NEW HAMPSHIRE
STATE EMERGENCY OPERATIONS CENTER

EMERGENCY SUPPORT FUNCTION 17 - CYBERSECURITY

2019

Table of Contents

Acronyms

CDP	Cyber Disruption Plan
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DOD	Department of Defense
DOIT	Department of Information Technology
DOS	NH Department of Safety
EMAC	Emergency Management Assistance Compact
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
HSEM	NH Division of Homeland Security and Emergency Management
IC	Incident Commander
IEMAC	International Emergency Management Assistance Compact
ITSG	Information Technology Security Group
JIC	Joint Information Center
LOA	Letter of Agreement
MOU	Memorandum of Understanding
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NCIRP	National Cyber Incident Response Plan
NH-CIC	NH Cyber Integration Center
NHIAC	NH Information and Analysis Center
NHNG	NH National Guard
NHSP	NH State Police
NIMS	National Incident Management System
NIMS	National Incident Management System
NRF	National Response Framework
PIO	Public Information Officer
SEOC	State Emergency Operations Center
SEOP	State Emergency Operations Plan
SME	Subject Matter Experts
SOP	Standard Operation Procedure

Lead Agency

NH Department of Information Technology (DoIT)

Support Agencies

NH Department of Safety (DOS), Information and Analysis Center (NHIAC)

NH Cyber Integration Center (NH-CIC)

NH National Guard (NHNG)

NH Department of Safety, Division of Homeland Security and Emergency Management (HSEM)

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Introduction

Cyber incidents may take a number of different forms: an organized cyberattack, an exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical cyber infrastructure. Cyber incidents can occur at any time with little or no warning, may quickly overwhelm public and private sector resources, and result in secondary consequences that threaten life, safety, property, critical infrastructure, the economy, and/or the ability to deliver essential services. Cyber incidents may not be associated with specific geographical areas and may lack an easily identifiable signature. Cyber incidents may impede communications necessary for coordinating response and recovery actions.

While owners and operators of critical infrastructure systems can and should take precautions to protect their systems prior to the occurrence of a cyber incident, it is reasonable to assume that some owners/operators may have failed to or are unable to do so. Most cyber infrastructure is owned and operated by the private sector. Effective response to and recovery from a cyber incident will require cooperation and coordination between the public and private sectors. Rapid identification, robust information sharing, and coordinated investigative and response or remediation activities may limit the impacts of a cyber incident.

Purpose

In the event of a significant cybersecurity incident, ESF 17 provides a centralized entity for responding to a cyber incident that affects the State of New Hampshire. ESF 17 provides a means of defining, specifying, and maintaining the functions and resources required to ensure timely and consistent actions, communications, and response efforts. Additionally, ESF 17 ensures appropriate coordination and inclusion of necessary state, federal, and local agencies and private industry, in order to minimize the impact of a cybersecurity incident. Significant cybersecurity incidents may occur independently or in conjunction with disaster emergency operations and potentially could impact public health, safety, or critical infrastructure.

Concept of Operations

This annex will be activated at the direction of the DOIT Commissioner and HSEM Director when there is potential for or an actual disaster situation or a planned event affecting cybersecurity.

General

1. ESF 17 can be partially or fully activated, depending on the demands of an incident. The full activation of ESF 17 will be a joint decision between DoIT and HSEM, in accordance with the cyber severity matrix.
2. Not all cyber incidents will require standing up the SEOC, even if ESF 17 has been engaged. The State has resources and expertise that can be used to supplement local and private sector efforts. Federal assistance may be requested to support state and local efforts if an incident exceeds state and local capabilities. Depending on the magnitude of the incident, resources from other states or the federal government may not be available for use in New Hampshire for as long as 72 hours after a cyber incident is detected.
3. Core members of ESF 17 (i.e., DoIT CISO [or designee], ITSG, and NH-CIC) will be activated for any cyber event or incident, regardless of severity, at Level 1. This core group will be responsible for initiating the process of escalating response to address the needs of the incident.
4. DoIT CISO will coordinate the activities of ESF 17, as directed by the DoIT Commissioner and Incident Commander.
5. At the discretion of DoIT and HSEM, ESF 17 may receive a notification or situational awareness update during a low severity incident, but will not be activated beyond the core members.
6. Once an incident escalates from low to medium severity, ESF 17 will be partially activated.
7. During a partial activation, a small contingency of ESF 17 will implement response operations under the direction of ESF 17 leadership.
8. Membership of this contingency will be determined by DoIT and HSEM, at the time of activation, in order to meet the needs of the incident.
9. Once an incident escalates from medium to high severity, ESF 17 will be fully activated.
10. During a full activation, the State Emergency Operations Center (SEOC) will be operational and complete (or near-complete) membership of ESF 17 will be utilized.
11. DoIT and HSEM will virtually activate ESF 17 as needed, to support response activities.

Organization

1. **Command & Control:** ESF 17 shall function under the direction and control of the Information and Planning Section under the SEOC Planning Chief. ***(See Organizational Chart in SEOP Base Plan.)***

2. **Operational Facilities/Sites**
   a. New Hampshire Cyber Integration Center (NH-CIC-E and NH-CIC-W)

3. **Federal Resources:** When ESF 17 anticipates or has a need for resources not otherwise available, action will be taken to secure such resources through the *National Response Framework* (NRF) or some other federal source. This request should be coordinated through the SEOC Planning Chief, as required.

   The National Cyber Incident Response Plan (NCIRP) outlines DHS/CISA statutory responsibilities. These include reporting suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary; restoring operations; and recommending ways to improve security.

   Report if the cyber incident may:

   a. Result in a significant loss of data, system availability, or control of systems
   b. Impact a large number of victims
   c. Indicate unauthorized access to or malicious software present on critical IT systems
   d. Affect critical infrastructure or core government functions
   e. Impact national security, economic security, or public health and safety

   The DHS/CISA National Cybersecurity and Communications Integration Center (NCCIC), NCCIC@hq.dhs.gov, (888) 282-0870, provides the following:

   a. Information exchange
   b. Training and exercises
   c. Risk and vulnerability assessments
   d. Data synthesis and analysis
   e. Operational planning and coordination
   f. Watch operations
   g. Incident response and recovery

4. **Contracts and Contractors:** Resources that are available through ESF 17 may, at times, best be obtained through a contractor. State of NH contracts or private sector contracts should be facilitated through Logistics and ESF 7 – Resource Support.

Notification

1. DOIT will notify HSEM when a cybersecurity event or incident is classified at Level 1 on the State Cyber Severity Matrix.
2. HSEM will notify the lead agency points of contact when there is an immediate or anticipated SEOC activation requiring ESF 17 representation.
3. The lead agency will then notify the support agencies and determine coverage for the ESF 17 desk in the SEOC.
4. ESF 17 agencies will make notifications to their appropriate regions, districts, local offices, etc.
5. The above notification process will be utilized for all phases of activation and activities in which the ESF 17 will be involved.

Event Reporting

1. WebEOC will be utilized to provide continuous situational awareness.
2. Position logs should be maintained by each ESF agency in sufficient detail to provide information on activities taken during the event.
3. Agencies are also expected to keep their lead agency updated upon all activities and actions.
4. The lead agency will be responsible for making periodic reports to the Operations Section Chief on activities taken by the ESF during the event and assure they are properly documented.
5. Lead and support agencies must maintain financial records of all activities and costs during the event. The records will be turned into the lead agency when requested.

ESF Actions

Prevention/Preparedness Actions

1. Maintain situational awareness through coordination with ESF 17 support agencies for current inventories of available resources.
2. Participate in state exercises or conduct an exercise to validate this Annex and supporting SOPs.
3. Support the Emergency Management Assistance Compact (EMAC) and the International Emergency Management Assistance Compact (IEMAC), including training of ESFs on EMAC/IEMAC responsibilities and pre-identification of assets, needs, and resources that may be allocated to support other states/provinces.
4. Annually review the Federal Department of Homeland Security Core Capabilities and integrating tasks as appropriate.
5. Integrate NIMS principles in all aspects of planning for ESF 17.
6. Maintain notification systems to support emergency/disaster response.
7. Maintain personnel lists and resource contacts in a state of readiness appropriate to existing and anticipated emergency conditions.

8. Ensure training and personnel rosters for assignment to the SEOC during activation. Prepare for sufficient personnel for an extended and/or 24-hour activation period.
9. Users of networked systems may prevent cyber incidents by proper usage of networks, systems, and applications in compliance with applicable information security policies.
10. Users of networked systems may prevent cyber incidents by creating, implementing, and maintaining policies, and procedures to secure networks, systems, and applications.
11. Ensure procedures and program/contact information are up-to-date. Discuss lessons identified from incidents and exercises and explore creative ways to leverage resources.
12. Communicate and share information with other lead and supporting agencies/organizations, and with other agencies/organizations, as appropriate.
13. Collaborate with other lead and supporting agencies/organizations and others, as appropriate, on prevention/protection/mitigation initiatives.
14. Develop and maintain operational plans and procedures, resource directories, and emergency contact lists to support ESF 17 activities, including response and recovery actions.
15. Ensure all lead and supporting agencies/organizations have at least primary and secondary points of contact and other pre-designated staff, as necessary, to support this annex and SEOC operations.
16. Ensure all lead and support agencies/organizations' responders are properly and regularly trained in WebEOC.
17. Ensure that HSEM's Operations Section has a current roster of lead and supporting agency/organization primary and secondary points of contact and that HSEM's Operations Section is promptly notified of staff changes. Contact information should be readily updated in WebEOC.
18. Ensure procedures are in place to quickly notify and communicate with primary and secondary points of contact each lead and supporting agency/organization, and for other personnel who may be called upon to support this plan.
19. Ensure that points of contact and support staff of lead and supporting agencies/organizations who may be called upon to support this annex or SEOC operations are and remain properly trained on ESF 17 and SEOC procedures and operations.
20. Develop coordination mechanisms, strategies, and requirements for post-incident assessments, plans, and activities that are scalable to incidents of varying types and magnitudes.
21. Conduct after action discussions of prior ESF 17 efforts and other studies to improve future operations.
22. Develop long-term strategies and plans in coordination with other relevant stakeholders to address key ESF 17 issues regarding cyber incidents.
23. Develop plans, procedures, and guidance delineating appropriate participation and available resources that take into account the differing technical needs and statutory responsibilities.

Response Actions

1. Assign and schedule sufficient personnel to cover an SEOC activation for an extended period.
2. Provide updates and briefings for personnel reporting for ESF 17 duty.
3. Notify ESF 17 counterparts in the threatened or impacted areas.
4. Generate information to be included in SEOC briefings, situation reports, and/or action plans.
5. Evaluate and respond to ESF 17 mission/task requests, including providing available resources, equipment, and personnel for fulfilling ESF missions. Maintain situational awareness of resources committed to an incident.
6. Consult Cyber Disruption Plan for specialized actions.
7. Support requests and directives resulting from a Governor's State of Emergency Declaration and/or Presidential Disaster Declaration.
8. Oversee and track containment and restoration activities, including actions taken, resource assignments, and notifications.
9. Provide situational awareness and subject-matter expertise and solutions during a response.
10. Identify appropriate subject matter experts to recognize threats and vulnerabilities to IT networks, with respect to emergency management objectives and priorities for potential cyber-related events.
11. Identify appropriate subject matter experts to ascertain remediation and mitigation measures (e.g., plans, procedures, hardening measures, etc.) for threats and vulnerabilities, with respect to emergency management objectives and priorities for potential cyber-related events.
12. Make an initial determination of damage, compromise, and risk; identify immediate corrective actions to contain damage, minimize risk, and preserve evidence.
13. Engage appropriate subject matter experts to assess threat and risk levels and make recommendation for immediate action.
14. Monitor disruption events to determine scale and scope and to determine if the event is contained or escalating.
15. Gather and share information that may indicate the development of a larger or more regional-level disruption event.
16. Provide other cybersecurity experts or representatives in the region with situational awareness and assistance during a catastrophic incident as necessary and possible.
17. Help coordinate IT-related response activities pursuant to an Incident Action Plan.
18. Coordinate with emergency management support staff to procure critical cyber-related resources.
19. Provide situational awareness and subject matter expertise and solutions for an Incident Commander during a response, including:

a. Assist Operations Staff in understanding technical and operational issues regarding cyber-related resources and networks.

b. Assist Planning Staff in the development of priorities and objectives of a long-term response to a large-scale cyber disruption incident.

20. Coordinate ESF 17 support to other ESFs regarding primary, secondary, or cascading impacts. Ensure that other ESFs have an understanding of these impacts and their relationship to potential, perceived, or actual threats.

21. Conduct ongoing reassessment of priorities and strategies to meet the most critical needs.

22. **Radiological Emergency Preparedness Actions**
    a. Refer to the ESF 17 section of the *NH Radiological Emergency Response for Nuclear Facilities Incident Annex, Attachment A – Implementing Procedures for State Agencies.*

Recovery Actions

1. Maintain information and status of cybersecurity infrastructure to SEOC Planning via WebEOC.
2. Continue to coordinate activities and requests with partner ESFs.
3. Coordinate replacement and restoration of damaged or destroyed equipment and facilities in the affected areas.
4. Generate information to be included in SEOC briefings, situation reports, and/or action plans.
5. Ensure ESF 17 lead and support agencies document event-related costs for any potential reimbursement.

Mitigation Actions

1. Participate in continuous employee education on cyber security.
2. Monitor network traffic for suspicious activity in coordination with DoIT, NHIAC, NHSP, and HSEM.
3. Know where sensitive data resides and be aware of the protection strategy, including encryption and monitoring.
4. Perform annual penetration testing and routine vulnerability assessments.
5. Prepare for worst-case scenarios.
6. Provide input to the State Hazard Mitigation Plan as needed.
7. Support and plan for mitigation measures, including monitoring and updating mitigation actions in the State Hazard Mitigation Plan.
8. Support requests and directives from the Governor and/or FEMA concerning mitigation and/or redevelopment activities.

Responsibilities

General

1. Agencies will provide Subject Matter Experts (SMEs) to support ESF 17 in the SEOC.
2. Agencies will maintain inventories/databases, status of availability, and procedures to obtain access to and use of their cybersecurity assets.
3. Participate in the evaluation and mission assignment of ESF 17 resource requests submitted to the SEOC, including resources that are available through mutual aid agreements, compacts, contracts, etc.

Agency Specific

Lead Agency

NH Department of Information Technology (DoIT)

1. Notify HSEM when a cybersecurity event or incident is classified at Level 1 on the State Cyber Severity Matrix.
2. Implement the state Cyber Disruption Plan, if appropriate.
3. Oversee the development of an incident-specific response strategy.
4. Monitor disruption events to determine scale and scope and to determine if the event is contained or escalating
5. Provide other cybersecurity experts or representatives in the region with situational awareness and assistance during a catastrophic incident, as necessary and possible.
6. Determine whether to activate cyber insurance policy or assign responsibility for doing so.
7. Oversee and track containment and restoration activities including actions taken, resource assignments, and notifications.
8. Conduct technical discovery, threat, and impact analysis in support of incident response.
9. Staffing the ESF 17 desk in the SEOC, as appropriate and as set forth in this Annex.
10. Identify, train, and assign personnel to staff ESF 17 in the SEOC.
11. Notify all ESF 17 supporting agencies upon activation.
12. Assign personnel to the ESF 17 duty schedule at the SEOC.
13. Provide staff and resources necessary to conduct impact assessments of the affected area(s).

Support Agencies

1. **NH Department of Safety, Information and Analysis Center (NHIAC)**
   a. Gather, analyze, and communicate pre-incident intelligence from multiple sources.
   b. Maintain critical infrastructure and key resources sector contact distribution lists.
   c. Provide accurate and timely intelligence products.
   d. Provide direct analytical support for investigations involving precursor criminal activity.

e. Promote awareness of priority intelligence requirements and of indicators of threats to the State.

f. Conduct threat information sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation.

g. Assist in attributing the source of cyber-attacks through NHIAC resources and the network of fusion centers.

2. **NH Cyber Integration Center (NH-CIC)**
   a. Facilitate information sharing amongst state response partners.

   b. Provide real-time intelligence during a cyber incident.

   c. Support response operations as requested.

   d. Conduct technical discovery, threat, and impact analysis in support of incident response.

   e. Provide updates to the DoIT Commissioner and CISO, or designees, as requested.

   f. Provide subject matter expertise as requested.

   g. Participate in coordination calls to communicate relevant updates and concerns to leadership.

   h. Gather and share information that may indicate the development of a larger or more regional-level disruption event.

   i. Record observations during response operations to inform after action reporting.

3. **NH National Guard (NHNG)**
   a. Assist with pre-disaster planning and resource acquisition.

   b. Assist with emergency response by providing technical expertise and guidance as allowed by activation status.

   c. Inform the development of the state's technical response strategy (i.e., pre-incident planning).

   d. Provide incident response augmentation, cyber incident hunt teams, cyber incident mitigation and recovery actions.

   e. Share and synchronize actions and information with and among mission partners in order to protect United State Department of Defense (DOD) information networks, software, and hardware and enhance situational awareness to improve preparedness for DOD mission requirements, and to improve cybersecurity unity of effort.

   f. Engage in training activities during which mission partners participate or observe for the purpose of sharing best practices and enhancing DoD cyberspace-related knowledge, skills, and capabilities.

g. Provide advice to mission partners that aids in the development of potential strategies, plans, and solutions for preventing, protecting, and defending against, responding to, mitigating the effects of, and recovering from cyber incidents.

h. Support mission partners in their prevention of, protection against, mitigation against, and recovery from a cyber incident.

4. **NH Department of Safety, Division of Homeland Security and Emergency Management**
   a. Coordinate with DoIT Commissioner to activate the CDP.
   b. Support DoIT in the coordination of response to a significant incident.
   c. Assign responsibility for communications during a significant incident.
   d. Coordinate with the DoIT Commissioner to schedule and facilitate a coordination call with key stakeholders.

5. **Multi-State Information Sharing and Analysis Center (MS-ISAC)**
   a. MS-ISAC Security Operations Center, 866-787-4722, soc@msisac.org
   b. Incident response assistance in the following areas:
      i. Emergency conference calls
      ii. Forensic analysis
      iii. Log analysis
      iv. Mitigation and response recommendations
      v. Reverse engineering
      vi. Threat intelligence

Coordination with Other Emergency Support Functions

ESF 17 will coordinate with other ESFs through the SEOC by:

1. Notifying organizations of available resources.
2. Providing availability of subject matter experts for specialized requests.
3. Providing communications and alerting support for other ESF responders and to meet needs as requested and as capable.

Mutual Aid

Lead and support agencies will maintain up-to-date agreements and Memoranda of Understanding/Letters of Agreement (MOU/LOA) with various other agencies, regions, states, or countries, as appropriate.

Each agency is responsible for keeping these documents updated and with appropriate points of contact. Support agencies should keep the lead agency informed of any such agreements that may affect resources or capabilities during an emergency incident.

The State of New Hampshire also maintains agreements and mutual aid compacts on behalf of various organizations. These may be activated as the situation warrants.

Resource List

Contracts

1. New Hampshire Cyber Insurance

Attachments

Plans/Procedures, Etc.

1. State of New Hampshire Cyber Disruption Plan, 2018, Department of Information Technology and Department of Safety, Homeland Security and Emergency Management

Record of Update

Date	Title and Agency of ESF Lead Approving Update