# 2017 National Seminar and Tabletop Exercise for Institutions of Higher Education

## Summary Report

THE UNIVERSITY OF UTAH
S.J. QUINNEY
COLLEGE OF LAW

U.S. DEPARTMENT OF HOMELAND SECURITY

CAMPUS RESILIENCE PROGRAM
OFFICE OF ACADEMIC ENGAGEMENT

# Handling Instructions

The title of this document is the *2017 National Seminar and Tabletop Exercise for Institutions of Higher Education Summary Report (the Summary Report).* This document should be safeguarded, handled, transmitted, and stored in accordance with appropriate security directives. This report should be handled in a sensitive manner. Reproduction of this document, in whole or in part, is prohibited without prior approval.

For more information, consult the following points of contact:

**Office of Academic Engagement**
Department of Homeland Security
AcademicEngagement@hq.dhs.gov

**National Exercise Program**
Federal Emergency Management Agency
NEP@fema.dhs.gov

**Cover Photos**

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=487360&site=photobank

https://pixabay.com/en/code-code-editor-coding-computer-1839406/

https://pixabay.com/en/car-police-cars-caravan-sirens-red-1531277/

https://www.fema.gov/media-library/assets/images/128682

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=497770&site=photobank

http://images.umc.utah.edu/netpub/server.np?find&catalog=catalog&template=detail.np&field=itemid&op=matches&value=14254&site=photobank

https://www.fema.gov/media-library/assets/images/71003

# TABLE OF CONTENTS

**Handling Instructions**........................................2
**Table of Contents**........................................3
**Introduction.**........................................4
Background........................................4
**Event Overview**........................................4
**Key Results…**........................................8
**Cyber Response**........................................14
Overview........................................14
Scenario........................................14
Discussion Results........................................14
**Emergency Response**........................................22
Overview........................................22
Scenario........................................22
Discussion Results........................................23
**Recovery….**........................................31
Overview........................................31
Scenario........................................31
Discussion Results........................................31
**Appendix A: Event Results**........................................A-1
**Appendix B: Participant Feedback Forms**........................................B-1
**Appendix C: Academic Resource Guide**........................................C-1
**Appendix D: Event Participants**........................................D-1
**Appendix E: Acronyms**........................................E-1

# INTRODUCTION

The ***2017 National Seminar and Tabletop Exercise (NTTX) for Institutions of Higher Education*** (IHEs) was part of a broader effort to empower IHEs to improve preparedness and build resilience. The NTTX was sponsored by the U.S. Department of Homeland Security (DHS) Office of Academic Engagement (OAE) and the DHS Federal Emergency Management Agency (FEMA) National Exercise Division (NED). The event took place on October 10-11, 2017 and was hosted by the S.J. Quinney College of Law at the University of Utah. The topic of the 2017 NTTX was a cyber-attack with physical impacts on critical infrastructure. The event consisted of seminar sessions and a tabletop exercise (TTX) and brought together nearly 355 participants from IHEs, federal agencies, and organizations representing academia, emergency management, and law enforcement fields.

This *2017 National Seminar and Tabletop Exercise for Institutions of Higher Education Summary Report* provides NTTX participants and the academic, emergency management, and law enforcement communities with a summary of the major findings and takeaways from the event.

## Background

The increased scale and diversification of threats and hazards to the academic community significantly challenges IHEs' ability to provide a safe and healthy learning environment for their students, faculties, and staffs. The goal of the NTTX is to bolster campus' ability to mitigate the impacts of an incident and provide IHEs with tools and resources to develop the necessary plans, policies, procedures, and capabilities to respond to and recover from a crisis (Refer to ***Appendix A*** for a resource guide).

### Campus Resilience Program

The Department of Homeland Security (DHS) launched the Campus Resilience Program in 2013, as an effort to engage institutions of higher education (IHEs) in developing and testing an emergency preparedness and resilience planning process tailored to IHEs. Managed by the Office of Academic Engagement (OAE), the program is dedicated to helping colleges and universities build, sustain and promote resiliency to the threats that confront institutions across the nation.

The National Tabletop Exercise (NTTX) for IHEs is part of a broader Tabletop Exercise Series offered through the Campus Resilience Program. Additional information on the Campus Resilience Program Tabletop Exercise Series is accessible here.

# EVENT OVERVIEW

| | |
|---|---|
| **Exercise Name** | 2017 National Seminar and Tabletop Exercise for Institutions of Higher Education |
| **Exercise Date** | October 10-11, 2017 |
| **Scope** | A two-day event with seminars and a tabletop exercise (TTX) geared toward examining issues related to a cyber-incident with physical impacts on campus infrastructure. The TTX portion consisted of a scenario-driven, facilitated discussion designed to examine roles, responsibilities, authorities, and capabilities at IHEs. |
| **Mission Areas** | Response and Recovery |
| **Objectives** | 1. Identify **common strengths and areas for improvement** when responding to a campus infrastructure breakdown or failure caused by cyber-attack that threatens the safety and security of students, including international students, and all faculty and staff.<br>2. Assess **processes and capabilities to develop timely and appropriate communication** for multiple IHE communities during a critical infrastructure failure to maintain public and institutional confidence, including messaging to: students, faculty and staff, family members, media, alumni, and relevant external business partners.<br>3. Examine **coordinated public health, mass transportation, and residential life services, as well as continuity of operations planning** related to response and recovery from physical infrastructure system failures, for on-campus students, staff, and visitors to campus.<br>4. Examine and assess plans, protocols, and procedures for IHEs to **communicate and collaborate on response and recovery operations with co-jurisdictional law enforcement**, sector-specific organizations, local, state, and federal authorities, as well as private sector partners and other stakeholders.<br>5. Examine **processes and tools for IHEs to automate/expedite communication and comprehension** of threat-relevant information, both internally and with external partners and stakeholders, during the response and recovery efforts. |
| **Scenario** | The scenario consisted of a cyber-attack that impacts an IHE's critical infrastructure systems. |
| **Sponsors** | The DHS Office of Academic Engagement (OAE), the FEMA National Preparedness Directorate (NPD) National Exercise Division (NED), the FEMA NPD Individual & Community Preparedness Division (ICPD), and the University of Utah S.J. Quinney College of Law. |
| **Participating Organizations** | Participants included campus emergency response and law enforcement, information technology professionals, and campus leadership from various colleges and universities across the country (Refer to ***Appendix X*** for a list of participants). |

## Exercise Structure

The two-day NTTX consisted of three 60-minute seminar sessions and three 90-minute exercise modules. The schedule alternated between seminar sessions and exercise modules, and seminar sessions introduced concepts which would be discussed in the subsequent exercise modules.

## Organization of Break-Out Groups

To reflect the diverse capabilities and challenges across the higher education community, the NTTX break-out sessions and the analysis in this report were organized according to four categories of IHEs (Table 1). IHEs were first divided by whether they offered a doctoral program as captured in the *Carnegie Classification of Institutions of Higher Education*[1]. This was based on the hypothesis that schools with developed doctoral programs would be more likely to provide critical infrastructure[2] services that would be impacted by the exercise scenario. Grouping doctoral IHEs would therefore promote discussion on shared challenges and best practices. The *Carnegie Classification of Institutions of Higher Education* uses the following definitions for doctoral and non-doctoral IHEs:

- **Doctoral:** Schools in this category offer a wide range of baccalaureate programs and are committed to graduate education through the doctorate. It includes IHEs that awarded at least 20 research/scholarship doctoral degrees during the update year (this does not include professional practice doctoral-level degrees, such as the JD, MD, PharmD, DPT, etc.).
- **Non-Doctoral:** This group encompasses Master's Colleges and Universities, Baccalaureate Colleges, Baccalaureate/Associate's Colleges, Associate's Colleges, Tribal Colleges, Medical Schools, and Theological and other specialized faith-related IHEs.

Doctoral IHEs were then divided upon their status as residential or non-residential institutions. The second group, non-doctoral IHEs, were secondarily divided based on size of the student body. Large institutions are four-year IHEs with more than 10,000 degree-seeking students. Small institutions are two-year IHEs with more than 5,000 degree-seeking students.

*Table 1: Break-out Group Descriptions*

| | |
|---|---|
| ***Doctoral, Residential:***<br>▪ Committed to graduate education through the doctoral level<br>▪ Approximately 25-49 percent of undergraduates live on campus | ***Non-Doctoral, Large:***<br>▪ IHEs that do not provide doctoral degree programs<br>▪ Four-year IHEs with more than 10,000 degree seeking students |
| ***Doctoral, Non-Residential:***<br>▪ Committed to graduate education through the doctoral level<br>▪ Fewer than 25 percent of undergraduates live on campus | ***Non-Doctoral, Small:***<br>▪ IHEs that do not provide doctoral degree programs<br>▪ Two-year IHEs with fewer than 5,000 degree seeking students |

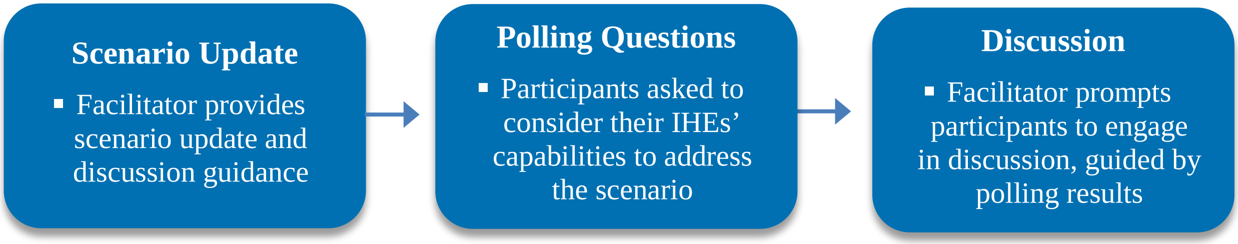
[1] http://carnegieclassifications.iu.edu/classification_descriptions/basic.php

[2] https://www.dhs.gov/what-critical-infrastructure

## Exercise Module Format

Each exercise module consisted of three separate activities: a scenario update, polling questions covering specific elements of the scenario, and a facilitated group discussion (Figure 1). Participants answered all polling questions on a four-point scale (Figure 2), and key discussion items were reviewed during the Plenary Session at the end of the event.

*Figure 1: Exercise Activities*



**Scenario Update**

- Facilitator provides scenario update and discussion guidance

**Polling Questions**

- Participants asked to consider their IHEs' capabilities to address the scenario

**Discussion**

- Facilitator prompts participants to engage in discussion, guided by polling results

*Figure 2: Polling Question Scale*

| Assessment | Criteria |
|---|---|
| 🟩 | I believe that my institution can successfully address this issue **without challenges.**<br>(Does not impose significant risk or strain on resources) |
| 🟨 | I believe that my institution can address this issue, but with **moderate challenges.**<br>(Imposes minor risks or strain on resources) |
| 🟥 | I believe that my institution can address this issue, but with **major challenges.**<br>(Imposes major risks or strains on resources) |
| ⬛ | I believe that my institution **does not have the capability** to address this issue. |

## Methodology

Per the Homeland Security Exercise and Evaluation Program[3] (HSEEP), this report's analysis is organized into two main categories: a) the strengths demonstrated by participating organizations, and b) the areas of improvement uncovered. In all cases, strengths and areas for improvement are categorized according to participants' confidence in their institution's capabilities related to the activities described in the ***2017 National Seminar and Tabletop Exercise for Institutions of Higher Education Situation Manual.***

[3] https://www.fema.gov/hseep

# Key Results

Below is a summary of the key findings compiled from the NTTX pre-event survey, in-exercise polling questions, Participant Feedback Form, and post-event survey. Results provide insight on participants' experience with cyber-attacks, capabilities across IHE groups (doctoral/non-doctoral and small/large), overall impressions of the event, and the impact of the NTTX on participants' completed and planned actions related to their institution's cybersecurity capabilities.

## Pre-Event Survey Findings

Prior to the NTTX, participants were polled on their experience with cyber-attacks and the status of specific actions related to cybersecurity preparedness. The key results from the Pre-Event Survey are summarized below in Figure 3 and detailed in Appendix A: NTTX Survey Results.

*Figure 3: Pre-Event Survey Findings*

| 33% | 6% | 16% | 22% | 9% |
|---|---|---|---|---|
| of participants' institutions experienced a cyber-attack resulting in loss or theft of Personally Identifiable Information | of participants' institutions experienced a cyber-attack resulting in loss or theft intellectual property | of participants' institutions had integrated cybersecurity into their emergency management plans | of participants' institutions had conducted training or exercises to better prepare for a cyber-attack | of participants' institutions had signed a mutual aid agreement to increase cybersecurity staffing and resources |

## Institution Strengths

During the tabletop exercise, one representative per IHE reported on their institution's capabilities related to 10 specific issues in the exercise scenarios. In this section, 3 of the 10 issue areas are categorized as strengths of participating institutions. Strengths are defined as categories in which **more than 40% of institutions** reported no challenges and **more than 75% of institutions** reported having moderate to no challenges in addressing the issue.

*Table 2: Key Strengths*

**<u>Response Coordination with Stakeholders:</u>**

77% of institutions indicated **they would experience moderate or no challenges in establishing an incident command system (ICS) to respond to impacts on both computer systems/networks and campus operations.**

- 41% of institutions said they would not have any challenges, citing **well-established plans, consistent exercises, and frequent training**.
- 36% of institutions cited moderate challenges, including a **lack of awareness of federal assistance**, **outdated mutual aid agreements, and weak relationships with key external partners**.
- 38% of small, non-doctoral institutions would have major challenges or be unable to implement an ICS. Participants noted that this was due to **lack of exercise and training experience** across IHE response staff.

**Crisis Communications and Public Messaging:**

89% of institutions indicated **they would experience moderate or no challenges delivering coordinated and prompt alerts to internal and external stakeholders following a cyber-attack that disrupted their institution's operations.**

- 51% of institutions said they would not have any challenges, citing **established coordination processes, and experience with preemptive communication**.
- 37% of institutions cited moderate challenges, **including providing messaging to international students and students with access and functional needs**.

**Post-Incident Communications**

94% of institutions indicated **they would experience moderate or no challenges engaging stakeholders, the public, and the media in the aftermath of the incident, including managing impacts to their institution's reputation and brand**.

- 45% of institutions indicated they would experience no challenges, crediting **previous experience with public messaging during large events, protests, and other emergencies**.
- 18% of small, non-doctoral IHEs indicated that engaging stakeholders in the aftermath of a cyber-attack would present major challenges, citing a need to **develop pre-scripted messaging and relationships with the media**.

## Institution Areas for Improvement

Areas for Improvement are defined as categories in which **more than 15% of institutions** reported having major challenges or be unable to address the issue presented, and **less than 15% of institutions** reported no challenges.

*Table 3: Key Areas for Improvement*

**Assessment of Impacts:**

27% of institutions indicated **they would have major challenges identifying the precise nature, expected duration, and impact of the malware intrusion** on learning management software and campus emergency notification systems during an incident.

- 63% of institutions cited moderate challenges, including **pre-identifying critical systems and pre-appointing incident command staff**.
- Institutions that reported no challenges recommended best practices including **mapping interdependent systems** on campus to isolate malware and prevent cascading effects.

**Continuity of Operations:**

50% of institutions indicated **they would have major challenges or be unable to continue performance of their institution's essential functions during a critical infrastructure disruption to ensure continuity of operations (COOP)** during an incident.

- 39% of institutions cited major challenges and 11% of institutions reported that they would be unable to ensure COOP during an incident of this nature. IHEs identified a **need for COOP training and plans**.

- 5% of institutions reported no challenges, and recommended **regularly updating and reviewing COOP plans** to avoid reliance on outdated back-up systems and procedures.

**Restoring Campus Operations:**

27% of institutions indicated **they would experience major challenges recovering and resuming normal operations, including academic and research activities, after a disruption.**

- Institutions that reported no challenges cited **redundant critical infrastructure systems** (e.g., backup generators and emergency override functions) as a key component in their restoration plans and a failsafe against further disruption.

**Restoring Campus Systems:**

19% of institutions indicated **they would have major challenges in coordinating recovery efforts for compromised systems, including digital forensics and system restoration** following an incident.

- 72% of institutions cited moderate challenges, including conducting **simultaneous forensic investigation and operational recovery efforts** and a **lack of awareness of federal assistance** (e.g., fusion centers) to aid in investigation. These institutions reported a need for cyber-incident plans and procedures.
- 9% of institutions reported no challenges. They recommended best practices including **engaging external government and private sector stakeholders** as necessary to identify solutions.

## Event Feedback

Following the event, NTTX participants were offered the opportunity to provide event feedback on a **Participant Feedback Form.** Key insights from the form are described in Tables 4 and 5 below. Detailed results can be found in ***Appendix B: Participant Feedback Forms.***

*Table 4: Key Insights from the Seminar Assessment*

| |
|---|
| ▪ 80% of participants thought **presentations during the sessions were relevant to their institutions** |
| ▪ 69% of participants believed that **seminars/ workshops increased their understanding of available resources** to respond to and recover from a cyber-attack |
| ▪ 79% of participants said the **presentations helped them gain a better understanding of the response and recovery actions their institution should implement when considering the threat of cyber-attack** |
| ▪ 77% of participants indicated that **presentations helped them gain a better understanding of the response and recovery actions their institution should implement when considering the threat of a failure in campus infrastructure** |

*Table 5: Key Insights from the Exercise Assessment*

| |
|---|
| ▪ 88% of participants said **that exercise discussion topics were relevant to their institution** |
| ▪ 95% of participants believed that **exercise discussion topics encouraged someone with their level of training and experience to participate** |
| ▪ 91% of participants indicated that **the exercise increased their understanding of their institution's risk and vulnerabilities when considering the threat of a cyber-attack** |
| ▪ 91% of participants said that **the exercise increased their understanding of their institution's risks and vulnerabilities when considering the treat of a failure in campus infrastructure** |
| ▪ 94% of participants believed that the exercise **helped them gain a better understanding of the response and recovery actions their institution should implement when considering the threat of a cyber-attack** |
| ▪ 88% of participants indicated that the exercise **helped them gain a better understanding of the response and recovery actions their institution should implement when considering the threat of a failure in campus infrastructure** |

## Event Impact

The NTTX made an immediate impact on participants' confidence and cyber preparedness activities. The NTTX post-event survey indicated participants left the event more confident in their ability to respond (13% increase) and recover (14% increase) from a cyber-attack (Figure 4). 100% of participants identified a new risk or vulnerability at their institution, and a comparison between the pre-event and post-event survey indicated the following (Figure 5):

- Increase in participants who have **completed or plan to complete** the following actions:
    - Sign a mutual aid agreement to increase cybersecurity staffing and resources (42%)
    - Sign a mutual aid agreement to increase infrastructure protection staffing and resources (31%)
    - Integrate cybersecurity preparedness into emergency planning (28%)
    - Integrate infrastructure protection into emergency planning (15%)
    - Conduct a risk assessment of cybersecurity vulnerabilities (12%)
    - Conduct a risk assessment of infrastructure protection vulnerabilities (15%)
    - Conduct training and/or exercises to better prepare for a cyber-attack (15%)
    - Conduct training and/or exercises to better prepare for a failure in campus infrastructure (15%)

*Figure 4: Change in participants' confidence in their institution following the NTTX*

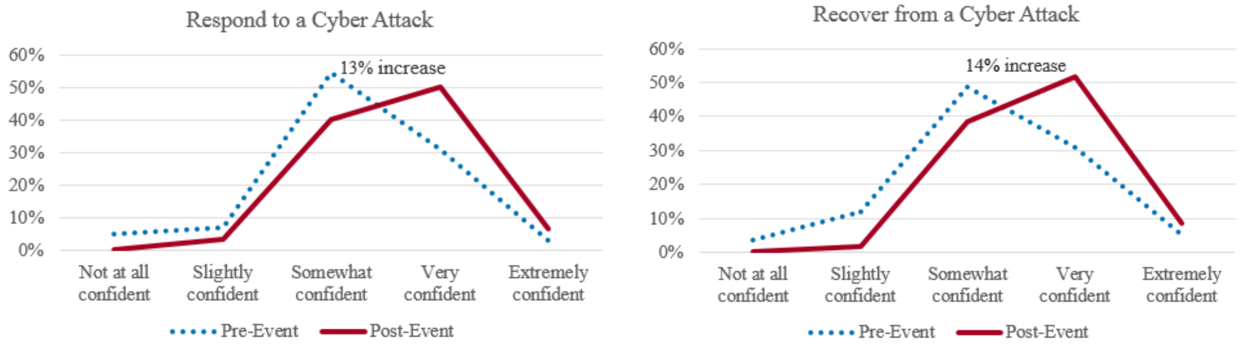
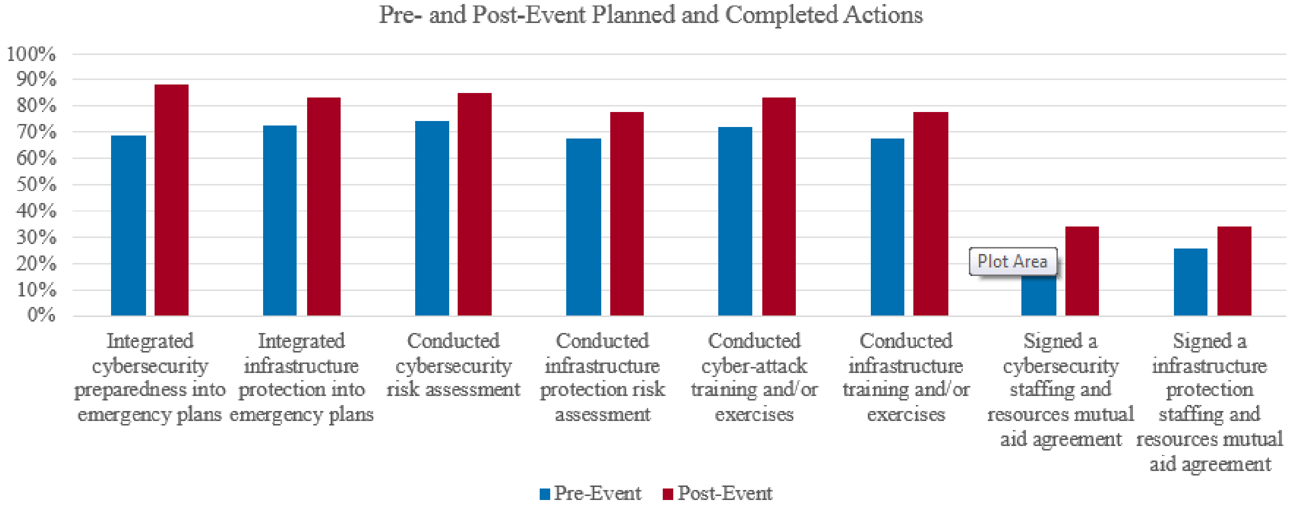


*Figure 5: Change in completed and plan to complete actions by NTTX participants*



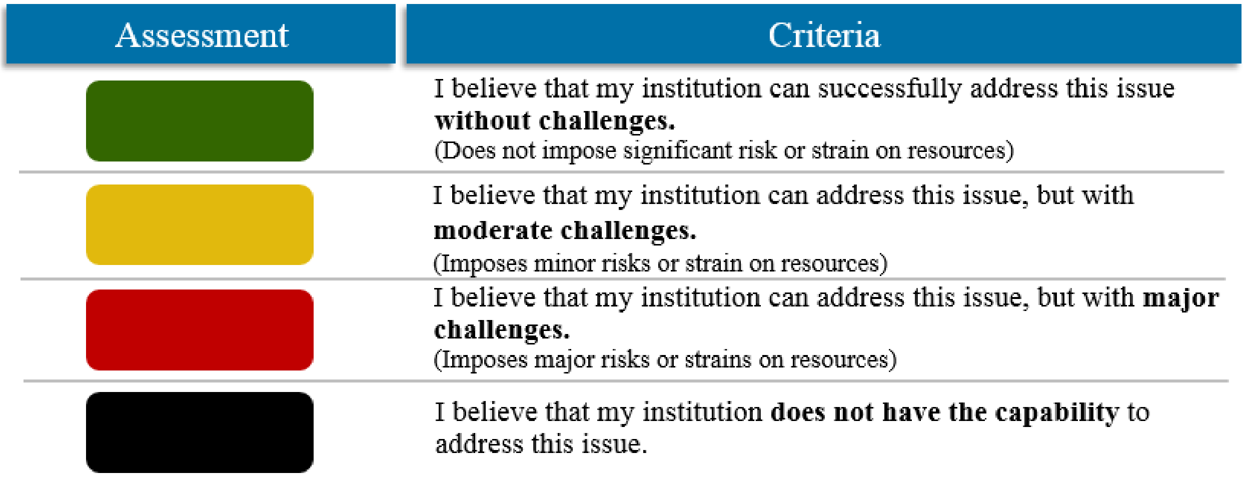
## Summary of Discussions

The following sections provide an overview of the exercise scenarios, polling question results, and key insights on IHE strengths and areas for improvement. Findings are broken down by each of the three major phases presented in the scenario: ***Cyber Response***, ***Emergency Response***, and ***Recovery***. These phases were developed based off FEMA's five Mission Areas (*Prevention*, *Protection*, *Mitigation*, *Response*, and *Recovery*), which are organized according to the specific capabilities needed to address an incident throughout its lifecycle[4]. Each section includes:

- An **overview of the capabilities** addressed during that phase;
- A **snapshot of the scenario** presented to the participants;
- The **associated findings** from each discussion; and
- **Recommended resources** relevant to the key issues.

Associated findings were developed based on polling questions using the scale in Figure 6 and observational notes provided by HSEEP-trained staff.

*Figure 6: Exercise Polling Assessment Scale*



| Assessment | Criteria |
|---|---|
| 🟩 | I believe that my institution can successfully address this issue **without challenges.**<br>(Does not impose significant risk or strain on resources) |
| 🟨 | I believe that my institution can address this issue, but with **moderate challenges.**<br>(Imposes minor risks or strain on resources) |
| 🟥 | I believe that my institution can address this issue, but with **major challenges.**<br>(Imposes major risks or strains on resources) |
| ⬛ | I believe that my institution **does not have the capability** to address this issue. |

The report that follows also provides insights garnered from several channels of feedback conducted during or after the NTTX on the quality and effectiveness of the event. The report includes a summary of the key results and recommendations for future events, and detailed results are included in the appendices. These feedback opportunities include:

- **Plenary hotwash** session, conducted in-person immediately following the NTTX;
- **Post-event survey,** distributed after the NTTX;
- **Participant Feedback Form**, provided to participants at the NTTX; and
- **Event Review Virtual Session**, conducted via teleconference on November 8, 2017.

Detailed results from these sessions are provided in Appendices A and B.

[4] https://www.fema.gov/national-preparedness-goal

# CYBER RESPONSE

## Overview

The cyber response phase covers the actions taken during or immediately following a cyber-incident to identify the potential impacts across critical systems and networks, implement defensive measures to protect systems from further exploitation, and disseminate necessary alerts and notifications to relevant stakeholders.

The cyber response module examined the following core capabilities[5]:

- Planning
- Threat Information Sharing
- Operational Coordination

## Scenario

### September 1, 2017

- A controversial figure exiled from his/her home country is invited to speak at your institution.
- This event upsets leadership in that country, who call out your institution for giving them a platform to spread “lies”.

### Several Weeks Later

- Following the speaking event, a supposed leaked document is circulated about your institution on social media; students and faculty share the document.

### October 10, 2017

- Your IT department receives calls from faculty/staff about issues accessing learning management software – some now have previously unavailable administrative privileges.
- Within hours, data housed in your learning management software is either missing or corrupted.
- An unauthorized message is sent out through your emergency alert system directing users to a webpage containing malware.
- Your local 911 call center reports a larger than average call volume from your campus population – calls immediately “hang up” when answered.

## Discussion Results

The cyber response phase of this incident will examine the following capabilities:

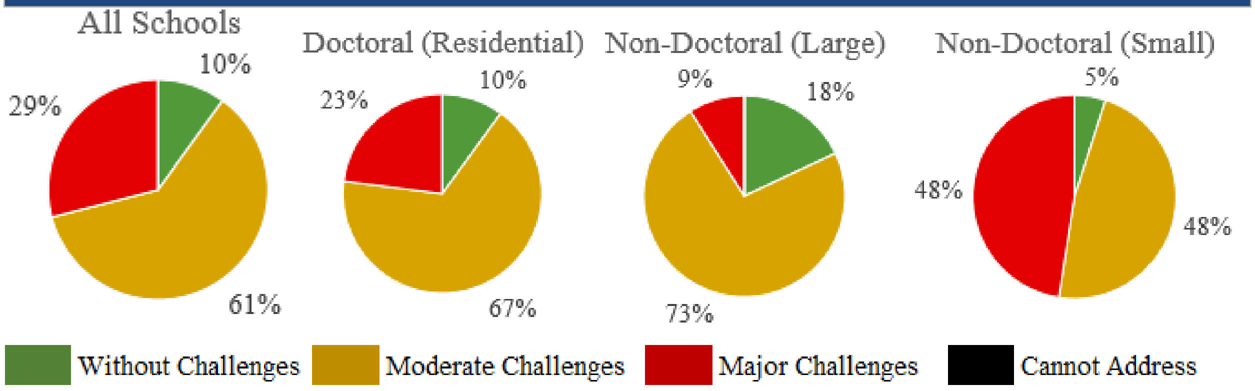
- **Cyber-incident planning**
- **Assessment of impacts**
- **Event notification methods and thresholds**

[5] https://www.fema.gov/core-capabilities

## Key Issue 1: Cyber-Incident Planning

Cyber-incident planning involves containing an incident and ensuring that technically skilled personnel are engaged in crisis planning efforts. IHEs should possess the necessary plans and procedures to respond to a cyber-incident. Ensuring back-up systems are in place is essential for an effective response.

**Assess the extent to which your institution's current emergency plans address the processes and resources required to assemble a multi-functional response team to respond to and recover from this scenario.**



Note: Polling Data is unavailable for doctoral, non-residential IHEs due to a data collection device malfunction

**Strengths:** 71% of institutions said they could address this issue with moderate or no challenges.

- 10% of all institutions expressed that they would have no challenges in assembling a multi-functional response team. These institutions indicated that having **established plans, policies, and procedures in place to coordinate representatives from IT and emergency management** was key to successful incident command.

**Areas for Improvement:** 29% of institutions indicated that they would experience major challenges when addressing this issue.

- Particularly among the 90% of residential, doctoral institutions with moderate to major challenges, participants noted risks in relying on third-party software contractors. Participants also stressed the **importance of reviewing third-party contracts** to ensure up-to-date incident reporting, backups, and other safeguards.

## Key Resources

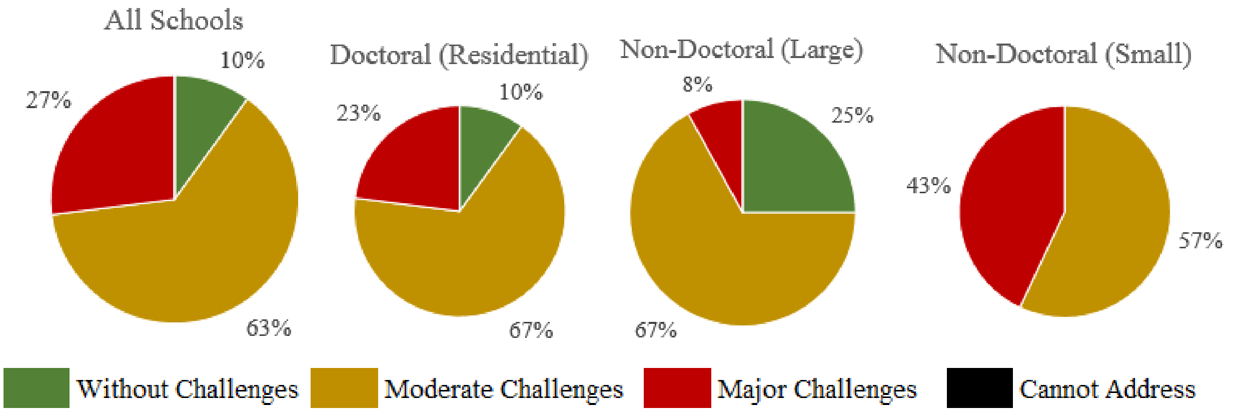
- **National Cyber Incident Response Plan (NCIRP).** The NCIRP describes the various roles and responsibilities in cyber incidents of the Federal Government, the private sector, and SLTT governments and how we will organize its activities to manage the effects of significant cyber incidents. The NCIRP, developed in accordance with Presidential Policy Directive (PPD) 41 on U.S. Cyber Incident Coordination, leverages doctrine from the National Preparedness System to articulate how the Nation responds to and recovers from cyber incidents. The NCIRP should serve as the basis when developing agency-, sector-, and organization-specific operational planning. Additionally, the NCIRP also contains information and resources to create incident response plans including the U.S. Cyber Incident Severity Schema. For more information, visit: https://www.us-cert.gov/ncirp
- **Critical Infrastructure Cyber Community (C3) Voluntary Program.** As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. The C³ Voluntary Program helps sectors and organizations that want to use the Framework by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector. For more information, visit: https://www.us-cert.gov/ccubedvp/academia
- **Department of Education, Response and Emergency Management for Schools (REMS) Technical Assistance Center**. The REMS TA Center, administered by the U.S. Department of Education, Office of Safe and Healthy Students (OSHS), supports public and private schools, school districts, and institutions of higher education, with their community partners, in building their preparedness capacity (including mitigation, prevention, protection, response and recovery efforts) and creating comprehensive emergency operations plans that address a variety of security, safety, and emergency management issues. For more information, visit: https://rems.ed.gov/
- **Industrial Control Systems Cyber Emergency Response Team Web Page**. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. For more information, visit: https://ics-cert.us-cert.gov/
- **Stay Safe Online**. A community-focused and partnership-based cybersecurity resource, with security practices, tips, and resources ready-made for use and implementation by individual users, business and industry, and academia. Sponsored by the National Cyber Security Alliance and promoted by DHS as a one-stop informational source for cybersecurity. For more information, visit: https://staysafeonline.org/

- **Stop.Think.Connect. Academic Alliance.** Opportunities with technology and the Internet appear to have no limit. Academia is often at the forefront of expanding our ever-evolving cyber universe. As new ground is forged and benefits of a digitally connected world are enhanced, academia has an opportunity to lead by example in ensuring that online practices of students, faculty, staff, alumni, and the community are as secure as possible. The Stop.Think.Connect. Academic Alliance is a nationwide network of nonprofit colleges and universities committed to promoting safe online practices. For more information, visit: http://www.dhs.gov/stopthinkconnect-academic-alliance
- **United States Computer Emergency Readiness Team (US-CERT)**. US-CERT provides publications, alerts and tips, and resources about cybersecurity and cyber threats. For more information, visit: http://www.us-cert.gov/

## Key Issue 2: Assessment of Impacts

The assessment of impacts involves coordinating efforts across multiple subject-matter experts to detect, analyze, and contain a cyber-attack. Effective assessment can inform prioritization of activities to limit the damages to the institution.

**Assess your institution's ability to identify the precise nature, expected duration, and impact of the malware intrusion on the learning management software and campus emergency notification system.**



Note: Polling Data is unavailable for doctoral, non-residential IHEs due to a data collection device malfunction

**Strengths:** 73% of institutions indicated they could address this issue with moderate or no challenges.

- 10% of all institutions expressed they would have no challenges, and credited **efforts to map system-interdependencies, prioritize critical systems, and pre-identify incident command staff** for this confidence.
- 25% of large, non-doctoral institutions were very confident in their ability to **identify the nature, duration, and impact of a malware intrusion**. Participants from these IHEs indicated that they had already used available human and financial capital to map interdependencies and identify critical systems.

**Areas for Improvement:** 27% of institutions indicated they would experience major challenges when addressing this issue.

- 100% of small, non-doctoral institutions indicated they would experience moderate or major challenges, citing a **significant strain on financial and human capital** and a lack of **pre-identified critical systems and mapped interdependencies**.

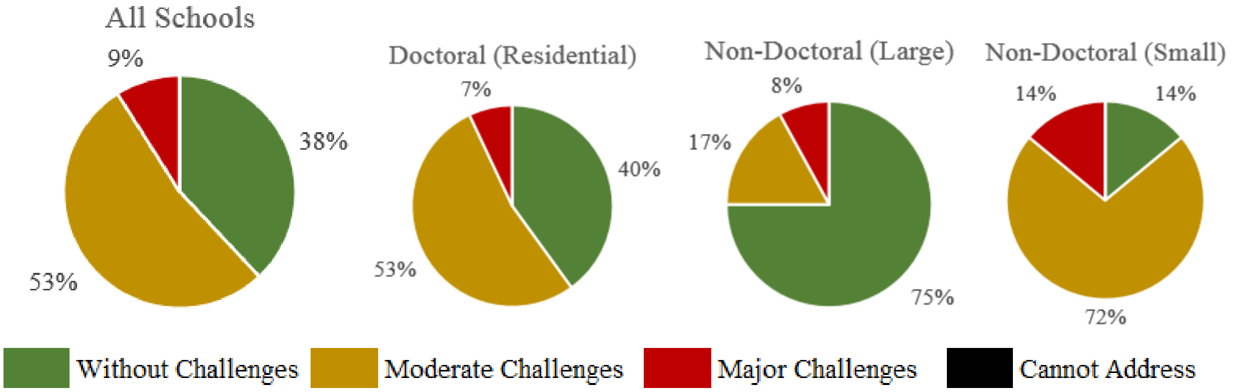
## Key Resources

- **Cyber Resilience Review (CRR).** The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The review assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity and others. For more information, visit: http://www.us-cert.gov/ccubedvp/self-service-crr
- **Cybersecurity Evaluation Tool (CSET®).** The Cyber Security Evaluation Tool (CSET®) is a DHS product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team. The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. For more information, visit: http://ics-cert.us-cert.gov/assessments
- **Higher Education Cloud Vendor Assessment Tool**. The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher education information security and data protection questions and issues regarding cloud services for consistency and ease of use. The matrix: 1) Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education; 2) Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through cloud services without increasing risks; and 3) Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions. For more information, visit: https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool
- **Mutually Agreed Norms for Routing Security (MANRS)**. The Routing Resilience Manifesto initiative, underpinned by the "Mutually Agreed Norms for Routing Security (MANRS)" document that includes a set of actionable recommendations, aims at supporting this goal. For more information, visit: https://www.routingmanifesto.org/

## Key Issue 3: Event Notification Methods and Thresholds

Event notification methods and thresholds enable institutions to deliver timely and appropriate information to key stakeholders during response to an incident.

**Assess your institution's ability to coordinate response activities during this incident by engaging appropriate stakeholders and utilizing appropriate communications channels.**



Note: Polling Data is unavailable for doctoral, non-residential IHEs due to a data collection device malfunction

**Strengths:** 91% of all institutions indicated they could address this issue with moderate or no challenges.

- 53% of institutions indicated they would experience moderate challenges, citing a **lack of awareness of the full range of federal resources available, such as Fusion Centers.**[6]
- 40% of doctoral, residential institutions indicated they would experience no challenges, **crediting past experience with similar incidents and training provided to staff.**

**Areas for Improvement:** 9% of institutions indicated they would experience major challenges when addressing this issue.

- 14% of small, non-doctoral institutions indicated they would express major challenges due to **limited availability of staff and resources**.
- Institutions noted the need to **strengthen communication with other IHEs** on cyber-threats and share best practices in response and recovery.

[6] https://www.dhs.gov/state-and-major-urban-area-fusion-centers

## Key Resources

- **Cyber Security Advisors (CSAs).** CSAs are regional located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and state, local, tribal, and territorial governments. CSAs offer immediate and sustained assistance to prepare and protect state, local, tribal, and territorial governments and private entities. For more information, visit: http://www.us-cert.gov/ccubedvp/getting-started-academia

- **DHS Cybersecurity Publications**. A ready-reference collection of documents published by DHS cybersecurity programs that can help private and public organizations with everything from setting up your first computer to understanding the nuances of emerging threats. For more information, visit: https://www.us-cert.gov/security-publications
- **National Cybersecurity & Communications Integration Center (NCCIC).** The NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government intelligence community, and law enforcement. For more information, visit: https://www.dhs.gov/about-national-cybersecurity-communications-integration-center

- **Protective Security Advisor (PSA) Program**. DHS provides local critical infrastructure protection support and guidance for academic institutions through the PSA Program. PSAs serve as local DHS representatives for security officers at schools and IHEs, and coordinate requests for training and grants. PSAs also conduct specialized security assessments of school facilities that assist schools in identifying potential security vulnerabilities and risks. For more information, visit: http://www.dhs.gov/protective-security-advisors.

# Emergency Response

## Overview

The emergency response phase covers the actions taken during or immediately following a cyber-incident with physical impacts to critical infrastructure that serve to save lives, protect property, and meet basic human needs. This phase focuses on how a community can effectively respond to physical threats or hazards caused by a cyber-incident.

The emergency response phase module examined the following core capabilities[7]:

- Public Health
- Critical Transportation
- Mass Care Services
- Operational Coordination
- Planning
- Threat Information Sharing

## Scenario

### Afternoon, October 10

***911 Center***

- Your institution is alerted by the local 911 call center that the number of dummy 911 calls from your campus is overwhelming their capabilities.

***Industrial Control Systems***

- An unauthorized user gains access to your campus' industrial control systems, interrupting your school's power breakers.
- Some campus buildings lose electricity and water, disrupting key card access and refrigeration in dining halls, medical facilities, and labs.
- Heating, Ventilation, and Air Conditioning (HVAC) systems shut down and temperatures rise in classrooms, dorms, medical facilities, research labs, and server rooms.
- Several of your institution's servers melt down as a result.

***Emergency Notification System***

- A mass notification is sent out to your campus community containing the following message: "*Emergency Alert: Campus is unsafe. Evacuate immediately*".
- Students leave campus by foot and by car, causing traffic congestion on roads around your institution.

[7] https://www.fema.gov/core-capabilities

## Discussion Results

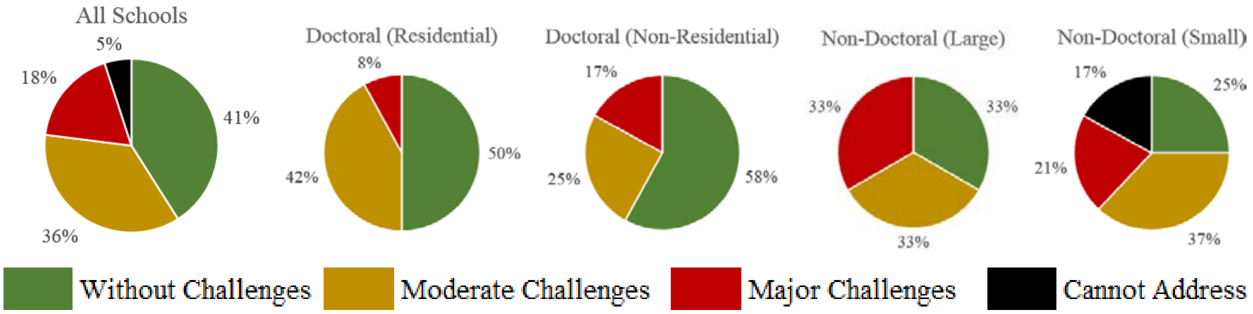
The emergency response phase of this incident will examine the following capabilities:

- **Response coordination with stakeholders**
- **Identifying and managing cascading impacts**
- **Continuity**
- **Crisis communications and public messaging**

### Key Issue 1: Response Coordination with Stakeholders

Response coordination with stakeholders should consider the extent to which an IHE can adopt and implement incident command protocols. This coordination should recognize procedural discrepancies between internal and external stakeholders. The ICS helps standardize response management systems and streamline operations, especially when multiple resources, departments, agencies, and organizations are involved.

**Assess your institution's ability to establish the incident command structure (ICS) to respond to impacts on both computer systems/networks and campus operations.**



**Strengths:** 77% of institutions indicated they could address this issue with moderate or no challenges.

- 41% of all institutions reported no challenges, with IHE representatives **crediting regular and recurring exercises and well-established plans** for their ability to successfully establish ICS.
- 92% of doctoral, residential institutions indicated they would experience moderate or no challenges, citing **use of external subject-matter experts (e.g. law enforcement, cyber-forensics)** as a best practice.

**Areas for Improvement:** 23% of institutions indicated they would experience major challenges or would be unable to address this issue.

- 38% of small, non-doctoral institutions indicated that they would experience major challenges or be unable to address this issue, citing a **lack of ICS knowledge and training** and the need for **updated mutual-aid agreements and contact lists**.
- 66% of large, non-doctoral institutions indicated that they would face moderate or major challenges in addressing this issue, citing **a lack of awareness of the availability of technical support from the federal government**.

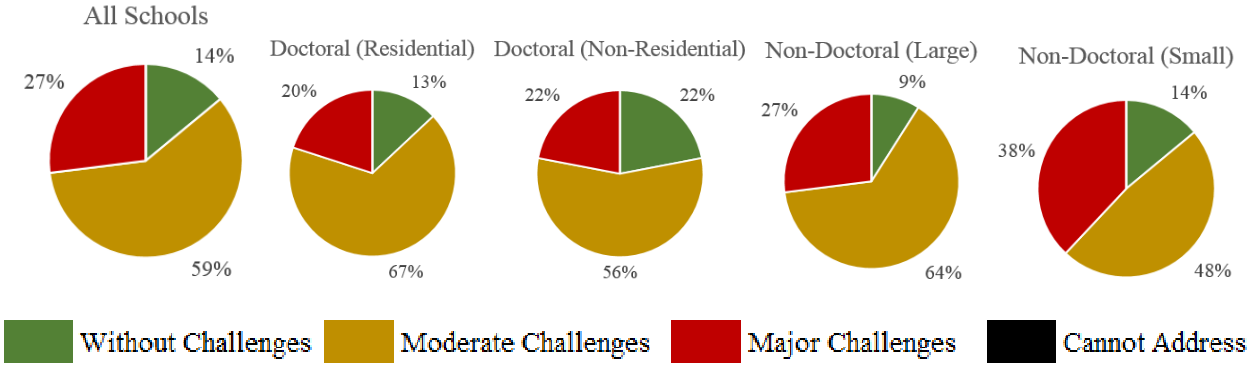
## Key Resources

- **IS-100.HE Introduction to the Incident Command System for Higher Education**. This FEMA training course introduces the Incident Command System (ICS) and provides the foundation for higher level ICS training. This course describes the history, features and principles, and organizational structure of ICS. It also explains the relationship between ICS and the National Incident Management System (NIMS). This course uses the same objectives and content as other ICS courses with higher education examples and exercises. For more information, visit: https://training.fema.gov/is/courseoverview.aspx?code=IS-100.HE
- **Incident Command System (ICS) Resource Center**. The FEMA ICS Resource Center website has a multitude of ICS reference documents including, but not limited to, ICS Forms, checklists, training course information and links to other related resources. For more information, visit: https://training.fema.gov/emiweb/is/icsresource/

## Key Issue 2: Identifying and Managing Cascading Impacts

The ability to identify cascading impacts to an institution supports strategic decisions by IHE staff to prioritize activities and allocate resources during a cyber-attack.

**Assess your institution's ability to prioritize and respond to the cyber-attack and impacts to campus operations as a result of the critical infrastructure failure.**



**Strengths:** 73% of institutions indicated they could address this issue with moderate or no challenges.

- 14% of institutions indicated they would experience no challenges when addressing this issue, noting **a best practice is to increase faculty and staff awareness of critical systems to aid in the identification of vulnerabilities**.
- 80% of doctoral, residential IHEs indicated they would experience moderate or no challenges, crediting **pre-existing, comprehensive emergency management plans and procedures**.

**Areas for Improvement:** 27% of institutions indicated they would experience major challenges when addressing this issue.

- 38% of small, non-doctoral IHEs cited major challenges and reported that while closing campus operations was not the preferred solution, **suspending operations in the short-term would be the only way to manage these impacts since emergency plans and procedures did not account for critical infrastructure failure**.
- Institutions noted that they **had not fully considered lab and data security needs** and felt that they presented a large vulnerability, including maintaining the integrity of lab environment conditions, and would need to draft and revise current emergency plans.
- Institutions also noted **concern with their ability to manage false emergency alert notifications and compromised industrial control systems**. IHE representatives identified the need to develop an alternative emergency communication system.

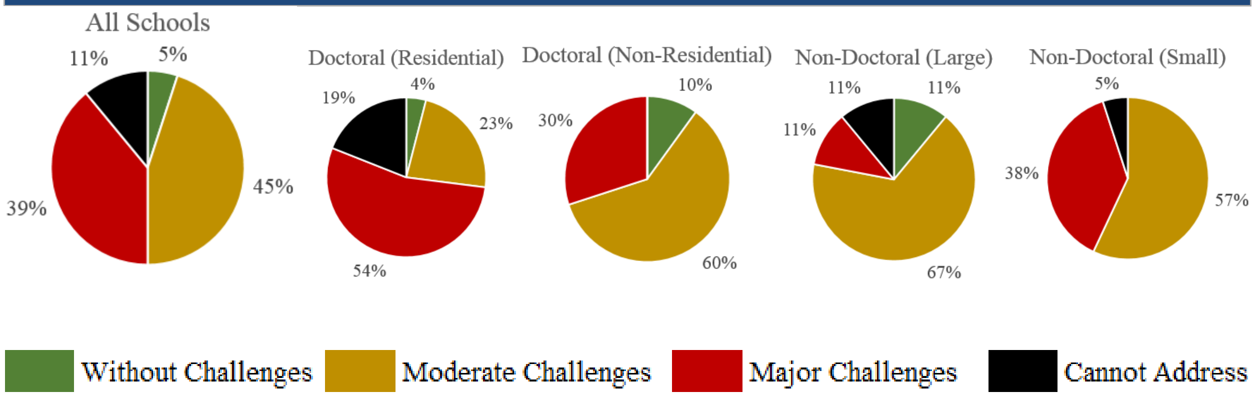
## Key Resources

- **Industrial Control Systems Cyber Emergency Response Team Web Page**. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. For more information, visit: https://ics-cert.us-cert.gov/
- **Science and Technology Directorate's (S&T) First Responder Communities of Practice**. The S&T First Responder Communities of Practice is a professional networking, collaboration, and communication platform created by DHS's S&T to support improved collaboration and information sharing amongst the nation's First Responders and other federal, state, local, tribal and territorial governments and private sector stakeholders supporting homeland security efforts. This vetted community of members focuses on emergency preparedness, response, recovery and other homeland security issues. For more information, visit: https://communities.firstresponder.gov/web/guest;jsessionid=D50CF79D14F5037D431C59C039D56172.w4.
- **Cybersecurity Evaluation Tool (CSET®).** The Cyber Security Evaluation Tool (CSET®) is a DHS product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team. The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. For more information, visit: http://ics-cert.us-cert.gov/assessments

## Key Issue 3: Continuity

Continuity is the ability to maintain critical functions during an incident to minimize disruptions that result in financial, reputational, regulatory, and stakeholder impacts. To ensure the restoration of operations, an IHE must understand what alternative processes and services need to be activated, the infrastructure required to support such efforts, and how stakeholders can assist with continuity.

**Assess your ability to continue performance of your institution's essential functions during a critical infrastructure disruption to ensure continuity of operations (COOP).**



**Strengths:** 50% of institutions indicated they could address this issue with moderate or no challenges.

- 45% of institutions indicated moderate challenges, citing the need to **incorporate continuity operations into training and exercises.**

**Areas for Improvement:** 50% of institutions indicated they would experience major challenges or would be unable to address this issue.

- 11% of institutions indicated they would be unable to address this issue, citing **a lack of COOP plan documentation, nonexistent staff training, and high turnover in personnel and leadership**.
- 73% of residential, doctoral institutions indicated they would experience major challenges or would be unable to address this issue, citing the **challenge for law enforcement and school administration to account for all students.**

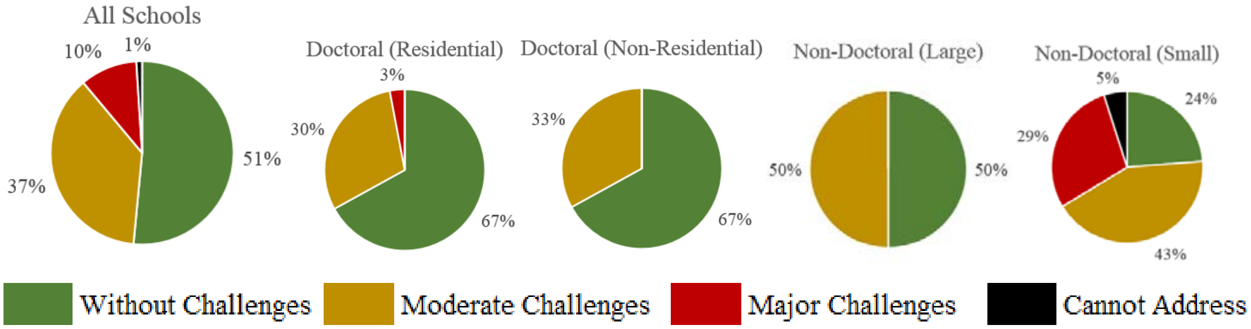
## Key Resources

- **Continuity Resource Toolkit**. The Continuity Resource Toolkit provides examples, tools, and templates for establishing and implementing a continuity strategies based on the FEMA Continuity Guidance Circular (CGC). To view the Toolkit, visit: www.fema.gov/continuity-resource-toolkit. For more information on the FEMA Continuity Guidance Circular, visit: CGC: www.fema.gov/continuity-guidance-circular
- **FEMA Emergency Management Institute (EMI) Independent Study Program**. Virtual training on a multitude of emergency preparedness and continuity resilience strategies is available through the FEMA, EMI, Independent Study Program. For more information and a list of courses, visit: http://training.fema.gov/IS/
- **FEMA Monthly Continuity Webinar Series**. The Series covers a variety of continuity topics from a diverse cadre of speakers. For more information, visit: http://www.fema.gov/continuity-webinar-series/
- **FEMA National Continuity Programs (NCP) Office**. FEMA, NCP is an element of the FEMA Administrator's Office which supports the continuity planning and preparedness efforts of both government and non-government stakeholders in order to sustain the continuous performance of National Essential Functions under all conditions. For more information, visit: http://www.fema.gov/continuity-operations/

## Key Issue 4: Crisis Communications and Public Messaging

Effective crisis communications and public messaging helps bolster the campus community's confidence in response efforts. This requires the ability to respond to a high volume of requests from community partners and law enforcement personnel. Additionally, proactive messaging to stakeholders and the public is essential.

**Assess your institution's ability to deliver coordinated and prompt alerts to internal and external stakeholders following a cyber-attack that disrupts your institution's operations.**



**Strengths:** 89% of institutions indicated they could address this issue with moderate or no challenges.

- 51% of institutions indicated they would experience no challenges, crediting **experience with public messaging after a large event (e.g. high profile campus visit), preemptive communications and coordination procedures, and incorporating Public Information Officers (PIOs) into the ICS**.

**Areas for Improvement:** 11% of institutions indicated that they would experience major challenges or would be unable to address this issue.

- 34% of small, non-doctoral institutions indicated they would experience major challenges or be unable to address this issue, citing **difficulty in delivering alerts to key stakeholders when the cyber-attack impacts communication devices.** Larger institutions noted that they use students' personal emails as a back-up communication method.
- Institutions noted that **messaging to international students, students with access and functional needs, and students living off-campus** presents additional challenges.

## Key Resources

- **G0367 Emergency Planning for Campus Executives**. This 2-hour overview of emergency planning serves as a briefing for executives of institutions of higher education. It provides them with insights into multi-hazard emergency planning and their role in protecting lives, property, and operations. For more information, visit: https://training.fema.gov/hiedu/aemrc/eplanning/g367.aspx
- **Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education**. This guide provides guidance to IHEs on best practices for taking preventative and protective measures to stop an emergency from occurring or reduce the impact of an incident. The guide aligns and builds upon years of emergency planning work by the Federal Government and is a joint product of DHS, the DOJ, the DOE, and the Department of Health and Human Services (HHS). IHEs can use the guide to create and/or revise existing emergency operations plans. For more information, visit: http://www.fema.gov/media-library-data/20130726-1922-25045-3638/rems_ihe_guide.pdf
- **FEMA Integrated Public Alert and Warning System (IPAWS)**. FEMA has a tool that will allow officials to send out an alert to a designated population during/after an incident. IPAWS will allow IHE to disseminate information to their students, faculty, and staff very quickly. For more information, visit: https://www.fema.gov/integrated-public-alert-warning-system

# RECOVERY

## Overview

The recovery phase covers post-incident efforts to assist affected communities and promptly restore critical services and functions. Successful recovery ensures that a community emerges from any threat or hazard stronger and better positioned to support those who experience financial, emotional, and/or physical hardships from an incident.

The recovery phase module examined the following core capabilities[8]:

- Public Information and Warning
- Planning
- Mass Care Services
- Operational Coordination

## Scenario

### October 11, 2017

- Your IT Department determines that your institution was the target of a complex cyber-attack possibly by a set of continuous hacks, called an advanced persistent threat (APT).
- Emergency services have been working to help those affected by the power outages, including the evacuation of patients from on-campus medical facilities.

### The Next Few Days

- IT has yet to confirm that there is no malware remaining on your industrial control systems.
- Research faculty are growing increasingly concerned over the impacts to their research projects.
- Students and parents are concerned about how this event will impact the remainder of their semester and whether their records (or sensitive information) has been compromised.
- Rumors spread on Twitter claiming the attack was a result of a malicious insider at your institution.
- In response, people are questioning whether your institution did enough to prevent this from happening.

## Discussion Results

The recovery phase of this incident will examine the following capabilities:

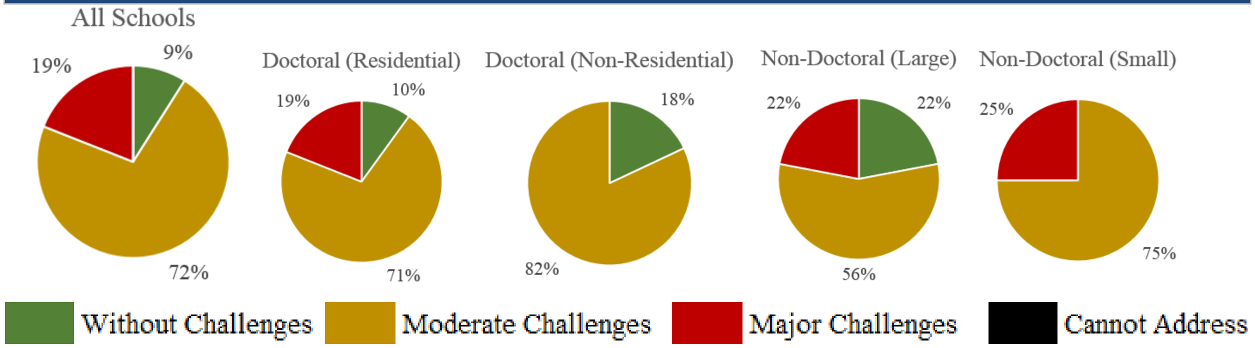
- **Recovering campus systems**
- **Restoring campus operations**
- **Post-incident communications**
- **Legal and financial considerations**

[8] https://www.fema.gov/core-capabilities

## Key Issue 1: Restoring Campus Systems

To successfully restore campus systems, IHEs must identify root causes and affected systems. IHEs should ensure they possess digital evidence recovery capabilities and access to forensic resources. IHEs also must prioritize the implementation of stopgap patches to restore operations in the near term against collecting and preserving evidence to fully understand the extent of a cyber-attack.

**Assess your institution's ability to coordinate recovery efforts for compromised systems including digital forensics and system restoration.**



**Strengths:** 81% of institutions indicated they could address this issue with moderate or no challenges.

- 10% of institutions indicated they would experience no challenges, crediting their **ICS experience and clearly defined roles and responsibilities within incident command**. These institutions also noted they have **contracts in place to retain access to external stakeholders that could assist with forensic analysis (e.g., a third-party IT company, software**.

**Areas for Improvement:** 19% of institutions indicated that they would face major challenges when addressing this issue.

- 30% of small, non-doctoral institutions indicated they would experience major challenges, citing **unclear decision-making authorities and a lack of cyber-forensics training and capabilities**. In addition, the **simultaneous execution of forensic investigation and operational recovery efforts would pose major resource constraints**.
- Institutions also noted the **need to review and revise their policies and practices for sharing data with law enforcement,** as IHEs often voluntarily turn over their systems to the FBI for investigation without a subpoena. University legal counsel participants voiced concern over this practice, as it could legally compromise an IHE and recommended that all require a subpoena before granting law enforcement personnel access to their systems.

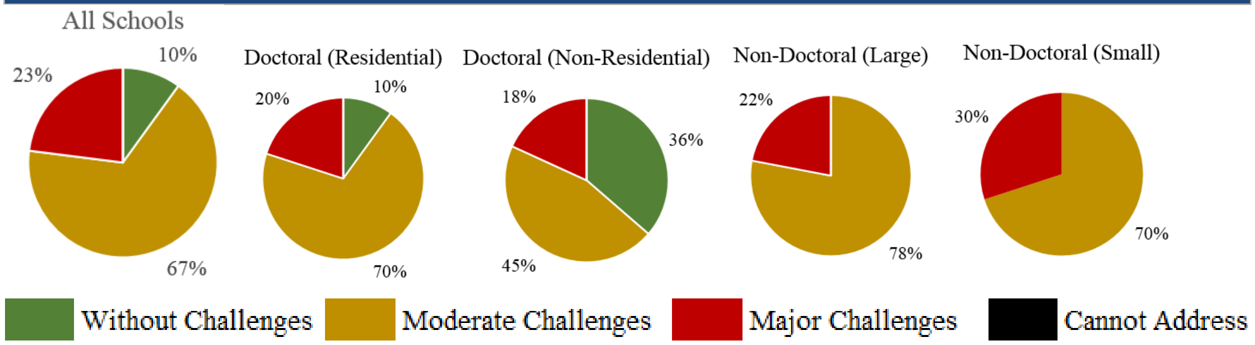
## Key Resources

- **Cyber Resilience Review (CRR).** The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The review assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity and others. For more information, visit: http://www.us-cert.gov/ccubedvp/self-service-crr
- **DHS State and Local Law Enforcement Resource Catalog**. The DHS State and Local Law Enforcement Catalog highlights DHS resources available to state, local, tribal, and territorial law enforcement. The guide provides summaries of, and links to, training, publications, guidance, alerts, newsletters, programs, and services available to non-Federal law enforcement from across DHS. For more information, visit: http://dhs.gov/publication/dhs-state-and-local-law-enforcement-resource-catalog.
- **Higher Education Cloud Vendor Assessment Tool**. The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher education information security and data protection questions and issues regarding cloud services for consistency and ease of use. The matrix: 1) Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education; 2) Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through cloud services without increasing risks; and 3) Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions. For more information, visit: https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

## Key Issue 2: Restoring Campus Operations

Restoring critical infrastructure capabilities as soon as possible maximizes operational resilience and reduces financial impacts caused by a disruption. Understanding restoration priorities, internal and external stakeholder requirements, and what resources are needed is essential to fully restoring campus operations.

**Assess your institution's ability to recover and resume normal operations, including academic and research activities, after a disruption.**



**Strengths:** 90% of institutions indicated they could address this issue with moderate or no challenges.

- 36% of doctoral, non-residential IHEs indicated they would experience no challenges, citing a best practice to **ensure faculty have access to both physical and digital copies of key information (e.g., lessons plans).**

**Areas for Improvement:** 23% of institutions indicated that they would face major challenges when addressing this issue.

- 30% of small, non-doctoral institutions noted that they would face major challenges when resuming normal operations. Representatives from these IHEs noted that **if their learning management system were to be compromised it would interrupt online and distance learning courses**.
- Institutions noted the importance of **maintaining redundant critical infrastructure systems** (e.g., backup generators and emergency override functions) in the event of an attack as these manual override capabilities help combat cyber-interference.
- Institutions also noted the need to build **relationships with critical infrastructure equipment manufacturers** (e.g., HVAC and server) to help with system restoration efforts after an incident.

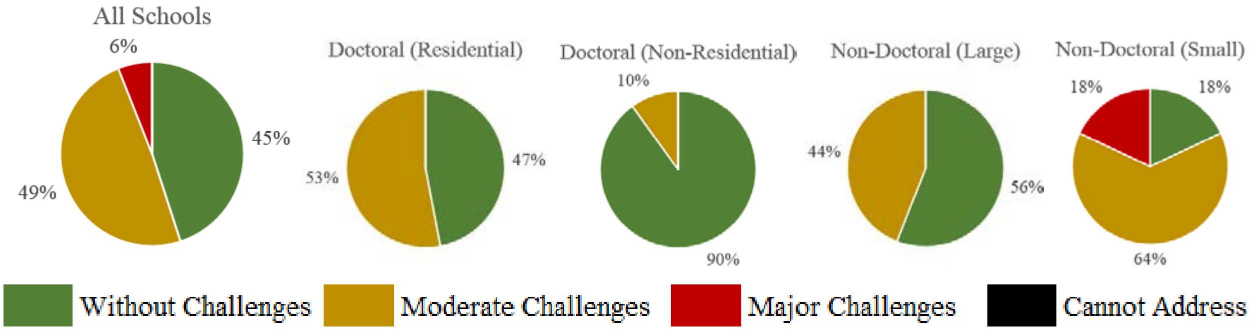
## Key Resources

- **Department of Education, Response and Emergency Management for Schools (REMS) Technical Assistance Center**. The REMS TA Center, administered by the U.S. Department of Education, Office of Safe and Healthy Students (OSHS), supports public and private schools, school districts, and institutions of higher education, with their community partners, in building their preparedness capacity (including mitigation, prevention, protection, response and recovery efforts) and creating comprehensive emergency operations plans that address a variety of security, safety, and emergency management issues. For more information, visit: https://rems.ed.gov/
- **Building A Disaster-Resistant University**. *Building A Disaster-Resistant University* is a how-to guide and distillation of the experiences of six universities and colleges that have been working to become disaster-resistant. The guide provides basic information designed for institutions just getting started, as well as ideas, suggestions, and practical experiences for institutions that have already begun to take steps to becoming more disaster-resistant. For more information, visit: http://www.fema.gov/media-library/assets/documents/2288.
- **DHS Campus Resilience Program.** The DHS Campus Resilience Program was created upon a recommendation from the Homeland Security Academic Advisory Council (HSAAC). DHS is currently in the developmental stages of the Campus Resilience Program. This initiative builds upon best practices, lessons learned and resources already developed to make U.S. colleges and universities more resilient. For more information on the DHS Campus Resilience Program, visit https://www.dhs.gov/campus-resilience or contact the Office of Academic Engagement at AcademicEngagement@hq.dhs.gov.
- **Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education**. This guide provides guidance to IHEs on best practices for taking preventative and protective measures to stop an emergency from occurring or reduce the impact of an incident. The guide aligns and builds upon years of emergency planning work by the Federal Government and is a joint product of DHS, the DOJ, the DOE, and the Department of Health and Human Services (HHS). IHEs can use the guide to create and/or revise existing emergency operations plans. For more information, visit: http://www.fema.gov/media-library-data/20130726-1922-25045-3638/rems_ihe_guide.pdf.

## Key Issue 3: Post-Incident Communications

Effective post-incident communications proactively engage the public and media to address their concerns, building confidence in an IHE's handling of an incident. Insufficient public messaging could lead to long-term reputational and possibly financial impacts as bad press hampers student enrollment and ability to secure grant funding.

**Assess your ability to engage stakeholders, the public, and the media in the aftermath of the incident, including managing impacts to your institution's reputation and brand.**



**Strengths:** 94% of institutions indicated they could address this issue with moderate or no challenges.

- 100% of all institution groups besides small non-doctoral institutions indicated they would experience moderate or no challenges, citing **pre-scripted messaging, integration of PIOs, speech writers, and other key stakeholders into a central entity, and previous experience with public messaging during large events, protests, and other emergencies**. The experience established **pre-existing relationships with the media** to conduct post-incident communications.

**Areas for Improvement:** 6% of institutions indicated that they would face major challenges when addressing this issue.

- 82% of small, non-doctoral IHEs indicated they would experience moderate or major challenges, citing the need to **develop pre-scripted messaging and utilize channels beyond online media (e.g., traditional media and public forums).**
- Institutions noted the importance of **issuing "non-updates" to key stakeholders (e.g., "there are no updates at this time")**.

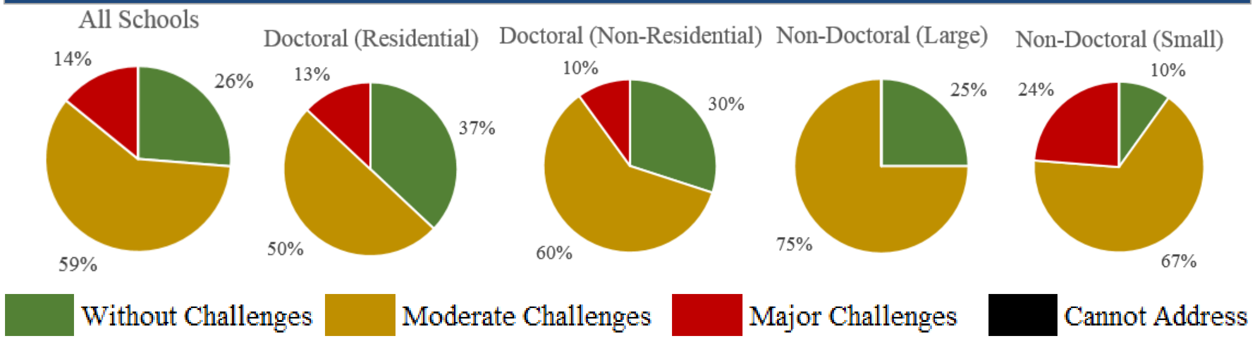
## Key Resources

- **G0367 Emergency Planning for Campus Executives**. This 2-hour overview of emergency planning serves as a briefing for executives of institutions of higher education. It provides them with insights into multi-hazard emergency planning and their role in protecting lives, property, and operations. For more information, visit: https://training.fema.gov/hiedu/aemrc/eplanning/g367.aspx
- **Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education**. This guide provides guidance to IHEs on best practices for taking preventative and protective measures to stop an emergency from occurring or reduce the impact of an incident. The guide aligns and builds upon years of emergency planning work by the Federal Government and is a joint product of DHS, the DOJ, the DOE, and the Department of Health and Human Services (HHS). IHEs can use the guide to create and/or revise existing emergency operations plans. For more information, visit: http://www.fema.gov/media-library-data/20130726-1922-25045-3638/rems_ihe_guide.pdf.
- **Student Tools for Emergency Planning (STEP)**. The STEP Program was designed by teachers and is sponsored by a state's Emergency Management Agency and FEMA. The program provides students and their families with concrete strategies to prepare for and deal with various emergencies. For more information, visit: http://www.fema.gov/student-tools-emergency-planning-step.
- **DHS Office of Emergency Communications**. Established in 2007 in response to communications challenges faced during the attacks on September 11, 2001 and Hurricane Katrina, the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. OEC provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide. For more information, visit: https://www.dhs.gov/office-emergency-communications

## Key Issue 4: Legal and Financial Considerations

Risk assessments of the legal and financial impacts of a cyber-attack should be conducted prior to an incident. Essential elements of recovery include capturing data, logging decisions, managing finances, handling insurance claims, and documenting lessons learned. Following an incident, IHEs need to reevaluate their budget constraints, legal liabilities, regulatory and reporting requirements, and plans to address these issues.

**Assess your ability to manage legal and financial liabilities/obligations stemming from a cyber-attack that impacts campus operations.**



**Strengths:** 86% of institutions indicated they could address this issue with moderate or no challenges.

- 37% of doctoral residential institutions indicated they would experience no challenges, citing regular **review of grant contracts to determine when they need to notify donors, foundations, and the government of a cyber-attack and affiliated risks**.

**Areas for Improvement:** 14% of institutions indicated they would face major challenges when addressing this issue.

- 24% of small non-doctoral institutions indicated they would experience major challenges, citing **high costs could force them to seek support from their respective state governments**.
- Institutions noted **they would be legally required to issue an alert in accordance with the Clery Act if critical infrastructure is impacted.** Per the Clery Act, campuses are required to issue timely warnings if a crime presents a threat to student and employee safety. Interruption of campus services (e.g., power, HVAC, water) could constitute such a threat.

## Key Resources

- **DHS State and Local Law Enforcement Resource Catalog**. The DHS State and Local Law Enforcement Catalog highlights DHS resources available to state, local, tribal, and territorial law enforcement. The guide provides summaries of, and links to, training, publications, guidance, alerts, newsletters, programs, and services available to non-Federal law enforcement from across DHS. For more information, visit: http://dhs.gov/publication/dhs-state-and-local-law-enforcement-resource-catalog.

- **Law Enforcement Conferences, Gatherings, and Meetings**. The Office for State and Local Law Enforcement maintains a comprehensive list of law enforcement conferences, gatherings, and meetings across the country. These events provide campus law enforcement professionals training opportunities and the ability to share best practices with other members of the law enforcement community. For more information, visit: https://www.dhs.gov/office-state-and-local-law-enforcement.

- **Cybersecurity Insurance**. Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. In recent years, the Department of Homeland Security National Protection and Programs Directorate (NPPD) has engaged key stakeholders to address this emerging cyber risk area. This webpage provides additional resources regarding those engagements. For more information, visit: https://www.dhs.gov/cybersecurity-insurance

- **Research on Threat Assessments and Various Types of Targeted Violence on Campuses**. The United States Secret Service (USSS) provides research and reports on violence at schools and IHEs. Released in April 2010, "Campus Attacks: Targeted Violence Affecting Institutions of Higher Education" contains information useful for campus safety professionals charged with identifying, assessing, and managing violence risk at institutions of higher education. Additionally, the Safe School Initiative, a study of attacks on K-12 schools, was released in 2002. For more information, visit: https://www2.ed.gov/admins/lead/safety/campus-attacks.pdf.

# APPENDIX A: NTTX SURVEY RESULTS

The following sections detail the results of the pre- and post- event surveys.

## Event Surveys

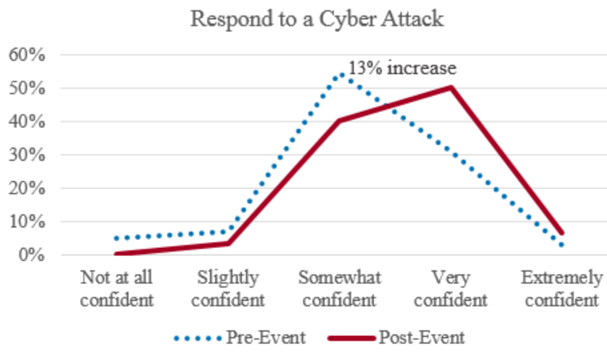
Following the event, pre- and post-event survey data was analyzed to understand participants' recognition of their institution's risks and vulnerabilities, participant confidence in their institution to address its risks and vulnerabilities, and the status of specific actions to address them.

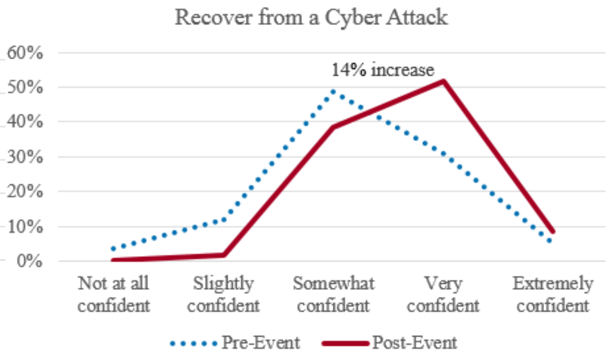
**100% of respondents identified at least one new risk or vulnerability at their institution** based on their participation at this year's NTTX.

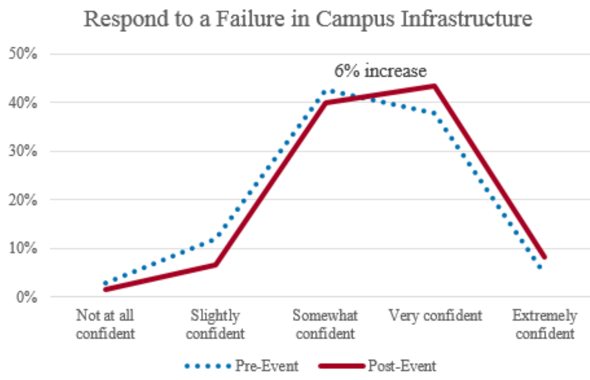
***Top 3 Categories of Risk and Vulnerability Identification***

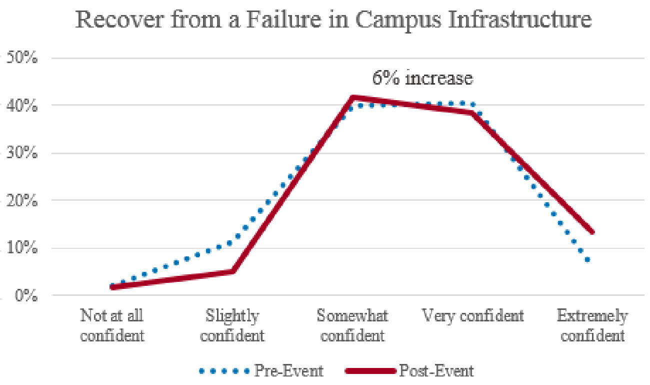
1. Cyber-incident planning (61%)
2. Continuity of Operations Planning for essential functions (50%)
3. Assessment of cyber-attack impacts (45%)

The following graphs highlight differences in participant confidence levels before and after the NTTX in regards to responding to and recovering from a cyber-attack and failure of campus infrastructure. IHEs became 13% more confident in their ability to respond to a cyber-attack and 14% more confident in their ability to recover from a cyber-attack after attending the 2017 NTTX. IHEs also felt 6% more confident in their ability to respond to and recover from a failure in campus infrastructure.









After the event, participants noted that they became more motivated to review and revise their IHE's plans and procedures. The chart below shows desired actions and the percent increase of IHEs to complete or make plans to implement these actions.

*Table 3: Key Insights from the Post-Event Survey*

| Action | % increase of IHEs that completed/ plan to complete |
|---|---|
| Integrate cybersecurity preparedness into their emergency plans | 28% |
| Integrate infrastructure protection into emergency plans | 15% |
| Conduct a risk assessment of cybersecurity vulnerabilities | 12% |
| Conduct a risk assessment of infrastructure protection vulnerabilities | 15% |
| Conduct training and/or exercises to better prepare for a cyber-attack | 15% |
| Conduct training and/or exercises to better prepare for a failure of infrastructure | 15% |
| Sign a mutual aid agreement to increase cybersecurity staffing and resources | 42% |
| Sign a mutual aid agreement to increase infrastructure protection staffing and resources | 31% |

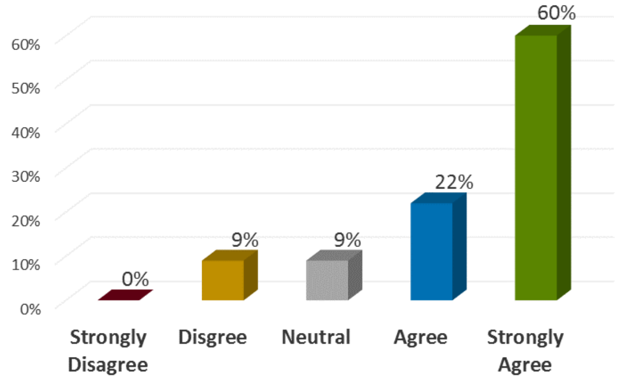
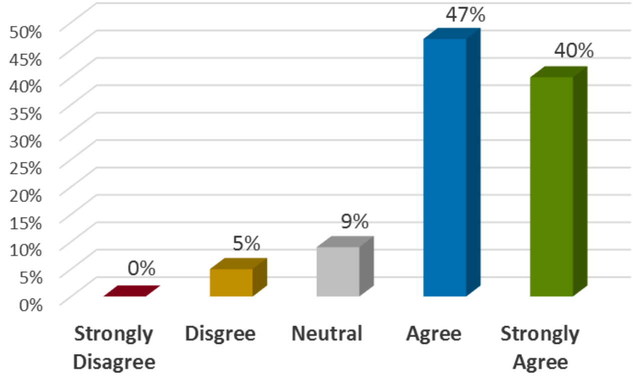
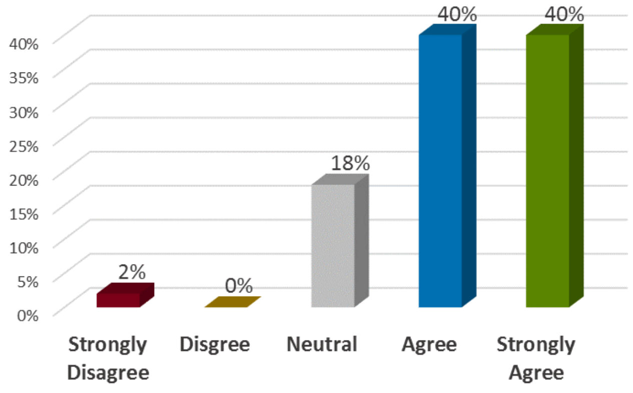
# APPENDIX B: PARTICIPANT FEEDBACK FORMS

The following sections provide detail on all responses to the Participant Feedback Form.

## Seminar and Exercise Assessment

In this section, participants were asked to provide an overall assessment of the exercise and seminar portions of the event and to rate them on a one-to-five scale, with one indicating "strongly disagree and five "strongly agree." ***Table 6: Seminar Assessment Feedback and Table 7: Exercise Assessment Feedback*** below documents the distribution of responses for each statement.

*Table 6: Seminar Assessment Feedback*

| Statement | Distribution |
|---|---|
| The seminar workshop registration process was simple and easy to understand |  |
| The seminar/workshop sessions were relevant to the exercise scenario |  |
| The presentations during the sessions were relevant to my institution |  |

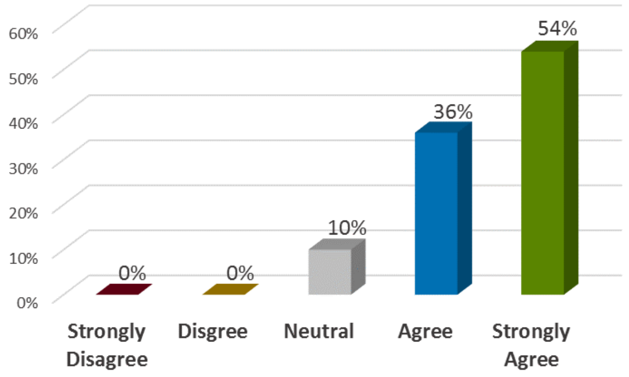
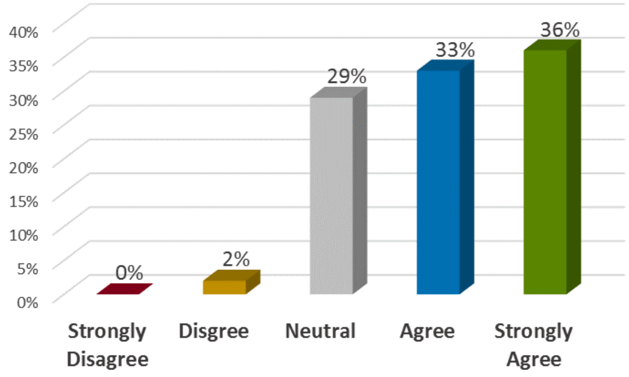
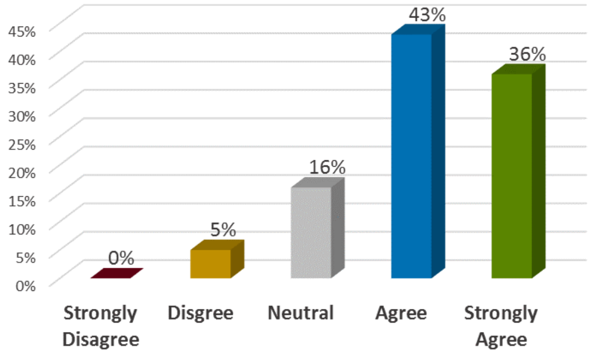
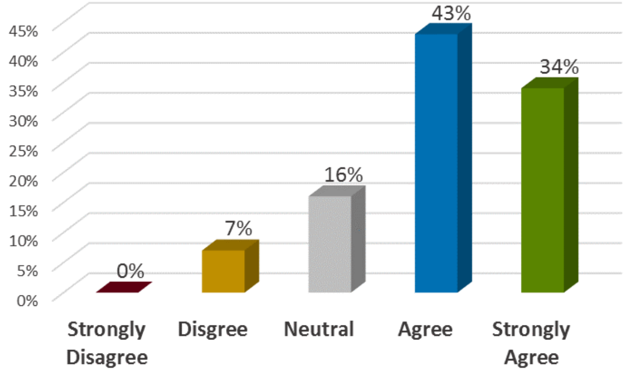
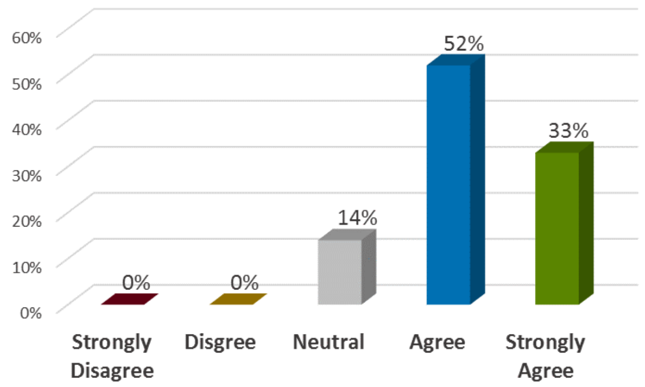
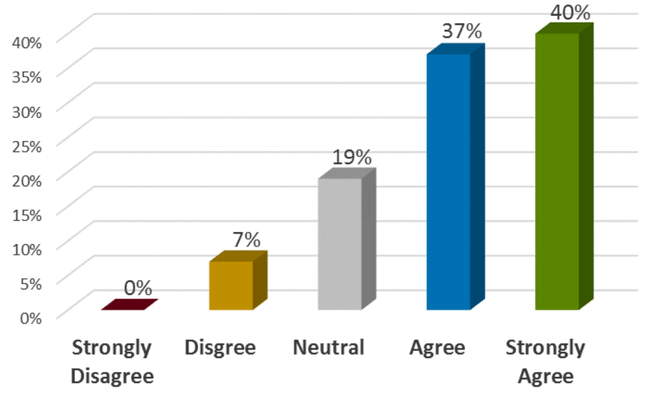
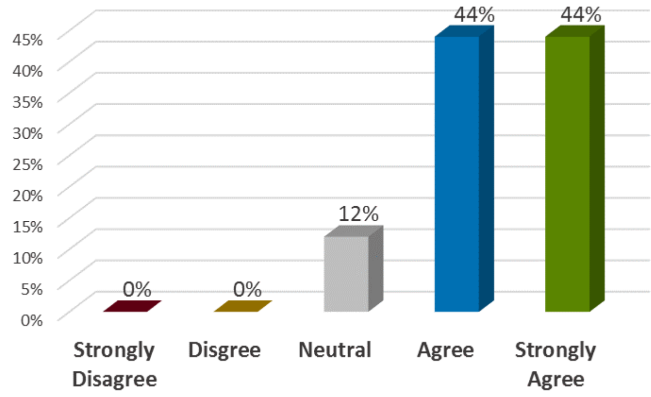
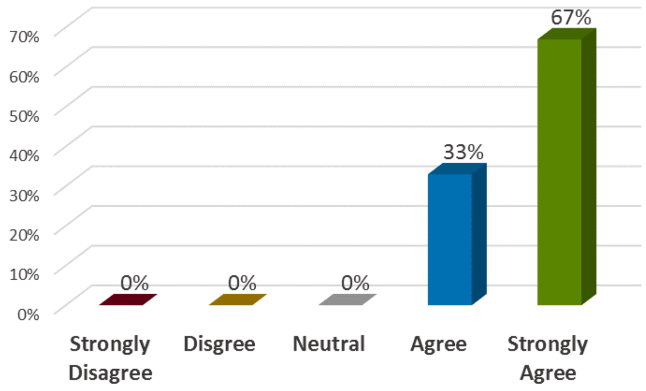
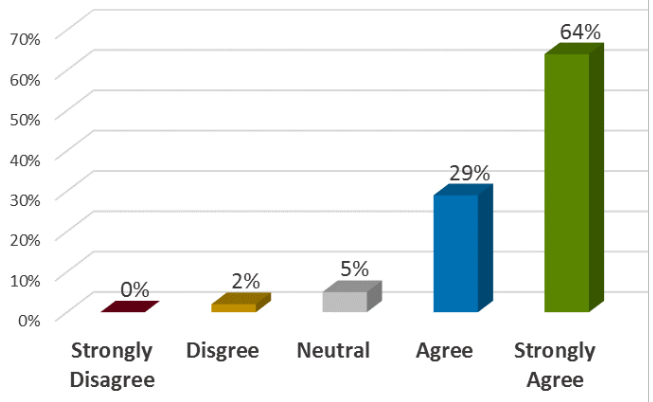
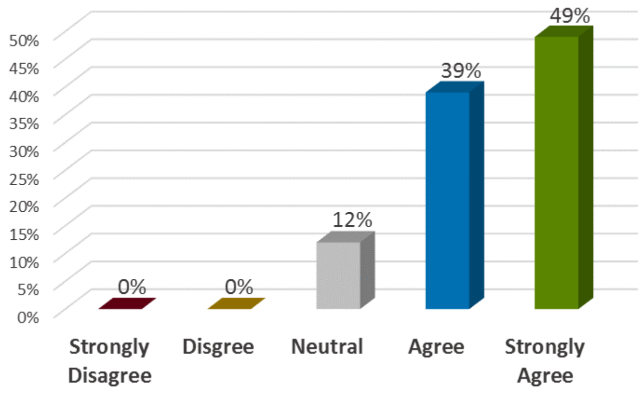
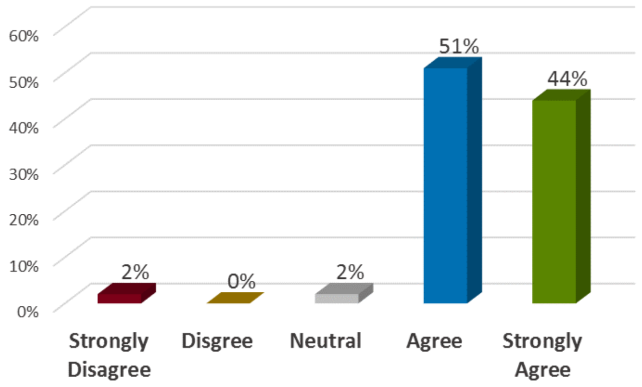
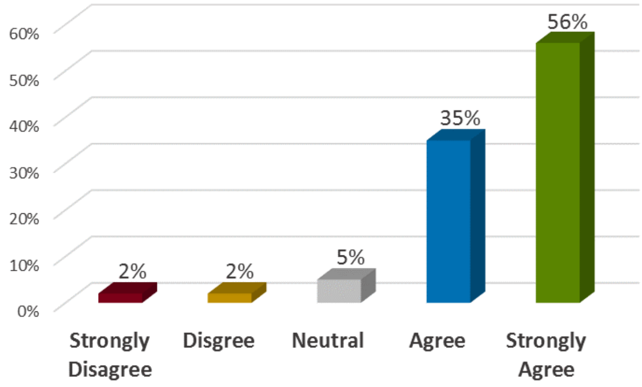
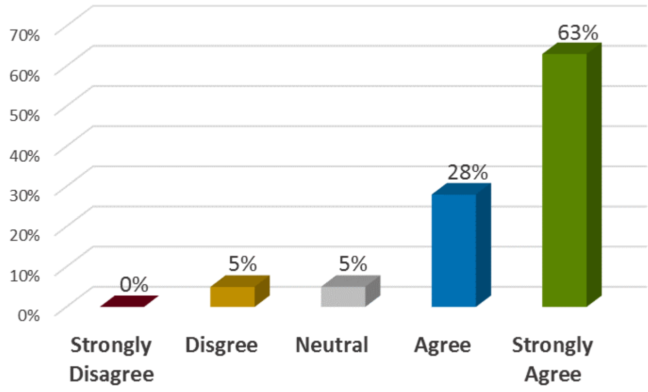
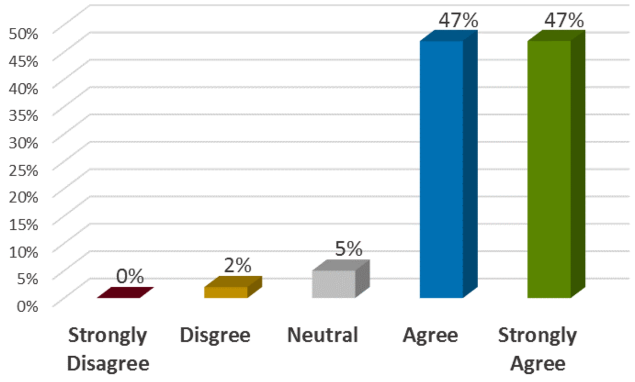
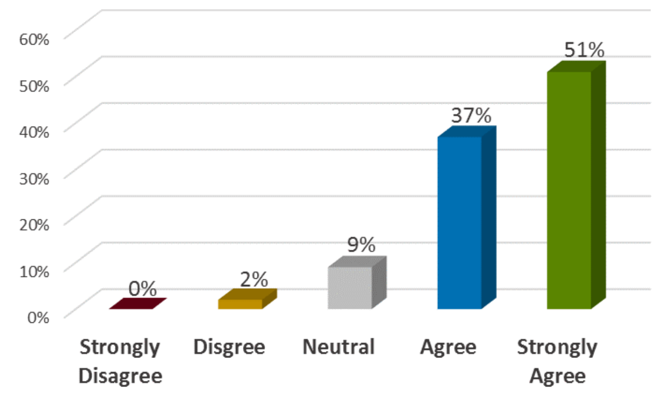
| Statement | Distribution |
|---|---|
| The duration of each presentation was appropriate |  |
| The seminars/workshops increased my understanding of available resources to respond to and recover from a cyber-attack |  |
| The presentations helped me gain a better understanding of the response and recovery actions my institution should implement when considering the threat of cyber-attack |  |
| The presentations helped me gain a better understanding of the response and recovery actions my institution should implement when considering the threat of a failure in campus infrastructure |  |

*Table 7: Exercise Assessment Feedback*

| Statement | Distribution |
|---|---|
| Pre-exercise information and documentation were easy to understand and helped me prepare for exercise discussions |  |
| The exercise scenario was realistic |  |
| The exercise lasted for an appropriate length of time |  |

| Statement | Distribution |
|---|---|
| The exercise facilitator and moderators engaged participants and helped guide meaningful discussions |  |
| The use of handheld polling devices enhanced participant involvement in the exercise |  |
| Exercise discussion topics were relevant to my institution |  |

| Statement | Distribution |
|---|---|
| Exercise discussion topics encouraged someone with my level of training and experience to participate |  |
| The exercise increased my understanding of my institution's risk and vulnerabilities when considering the threat of a cyber-attack |  |
| The exercise increased my understanding of my institution's risks and vulnerabilities when considering the threat of a failure in campus infrastructure |  |
| The exercise helped me gain a better understanding of the response and recovery actions my institution should implement when considering the threat of a cyber-attack |  |

| Statement | Distribution |
|---|---|
| The exercise helped me gain better understanding of the response and recovery actions my institution should implement when considering the threat of a failure in campus infrastructure |  |

# Appendix C: Academic Resource Guide

This section provides a list of resources for preparedness, response, and recovery for a failure in campus infrastructure caused by a cyber-attack.

Any additional requests for information should be directed to DHS / OAE at: AcademicEngagement@hq.dhs.gov.

## Campus Resilience Resources

### Emergency Preparedness Resources

**Continuity Resource Toolkit**. The Continuity Resource Toolkit provides examples, tools, and templates for establishing and implementing a continuity strategies based on the FEMA Continuity Guidance Circular (CGC). To view the Toolkit, visit: www.fema.gov/continuity-resource-toolkit. For more information on the FEMA Continuity Guidance Circular, visit: CGC: www.fema.gov/continuity-guidance-circular

**Department of Education, Response and Emergency Management for Schools (REMS) Technical Assistance Center**. The REMS TA Center, administered by the U.S. Department of Education, Office of Safe and Healthy Students (OSHS), supports public and private schools, school districts, and institutions of higher education, with their community partners, in building their preparedness capacity (including mitigation, prevention, protection, response and recovery efforts) and creating comprehensive emergency operations plans that address a variety of security, safety, and emergency management issues. For more information, visit: https://rems.ed.gov/

**FEMA National Continuity Programs (NCP) Office**. FEMA, NCP is an element of the FEMA Administrator’s Office which supports the continuity planning and preparedness efforts of both government and non-government stakeholders in order to sustain the continuous performance of National Essential Functions under all conditions. For more information, visit: http://www.fema.gov/continuity-operations/

**FEMA Emergency Management Institute (EMI) Independent Study Program**. Virtual training on a multitude of emergency preparedness and continuity resilience strategies is available through the FEMA, EMI, Independent Study Program. For more information and a list of courses, visit: http://training.fema.gov/IS/

**FEMA Monthly Continuity Webinar Series**. The Series covers a variety of continuity topics from a diverse cadre of speakers. For more information, visit: http://www.fema.gov/continuity-webinar-series/

**Community Emergency Response Team (CERT) Programs**. The CERT programs focus on disaster preparedness and training in basic disaster response skills such as fire safety, light search and rescue, team organization, and disaster medical operations. Using the training learned in the classroom and during exercises, CERT members can assist others in their neighborhood or workplace following an event when professional responders are not immediately available to help. CERT members also are encouraged to support emergency response agencies by taking a more active role in emergency preparedness projects in their communities. For more information, visit: https://www.fema.gov/community-emergency-response-teams.

**Incident Command System (ICS) Resource Center**. The FEMA ICS Resource Center website has a multitude of ICS reference documents including, but not limited to, ICS Forms, checklists, training course information and links to other related resources. For more information, visit: https://training.fema.gov/emiweb/is/icsresource/

## Cybersecurity Resources

**Critical Infrastructure Cyber Community (C3) Voluntary Program.** As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) launched the Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. The C³ Voluntary Program helps sectors and organizations that want to use the Framework by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector. For more information, visit: https://www.us-cert.gov/ccubedvp/academia

**Cyber Resilience Review (CRR).** The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The review assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity and others. For more information, visit: http://www.us-cert.gov/ccubedvp/self-service-crr

**Cyber Security Advisors (CSAs).** CSAs are regional located DHS personnel who direct coordination, outreach, and regional support to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's critical infrastructure and state, local, tribal, and territorial governments. CSAs offer immediate and sustained assistance to prepare and protect state, local, tribal, and territorial governments and private entities. For more information, visit: http://www.us-cert.gov/ccubedvp/getting-started-academia

**Cybersecurity Evaluation Tool (CSET®).** The Cyber Security Evaluation Tool (CSET®) is a DHS product that assists organizations in protecting their key national cyber assets. It was developed by cybersecurity experts under the direction of the DHS Industrial Control Systems Cyber Emergency Response Team. The tool provides users with a systematic and repeatable approach to assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. For more information, visit: http://ics-cert.us-cert.gov/assessments

**Cybersecurity Preparedness.** Cybersecurity involves preventing, detecting, and responding to cyber incidents that can have wide ranging effects on the individual, organizations, the community and at the national level. For more information, visit: https://www.ready.gov/cybersecurity

**DHS Cybersecurity Publications**. A ready-reference collection of documents published by DHS cybersecurity programs that can help private and public organizations with everything from setting up your first computer to understanding the nuances of emerging threats. For more information, visit: https://www.us-cert.gov/security-publications

**Higher Education Cloud Vendor Assessment Tool**. The Higher Education Cloud Vendor Assessment Tool attempts to generalize higher education information security and data protection questions and issues regarding cloud services for consistency and ease of use. The matrix: 1)

Helps higher education institutions ensure that cloud services are appropriately assessed for security and privacy needs, including some that are unique to higher education; 2) Allows a consistent, easily-adopted methodology for campuses wishing to reduce costs through cloud services without increasing risks; and 3) Reduces the burden that cloud service providers face in responding to requests for security assessments from higher education institutions. For more information, visit: https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

**Mutually Agreed Norms for Routing Security (MANRS)**. The Routing Resilience Manifesto initiative, underpinned by the "Mutually Agreed Norms for Routing Security (MANRS)" document that includes a set of actionable recommendations, aims at supporting this goal. For more information, visit: https://www.routingmanifesto.org/

**National Center of Academic Excellence in Cyber Defense.** The National Security Agency (NSA) and DHS jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise for the Nation. For more information, visit: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

**National Cyber Exercise & Planning Program (NCEPP).** The National Cybersecurity and Communications Integration Center's (NCCIC) National Cyber Exercise and Planning Program (NCEPP) develops and supports integrated cyber-focused exercises and guidance for federal departments and agencies, state, local, tribal, and territorial (SLTT) governments, critical infrastructure sectors, international partners, and special events. NCEPP offers end-to-end cyber exercise planning and conduct services at no cost on an as-needed and as-available basis. For more information, email cep@hq.dhs.gov.

**National Cybersecurity & Communications Integration Center (NCCIC).** The NCCIC is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government intelligence community, and law enforcement. For more information, visit: https://www.dhs.gov/about-national-cybersecurity-communications-integration-center

**Stay Safe Online**. A community-focused and partnership-based cybersecurity resource, with security practices, tips, and resources ready-made for use and implementation by individual users, business and industry, and academia. Sponsored by the National Cyber Security Alliance and promoted by DHS as a one-stop informational source for cybersecurity. For more information, visit: https://staysafeonline.org/

**Stop.Think.Connect. Academic Alliance.** Opportunities with technology and the Internet appear to have no limit. Academia is often at the forefront of expanding our ever-evolving cyber universe. As new ground is forged and benefits of a digitally connected world are enhanced, academia has an opportunity to lead by example in ensuring that online practices of students, faculty, staff, alumni, and the community are as secure as possible. The Stop.Think.Connect. Academic Alliance is a nationwide network of nonprofit colleges and universities committed to promoting safe online practices. For more information, visit: http://www.dhs.gov/stopthinkconnect-academic-alliance

## Protecting Critical Infrastructure

**Industrial Control System Cyber Emergency Response Team's (ICS-CERT) Year in Review FY 16**. The ICS-CERT works to reduce risks within and across all critical infrastructure sectors (https://www.dhs.gov/critical-infrastructure-sectors) by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. View the report: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2016_Final_S508C.pdf

**Industrial Control Systems Cyber Emergency Response Team Web Page**. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. For more information, visit: https://ics-cert.us-cert.gov/

**Protective Security Advisor (PSA) Program**. DHS provides local critical infrastructure protection support and guidance for academic institutions through the PSA Program. PSAs serve as local DHS representatives for security officers at schools and IHEs, and coordinate requests for training and grants. PSAs also conduct specialized security assessments of school facilities that assist schools in identifying potential security vulnerabilities and risks. For more information, visit: http://www.dhs.gov/protective-security-advisors.

**Science and Technology Directorate's (S&T) First Responder Communities of Practice**. The S&T First Responder Communities of Practice is a professional networking, collaboration, and communication platform created by DHS's S&T to support improved collaboration and information sharing amongst the nation's First Responders and other federal, state, local, tribal and territorial governments and private sector stakeholders supporting homeland security efforts. This vetted community of members focuses on emergency preparedness, response, recovery and other homeland security issues. For more information, visit: https://communities.firstresponder.gov/web/guest;jsessionid=D50CF79D14F5037D431C59C039D56172.w4.

**Student Tools for Emergency Planning (STEP)**. The STEP Program was designed by teachers and is sponsored by a state's Emergency Management Agency and FEMA. The program provides students and their families with concrete strategies to prepare for and deal with various emergencies. For more information, visit: http://www.fema.gov/student-tools-emergency-planning-step.

**United States Computer Emergency Readiness Team (US-CERT)**. US-CERT provides publications, alerts and tips, and resources about cybersecurity and cyber threats. For more information, visit: http://www.us-cert.gov/.

## Exercise & Training Resources

**G0367 Emergency Planning for Campus Executives**. This 2-hour overview of emergency planning serves as a briefing for executives of institutions of higher education. It provides them with insights into multi-hazard emergency planning and their role in protecting lives, property, and operations. For more information, visit: https://training.fema.gov/hiedu/aemrc/eplanning/g367.aspx

**IS-100.HE Introduction to the Incident Command System for Higher Education**. This FEMA training course introduces the Incident Command System (ICS) and provides the foundation for higher level ICS training. This course describes the history, features and principles, and organizational structure of ICS. It also explains the relationship between ICS and the National Incident Management System (NIMS). This course uses the same objectives and content as other ICS courses with higher education examples and exercises. For more information, visit: https://training.fema.gov/is/courseoverview.aspx?code=IS-100.HE

**L0363 Multi-Hazard Emergency Management for Higher Education**. This FEMA training course is designed to provide institutions of higher education with knowledge and planning strategies to better protect lives, property, and operations more effectively and efficiently within the context of comprehensive emergency management. For more information, visit: https://training.fema.gov/hiedu/aemrc/eplanning/l363.aspx

**Tabletop and Emergency Planning Exercises**. FEMA offers free, downloadable tabletop and emergency planning exercises and presentations for the private sector, including academic institutions. The exercises are designed to help organizations such as IHEs test emergency situations, such as a natural or man-made disaster, evaluate the ability to coordinate, and test readiness to respond. For more information, visit: http://www.fema.gov/emergency-planning-exercises.

## Resilience Planning Resources

**Academia and Resilience Web Page**. FEMA's Academia and Resilience web page provides tools, resources, program guides, and training information for campus emergency managers, faculty, and students. For more information, visit: http://www.fema.gov/academia-resilience.

**Building A Disaster-Resistant University**. *Building A Disaster-Resistant University* is a how-to guide and distillation of the experiences of six universities and colleges that have been working to become disaster-resistant. The guide provides basic information designed for institutions just getting started, as well as ideas, suggestions, and practical experiences for institutions that have already begun to take steps to becoming more disaster-resistant. For more information, visit: http://www.fema.gov/media-library/assets/documents/2288.

**DHS Campus Resilience Program.** The DHS Campus Resilience Program was created upon a recommendation from the Homeland Security Academic Advisory Council (HSAAC). DHS is currently in the developmental stages of the Campus Resilience Program. This initiative builds upon best practices, lessons learned and resources already developed to make U.S. colleges and universities more resilient. For more information on the DHS Campus Resilience Program, visit https://www.dhs.gov/campus-resilience or contact the Office of Academic Engagement at AcademicEngagement@hq.dhs.gov.

**Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education**. This guide provides guidance to IHEs on best practices for taking preventative and protective measures to stop an emergency from occurring or reduce the impact of an incident. The guide aligns and builds upon years of emergency planning work by the Federal Government and is a joint product of DHS, the DOJ, the DOE, and the Department of Health and Human Services (HHS). IHEs can use the guide to create and/or revise existing emergency operations plans. For more information, visit: http://www.fema.gov/media-library-data/20130726-1922-25045-3638/rems_ihe_guide.pdf.

**National Tabletop Exercise for Institutions of Higher Education Series**. Sponsored by FEMA and OAE, this series of national tabletop exercises was designed in collaboration with academia and interagency planners to test and enhance campus resilience. The tabletop exercise promotes the all-hazard *Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education* and provides insight into common planning, preparedness, and resilience best practices and challenges of the academic community when faced with a disruptive campus event. For more information, visit: http://www.dhs.gov/nttx.

## Law Enforcement Resources

**DHS State and Local Law Enforcement Resource Catalog**. The DHS State and Local Law Enforcement Catalog highlights DHS resources available to state, local, tribal, and territorial law enforcement. The guide provides summaries of, and links to, training, publications, guidance, alerts, newsletters, programs, and services available to non-Federal law enforcement from across DHS. For more information, visit: http://dhs.gov/publication/dhs-state-and-local-law-enforcement-resource-catalog.

**Law Enforcement Conferences, Gatherings, and Meetings**. The Office for State and Local Law Enforcement maintains a comprehensive list of law enforcement conferences, gatherings, and meetings across the country. These events provide campus law enforcement professionals training opportunities and the ability to share best practices with other members of the law enforcement community. For more information, visit: https://www.dhs.gov/office-state-and-local-law-enforcement.

**Research on Threat Assessments and Various Types of Targeted Violence on Campuses**. The United States Secret Service (USSS) provides research and reports on violence at schools and IHEs. Released in April 2010, "Campus Attacks: Targeted Violence Affecting Institutions of Higher Education" contains information useful for campus safety professionals charged with identifying, assessing, and managing violence risk at institutions of higher education. Additionally, the Safe School Initiative, a study of attacks on K-12 schools, was released in 2002. For more information, visit: https://www2.ed.gov/admins/lead/safety/campus-attacks.pdf.

**DHS Office of Emergency Communications**. The Department of Homeland Security (DHS) Office of Emergency Communications (OEC) supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient. OEC provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial and industry partners develop their emergency communications capabilities. OEC's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide. For more information, visit: https://www.dhs.gov/office-emergency-communications

# Appendix D: Event Participants

## Institutions of Higher Education

- American Preparatory Academy
- Arizona State University-Tempe
- Auburn University
- Boston University
- Brigham Young University-Provo
- California State University-Los Angeles
- California State University-Northridge
- Chapman University
- Clark Atlanta University
- College of Charleston
- Collin County Community College District
- Columbia College-Sonora
- Cornell University
- Dakota State University
- Dixie State University
- Fashion Institute of Technology
- Florida Agricultural and Mechanical University
- Florida Atlantic University
- George Washington University
- Grand Valley State University
- Hamilton College
- Howard University
- Iliff School of Theology
- Indiana University-Purdue University-Fort Wayne
- Iowa State University
- Johnson C Smith University
- Los Angeles Community College District
- Louisiana State University and Agricultural & Mechanical College
- Massachusetts Institute of Technology
- Metropolitan Community College-Kansas City
- Mississippi State University
- Modesto Junior College
- Neosho County Community College
- Nicholls State University
- North Carolina State University at Raleigh
- North Central Missouri College
- Northeastern Illinois University
- Northern Arizona University
- Oklahoma State Regents for Higher Education
- Pace University-New York
- Pennsylvania State University-Main Campus
- Pima Community College
- Pomona College
- Portland State University
- Princeton University
- Reed College
- Rice University
- Rochester Institute of Technology
- Saint Joseph's University
- Salt Lake Community College
- Smith College
- Snow College
- South Texas College
- Southern Adventist University
- Southern Connecticut State University
- Southern Virginia University

| | |
|---|---|
| Stanford University | SUNY at Albany |
| SUNY at Binghamton | Syracuse University |
| Tennessee State University | Texas A & M University-College Station |
| Texas Christian University | The University of Tennessee-Knoxville |
| The University of Texas Health Science Center at Houston | Trocaire College |
| University at Buffalo | University of Alabama at Birmingham |
| University of Alaska Anchorage | University of Alaska Fairbanks |
| University of Alaska Southeast | University of Arizona |
| University of Denver | University of Georgia |
| University of Houston | University of Idaho |
| University of Kansas | University of Kentucky |
| University of Maryland-College Park | University of Massachusetts-Amherst |
| University of Nevada-Reno | University of New England |
| University of North Dakota | University of Northern Iowa |
| University of Oklahoma-Norman Campus | University of St Thomas |
| University of Utah | University of Virginia-Main Campus |
| University of Washington-Seattle Campus | University of Wisconsin-Madison |
| Utah State University | Utah Valley University |
| Washtenaw Community College | Weber State University |
| Western Governors University | Wisconsin Lutheran College |
| Yavapai College | Yosemite Community College District |

## Organizations and Associations (Observers)

| | |
|---|---|
| David Suzuki Foundation | Field Innovation Team |
| Intermedix Corporation | International Association of Campus Law Enforcement Administrators (IACLEA) |
| Internet2 | National Center for Campus Public Safety (NCCPS) |
| Western Interstate Commission for Higher Education (WICHE) | Research & Education Networking Information Sharing and Analysis Center -- Indiana University Bloomington |
| University of Akron Main Campus | University of Nebraska at Omaha |

## Government Partners (Observers)

- DHS Federal Emergency Management Agency
- DHS National Cybersecurity & Communications Center (NCCIC) National Cyber Exercise & Planning Program (NCEPP)
- DHS National Protection & Programs Directorate (NPPD) Office of Infrastructure Protection (OIP) Protective Security Coordination Division (PSCD)
- DHS Office of Academic Engagement
- DHS Office of Intelligence & Analysis (I&A) Field Operations Division (FOD)
- Exercise Support Team
- Federal Emergency Management Agency (FEMA) National Exercise Division (NED)
- FEMA Region VII (CTR)
- State of Utah - Department of Public Safety
- State of Utah - Division of Emergency Management
- United States Secret Service (USSS)
- DHS Federal Emergency Management Agency (FEMA) National Training and Education Division (NTED)
- DHS NPPD
- DHS Immigration & Customs Enforcement (ICE) Student & Exchange Visitor Program (SEVP)
- DHS National Protection & Programs Directorate (NPPD) Office of Cyber and Infrastructure Analysis (OCIA)
- DHS Office of Academic Engagement (OAE) Support Team
- DHS United States Secret Service
- Federal Bureau of Investigation (FBI)
- Federal Emergency Management Agency (FEMA) Region II
- Naval Postgraduate School (NPS) Center for Homeland Defense & Security (CHDS)
- State of Utah - Department of Public Safety - Statewide Information and Analysis Center
- State of Utah, Department of Public Safety
- Utah DPS Statewide Information & Analysis Center

# APPENDIX E: ACRONYMS

| | |
|---|---|
| APT | Advanced Persistent Threat |
| CAE-CD | National Centers of Academic Excellence in Cyber Defense |
| CERT | Community Emergency Response Team |
| CHDS | Center for Homeland Defense & Security |
| COOP | Continuity of Operations |
| CR | Campus Resilience |
| CRR | Cyber Resilience Review |
| CSA | Cyber Security Advisor |
| CSET | Cybersecurity Evaluation Tool |
| DHS | Department of Homeland Security |
| DOE | Department of Education |
| DOJ | Department of Justice |
| DOS | Department of State |
| EOC | Emergency Operating Center |
| EMI | Emergency Management Institute |
| FBI | Federal Bureau of Investigation |
| FEMA | Federal Emergency Management Agency |
| FOD | Field Operations Division |
| HHS | Department of Health and Human Services |
| HSAAC | Homeland Security Academic Advisory Council |
| HVAC | Heating, Ventilation, and Air Conditioning |
| I&A | Intelligence & Analysis |
| ICE | Immigration and Customs Enforcement |
| ICPD | Individual and Community Preparedness Division |
| ICS | Incident Command System |
| IHE | Institution of Higher Education |
| NCCIC | National Cybersecurity & Communications Integration Center |
| NCEPP | National Cyber Exercise & Planning Program |
| NED | National Exercise Division |
| NICE | National Initiative for Cybersecurity Education |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| NPD | National Preparedness Directorate |
| NPPD | National Protection & Programs Directorate |
| NPS | Naval Postgraduate School |
| NSA | National Security Agency |
| NTED | National Training and Education Division |
| NTTX | National Seminar and Tabletop Exercise |
| OAE | Office of Academic Engagement |
| OCIA | Office of Cyber and Infrastructure Analysis |
| OIP | Office of Infrastructure Protection |
| PIO | Public Information Officer |
| PSA | Protective Security Advisor |
| PSCD | Protective Security Coordination Division |
| SEVP | Student and Exchange Visitor Program |
| SME | Subject-Matter Expert |
| S&T | Science and Technology Directorate |
| STEP | Student Tools for Emergency Planning |
| TTX | Tabletop Exercise |
| US-CERT | United States Computer Emergency Readiness Team |
| USSS | United States Secret Service |