Cyber Breach Tabletop Exercise

Situation Manual

Campus Resilience Program Exercise Starter Kit

October 23, 2018

U.S. DEPARTMENT OF HOMELAND SECURITY
FEMA

CAMPUS RESILIENCE PROGRAM
OFFICE OF ACADEMIC ENGAGEMENT
Office of Academic Engagement

HANDLING INSTRUCTIONS

The title of this document is the *Cyber Breach Tabletop Exercise (TTX) Situation Manual*. This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. Reproduction of this document, in whole or in part, is prohibited without prior approval from the exercise planning team. This document has been marked as "FOR DISCUSSION PURPOSES ONLY."

For more information on this exercise, please consult the following point of contact:

Cheryl Dowd
Cyber Fellow
WICHE
WCET
(303)541-0210
cdowd@wiche.edu

TABLE OF CONTENTS

AGENDA

Cyber Breach Tabletop Exercise

10/23/18; 9:00am

WCET Annual Meeting Precon – Portland, Oregon

*Note that the typical tabletop exercise consists of the following schedule for a 4 - hour exercise. This is an abridged version to share the basic elements of tabletop exercises with the participants

Welcome and Introductions [Recommended Time: 5 Minutes]

Exercise Overview [Recommended Time: 10 Minutes]

Module 1: Initial Response [Recommended Time: 60 Minutes]

Break [Recommended Time: 10 Minutes]

Module 2: Extended Response [Recommended Time: 60 Minutes]

Break [Recommended Time: 10 Minutes]

Module 3: Short-Term Recovery [Recommended Time: 60 Minutes]

Exercise Hot Wash [Recommended Time: 15 Minutes]

Closing Comments [Recommended Time: 10 Minutes]

OVERVIEW

Exercise Name	Cyber Breach Tabletop Exercise
Exercise Date	10/23/18; 9:00 AM – 11:00 AM
Scope	This exercise is a discussion-based “abridged” tabletop exercise, planned for two hours at the WCET Annual Meeting Precon. Divided into three Modules, this exercise will examine response and recovery operations related to a cyber breach targeted against institutional data.
Mission Areas	Response and Recovery
Objectives	1. **Operational Coordination:** Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident 2. **Cybersecurity:** Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident 3. **Situational Awareness:** Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers 4. **Public Information and Warning:** Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations
Scenario	The exercise scenario will include a cyber breach that results in the compromise of personal and institutional data.
Participating Groups/Departments	▪ **WICHE** − **WCET** ▪ **Cooley, LLP**
Sponsoring Organization	WCET
Point of Contact	Cheryl Dowd, Cyber Fellow, WICHE (303)541-0210, cdowd@wiche.edu

GENERAL INFORMATION

Introduction

This document serves as the Cyber Breach Tabletop Exercise Situation Manual (SitMan). It includes the exercise goals and objectives, scenario details, as well as discussion questions for use during the exercise. In addition to aligning with the National Preparedness Goal, the content contained in this SitMan has been designed in accordance with Homeland Security Exercise and Evaluation Program (HSEEP) doctrine.

Overview

The U.S. Department of Homeland Security (DHS), Office of Academic Engagement (OAE) is pleased to support the Cyber Breach Tabletop Exercise as part of the broader Campus Resilience (CR) Program Exercise Starter Kits. This Exercise Starter Kit was made possible through collaboration and coordination with the Federal Emergency Management Agency (FEMA) National Exercise Division (NED).

The broader purpose of each Exercise Starter Kit offered through the CR Program is to support practitioners and senior leaders from the academic community in assessing emergency plans, policies, and procedures while also enhancing overall campus resilience. Specifically, this Exercise Starter Kit will provide the opportunity to examine response and recovery operations related to a cyber breach targeting critical institutional data and information.

Objectives and Core Capabilities

The objectives in **Table 1** describe the expected outcomes for this exercise. The objectives are linked to core capabilities, which are distinct critical elements necessary to achieve the specific mission area(s).

Table 1: Exercise Objectives and Core Capabilities

Exercise Objective	Core Capability
1. Assess the ability to establish an effective command structure that integrates all critical stakeholders to ensure campus and community resources are used efficiently to respond to and recover from a cyber incident	▪ Operational Coordination
2. Evaluate existing capabilities to protect and restore electronic systems, networks, information, and services from damage, unauthorized use, and exploitation during a cyber incident	▪ Cybersecurity
3. Examine the ability to provide timely and relevant information regarding the cyber incident to critical campus and community decision-makers	▪ Situational Awareness
4. Assess the ability to deliver coordinated, actionable, and timely information to critical partners and stakeholders when faced with a cyber incident targeting institutional operations	▪ Public Information and Warning

Participant Information and Guidance

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are detailed below.

Facilitator(s)

The Facilitator will guide exercise play and is responsible for ensuring that participant discussions remain focused on the exercise objectives. They provide additional information and resolve questions as required. They are also responsible for making sure everyone is included in the conversation and has the opportunity to participate.

Players

Players have an active role in discussing their preparedness, response, and recovery activities during the exercise. Players should discuss or initiate actions based on the simulated exercise scenario.

Observers

Observers may visit or view selected segments of the exercise but do not actively engage in exercise discussions.

Support Staff

The exercise support staff includes individuals who perform administrative and logistical support tasks during the exercise (e.g., registration, catering, etc.).

Exercise Structure

The Cyber Breach Tabletop Exercise will consist of three, [insert duration]-minute Modules that focus on response and recovery operations. Each Module will consist of two separate activities: a scenario overview and facilitated discussions. The exercise facilitator will first provide an overview of the scenario and will then engage participants in facilitated discussions around a set of questions. Discussions should focus on key actions, activities, and decisions that each player would perform given the specific scenario conditions. The three exercise Modules include:

- **Module 1** will focus on immediate response operations four hours following the initial notification of a cyber breach
- **Module 2** will focus on extended response operations up to 36 hours following the notification of a cyber breach
- **Module 3** will focus on short-term recovery operations seven days following the notification of a cyber breach

The approximate duration of each exercise activity is noted in **Table 2** below.

Table 2: Module Structure

	Module 1	Module 2	Module 3
Total Minutes	**15 Minutes**	**15 Minutes**	**15 Minutes**
Scenario Review	**10 Minutes**	**10 Minutes**	**10 Minutes**
Facilitated Discussions	**5 Minutes**	**5 Minutes**	**5 Minutes**

Exercise Guidelines

This exercise will incorporate a scenario-based format guided by the event objectives. The Modules and associated discussion questions support achievement of the objectives by initiating discussions, facilitating decision-making, and assisting participants in the arrival of appropriate response outcomes. This approach allows the discussions to focus on situations within a moving timeline and for participants to contribute to the discussion from the perspective of their role in the scenario. The Facilitator will ensure that the scenario moves along at an appropriate pace and that all participants have an opportunity to contribute.

Assumptions and Artificialities

Assumptions

Assumptions are the implied factual foundation for the exercise and are assumed to be present before the exercise starts. The following assumptions apply to the exercise:

- Exercise players will use existing plans, policies, procedures, and resources to guide responses
- Participants may need to balance exercise play with real-world emergencies; real-world emergencies take priority

Artificialities

During this exercise, the following artificialities apply:

- The scenario is plausible, and events occur as they are presented
- There is no “hidden agenda” nor are there any trick questions
- The scenario assumes certain player actions as it moves through each phase; players should first discuss the actions stipulated by the scenario
- Players are welcome to engage in “what if” discussions of alternative scenario conditions

MODULE 1: INITIAL RESPONSE

Background

Figure 1: Cyber Security Personnel

In recent years, malicious cyber actors have targeted institutions of higher education (IHEs) with typical cybercrime activities. These include spear-phishing students and faculty with institution-themed messages, creating fake websites, and infecting computers with malicious software – often in an attempt to gain access to student and faculty emails, personally identifiable information (PII), as well as financial records and payment systems.

While malicious cyber actors continue to exploit institutional networks for financial gain, an emerging threat facing IHEs is individuals conducting cyber espionage. In addition to innovative scientific and medical research, colleges and universities are often involved in sensitive government and private sector research projects. These associations are very appealing to cyber espionage actors looking to gain access to sensitive programs and exfiltrate information. Institutional networks, which often have multiple levels of connectivity and accessibility to encourage and enable collaboration, may present an easier target for cyber espionage actors than sensitive government or private industry networks. Furthermore, institutions may be at a higher risk due to a lack of cyber security awareness among students, faculty, and staff.

Scenario

October 26, 2018 10:00am

Your institution’s Chief Information Security Officer (CISO) is contacted by a Special Agent from the Cyber Division of the Federal Bureau of Investigation (FBI). The agent states that a cyber attack has been launched against your institution’s network by an outside entity. At this time, the precise duration, scope, and source of the attack are not completely clear. Working in collaboration with the FBI, the initial investigation quickly reveals the presence of an advanced persistent threat (APT) that appears to be consistent with sophisticated malware that has been previously used by individuals to access critical institution data and proprietary information.

October 26, 2018 2:00pm

By this time, enough evidence is discovered to determine the attack was initiated at least three months prior, and during that time, attackers had free and unlimited access to all networks, databases, servers, and other sensitive resources associated with various departments and colleges. While exfiltration of data cannot be confirmed now, it is reasonable to assume sensitive information has been compromised. While the attack appears to specifically target PII data within your institutions departments and colleges, a thorough analysis of the entire institution network is underway. It is anticipated this process may take several days to complete

Discussion Questions

Operational Coordination

1. What plans, policies, and procedures does your institution have in place to respond to the effects of a data breach?
2. What are your institution’s initial priorities?

3. How would your institution establish a command structure to coordinate your immediate response efforts?
    a. Who are your key internal and external stakeholders and how would your institution incorporate them into this command structure?
    b. How can your institution coordinate with private and public partners to ensure a unified response effort?
4. What resource gaps could limit your institution's ability to respond to a cyber attack?
    a. What community resources and aid agreements could compensate for these resource gaps?

Cybersecurity

1. Does your institution have a formalized cyber incident response plan?
    a. Does your plan clearly outline what individuals/positions are involved in response efforts and how they are expected to coordinate with one another?
    b. Do you periodically test your plan and train staff?
    c. Does your institution currently have cyber insurance? If so, at what point would you notify your provider of a potential breach? If not, what other financial plans do you have in place to offset potential costs of this type of incident?
2. Does your institution's response strategy outline how to align broader response efforts with ongoing security management and IT efforts?
3. What steps will your institution take to verify the likelihood of a data breach resulting in the release of PII?
    a. How does your institution determine what systems/data/services may have been breached?
4. What measures are in place to protect confidential, personal, financial, and academic information concerning students, faculty, staff, and alumni from a potential cyber incident?
    a. Are these existing protective measures, or measures that would be implemented following a cyber incident?

Situational Assessment

1. How does your institution collect, verify, and analyze information immediately following awareness of, or notification of a cyber incident?
2. How do you conduct initial decision-making and offer decision-making recommendations to senior leadership?
3. Do you have identified information requirements that support leadership decision-making processes (e.g., type of cyber incident, scope of incident, numbers of individuals impacted, implementation of cyber response plan)?

Public Information and Warning

1. What plans, policies, and procedures does your institution have in place to guide communications with potentially affected parties at this time?
    a. What internal and external stakeholders are you engaging?
    b. What information would you release and how?
    c. How does your institution use pre-scripted or automated messaging that would expedite critical communications?
2. What individual, office, or department coordinates and delivers your institution's messaging?

3. How will your institution use social media platforms in support of incident communications and messaging?
4. At this point in the scenario, would your institution notify non-affected members of the campus community?

MODULE 2: EXTENDED RESPONSE

Scenario

October 26, 2018 10:00 pm

A second intrusion has been detected on the network. While investigating the initial breach, a malware variant known to be used by cyber criminals to harvest and exfiltrate PII was discovered on several computers, to include workstations in the Office of Human Resources, the Admissions and Registration Offices, and the Financial Aid and Scholarship Offices.

Figure 2: Data Center Server

October 27, 2018 10:00 am

A detailed review of internal logging systems indicates stolen employee login credentials may have been used to access databases containing both student and faculty records. Further examination of server logs indicates large amounts of student, faculty, and staff data has been exfiltrated over the past several months. Evidence indicates the stolen data includes the name, address, date of birth, and social security number for students, faculty, and staff (domestic and international) from 2012 to the present.

October 27, 2018 10:00 pm

Local news outlets begin contacting your institution's public affairs office. Reporters indicate they have heard there has been a data breach at your institution and that personal information for hundreds of students, faculty, and staff has been stolen and is being used on the dark web. They want to know the extent of the breach.

Concerned students and parents begin inundating your institution's phone lines requesting additional guidance on the status of their information as well as the extent of the potential breach.

Discussion Questions

Operational Coordination

1. What plans, policies, and procedures does your institution have in place to guide response efforts at this point?
    a. What are your mid-term response priorities?
2. How would your institution maintain an effective command structure to coordinate cyber response efforts?
    a. Who are the key decision-makers at this point?
    b. What are their specific roles and responsibilities?
3. How do key decision-makers collect information on system damages and critical needs?
4. What resources are currently available to support response efforts?
    a. What plans, agreements, and contingency contracts are in place to address potential system issues?
5. Who are the key external stakeholders that would support response efforts?

   a. How would your institution coordinate and communicate with these stakeholders?

Cybersecurity

1. What tools are in place to prevent the remote extraction of information from a network by unauthorized users?
   a. Who is responsible for assisting the security of the network?
   b. How often are security tests completed?
2. Do you currently possess sufficient capabilities in-house to investigate and mitigate a potential incident of this type?
   a. If not, what stakeholders would you engage to address capability gaps?
3. What types of impacts could your institution expect from the potential loss of PII?
   a. At this point, do you envision any financial and legal consequences?
4. What plans, policies, and procedures exist to ensure students, faculty, and staff engage in information security best practices?
   a. Who determines these organizational best practices?
   b. How are students, faculty, and staff educated about these practices?

Situational Assessment

1. Have your information needs changed during this phase of the response?
   a. How are you collecting critical information at this time?
   b. Who do you receive this information from and who do you disseminate this information to?
   c. How are you analyzing and disseminating this information?
2. What are the processes for communication and coordination between internal and external partners to support any emerging needs or response requirements?
3. Are there identified reporting requirements for internal stakeholders? For external partners? For leadership and key decision-makers?
   a. What, if any, federal, state, or local reporting requirements must you comply with if impacted by a cyber incident?
   b. Who within your institution is responsible for fulfilling these reporting requirements?

Public Information and Warning

1. At this point in the scenario, how would your institution be communicating with potentially affected as well as non-affected parties?
   a. What would your messaging priorities be at this point?
   b. How would your institution ensure messaging is consistent and coordinated throughout the response period?
   c. Who is responsible for delivering this messaging?

   d. How does this messaging accommodate international students and families as well as students with access and functional needs?

2. How does your institution ensure timely and accurate situational updates for external stakeholders (e.g., media) throughout the response period?
   a. Who is responsible for delivering these updates?
   b. What sort of information is your institution releasing at this point?
3. Does your institution have a crisis communications plan or other means of communicating with all stakeholders in case of a disruption or corruption of standard communications?
   a. How and when does your institution activate its crisis communications plan?

MODULE 3: SHORT-TERM RECOVERY

Scenario

November 2, 2018 10:00 am

Figure 3: Media Personnel

A full and thorough analysis of the entire network and associated server logs reveals that the scope of the data breach may be more extensive than previously suspected and may also include health-related data and donor information.

While still working through the repercussions and effects of the breach, many students, faculty, and staff members express concerns regarding their information and request guidance on what your institution is doing to protect their data.

Media outlets continue to report on the breach. Many cyber experts criticize the way your institution has handled the situation and are suggesting that your slow response allowed for wider system impacts.

Discussion Questions

Operational Coordination

1. How does your institution coordinate the transition from response to short-term recovery efforts?
2. What plans, policies, and procedures guide your institution’s recovery process?
    a. Who is responsible for coordinating short- and long-term recovery efforts?
    b. What are your institution’s priorities for short-term recovery?
3. What resource gaps could limit your institution’s ability to meet these priorities?
    a. What community resources or aid agreements could compensate for those gaps?

Cybersecurity

1. What partnerships does your institution have to support recovery efforts (e.g., cyber insurance) in the aftermath of a cyber incident?
    a. If none, how would your institution formalize partnerships with the necessary stakeholders?
    b. Who at your institution would be responsible for coordinating these efforts?
2. What are your institution’s plans for the recovery and restoration of critical systems and data that have been compromised as a result of a cyber related incident?
3. What strategies would be implemented to mitigate potential negative impacts resulting from stolen and/or leaked PII?
    a. If you have an established cyber incident response plan, how does it provide guidance for this type of incident recovery?
4. What future cybersecurity measures could you implement to develop more secure systems and protect critical institutional data from a future breach?

Situational Assessment

1. What critical decisions would need to be made at this point to inform recovery efforts?
    a. What are the long-term financial implications of a breach of this nature for your institution?
2. What legal obligations exist, if any, that may affect how intelligence and information is processed and communicated following a cyber related incident?
    a. How are these legal obligations accounted for in overall recovery efforts?
    b. What stakeholders would likely be involved in this information sharing?
3. Following this type of incident, what decisions or actions would you take to maintain public and institutional confidence?
    a. What internal or external partners would be engaged in this process?
    b. What leadership decisions would support this process?

Public Information and Warning

1. How does your institution ensure consistent, coordinated messaging throughout the recovery period?
    a. How does your institution's communications strategy transition from response-oriented to recovery-oriented messaging?
    b. Who is responsible for monitoring and managing inquiries from students, faculty, staff, and alumni?
    c. How does this messaging accommodate international audiences as well as those with access and functional needs?
2. How does your institution provide external stakeholders (e.g., media) with timely updates concerning recovery efforts?
3. How would you maintain overall brand reputation for an incident involving a cyber breach?
    a. How would potentially false or misleading information be handled?
    b. How would potentially sensitive or classified information be handled?
4. How are students, faculty, and staff briefed on protective actions and measures to prevent future cyber incidents?

NOTES

APPENDIX A: ACRONYMS

Acronym	Term
APT	Advanced Persistent Threat
CISO	Chief Information Security Officer
CR Program	Campus Resilience Program
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSEEP	Homeland Security Exercise and Evaluation Program
IHE	Institution of Higher Education
IT	Information Technology
NED	National Exercise Division
OAE	Office of Academic Engagement
PII	Personally Identifiable Information
SitMan	Situation Manual
TTX	Tabletop Exercise

Appendix B: Glossary

Term	Definition
Academic Recovery	A component of the Continuity of Operations (COOP) annex identifying strategies to continue teaching after an incident.
Access and Functional Needs	A population whose members may have additional needs before, during, and after an incident in functional areas, including but not limited to: maintaining independence, communication, transportation, supervision, and medical care. Individuals in need of additional response assistance may include those who have disabilities, who are from diverse cultures, who have limited English proficiency, who are non-English-speaking, or who are transportation disadvantaged.
Active Shooter	An individual actively engaged in killing or attempting to kill people in a confined and populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims.
After Action Report (AAR)	A document intended to capture observations of an exercise and make recommendations for post-exercise improvements. The final AAR and Improvement Plan (IP) are printed and distributed jointly as a single AAR/IP following an exercise.
Capabilities-Based Planning	Determining capabilities suitable for a wide range of threats and hazards while working within a framework that necessitates prioritization and choice. Capabilities-based planning addresses uncertainty by analyzing a wide range of scenarios to identify required capabilities.
Chain of Command	The orderly line of authority within the ranks of the incident management organization
Command Staff	The staff who report directly to the Incident Commander, including the Public Information Officer, Safety Officer, Liaison Officer, and other positions as required. They may have an assistant or assistants as needed.
Community Hazards	Natural, technological, or human-caused hazards in the community that affect the school both directly, such as damage to the school building, and indirectly, such as making a road to the school impassable.
Comprehensive Planning Guide (CPG) 101	A guide designed to assist jurisdictions with developing plans. It promotes a common understanding of the fundamentals of planning and decision-making to help emergency planners examine a hazard and produce integrated, coordinated, and synchronized plans.

Term	Definition
Concept of Operations (CONOPS)	A component of the basic plan that clarifies the school's overall approach to an emergency (i.e., what should happen, when, and at whose direction) and identifies specialized response teams and/or unique resources needed to respond to an incident.
Continuity of Operations (COOP)	A functional annex providing procedures to follow in the wake of an incident where the normal operations of the school are severely disrupted.
Critical Infrastructure	Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacitation or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.
Disaster	An occurrence of a natural catastrophe, technological accident, or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries.
Emergency	Any incident, whether natural, technological, or human-caused, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.
Emergency Operations Center (EOC)	The physical location at which the coordination of information and resources to support incident management (on-scene operations) activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g., fire, law enforcement, medical services), by jurisdiction (e.g., Federal, State, regional, tribal, city, county), or by some combination thereof.
Emergency Operations Plan (EOP)	An ongoing plan for responding to a wide variety of potential hazards. An EOP describes how people and property will be protected; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available; and outlines how all actions will be coordinated.
Emergency Support Functions (ESF)	ESFs provide the structure for coordinating Federal interagency support for a Federal response to an incident. They are mechanisms for grouping functions most frequently used to provide Federal support to States and Federal-to-Federal support, both for declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents.

Term	Definition
Evacuation	The organized, phased, and supervised withdrawal, dispersal, or removal of students, personnel, and visitors from dangerous or potentially dangerous areas.
Family Reunification	See Parent-Student Reunification
Hazard	Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.
Hazard Mitigation	Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster or incident.
Homeland Security Exercise and Evaluation Program (HSEEP)	A capabilities- and performance-based exercise program that provides standardized policy, doctrine, and terminology for the design, development, conduct, and evaluation of homeland security exercises.
Human-caused Hazards	Hazards that rise from deliberate, intentional human actions to threaten or harm the well-being of others. Examples include school violence, terrorist acts, or sabotage.
Incident	An occurrence, natural or human-caused, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.
Incident Command System (ICS)	A standardized on-scene emergency management construct specifically designed to provide an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. The Incident Command System is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. ICS is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations.
Incident Management	The broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all levels of government, utilizing both governmental and nongovernmental resources to plan for, respond to, and recover from an incident, regardless of cause, size, or complexity.

Term	Definition
Joint Information Center (JIC)	A facility established to coordinate critical emergency information, crisis communications, and public affairs functions. The Joint Information Center is the central point of contact for all news media. The Public Information Officer may activate the JIC to better manage external communication.
Joint Information System (JIS)	A structure that integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, accurate, accessible, timely, and complete information during crisis or incident operations. The mission of the Joint Information System is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the Incident Commander (IC); advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort.
Mass Care	Actions taken to protect evacuees and other disaster victims from the effects of the disaster. Activities include providing temporary shelter, food, medical care, clothing, and other essential life support needs to the people who have been displaced because of a disaster or threatened disaster.
Mitigation	Includes activities to reduce the loss of life and property from natural and/or human-caused disasters by avoiding or lessening the impact of a disaster and providing value to the public by creating safer communities. Mitigation seeks to fix the cycle of disaster damage, reconstruction, and repeated damage. These activities or actions, in most cases, will have a long-term sustained effect. Examples: Structural changes to buildings, elevating utilities, bracing and locking chemical cabinets, properly mounting lighting fixtures, ceiling systems, cutting vegetation to reduce wildland fires, etc.
Multi-jurisdictional Incident	An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In the Incident Command System, these incidents are managed under Unified Command.
National Disaster Recovery Framework (NDRF)	The NDRF serves as a companion document to the National Response Framework, and is a guide to promote effective recovery, particularly for those incidents that are large-scale or catastrophic.
National Incident Management System (NIMS)	A set of principles that provides a systematic, proactive approach guiding government agencies at all levels, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life or property and harm to the environment.

Term	Definition
National Infrastructure Protection Plan (NIPP)	A coordinated approach used to establish national priorities, goals, and requirements to protect U.S. critical infrastructure and key resources.
National Preparedness Goal (NPG)	A document outlining the top priorities intended to synchronize pre-disaster planning, prevention, and mitigation activities throughout the nation, and to guide Federal, State, and local spending on equipment, training, planning, and exercises. The Goal provides an overarching vision, tools, and priorities to shape national preparedness.
National Response Framework (NRF)	A guide establishing a comprehensive, national, all-hazards approach to domestic incident response. It intends to capture specific authorities and best practices for managing incidents ranging from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters.
Natural Hazard	Hazards related to weather patterns and/or physical characteristics of an area. Often natural hazards occur repeatedly in the same geographical locations.
Parent-Student Reunification	A common procedure implemented after an incident or emergency. A reunification area away from the incident is established for parents/guardians to reunite with their children. Parent-student reunification may be needed if the school is evacuated or closed as a result of a hazardous materials incident, fire, school violence, or other hazard. Related word: Relocation.
Preparedness	A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response. Within the National Incident Management System (NIMS), preparedness focuses on the following elements: planning, procedures and protocols, training and exercises, personnel qualification and certification, and equipment certification. Examples: Conducting drills, preparing homework packages to allow continuity of learning if school closures are necessary, etc.
Prevention	Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. Examples include: cyberbullying prevention, pandemic influenza sanitation measures, building access control procedures, security systems and cameras, etc.
Psychological Healing	A functional annex describing how schools will address medical and psychological issues resulting from traumatic incidents.
Public Information	Processes, procedures, and systems for communicating timely, accurate, and accessible information on an incident's cause, size, and current situation; resources committed; and other matters of general interest to the public, responders, and additional stakeholders (both directly affected and indirectly affected).

Term	Definition
Recovery	Encompasses both short-term and long-term efforts for the rebuilding and revitalization of affected communities. Short-term recovery focuses on crisis counseling and restoration of lifelines such as water and electric supply, and critical facilities. Long-term recovery includes more permanent rebuilding.
Relocation	A common procedure implemented when the school building or environment surrounding is no longer safe. Students and staff are moved to an alternative facility where parents/guardians can reunite with children and/or teaching can continue. Related word: Parent-Student Reunification.
Resilience	Ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.
Response	Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. Examples: lockdown, shelter-in-place, evacuation of students, search and rescue operations, fire suppression, etc.
Reverse Evacuation	A common procedure implemented when conditions inside the building are safer than outside the building.
Shelter-in-Place	A common procedure implemented in the event of a chemical or radioactive release. Students and staff take immediate shelter, sealing up windows and doors, and turning off air ducts.
Special Needs Population	See Access and Functional Needs
Specialized Procedures	Standardized actions for specific populations or situations during an incident or emergency. Examples include special needs population, off-campus events, continuity of operations, mass care, and psychological healing.
Technological Hazards	These hazards originate from technological or industrial accidents, infrastructure failures, or certain human activities. These hazards cause the loss of life or injury, property damage, social and economic disruption, or environmental degradation, and often come with little to no warning.

Term	Definition
Terrorism	As defined in the Homeland Security Act of 2002, activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources; is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping.
Threat	Natural, technological, or human-caused occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
Unified Command	In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.
Warning	The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause. A warning issued by the National Weather Service (e.g., severe storm warning, tornado warning, tropical storm warning) for a defined area indicates that the particular type of severe weather is imminent in that area.
Watch	Indication by the National Weather Service that in a defined area, conditions are favorable for the specified type of severe weather such as flash floods, severe thunderstorms, tornadoes, and tropical storms.

*NOTE: The terms listed in this Glossary are gathered from FEMA sources, specifically Ready.gov and FEMA’s Training Glossary.