State of New Hampshire

Cyber Incident Response Plan

(CIRP)

February 2024

Foreword

February 2024

The State of New Hampshire's Cyber Incident Response Plan (CIRP) was developed jointly by the Department of Information Technology and the Department of Safety, Homeland Security and Emergency Management through a series of Tabletop Exercises (TTX). It is complementary to, and provides a level of detail required to execute, Emergency Support Function Seventeen (ESF-17) under the New Hampshire State Emergency Operations Plan (SEOP).

Purpose: The purpose of the CIRP is to provide an executive level framework to effectively respond to and recover from cyber incidents. It aims to minimize the impact of cyber incidents on Agencies' operations, reputation, and ability to deliver essential government services.

Method: The CIRP is in continuous execution. We will continuously use Risk Assessments to identify and assess potential cyber threats and vulnerabilities based on the potential impact to operations. The plan will document roles and responsibilities and a communications plan for use when an incident occurs. When an incident occurs, it will be managed through the following phases.

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity

The CIRP will also be reviewed and exercised at least annually using a Tabletop Exercise (TTX) with one or more Agencies participating. Lessons learned from these TTXs will be used to refine and improve the CIRP.

End State: The Executive Branch of the State Government of New Hampshire can effectively detect, respond to, and recover from cyber incidents. The State Government is resilient to cyber threats, minimizing the impact on critical operations and maintaining trust with residents, visitors, and businesses that do business with New Hampshire. The CIRP is continuously refined to address emerging cyber threats and comply with regulatory standards.

Denis C. Goulet
Commissioner, Department
of Information Technology

Robert M. Buxton
Director, Homeland Security and
Emergency Management

Revision List

Table 1: Plan Revisions

Name	Title	Content Revised	Date of Revisions
Janice Schultz	Security Specialist	Add confidential/limited release language to header and Promulgation.	16 Apr 2019
Janice Schultz	Security Specialist	Changed Cyber Emergency Support Function Identifier.	28 Jan 2020
Doug Schelb	Deputy CISO	Removed confidential/limited release language. General update of CIRP and addition of Scenario Playbooks.	10 Jan 2024

Contents

Background

The New Hampshire CIRP was developed in recognition of (1) society's deep dependence on technologically systems and (2) the profound, detrimental effects that disruptions to these systems can have on public safety, critical infrastructure, and delivery of essential government services.

Situation

Cyber threats are continuously evolving, becoming a more complex and costly issue for individuals, companies, and government entities alike. Now more than ever, threat actors at home and abroad are using cyber-attacks as a means for profit, espionage, and warfare. The low-risk, high-reward nature of cyber-attacks make them an attractive mechanism for inflicting social, economic, and technological damage.

As noted in **Cybersecurity Trends Point to More Sophisticated Attacks Ahead (govtech.com),** current trends suggest a steady increase in the frequency, number, and sophistication of cyber-attacks that the State of New Hampshire will face. The single biggest threat in New Hampshire will remain a ransomware attack directed at theft or compromise of sensitive data in state government agencies, municipalities, school districts, and the health care and emergency services sectors. The primary attack vector will remain human behavior, with social engineering techniques being leveraged in an estimated 74 percent of breaches globally per the **Verizon 2023 Data Breach Investigations Report.**

Although good cyber hygiene practices, a focus on cyber resiliency, continuous cybersecurity awareness training and management of third-party cyber risks can help prevent or lessen the impact of such attacks, there is no perfect defense. Since the impacts of a cyber incident can pose great risk to government and public services, the State of New Hampshire is focused on preparing for and mitigating the effects of such incidents. The coordination between Agencies, Emergency Management, and Law Enforcement is vital to effectively prevent, respond to, and recover from disruption resulting from cyber incidents.

Purpose

The CIRP will provide an operational guide for response to a cyber incident in New Hampshire and provides emergency management, information technology (IT), and other relevant stakeholders with a framework for planning, coordinating, and communicating response activities. To accomplish this, the CIRP will outline:

- A schema to identify the severity of a cyber event or incident and the points by which escalation or de-escalation may be required.
- Roles and responsibilities for response partners and stakeholders to a cyber incident.
- A concept of operations, including phases of response to a cyber incident, reporting requirements, and response operations; and
- An approach to operational communications.

Scope

The CIRP provides guidance to all State agencies and ESF-17 members. Depending on the severity of the incident it may supersede Agency policies. The CIRP defines a framework to coordinate cyber incident response across the State Government.

Emergency Support Function 17

The CIRP framework supports response to significant cyber incidents through Emergency Support Function 17 – Cyber (ESF-17). ESF-17 is comprised of subject-matter experts in the emergency management, IT, and law enforcement fields. ESF-17 was specifically developed to plan for and respond to cyber incidents impacting the State of New Hampshire. For the specific uses of this document, ESF-17 and Unified Command shall be engaged if the initial triage of an event indicates the need for a significant response.

Plan Alignment

- The CIRP aligns with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and address the requirement in NIST 800-53 Rev 5 (IR control family) for organizations to develop and implement an incident response plan to guide response activities, and that addresses organizational roles and responsibilities, resources available, and coordination and information sharing.
- The CIRP also aligns with the National Cyber Incident Response Plan (NCIRP) which was developed in accordance with Presidential Policy Directive (PPD) 41 on U.S. Cyber Incident Coordination. The NCIRP leverages doctrine from the National Preparedness System to support seamless integration with the Federal Emergency Management Agency (FEMA) and enable coordination of cyber and physical incident response at the national level.
- New Hampshire CIRP is designed to support similar coordination at the State level through alignment with the State Emergency Operations Plan (SEOP) and integration of Emergency Support Function 17 (ESF-17).

Definitions

- For the purposes of this plan, cyber incidents will be defined according to National Institute of Standards and Technology’s Cybersecurity Framework and the National Cyber Incident Response Plan (NCIRP) and Presidential Policy Directive 41:
  - A **“cybersecurity event”** is a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
  - A **“cybersecurity incident”** is a cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery.
  - A **“significant cyber incident”** is a cyber incident (or group of cyber incidents) that is (or together, are) likely to result in demonstrable harm to the State of New Hampshire security interests or economy or to the public confidence, civil liberties, or public health and safety of its residents.

Planning Assumptions

- ESF-17 leadership and member involvement will vary depending upon the nature of the impact and cause of the event.
- State Agencies and organizations may be tasked with response operations, regardless of federal agency involvement.
- Each Agency and organization involved in the response operations will make every effort to adequately staff response roles and functions. However, State, and federal partners, as well as private- and public-sector organizations may be contacted for support when staffing needs exceed the State's capacity.
- State Agencies are responsible for coordinating with NH CIC and ESF-17 to support collective cyber incident response.

Roles and Responsibilities

The State of New Hampshire works with public and private sector partners to respond to, resolve, and recover from disruptive effects of cyber incidents regardless of what caused the incident. The State facilitates collaboration across all entities participating in cyber incident response.

Although the nature of response varies by event type and impact, overall planning and response roles and responsibilities are defined for key partners. The sections below describe planning and response roles and responsibilities supporting ESF-17.

Planning Roles and Responsibilities

Party	Planning Roles and Responsibilities
HSEM Director (or designee)	• Maintain ESF-17 contact list in WebEOC (in coordination with DoIT) for easy access and use during a cyber incident. • Maintain critical infrastructure and key resources sector contact distribution lists (in coordination with the State Information and Analysis Center). • Assign support to DoIT for after-action reporting, as needed. • Coordinate pre-incident emergency management resource acquisition. • Maintain situational awareness of the State's technical response strategy (i.e., pre-incident planning) in coordination with the DoIT Commissioner and the Chief Information Security Officer. • Coordinate with DoIT to facilitate training, exercising, and updating the CIRP. • Coordinate across the Department of Safety as necessary to support pre-incident planning and coordination.
DoIT Commissioner (or designee)	• Oversee the development of a technical response strategy (i.e., pre-incident planning) in coordination with HSEM and the Chief Information Security Officer (CISO). • Coordinate pre-incident information technology resource acquisition. • Assign responsibility for facilitation of after-action reviews and reporting (with support from HSEM). • Coordinate with HSEM to facilitate training, exercising, and updating the CIRP. • Attend training, exercises, and planning meetings as requested.

Party	Planning Roles and Responsibilities
DoIT Chief Information Security Officer (or designee)	• Oversee the development technical response strategy. • Facilitate pre-incident planning (in coordination with HSEM and the DoIT Commissioner). • Support or facilitate after-action reviews and reporting (with support from HSEM). • Coordinate with HSEM to facilitate training, exercising, and updating the CIRP. • Attend training, exercises, and planning meetings as requested. • Regularly review Cybersecurity Advisory Committee membership and ensure that members are appropriately trained on the CIRP. • Budget and contract for cybersecurity services to include retainers for Forensics/Incident Response, Negotiations, and Cryptocurrency services.
New Hampshire Cyber Integration Center (NH-CIC)	• Partner with DoIT Departments to development the State's technical response strategy (i.e., pre-incident planning). • Conduct discovery, threat, and impact analysis pre- and post-incident. • Prepare for after-action reporting. • Gather, analyze, and share cyber intelligence from multiple sources. • Attend training, exercises, and planning meetings as requested.
Incident Response Team (IRT)	• Inform the development of the state's technical response strategy (i.e., pre-incident planning). • Support after-action reporting, as needed. • Attend training, exercises, and planning meetings as requested. • Inform the State's approach to security by providing input during standing meetings.
New Hampshire Cybersecurity Advisory Committee (CAC) / Agency Information Security Officers (ISO)	• Inform the development of the State's technical response strategy (i.e., pre-incident planning) • Represent the security perspective of assigned agency(ies) during planning, training, exercises, and after-action reporting and conversely, share feedback with assigned agency(ies). • Attend training, exercises, and planning meetings as requested. • Inform the State's approach to cybersecurity by providing input during standing meetings. • Review and understand cyber risk and impact to the Agencies ability to deliver government services. • Review and understand cyber risk and impact based on Agency continuity of operations plans and procedures.

Party	Planning Roles and Responsibilities
DOIT Business Relationship Management Division (BRMD) IT Leaders	• Inform the development of the State's technical response strategy (i.e., pre-incident planning). • Coordinate with assigned agency(ies) during planning, training, exercises, and after-action reporting and conversely, share feedback with assigned agency(ies). • Attend training, exercises, and planning meetings as requested. • Review and understand cyber risk and impact based on Agency delivery of government services. • Review and understand cyber risk and impact based on Agency continuity of operations procedures. • Provide Agency system information and assessed operational impact to CISO or designee.
Advisory Committee on Emergency Preparedness and Safety (ACEPS), Cybersecurity Subcommittee	• Inform the state's approach to cybersecurity by providing input during standing meetings.
State Agency Leadership	• Attend cybersecurity training, exercises, and planning meetings as requested. • Review and understand cyber risk and impact based on agency delivery of government services. • Include cyber risk and impact in Agency continuity of operations procedures. • Report suspicious events expeditiously to the DoIT Help Desk. • Adhere to regulatory and legal requirements when reporting cyber incidents. • Assume stewardship of the agency's data. • Where needed, develop Agency specific cyber incident response plans and procedures that support the CIRP.
Department of Safety (and relevant subdivisions)	• Inform the development of the State's technical response strategy (i.e., pre-incident planning). • Support after-action reporting. • Attend training, exercises, and planning meetings as requested. • Collaborate with DOIT to implement, maintain, and update the CIRP.
New Hampshire Information and Analysis Center (IAC)	• Gather, analyze, and communicate pre-incident intelligence from multiple sources. • Maintain critical infrastructure and key resources sector contact distribution lists (in coordination with HSEM).

Party	Planning Roles and Responsibilities
New Hampshire National Guard	• Assist with pre-disaster planning and resource acquisition. • Inform the development of the State’s technical response strategy (i.e., pre-incident planning). • Attend training, exercises, and planning meetings as requested (and as allowed by activation status).
Federal Partners	• At the request of the State of New Hampshire, provide intelligence support, resources, and technical assistance to inform pre-incident planning, training, or exercises.

Response Roles and Responsibilities

Party	Response Roles and Responsibilities
HSEM Director (or designee)	• Coordinate with DoIT Commissioner to activate ESF-17. • Activate the State Emergency Operations Center and Unified Command as required by the level of impact. • Coordinate the response to a significant incident. • Enable internal and external communications during a significant incident. • Provide unified command response leadership (i.e., facilitate response activity prioritization). • Facilitate engagement of local, State, and federal entities. • Liaise with and engage subdivisions of the Department of Safety. • Coordinate with the DoIT Commissioner to schedule and facilitate a coordination call with key stakeholders. • Assist Planning Staff in the development of priorities and objectives of a long-term response to a significant cyber incident. • Assist Operations Staff in understanding technical and operational issues regarding cyber-related resources and networks. • Record observations during response operations to inform after-action reporting.
DoIT Commissioner (or designee)	• Coordinate with HSEM Director to activate ESF-17. • Recommend activation of the Unified Command as required. • Oversee the development of an incident-specific response strategy. • Coordinate with the CISO and NH-CIC to determine appropriate, incident-specific membership of the response team. • Provide unified command response leadership (i.e., facilitate response activity prioritization). • Coordinate with the HSEM Director to schedule and facilitate coordination calls with key stakeholders. • Monitor events to determine scale and scope, and to determine if the event is contained or escalating (in coordination with DoIT CISO). • Provide other cybersecurity experts or representatives in the region with situational awareness and assistance during a catastrophic incident as necessary and possible. • Record observations during response operations to inform after-action reporting. • Determine whether to request support from State contracted cybersecurity services retainer (Forensics/Incident Response, Negotiations, Cryptocurrency services).

Party	Response Roles and Responsibilities
DoIT Chief Information Security Officer (or designee)	• Notify HSEM when a cyber event is assessed to be a "significant cyber incident" (in coordination with the DoIT Commissioner [or designee]). • Develop an incident-specific response strategy. • Coordinate with the DoIT Commissioner and NH-CIC to determine appropriate, incident-specific membership of the response team. • Lead or appoint a designee to the lead the NH-CIC. • Provide situational awareness, guidance, remediation options, and communicate updates to the DoIT Commissioner and/or HSEM Director (or designees) as required. • Oversee and track containment and restoration activities including actions taken, resource assignments, and notifications. • Monitor disruption events to determine scale and scope, and to determine if the event is contained or escalating (in coordination with DoIT Commissioner). • Record observations during response operations to inform after-action reporting. • Coordinate the activities of ESF-17, as directed by the DoIT Commissioner and Incident Commander. • Serve as lead for coordination with State contracted cybersecurity services retainer (Forensics/Incident Response, Negotiations, Cryptocurrency services).
New Hampshire Cyber Integration Center (NH-CIC)	• Coordinate with the DOIT Commissioner and CISO to determine appropriate membership for incident response team (IRT). • Serve as core members of the IRT for all responses. • Facilitate information sharing amongst State response partners. • Provide real-time updates during a cyber incident. • Support response operations as requested. • Conduct technical discovery, threat, and impact analysis in support of incident response. • Provide updates to the DoIT Commissioner and CISO, or designees, as requested. • Provide subject matter expertise as requested. • Participate in coordination calls to communicate relevant updates and concerns to leadership. • Gather and share information that may indicate the development of a larger or more regional-level disruption event. • Record observations during response operations to inform after-action reporting.
Incident Response Team (IRT)	• Execute incident response actions to support threat detection and analysis, containment and eradication, and recovery. • Support response operations as requested. • Provide subject matter expertise as requested. • Participate in coordination calls to communicate relevant updates and concerns to leadership. • Record observations during response operations to inform after-action reporting.

Party	Response Roles and Responsibilities
New Hampshire Cybersecurity Advisory Committee (CAC) / Agency Information Security Officers (ISO)	• Serve as the senior Agency representative for incident response coordination in the absence of Commissioner, Deputy Commissioner, or Executive Director. • Support response operations as requested. • Provide subject matter expertise on Agency operations as requested. • Participate in coordination calls to communicate relevant updates and concerns to leadership. • Record observations during response operations to inform after-action reporting.
DoIT Business Relationship Management Division (BRMD) IT Leaders	• Provide system information and business operational impact to DoIT CISO, or designee. • Liaise with assigned state agency(ies) and DoIT operational work units as required. • Provide incident information to DoIT CISO, or designee. • Engage program experts/system owners as required. • Record observations during response operations to inform after-action reporting.
Advisory Committee on Emergency Preparedness and Safety (ACEPS), Cybersecurity Subcommittee	• Not part of response efforts.
State Agency Leaders	• Support response operations as requested. • Provide subject matter expertise on Agency Operations and Risk to delivery of essential government services. • Participate in coordination calls to communicate relevant updates and decisions. • Activate continuity of operations and/or data classification protocols as required. • Record observations during response operations to inform after-action reporting.
Department of Safety	• Provide subject matter expertise as requested. • Engage law enforcement or other specialized partners as necessary to investigate potentially criminal incidents and/or secure public safety. • Support response operations as requested. • Record observations during response operations to inform after-action reporting.

Party	Response Roles and Responsibilities
New Hampshire Information and Analysis Center (IAC)	• Provide real-time intelligence during a cyber incident. • Provide subject matter expertise as requested. • Support response operations as requested. • Gather and share information that may indicate the development of a larger or more regional-level disruption event. • Record observations during response operations to inform after-action reporting.
New Hampshire National Guard	• Assist with emergency response by providing technical expertise and guidance as allowed by activation status. • Record observations during response operations to inform after-action reporting.
Federal Partners	• At the request of the State of New Hampshire, provide response support, including provision of intelligence, resources, and technical assistance. • Gather and share information that may indicate the development of a larger or more regional-level disruption event. • Record observations during response operations to inform after-action reporting as appropriate or able.

Concept of Operations

Plan Execution

In the modern information environment, cyber incidents are a part of normal operations. The roles and responsibilities, phases, and actions outlined in the CIRP will guide State response for all cyber incidents regardless of scale or severity. During normal operations, most cyber incidents can be managed at the entity-level (i.e., limited State response and support is required) and will not require activation of ESF-17. However, if any of the following conditions are met or appear to be met, the DOIT Commissioner will classify the event as a significant cyber incident and coordinate with the HSEM Director to activate ESF-17 and the Unified Command and thereby transition incident management from the entity level to Incident Command System:

- Scope/Severity: Potential breach and/or disruption affecting more than one State agency.
- Scope/Severity: The majority of a single agency's workforce and/or significant impact to 1000 or more users.
- Scope/Severity: Any impact to public health or safety.
- Business Impact: Significant impact to a core business function of one or more agencies.
- Public Impact: The incident will/may have significant public impact (e.g., core public services or constituent data is affected).
- Public Interest: The incident could generate significant public interest (e.g., press interest).

ESF-17 Organization

ESF-17, the State of New Hampshire's primary means to respond to a cyber incident, is comprised of leaders and subject matter experts responsible for preparation and response to cyber incidents that cause disruption to the State of New Hampshire's critical infrastructure or critical public or governmental services. Other key federal, state, regional, local, and private organizations may be engaged, as necessary. ESF-17 provides a centralized entity for coordinating a cyber incident that impacts the State of New Hampshire. ESF-17 details can be found at **NH ESF-17 Cybersecurity.**

ESF-17 Activation

The decision to activate ESF-17 will be made jointly by the DOIT Commissioner and the HSEM Director. To ensure scalability, ESF-17 can be partially or fully activated depending on the demands of an incident. Partial activation would include ESF-17 core members and any other specific teams or individuals required to manage the incident virtually. Full activation would include all ESF-17 members and could include additional Emergency Support Functions (ESF) as well as full activation of the State Emergency Operations Center (SEOC). The following factors should be considered when assessing the need to escalate:

- The scope or complexity of the incident requires the additional command and control resources of the SEOC, or the statutory authorities of the HSEM Director.

- The incident may require significant legal or law enforcement support from the Office of the Attorney General or State law enforcement authorities.
- The incident requires Federal support to incident response (e.g., CISA, FBI, or Secret Service).
- The incident requires the support of the Joint Information Center to manage public/external communications.

ESF-17 Response Tasks

DoIT and HSEM will virtually activate ESF-17 as needed to support response activities. The ESF-17 incident response triage process described above seamlessly integrates the SEOC during severe incidents. Collectively, ESF-17 is responsible for the following activities:

- Oversee and track containment and restoration activities including actions taken, resource assignments, and notifications.
- Provide situational awareness and subject-matter expertise and solutions during a response.
- Identify appropriate subject matter experts to identify 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 incidents.
- Make an initial determination of damage, compromise, and risk; identify immediate corrective actions to contain damage, minimize risk, and preserve evidence.
- Engage appropriate subject matter experts to assess threat and risk levels and make recommendation for immediate action.
- Monitor disruption events to determine scale and scope, and to determine if the event is contained or escalating.
- Gather and share information that may indicate the development of a larger or more regional-level cyber incident.
- Provide other cybersecurity experts or representatives in the region with situational awareness and assistance during a catastrophic incident as necessary and possible.
- Coordinate with emergency management support staff to procure critical cyber-related resources.
- Provide situational awareness and subject matter expertise and solutions for an Incident Commander during a response, including:
    - Assisting Planning Staff in the development of priorities and objectives of a long-term response to a significant cyber incident.

These roles and responsibilities are broken out amongst individual entities or parties in the “Roles and Responsibilities” section of this document for further clarity.

ESF-17 Demobilization

When the incident has been contained, ESF-17 leadership, in coordination with the Incident Commander, will notify members of ESF-17 to stand-down response operations and return to steady-state operations.

Communications

Internal Communications

Internal communications are defined as those between and amongst State entities or employees.

During cyber incident response, communications will primarily flow between the core members of ESF-17 (i.e., DoIT CISO, and NH-CIC) and the impacted entity(ies) through one or more of the following channels:

- Digital collaboration tools (e.g., Microsoft Teams)
- Teleconference lines
- Landline phone or State-issued mobile phone
- Email
- In-person

ESF-17 members are expected to practice standard cyber hygiene and be mindful of potential threats to security when using these channels.

External Communications

External communications are defined as those where the State engages entities external to the State (e.g., private sector, local government, public).

At times, communication with external response partners may be necessary to disseminate or gather information about a cyber incident. In any case where external communications are required, or in the event of a full or partial activation, the SEOC will direct communications with external entities based on the State Emergency Operations Plan and its appendices. It is likely that in cases of full or partial SEOC activation, a Joint Information Center (JIC) will be established to provide State-level emergency public information to the media and public.

ESF-17 leadership (i.e., DoIT Commissioner, CISO, or designee) will coordinate with the SEOC to request communications support. When requesting support, ESF-17 leadership should be prepared to answer the following questions, at minimum:

- Who is the intended audience?
- What is the reason for contacting the audience?
- What is the intended message?
- What is the required timeline for delivery?

Training and Exercises

Training and exercises are a crucial component of preparedness. These events allow relevant stakeholders to test their understanding of plans, policies, and procedures in a controlled, low consequence environment.

DoIT and HSEM, in coordination with ESF-17 and relevant stakeholders, will design, execute, and evaluate regular training and exercises to validate plans and identify areas of improvement.

Training

DoIT and HSEM will assist relevant agencies and organizations with cyber incident response training. Training may be performed as a seminar, workshop, or online course, and should provide clarification or instruction on strategies, objectives, and/or protocols within the CIRP. Relevant training courses can be requested through the HSEM State Training Officer and can be found at **HSEM Training.**

Exercises

Exercises are critical activities to increase and validate staff knowledge, as well as identify areas for improvement within current plans, policies, and procedures. The exercise program should use an incremental, iterative approach, including discussion-based exercises and operations-based exercises. Exercises to consider, include:

- Discussion-based exercises focused on identifying the trigger points for escalation and de-escalation of the cyber incident response actions.
- Functional exercises focused on incident reporting and handling for a cyber incident.
- Functional exercises focused on internal and external communications during a cyber incident.
- Broad-scale exercises focused on the operational aspects of response through all phases and involving multiple State and local entities.

The State of New Hampshire will conduct incident response exercises annually, at a minimum. The focus of these exercises will be on scenarios of the State’s choosing during the planning for each testing cycle. All exercises will comply with Homeland Security Exercise Evaluation Program standards for development and evaluation.

Although the scope of the New Hampshire CIRP does not include IT/cyber system recovery operations, effective Continuity of Operations (COOP) and Disaster Recovery (DR) plans are critical to building pre-incident cyber resiliency and identifying and prioritizing the restoration of mission critical assets after a cyber incident. Alignment of COOP and DR exercise plans with cyber incident response exercises should be considered to realize maximum training benefit and support seamless transition from response to recovery.

After-Action Reporting

After-action reports should be developed after any exercise or real-world event to document strengths, areas for improvement, and corrective actions. After-action reporting will be the responsibility of the plan owner (DoIT) with assistance or guidance from HSEM.

Plan Maintenance

The State of New Hampshire Cyber Incident Response Plan is written and maintained by the State of New Hampshire Department of Information Technology (DoIT) and the Department of Safety, Homeland Security and Emergency Management (HSEM). The State of New Hampshire DoIT and HSEM are responsible for updating the plan annually, when and if additional guidance is provided that would impact the plan, or the plan used to support real-world incidents. The CIRP will also be reviewed and updated when there are significant architecture and relevant organizational changes. Revisions will be cataloged in the Record of Changes section of this document.

Appendix A: Abbreviations and Acronyms

ACEPS	Advisory Council on Safety and Emergency Preparedness
BRMD	Business Relations Management Division
CAC	Cybersecurity Advisory Committee
CIRP	Cyber Incident Response Plan
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DoD	United States Department of Defense
DoIT	Department of Information Technology
EM	Emergency Management
ESF	Emergency Support Function
HSEM	Homeland Security and Emergency Management (Department of Safety)
IAC	Information and Analysis Center
IAP	Incident Action Plan
ISAC	Information Sharing and Analysis Center
ISO	Information Security Officer
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCI	National Council of ISACs
NH	New Hampshire
NH-CIC	New Hampshire Cyber Integration Center
SEOC	State Emergency Operations Center
IRT	Incident Response Team
SLTT	State, Local Territory, and Tribal
US	United States

Appendix B: External Cyber Response Resources

Multi-State Information Sharing and Analysis Center

The Multi-State Information Sharing and Analysis Center (MS-ISAC), a division of the Center for Internet Security, is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local territory and tribal (SLTT) governments.

The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, territory and tribal governments. Collaboration and information sharing among members, the U.S. Department of Homeland Security (DHS) and private sector partners are the keys to success.

The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and two-way sharing of information between and amongst public and private sectors to identify, protect, detect, respond and recover from attacks on public and private critical Infrastructure. The MS-ISAC's 24-hour watch and warning center provides real-time network monitoring, dissemination of early cyber threat warnings, vulnerability identification and mitigation, along with education and outreach aimed at reducing risk to the nation's SLTT government cyber domain.

The MS-ISAC works closely with DHS and is recognized as the national ISAC for SLTTs to coordinate cyber readiness and response. The MS-ISAC also works closely with other organizations, such as the National Council of ISACs, the National Governors' Association, the National Association of State Chief Information Officers, and fusion centers, as well as other public and private sector entities to build trusted relationships to further enhance our collective cyber security posture.

New Hampshire National Guard

The New Hampshire National Guard has the following capabilities, which may be engaged to support mission partners with cyber incident preparedness, response, recovery, and mitigation within the State of New Hampshire, assuming the appropriate authority requirements are met:

- **Coordinate.** Defined as "Sharing and synchronizing 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."
- **Train.** Defined as "Engaging 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."
- **Advise.** Defined as "Providing 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."

- **Assist.** Defined as "Supporting mission partners in their prevention of, protection against, mitigation against, and recovery from a cyber incident."

These services may be activated under the following conditions:

- **State Active Duty.** The Guard is activated on order of the Governor through the Adjutant General typically for disaster response. Guard Soldiers and Airmen become state employees. This can be federally reimbursed if the Stafford Act is evoked via a Presidential Disaster Declaration.
- **US Code Title 32.** This is the baseline federal authority of the Guard, whereby the New Hampshire Governor becomes the Commander in Chief. Title 32 can be used for domestic operations through the authority of the President of the United States or the Secretary of Defense. This status is employed to conduct weekend drills and annual training.
- **US Code Title 10.** Regular military and federalized Guard Soldiers and Airmen for deployments or other active-duty service including permanent duty at the National Guard Bureau and similar stations. Guardsmen are activated under Title 10 anytime they train or operate outside of the Continental United States. The Commander in Chief under Title 10 is the President of the United States.

Federal Law Enforcement Partners

Federal law enforcement agencies can work with the State of New Hampshire to address both criminal and national security cyber threats. These agencies, such as the Federal Bureau of Investigation, US Secret Service, and US Immigration and Customs Enforcement, Homeland Security Investigations, can conduct threat response activities related to criminal activity involving their investigative jurisdictions.

- Cybersecurity and Infrastructure Security Agency (CISA)
  - Cybersecurity Division
    - **Cybersecurity Division | Cybersecurity and Infrastructure Security Agency**
- Federal Bureau of Investigation
  - Internet Crime Compliant Center (IC3) - the FBI's central hub for cybercrime information sharing and reporting:
    - **Internet Crime Complaint Center(IC3) | Home Page**
- Regional Cyber Task Force (Boston)
  - **FBI Field Office Boston**
  - Phone: **(857) 386-2000**
- United States Secret Service
  - **Secret Service Field Offices**
  - Phone: **(617) 565-5640** (Boston)

Appendix C: State of New Hampshire Incident Handling and Reporting Requirements

The following section contains relevant New Hampshire Revised Statutes describing cyber incident handling and reporting requirements to facilitate timely and lawful reporting of cyber incidents.

Title 31 – Trade and Commerce, Chapter 359-C – Right to Privacy

Section 359-C:19

Section 359-C:20

Section 359-C:21

Appendix D: NH-CIC Reporting Card

NH Cyber Integration Center (NH-CIC)
Business Hours: Monday-Friday; 7:30AM-4:30PM EST
Phone: 603-271-7555; Email: HelpDesk@doit.nh.gov
Non-Business Hours: 603-271-7555, Option 2

REPORT A CYBER INCIDENT

When to Report:

- Any suspected or confirmed cyber incident that:
- Indicates unauthorized access or malicious software.
- Interrupts system availability or control.
- Results in potential loss of sensitive data.
- Affects government functions; and/or
- Affects critical infrastructure services.

When in doubt, report!

What to Report:

- Your name, organization, and phone number.
- Date and time of incident; and
- Who is the primary point of contact?

What to Provide When Contacted:

- Brief description of incident.
- What data, systems and/or users are impacted.
- How the incident was identified.
- Who has been engaged and/or notified; and
- What response actions have been taken?

What is the NH-CIC?

The NH Cyber Integration Center (NH-CIC) is the unified state center for coordinating cybersecurity between and among executive branch agencies and departments. The NH-CIC is established and maintained within the Department of Information Technology (DoIT) per RSA 21-R:4.

The NH-CIC is staffed with personnel responsible for cybersecurity operations including monitoring networks, threat analysis, information sharing, and coordinating response activities.

What will the NH-CIC do?

The NH-CIC will review the incident information reported, engage those necessary to analyze impact, determine next steps based on the nature of the incident, coordinate response activities, and track effort.