


Leadership Tabletop Exercise (LTTX)

Cybersecurity Overview and Resource Guide

April 2018

TABLE OF CONTENTS

CONTENTS

INTRODUCTION

OVERVIEW

LTTX Description

Sponsored by the Department of Homeland Security's (DHS) Office of Academic Engagement and the Federal Emergency Management Agency's (FEMA) National Exercise Program (NEP), the **Leadership Tabletop Exercise (LTTX)** is a half-day event for campus leadership designed to highlight their role in managing institutional risk during emergency incidents. These executive events bring together campus leadership, local, state, and federal officials, and industry subject matter experts to simulate emergencies through tailored case studies on a range of threats.

Purpose & Organization of Report

This ***Leadership Tabletop Exercise Cybersecurity Overview and Resource Guide*** provides members of the academic community with a summary of the format and structure of the pilot LTTX event, hosted by the North Dakota University System, as a model for initiating critical conversations with campus leadership on their roles in preparedness for, response to, and recovery from campus emergencies. To accompany this overview, the Resource Guide includes a list of useful resources for promoting cybersecurity preparedness.

This report is intended for two purposes:

1) To provide an overview of the pilot LTTX to discuss the event as a model for leadership-focused events; and
2) Provide a list of key Federal resources within the focus area.

A description of the pilot event appears in the Event Overview section. While the focus of the pilot event was on cybersecurity, the LTTX is built to be adaptable to any threats or hazards that a host institution or system would like to explore.

BACKGROUND

The **Campus Resilience Program (CR Program)**, launched by DHS in 2013, was created to enhance the ability of IHEs to anticipate the unforeseen, withstand disruptions, manage crises, and seize opportunity amidst increasingly turbulent times. The program improves the resilience of IHEs by facilitating collaboration with other institutions and academic professionals interested in resilience; drawing on existing resources from Federal, state, tribal and territorial stakeholders; and providing access to tools and resources that strengthen their campuses through innovative resilience-building practices. The **CR Program** offers a number of other resources, including:

- The **Campus Resilience Program Tabletop Exercise Series (TTX Series)**: The TTX Series is a collection of tailored events, each with unique objectives and outcomes, designed for the higher education community. Each event in the series challenges participants with multi-faceted threat-based scenarios that test and strengthen their institution's preparedness, response, and recovery capabilities. The other events within the **TTX Series** are:
    - **The National Seminar and Tabletop Exercise Series for Institutions of Higher Education (NTTX)**: The NTTX is an annual event to test and promote campus resilience and emergency preparedness. The NTTX brings together senior higher education leaders, as well as Federal, state and local representatives from departments and agencies that support campus resilience to participate in seminars and work through a designed emergency scenario. For more information on the NTTX, including the 2018 event, visit: https://www.dhs.gov/nttx.

- **Regional Tabletop Exercises (RTTX)**: The RTTXs are one-day events that include a tabletop exercise designed to address specific regional threats. The regional events are hosted multiple times per year in locations across the U.S. For more information on the RTTX, including past and upcoming events in 2018, visit: https://www.dhs.gov/rttx.

- **The CR Program Resource Library**: The CR Program Resource Library organizes resources according to threat or hazard, and then further categorizes each resource according to its relevant mission area (*Preparedness, Response, Recovery*), as outlined in the Federal Emergency Management Agency's (FEMA) National Preparedness Goal. The resources included reflect the collaborative efforts of many program and partner organizations, and represent a variety of Federal, state, local, private-sector, emergency management, and academic association entities. For more information and to access the library, visit https://www.dhs.gov/campus-resilience-program-resource-library.

- **General information** on the CR Program, including upcoming events, available resources, and opportunities for engagement, is accessible at: https://www.dhs.gov/academicresilience.

OAE invites the higher education community and other stakeholders to receive updates on campus resilience and other issues in academic engagement at DHS by signing up for our email announcements. To subscribe, visit the Academic Engagement GovDelivery page and submit your email address.

EVENT OVERVIEW

The **2018 North Dakota University System Leadership Tabletop Exercise** took place on February 7, 2018, and was hosted by the National Energy Center of Excellence at Bismarck State College in Bismarck, North Dakota. The event brought together the presidents and senior level staff of 11 colleges and universities from across the state of North Dakota as well as five tribal colleges from the state. More than 75 individuals representing the emergency management, cybersecurity, tribal colleges and operational leadership of each institution in the System attended. Participants also included representatives from federal, state, and local departments and agencies that support campus resilience. The event focused on **cybersecurity threats** to higher education.

Pilot Objectives

This four-hour event focused on cybersecurity resilience and provided an opportunity for all participants to receive and share information technology (IT)-related information while also identifying IT risks, vulnerabilities, and best practices. ***Table 1: 2018 LTTX Objectives and Core Capabilities*** below outlines the overall objectives for the event. Each objective is linked to core capabilities, which are distinct critical elements necessary to achieve the associated objective and mission area.

Table 1: 2018 LTTX Objectives and Core Capabilities

Exercise Objective	Core Capability
1. Advance the understanding of the role of institution leadership in campus resilience	▪ Public Information and Warning ▪ Cybersecurity ▪ Intelligence and Information Sharing ▪ Community Resilience ▪ Long-term Vulnerability Reduction ▪ Environmental Response/Health and Safety ▪ Economic Recovery

Exercise Objective	Core Capability
2. Provide actionable approaches for institutional leadership to direct and bolster the resilience of their campus communities	▪ Public Information and Warning ▪ Cybersecurity ▪ Intelligence and Information Sharing ▪ Community Resilience ▪ Long-term Vulnerability Reduction ▪
3. Identify campus resilience vulnerabilities requiring attention from institutional leadership	▪ Cybersecurity ▪ Intelligence and Information Sharing ▪ Community Resilience ▪ Long-term Vulnerability Reduction

To achieve these objectives, the LTTX consisted of the following three (3) components:

- An unclassified **Cyber Threat Brief,** provided by the state Homeland Security Advisor, with higher education-specific context provided by an association subject matter expert from the Western Interstate Commission for Higher Education (WICHE) Cooperative for Educational Technologies (WCET), highlighting the current cyber threat landscape facing higher education in North Dakota;
- A **Tabletop Exercise (TTX),** facilitated by FEMA/NED, that focused on preparedness, response, and recovery efforts for two different types of cyber incidents; and
- An **Options for Consideration Briefing,** provided by the DHS/National Protection and Programs Directorate (NPPD) Cyber Security Advisor and Protective Security Advisor, summarized cybersecurity programs, offerings, and assessment opportunities available to the higher education community.

Pilot Format

The exercise portion of the event featured a two-hour TTX that examined two different cyber incidents based on real-world case studies. The TTX consisted of the following activities:

- **Opening Discussion:** Introduced the exercise topic and set expectations across each institution and across the university system
- **Module 1:** Featured discussions on a cyber attack on university HVAC systems scenario
- **Module 2:** Featured discussions on a ransomware attack on IT systems scenario

During the Opening Discussion, participants were presented with a set of discussion questions to initiate conversations on campus resilience and cybersecurity. Modules 1 and 2 that followed reviewed the scenario and engaged participants in a facilitated discussion centered on predetermined questions. While participants were seated by institution, they were encouraged to engage other IHEs and organizations in discussions.

Pilot Participants

Convened by the NDUS Chancellor, the event brought together the presidents and senior level staff of 11 colleges and universities from across the state of North Dakota as well as five tribal colleges from the state.

Nearly 100 individuals representing the emergency management, cybersecurity, tribal colleges and operational leadership of each institution in the System attended. Participants also included representatives from federal, state, and local departments and agencies that support campus resilience. The event focused on cybersecurity threats to higher education. Participants included:

- **Players** – Players have an active role in discussing their response and recovery activities during the exercise. Delegations of players respond to the situation presented based on expert knowledge of response procedures, as well as how they would perform their functions on their respective campus or organization. For the pilot LTTX, Players included:

    - ***Presidents***: The presidents of each campus were the 'touchstone' for the event, with other players being responsible for reporting in to these individuals on how they would respond to the institutional risks from leadership's perspective during a cyber crisis.

    - ***Campus Liaisons***: Prior to the event, each campus president appointed one Campus Liaison to serve as the key point-of-contact with the Department. This individual's role included responding to pre- and post-event surveys from the DHS on the institution's resilience-building efforts as well as serving as the proxy for the president, requiring both a knowledge of cybersecurity on campus and direct access to the president. As such, these Campus Liaisons were typically the Chief Information Officers from each campus.

    - ***Senior Staff / Subject Matter Experts (SMEs)***: In addition to the principals and liaisons from each of the campuses, key institution SMEs were essential in building the institution's response to the scenario. These individuals typically represented the leadership from information technology and security, risk and emergency management, student and academic affairs, and facilities / campus operations from each campus.

- **Event and Support Staff** – The event and support staff guided exercise play and were responsible for ensuring that participant discussions remained focused on the event objectives. They also provided additional information and resolved questions as required, and performed administrative and logistical support tasks during the exercise. (e.g., registration, catering, etc.).

- **Observers** – Observers visited and viewed selected segments of the exercise but were not actively asked to respond to the scenario in reference to their organization. During this LTTX, observers interacted with exercise players to support the development of player responses to the situation by asking relevant questions or providing subject-matter expertise.

Pilot Results

As a result of the event, the System received a detailed report with a summary of the major findings, takeaways, and discussion points from the event, as well as resources linked to the specific challenges identified during the event. The format of the event-specific ***Summary of Conclusions*** is:

Examples of key findings:

- ***Example #1: Public Communication and Engagement***: Institutions identified that they have existing plans, procedures, and mechanisms in place for communicating with students, faculty, and staff during emergencies. To improve the efficiency of these communications, participants noted the benefits of developing more formal protocols and agreements with local news/media outlets as well as establishing backup communication channels.

- ***Example #2: External Stakeholder Coordination and Engagement***: To enhance existing emergency plans, policies, and procedures, institutions would benefit from increased coordination with other Federal, regional, state, local, private-sector, academic, and non-governmental organizations. These external stakeholders can bring to bear useful guidance and resources to support preparedness, response, and recovery efforts for both cyber and natural incidents.

- ***Example #3: Cyber Partnerships***: In addition to improving overall security preparedness, institutions identified the need to establish teaming or partnership agreements with both municipalities and third-party vendors dedicated to guiding response actions in the event of a cyber-attack on campus systems.

These key findings are related to the self-evaluation and discussion during the exercise itself, and thus, are different for every participant. **Actual key findings from each event are considered sensitive and are only released to the participants from the event itself** and not released to the public or broader higher education community. The Department does not formally track or regulate these findings, but rather, looks to deliver relevant resources and support to participants in the event based on those conversations. As stated previously, all discussions and any information captured in the ***Summary of Conclusions*** is not for attribution and does not identify any specific vulnerabilities at an institution.

RESOURCE GUIDE

This section provides a list of resources for preparedness, response, and recovery efforts related to a cyber incident, including information security, enterprise risk management, and cyber-physical infrastructure protection. Any additional requests for information should be directed to DHS/OAE at: AcademicEngagement@hq.dhs.gov.

CYBER INFRASTRUCTURE RESOURCES

Critical Physical Infrastructure Tools & Assessments

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/.

Infrastructure Protection Gateway – Rapid Survey Tool. The Rapid Survey Tool (RST) is a non-regulatory data collection capability that examines the most critical aspects of a facility's security and resilience posture with efficient, baseline questions. It is a shorter survey that allows assessors to gather the general status of a facility before deciding whether an in-depth survey is required. The Web-based Rapid Survey Tool, available through the Infrastructure Protection Gateway (IP Gateway), captures a facility's physical and operational security and resilience data. The data is then analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities. The resulting analysis is used to develop a Rapid Survey Information Center that equips owners and operators with knowledge to detect and prevent physical, cyber, and natural threats and respond to, recover from, and remain resilient against all hazards. For more information, contact the IP Gateway Help Desk at IPGateway@hq.dhs.gov or 1-866-844-8163.

Protected Critical Infrastructure Information Program. The Protected Critical Infrastructure Information (PCII) program protects infrastructure information voluntarily shared with DHS to be used for homeland security purposes. The PCII program was created by Congress in the Critical Infrastructure Information Act of 2002, ensuring that PCII in the government's hands is protected from disclosure. PCII is used by DHS and other government homeland security professionals to identify vulnerabilities, mitigation strategies, and protective measures. DHS works closely with critical infrastructure asset owners and operators to provide a wide array of services and products to help them protect the Nation's critical infrastructure, and PCII is a key component in these efforts. PCII also allows DHS to collect and protect sensitive security critical infrastructure information, cyber-attack, risk, and vulnerability information to protect the nation's infrastructure. PCII protections allow access to a vast amount of critical information necessary to detect, deter, and defend against threats to the nation. For more information, contact the IP Gateway Help Desk at IPGateway@hq.dhs.gov or 1-866-844-8163.

CYBERSECURITY RESOURCES

Cybersecurity Tools & Assessments

Cyber Infrastructure Survey. The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. CIS provides an assessment of the organization's cybersecurity practices in place for a critical service. For more information, or to schedule a CIS, contact cyberadvisor@hq.dhs.gov.

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.

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 computers to understanding the nuances of emerging threats. For more information, visit: https://www.us-cert.gov/security-publications.

External Dependencies Management Assessment. The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization's management of their dependencies. Through the EDM assessment, organizations can learn how to manage risks arising from external dependencies within the information and communication technology (ICT) supply chain. The ICT supply chain consists of outside parties that operate, provide, or support ICT. For more information, or to schedule an EDM Assessment, contact cyberadvisor@hq.dhs.gov.

FEMA 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.

Department of Education / FFIEC Cybersecurity Assessment Tool. In light of the increasing volume and sophistication of cyber threats, the Federal Financial Institutions Examination Council1 (FFIEC) developed the Cybersecurity Assessment Tool (Assessment), on behalf of its members, to help institutions identify their risks and determine their cybersecurity maturity. The content of the assessment is consistent with the principles of the FFIEC Information Technology Examination Handbook (IT Handbook) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as industry accepted cybersecurity practices. The Assessment provides institutions with a repeatable and measurable process to inform management of their institution's risks and cybersecurity preparedness. For more information, visit: https://ifap.ed.gov/eannouncements/attachments/FFIEC_CAT_form.pdf.

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 aimed at supporting this goal. For more information, visit: https://www.routingmanifesto.org/.

Phishing Campaign Assessment. The Phishing Campaign Assessment (PCA) is a no-cost, six-week engagement offered to Federal, State, Local, Tribal and Territorial (SLTT) Governments, as well as Critical Infrastructure and Private Sector Companies, that evaluates an organization's susceptibility and reaction to phishing emails. The results of a PCA are meant to provide guidance, measure effectiveness, and justify resources needed to defend against spear-phishing and increase user training and awareness. For more information, contact nccicustomerservice@hq.dhs.gov.

Risk and Vulnerability Assessment. A Risk and Vulnerability Assessment (RVA) is a no-cost offering that combines national threat and vulnerability information with data collected and discovered through onsite assessment activities to provide customers with actionable remediation recommendations prioritized by risk. Engagements are designed to determine whether and by what methods an adversary can defeat network security controls. Components of the assessment include scenario-based network penetration testing, web application testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an organizations detection and response capabilities. For more information, or to schedule an RVA, contact nccicustomerservice@hq.dhs.gov.

Validated Architecture Design Review. The Validated Architecture Design Review (VADR) is a voluntary, no-cost assessment based on standards, guidelines, and best practices. The assessment encompasses architecture and design review, system configuration, log file review, and sophisticated analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices and, most importantly, to identify anomalous (and potentially suspicious) communication flows. For more information, contact nccicustomerservice@hq.dhs.gov.

Vulnerability Scanning. DHS offers Vulnerability scanning (formerly known as Cyber Hygiene scanning) of i-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities, which decreases stakeholder risk while increasing the nation's overall resiliency. For more information, contact nccicustomerservice@hq.dhs.gov.

Cybersecurity Resources & Awareness

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.

Information Products: National Cyber Awareness System. NCCIC offers no-cost, subscription-based information products to stakeholders through the www.us-cert.gov and www.ics-cert.gov websites. NCCIC designed these products — part of the National Cyber Awareness System (NCAS) — to improve situational awareness among technical and non-technical audiences by providing timely information about cybersecurity threats and issues and general security topics. Products include technical alerts, control systems advisories and reports, weekly vulnerability bulletins, and tips on cyber hygiene best practices. Subscribers can select to be notified when products of their choosing are published. For more information on available products, visit https://www.us-cert.gov/ncas and https://ics-cert.us-cert.gov/, and to subscribe to select products, visit https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.

National Initiative for Cybersecurity Careers and Studies. DHS developed the National Initiative for Cybersecurity Careers and Studies (NICCS) in close partnership with NIST, the Office of the Director of National Intelligence, the Department of Defense, and other government agencies, to leverage efforts of government, industry, and academia to provide a comprehensive, single resource to address the nation's cybersecurity knowledge needs. NICCS is an online resource for cybersecurity training that connects government employees, students, educators, and industry with cybersecurity training providers throughout the nation. For more information, visit https://niccs.us-cert.gov/ or contact NICCS@hq.dhs.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.

Information Sharing & Threat Analysis

Automated Indicator Sharing. Automated Indicator Sharing (AIS) enables the exchange of cyber threat indicators between the federal government, SLTT governments, and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses or the sender's address of a phishing email. AIS is part of a DHS effort to create a cyber ecosystem where as soon as a stakeholder observes an attempted compromise, the cyber threat indicator of compromise (IOC) is shared in real time with all partners, protecting everyone from that particular threat. For more information, or to sign up to participate in AIS, visit https://www.us-cert.gov/ais.

Homeland Security Information Network. The Homeland Security Information Network (HSIN) is a trusted network for homeland security mission operations to share sensitive but unclassified information. Federal, SLTT, and private sector partners can use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to perform their duties. NCCIC-developed products — such as TLP: GREEN and TLP: AMBER indicator bulletins and analysis reports — are available to registered stakeholders in authorized communities of interest.

For information on applying for a HSIN account, contact HSIN at 866-430-0162 or HSIN.HelpDesk@hq.dhs.gov. NCCIC TLP:WHITE products are available through www.us-cert.gov and www.ics-cert.gov.

Malware Analysis. The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining analysis results. Experts detail recommendations for malware removal and recovery activities. This service can be performed in conjunction with incident response services if required. To submit malware for analysis, visit https://www.malware.us-cert.gov. For further questions or requests, contact ncciccustomerservice@hq.dhs.gov.

General Resilience Resources

Emergency Preparedness Resources

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.

Continuity Resource Toolkit. The Continuity Resource Toolkit provides examples, tools, and templates for establishing and implementing 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 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/.

Incident Command System (ICS) Resource Center. The FEMA ICS Resource Center website has a multitude of ICS reference documents including ICS Forms, checklists, training course information and links to other related resources. For more information, visit: https://training.fema.gov/emiweb/is/icsresource/.

Exercise & Training Resources

Federal Virtual Training Environment. The Federal Virtual Training Environment (FedVTE) is a free, online, on-demand cybersecurity training system managed by DHS that is available to federal and SLTT government personnel, veterans, and federal government contractors. It contains more than 800 hours of training on topics such as ethical hacking, surveillance, risk management, and malware analysis. The department's efforts focus on building a strong cyber workforce that can keep up with evolving technology and increasing cybersecurity risks. DHS is coordinating its outreach about the program through the Multi-State Information Sharing and Analysis Center (MS-ISAC), the focal point for cyber threat prevention, protection, response, and recovery for the nation's SLTT governments. For more information, visit https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte. To register for an account and for more information on available courses, visit https://fedvte.usalearning.gov.

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 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.

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 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.

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.

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.

Federal Components & Offices

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.

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/.

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.

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.

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 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/.

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 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.

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 / territorial governments and private sector partners 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.

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/.

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.

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.

APPENDIX A: ACRONYMS

Acronyms	
CR Program	Campus Resilience Program
DHS	Department of Homeland Security
ED	Department of Education
FEMA	Federal Emergency Management Agency
HVAC	Heating, Ventilation, and Air Conditioning
IHE	Institution of Higher Education
IT	Information Technology
LTTX	Leadership Tabletop Exercise
NDSU	North Dakota State University
NDUS	North Dakota University System
NED	National Exercise Division
NPPD	National Protection and Programs Directorate
OAE	Office of Academic Engagement
TTX	Tabletop Exercise
UND	University of North Dakota
WCET	WICHE Cooperative for Educational Technologies
WICHE	Western Interstate Commission on Higher Education