

# Cyber Resilience Workshop

## WAUSAU

**Tuesday, February 10th**  
**12:30 PM - 4:30 PM**

Jefferson Street Inn  
201 Jefferson Street  
Wausau, WI 54403

## MADISON

**Thursday, February 12th**  
**8:30 AM - 12:30 PM**

Holiday Inn at the American Center  
5109 W. Terrace Avenue  
Madison, WI 53718

The DHS Office of Cybersecurity & Communications (CS&C) Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division facilitates workshops to promote resilience and enhance cyber security capabilities within the 16 Critical Infrastructure and Key Resources (CIKR) Sectors, as well as State, Local, Tribal, and Territorial (SLTT) governments.

## Workshop Overview

Each workshop introduces cyber security stakeholders and practitioners to cyber resilience concepts and to capability and capability building activities in key performance areas related to cyber security, IT operations, and business continuity. Workshop content and tutorial activities reinforce both operational risk management and emergency, crisis management for critical cyber infrastructure. Executives and operations managers within critical infrastructure (public and private) sectors will leave with tangible, useful “take-away” information related to risk-based decision-making and security planning for critical IT services.

Participants will be engaged in structured activities, via scenarios, and introduced to concepts through direct discussion. Built-in activities, supported by guidelines and templates, help to examine capability building in operational resilience practices and well beyond discussions centered exclusively on IT security controls and countermeasures. Participants should also gain an awareness of modern cyber security threats and current trends in the context of protecting and sustaining IT services, and leave having built decision criteria for cyber incidents, vulnerabilities, and business continuity.

## Goals and Objectives

DHS Cyber Resilience Workshops convey current information on emerging cyber threats, federal initiatives affecting critical infrastructure protection, and realistic practices for improving operational resilience, keeping communities informed and maintaining a working partnership on matters of cyber security. In addition, workshops:

- » **Raise awareness** to gaps in cyber management practices and to process improvements for CIKR and SLTT communities.
- » **Reinforce cyber security best practices** and examine resilience concepts and objectives.
- » **Discuss processes** to maintain and repeatedly carry out protection and sustainment activities for critical assets and services.
- » **Share information** with communities-of-interest related to national cyber security policies, initiatives, and federal capabilities.
- » **Enhance cyber incident response and business continuity capabilities** and discuss federal coordination for incident notification, containment, and recovery.

## What to Expect

- » A four-hour, collaborative workshop, with interactive discussions between operations and cyber security personnel.
- » Structured dialogs and scenario walk-throughs to reinforce resilience concepts and best practices.
- » Sector/industry-specific content and threat examples.