

Center for Domestic Preparedness
11th Annual Tribal Nations Training Week
September 12 - 19, 2026

**STRENGTHENING INDIGINEOUS READINESS HONORING SOVEREIGNTY AND
ACHIEVING RESILIENCE THROUGH AN
ALL-HAZARDS APPROACH**

Cyber Preparedness Track

These training courses allow Tribal Nations to strengthen their cybersecurity posture and resilience against evolving cyber threats. Participants learn to identify and plan for cyber incidents, develop robust cyber preparedness programs, and enhance information sharing and situational awareness. Through hands-on simulations and practical exercises, Tribal communities gain skills to protect, detect, respond to, and recover from cyberattacks, including those targeting Internet of Things (IoT) devices. Training in critical thinking and risk management further supports effective assessment and mitigation of cyber risks, while integrating cyber hazard response into exercise planning ensures comprehensive preparedness for both organizational and community-level cyber challenges.

Preparing for Cyber Attacks and Incidents

Learn to identify and differentiate cyber threats, understand the importance of incident planning, and develop or revise cyber preparedness programs. Gain skills in information sharing, collaboration, and situational awareness, and discover resources to strengthen cyber resilience.

Community Cybersecurity Preparedness Simulation

Explore the dynamics of community cyber-attacks and select effective cybersecurity functions to boost organizational and community resilience. Develop strategies to identify, protect, detect, respond, and recover from cyberattacks, and create actionable plans for cybersecurity preparedness.

Practical Internet of Things Security

Understand IoT communication and data collection methods, analyze how threat actors target IoT devices, and learn practical techniques for defending IoT systems against cyber threats.

Critical Thinking and Risk Management in a Cyber-Converged World

Examine the principles of critical thinking in risk assessment, review common risk management models and terminology, and apply the FAIR Model to enhance your organization's risk management program.

Integrating Cyber Hazard Response into Exercise Planning

Learn to incorporate cyber hazard response into exercise planning by understanding IoT communication, data collection, threat actor tactics, and defense strategies for IoT systems.

You must have a FEMA SID to apply for a course.

To register for a FEMA SID number, go to: <https://cdp.dhs.gov/FEMASID>

select "Register for FEMA SID" or "Forgot FEMA SID."

If you encounter any issues, please contact the FEMA SID help desk at:

femasidhelp@cdpemail.dhs.gov

Registering for a FEMA SID number does not register you for a class, students must APPLY using the link or QR code below.

For training or course questions please contact:

RubyDawn Manning at: Office: (256)847-2649 | Mobile: (256)419-3985
RubyDawn.Manning@fema.dhs.gov

Amy Strautman at: Office: (256) 847-2693 | Mobile: (202)856-2057
Amy.Strautman@fema.dhs.gov

For cultural or Tribal-related questions please contact: Tribal Nations Planning Group at:

FEMA-tribalnationscdp@fema.dhs.gov

For any registration issues or questions:

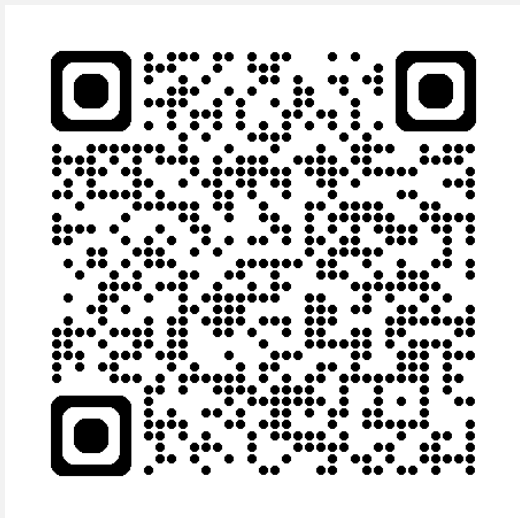
Zoie M. Butterworth at: (256) 847-2105
Zoie.Butterworth@cdpemail.dhs.gov

September 12 - 19, 2026 (Travel First and Last Days)



[Click Here to Apply](#)

QR Code to Apply to
CYBER Preparedness Track:



The Center for Domestic Preparedness
“Training the Best for the Worst.”