. State ESF Coordinator.....	10
3.2. Primary State Agency/Organization	11
3.3. Support State Agencies/Organizations.....	12
4. Authorities.....	14
5. References.....	14
6. Acronyms & Definitions.....	15



Record of Changes

When changes are made to this document, the following procedures will be followed:

1. Changes will be issued by the Inter-Agency Strategic Planning Cell at IEMA-OHS and transmitted to agencies, personnel, and other designees specified by the IEMA-OHS Director or designee via electronic means.
2. When a change is made, an entry will be made in the following log:

CHANGE NUMBER	DATE ENTERED	PAGES OR SECTIONS CHANGED	ENTERED BY
1	September 2025	Bi-annual Review	Glenn Smith



1. Introduction

1.1. Purpose

- 1.1.1. Provide strategic and operational guidance to organizations on coordinated incidents and events that involve information technology (IT) systems and assets of the state, and that impact critical and lifeline infrastructure, the environment, and public safety.

1.2. Scope

- 1.2.1. This appendix addresses cyber or physical threats and/or incidents that have a disruptive impact on critical services, such as the inability of state agencies to deliver public safety, transportation, and human services.
- 1.2.2. This appendix is only applicable to state-supported information technology systems and assets.
- 1.2.3. This appendix supplements policies and procedures contained in the Illinois Emergency Operations Plan (IEOP) and may be implemented independently of other planning documents.
- 1.2.4. This appendix does not provide handling procedures for all potential incidents affecting IT systems and assets.
- 1.2.5. Laws, rules, regulations, and policies of the United States government and agencies involved in risk management, assessment, protective measures, and prevention activities for IT are considered applicable within the state.
- 1.2.6. For this appendix, clarifying definitions are provided in the IEOP Base Plan, Appendix X-8 Glossary of Terms.

1.3. Policy

- 1.3.1. Procedures for utilization, control, and use will incorporate operational priorities that include, but are not limited to:
 - 1.3.1.1. Protection of life
 - 1.3.1.2. Public health and safety



- 1.3.1.3. Property protection
- 1.3.1.4. Environmental protection
- 1.3.1.5. Restoration of essential utilities
- 1.3.1.6. Restoration of essential program functions, and
- 1.3.1.7. Coordination as appropriate.
- 1.3.2. The Governor or designee may authorize and direct the use of state resources to provide support and assistance to IT incident handling efforts for internal and external organizations after consideration of both priority of need and cost.
- 1.3.3. In situations where an imminent threat exists to life safety or an identified need for the protection of critical infrastructure and environment exists, priorities established within the IEOP take precedence over agency priorities.

1.4. Situation

- 1.4.1. An incident or threat of an incident has occurred with the potential to impact IT systems and assets of state government, resulting in consequences to critical resources, networks, and systems or information that are processed, stored, or transmitted, requiring prevention, protection, response, recovery, and/or mitigation activities.
- 1.4.2. Interruptions in essential services and processes provided through critical infrastructure sectors cause imminent life safety and/or significant economic loss, such as the Colonial Pipeline ransomware attack.

1.5. Assumptions

- 1.5.1. Cyber incidents will take many forms, including accidental, malicious, and physical occurrences.
- 1.5.2. Large-scale cyber incidents may overwhelm government and private-sector resources.
- 1.5.3. Complications from disruptions in information and services provided through IT and cyber systems, networks, and infrastructure may threaten lives, property,



the economy, and the public and private sectors' ability to deliver life safety and life-essential services.

- 1.5.4. Cyber incidents will have national consequences.
- 1.5.5. Rapid identification, information exchange, investigation, and coordinated incident handling and remediation will limit and mitigate the damage caused by the threat or actual occurrence of a significant cyber incident.
- 1.5.6. Delays in recognition or incident handling will increase potential consequences.
- 1.5.7. Delays in coordination, dissemination, and communication of cyber incident handling actions will increase potential consequences.
- 1.5.8. State agencies operating under the authority of constitutional officers will cooperate and coordinate incident handling with the Illinois Department of Innovation and Technology (DoIT) and the State Emergency Operations Center (SEOC) as appropriate.

2. Concept of Operations

2.1. General

- 2.1.1. Support for incident handling is coordinated through resources assigned to state agencies; however, external organizations are utilized on a routine basis through established contractual services.
- 2.1.2. For situations not requiring activation of the SEOC, DoIT will serve as the single point of coordination for joint information, rumor control, and the dissemination of cyber-related alerts, warnings, and public information.
- 2.1.3. IEMA-OHS will coordinate state consequence management activities through the SEOC.
 - 2.1.3.1. For the IEOP, consequence management includes but is not limited to:
 - 2.1.3.1.1. Protect public health and safety
 - 2.1.3.1.2. Restore essential government services, and



- 2.1.3.1.3. Provide emergency relief to governments, businesses, and individuals affected by an incident.
 - 2.1.3.2. DoIT will assist in the coordination and management of incident handling for cyber assets and implement prevention and protection protocols for state agencies.
 - 2.1.3.3. For joint information, rumor control, and the dissemination of statewide alerts, warnings, and public information, the SEOC, upon activation, will serve as the single point of coordination.
- 2.1.4. ISP will coordinate and manage law enforcement activities, including, but not limited to, prevention, protection, investigation, evidence collection, and adjudication of cyber incidents.
- 2.1.5. The Office of the Illinois Attorney General (OIAG) will coordinate with the appropriate prosecuting authorities in the prosecution of cybercrimes and assist in investigatory efforts of state agencies and external organizations.
- 2.1.6. The Illinois National Guard (ILNG) may assist and report to DoIT in the analysis of incident intelligence, development of situational awareness, and technical assistance to prevent, protect, respond to, recover from, and mitigate the effects of a cyber incident.

2.2. Notification, Alert, and Warning (NAW)

- 2.2.1. NAW to state agencies regarding cyber incidents will be carried out in accordance with DoIT's Computer Security Incident Response Plan (CSIRP).
- 2.2.2. DoIT will notify the IEMA-OHS SEOC Manager and Statewide Terrorism Intelligence Watch Center of a cyber incident requiring NAWs to stakeholders, key decision makers, and executive officers.
 - 2.2.2.1. IEMA-OHS will notify and alert agencies and organizations of the implementation of the IEOP and activation of the SEOC as appropriate, in accordance with SIREN standard operating procedures (SOPs).
 - 2.2.2.2. IEMA-OHS will utilize the Business Emergency Operations Center (BEOC) for NAWs to private sector partners as appropriate.



- 2.2.2.3. The STIC will commence sharing pertinent information with internal and external, private and public networks.
- 2.2.3. Primary and support agencies and organizations are responsible for internal and support partner NAW.

2.3. Activation

- 2.3.1. SEOC Management and Coordination SOP will be used to determine staffing levels necessary for SEOC operations and will be carried out in accordance with SEOC guidelines and procedures.
- 2.3.2. State agencies are responsible for the activation of agency support staff.

2.4. Communications

- 2.4.1. Direct coordination with federal agencies will occur through appropriate and designated agencies.

2.5. Resource Management

- 2.5.1. Resource management and logistics will be carried out in accordance with ESF-7, Resource Management and Logistics.
- 2.5.2. Resource management includes mutual aid and assistance agreements, the use of special federal and state teams, and resource mobilization protocols.

2.6. Reporting Requirements

- 2.6.1. DoIT will serve as the central point of contact for state agencies reporting cyber incidents or intrusions.
- 2.6.2. As appropriate for the type, scope, and magnitude of a cyber incident, DoIT will report disruptions and intrusions to potentially affected stakeholders, key decision makers, and executive officers in accordance with DoIT CSIRP.
- 2.6.3. Upon activation of the SEOC, state agencies will maintain situational updates, develop required intelligence briefings, and provide critical and priority information established for cyber incidents.



2.7. Organization

2.7.1. Direction and Control

- 2.7.1.1. DoIT will administer and manage the state's incident handling efforts and coordinate as appropriate with community partners.
- 2.7.1.2. Upon implementation of the IEOP and activation of the SEOC, the IEMA-OHS Director or designee will establish strategic and operational command, coordination, and control of state resources and support organizations required for consequence management in accordance with ESF-5 X-1, Direction, and Control.
- 2.7.1.3. IEMA-OHS will manage and utilize the BEOC and coordinate with DoIT to receive and disseminate disaster intelligence, establish common strategic priorities, and prioritize short-, intermediate-, and long-term activities among the SEOC and private sector organizations.
- 2.7.1.4. The ISP/STIC will share information and intelligence through several mechanisms with partners.

3. Roles and Responsibilities

3.1. State ESF Coordinator

3.1.1. Illinois Emergency Management Agency and Office of Homeland Security (IEMA-OHS)

- 3.1.1.1. Coordinates, integrates, and manages overall State efforts for ESF-14 Cross Sector Business and Infrastructure.
- 3.1.1.2. Manages and updates resource availability for ESF-14 Cross Sector Business and Infrastructure.
- 3.1.1.3. Assists in planning during activations and updates for overall ESF Plans.



3.2. Primary State Agency/Organization

3.2.1. Illinois Department of Innovation and Technology (DoIT)

- 3.2.1.1. Categorize cyber incidents and determine prioritization of efforts for state agencies.
- 3.2.1.2. Conduct and/or coordinate forensic analysis and attribute cyber incidents to the source, including preparation efforts necessary to prevent initial or follow-on acts and/or develop counter-options.
- 3.2.1.3. Identify, assess, and prioritize risks to inform prevention and protection activities, countermeasures, and investments.
- 3.2.1.4. Implement processes to prevent ongoing, additional, and cascading incidents based on information obtained from intelligence, threat assessments, alert networks, surveillance programs, and internal and external stakeholders and customers.
- 3.2.1.5. Determine the level of response necessary to implement appropriate courses of action.
- 3.2.1.6. Notify, activate, deploy, coordinate, implement, and sustain Computer Security Incident Response Team(s) assets.
- 3.2.1.7. Notify, alert, and warn state agencies, key stakeholders, and executive officers of potential and realized cyber incidents.
- 3.2.1.8. Notify the SEOC Manager of cyber incidents requiring notifications, alerts, and/or warnings to stakeholders, key decision-makers, and executive officers.
- 3.2.1.9. Coordinate incident handling activities to monitor identified threats and hazards and adjust levels of activity commensurate with the risk.
- 3.2.1.10. Assist state agencies in response to and recovery from cyber incidents.
- 3.2.1.11. Establish and disseminate cyber-specific guidance and protocols to state agencies.



- 3.2.1.12. Analyze damage from cyber incidents impacting critical and lifeline infrastructure, the environment, and public safety, to include overall minor disruptions that may cause a disproportionately significant impact on specific users, such as those with access and functional needs.
- 3.2.1.13. Coordinate public information and education campaigns with state agencies, key stakeholders, and executive officers. Ensure that all communication with the public is timely, clear, and accessible, regardless of physical, mobility, visual, hearing, cognitive, or financial needs, abilities, or impairments.
- 3.2.1.14. Coordinate with IEMA-OHS to activate a Joint Information System and establish the state Joint Information Center (JIC). Ensure that all communication with the public is timely, clear, and accessible, regardless of physical, mobility, visual, hearing, cognitive, or financial needs, abilities, or impairments.
- 3.2.1.15. Coordinate with IEMA-OHS to request implementation of the IEOP and activation of the SEOC to assist in consequence management.
- 3.2.1.16. Coordinate with local units of government and/or external organizations as applicable.
- 3.2.1.17. Maintain representation with the SEOC upon activation.
- 3.2.1.18. Request activation of the ILNG Intergovernmental Agreement (IGA) or external response assets through the SEOC.

3.3. Support State Agencies/Organizations

3.3.1. Illinois Emergency Management Agency and Office of Homeland Security (IEMA-OHS)

- 3.3.1.1. Coordinate with the DoIT representative to determine the need to implement the IEOP and activate the SEOC for consequence management efforts.
- 3.3.1.2. Determine the appropriate level of activation for the SEOC.



- 3.3.1.3. Notify agency representatives of SEOC activation in accordance with SOPs.
- 3.3.1.4. Coordinate and manage strategic and operational command, coordination, and control of state resources and support organizations required for consequence management.
- 3.3.1.5. Manage the state resource management system to address the identification, location, acquisition, storage, maintenance, testing, timely distribution, and accounting for services and materials.

3.3.2. Illinois State Police (ISP)

- 3.3.2.1. Assist law enforcement authorities having jurisdiction or investigative agencies in the forensic analysis, attribution, investigation, and adjudication of cyber incidents.
- 3.3.2.2. Coordinate and manage state law enforcement activities to halt, apprehend, or secure threats and/or hazards.
- 3.3.2.3. Identify, discover, or locate threats and/or hazards through active and passive surveillance and search procedures, including the use of systematic examinations and assessments, sensor technologies, or physical investigation and intelligence.
- 3.3.2.4. Through the Statewide Terrorism and Intelligence Center (STIC)
 - 3.3.2.4.1. Collect, analyze, and disseminate intelligence information.
 - 3.3.2.4.2. Conduct threat and risk analyses.
 - 3.3.2.4.3. Assist law enforcement as appropriate.
 - 3.3.2.4.4. Maintain representation with the SEOC upon activation.
 - 3.3.2.4.5. Share relevant information with vetted private and public organizations.

3.3.3. Office of the Illinois Attorney General (OIAG)



- 3.3.3.1. Coordinate with appropriate prosecuting authorities for the prosecution of criminal cases brought by the state.

3.3.4. Illinois National Guard (ILNG)

- 3.3.4.1. Assist in analysis of incident intelligence, development of situational awareness, and provide specialized technical expertise to prevent, protect, respond to, recover from, and mitigate the effects of a cyber incident.
- 3.3.4.2. Provide surge capacity in support of IEMA-OHS, DoIT, and ISP to help protect critical infrastructure and restore essential systems.
- 3.3.4.3. Activate IGA for external response assets with DoIT upon request and gubernatorial approval.

4. Authorities

1. Illinois Emergency Operations Plan, as amended.
2. Illinois Emergency Management Act, 20 ILCS 3305, as amended.
3. State Police Act, 20 ILCS 2610, as amended.
4. Attorney General Act, 15 ILCS 205, as amended.
5. Executive Order 2016-01, as amended.
6. State Guard Act, 20 ILCS 1815, as amended.
7. Department of Central Management Services Law, 20 ILCS 405, as amended.
8. DoIT/ILNG Intergovernmental Agreement, as amended.

5. References

1. Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 U.S.C. § 5121 et seq., as amended.
2. Homeland Security Presidential Directive 12 (HSPD 12)



State of Illinois Emergency Operations Plan (IEOP)
Emergency Support Function (ESF) ESF-14 Cross Sector Business and Infrastructure
Appendix X-1 Information and Cyber Security
Version: September 23, 2026

3. Department of Innovation & Technology Computer Security Incident Response Plan (DoIT CSIRP), as amended.
4. Illinois Emergency Operations Plan ESF-13, Public Safety and Security.

6. Acronyms & Definitions

1. For all definitions and acronyms addressed in this plan, please refer to the IEOP Base Plan, Appendix X-7 Glossary of Terms.