Arkansas's Cyber Center of Excellence
OST State Cybersecurity Office
SCSO@arkansas.gov

Fall 2025 Training Catalog

last updated on 8/15/25

Session Overview

Session Title	Session Type	Session Time	Session Date(s)	Repeat Session
FEMA ICS-100.C	Virtual	9:00 a.m. – 11:00 a.m.	09/17/25 (2 hrs)	11/12/25
FEMA ICS-200.C	Virtual	8:30 a.m. – 12:30 p.m.	09/24/25 (4 hrs)	11/19/25
(ISC)^2 Certified in Cybersecurity (CC)	Virtual	11:00 a.m. – 12:00 p.m. on Fridays	10/10/25 – 11/21/25	
Executive Threat Briefing with the SCSO	Virtual	9:30 a.m. – 10:30 a.m.	10/15/25 (1 hr)	
NIST SP 800-37, Risk Management Framework (RMF)	Virtual	9:00 a.m. – 12:00 p.m.	10/22/25 (3 hrs)	12/03/25
NIST SP 800-53, 800-53A, & 800-53B	Virtual	9:00 a.m. – 12:00 p.m.	10/29/25 (3 hrs)	12/10/25
NCPC Cybersecurity Proactive Defense (CPD)	In-person	8:00 a.m. – 5:00 p.m.	12/15/25 – 12/18/25 (4 days)	

For questions about the program or course information, contact:
OST State Cybersecurity Office (SCSO)
Ray Girdler
Raymond.Girdler@arkansas.gov

Visit the SCSO webpage for more information:
https://sas.arkansas.gov/state-technology/cybersecurity/

FEMA ICS-100.C: Introduction to the Incident Command System (ICS)

Date	09/17/25
Time	9:00 a.m. – 11:00 a.m.
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership (max 100)
Location	Virtual
Registration	https://forms.office.com/g/sWVrj59nkw
Presenter Name	Ray Girdler
Session Title	Introduction to the Incident Command System (ICS)
Session Description	ICS 100, Introduction to the Incident Command System, provides the foundation for ICS training by covering its history, features, principles, and organizational structure, as well as its relationship to the National Incident Management System (NIMS). By the end of the course, you will be able to explain ICS principles and structure; describe NIMS management characteristics; outline ICS functional areas and key leadership roles; and apply NIMS management characteristics to various roles and disciplines.
Min. Requirements	No minimum skills required. The target audience includes persons involved with emergency planning, and response or recovery efforts.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0724: Knowledge of incident response principles and practices • K0824: Knowledge of incident response roles and responsibilities

FEMA ICS-200.C: Basic Incident Command System for Initial Response

Date	09/24/25
Time	8:30 a.m. – 12:30 p.m.
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership (max 100)
Location	Virtual
Registration	https://forms.office.com/g/6veS0Gq71R
Presenter Name	Ray Girdler
Session Title	Basic Incident Command System for Initial Response
Session Description	IS-200, Basic Incident Command System for Initial Response, is designed for personnel likely to assume supervisory roles within ICS. The course reviews ICS in the context of initial response, builds on foundational ICS knowledge, and supports higher-level training. Participants learn how NIMS management characteristics apply to Incident and Unified Command, delegation of authority, ICS organizational components and tools, briefing types, and transfer of command procedures, as well as how to use ICS to manage incidents and events.
Min. Requirements	No minimum skills required. Intended for supervisory-level personnel involved in emergency planning, response, or recovery.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • T0510: Coordinate incident response functions

(ISC)^2 Certified in Cybersecurity (CC) Cohort

Date	10/10/25 - 11/21/25
Time	11:00 a.m. - 12:00 p.m. on Fridays
Targeted Audience	IT Staff (max 35)
Location	Virtual
Registration	https://forms.office.com/g/Dt2faRRMX7
Presenter Name	Ray Girdler
Session Title	(ISC)^2 Certified in Cybersecurity (CC) Cohort
Session Description	This course provides the foundational knowledge, skills, and abilities necessary for entry- or junior-level cybersecurity roles. It establishes a baseline understanding of fundamental security best practices, policies, and procedures. Participants will meet every Friday to review material, discuss key concepts, and engage with a content expert to deepen their understanding. The course covers five key domains: • Security Principles • Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts • Access Controls Concepts • Network Security • Security Operations
Min. Requirements	There are no specific prerequisites. It is recommended that candidates have basic information technology (IT) knowledge.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0680: Knowledge of cybersecurity principles and practices

Executive Threat Briefing with the State Cybersecurity Office (SCSO)

Date	10/15/25
Time	9:30 a.m. - 10:30 a.m.
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership (max 300)
Location	Virtual
Registration	https://forms.office.com/g/05Wiu5v34Y
Presenter Name	State Cybersecurity Office
Session Title	Executive Threat Briefing with the State Cybersecurity Office (SCSO)
Session Description	The Executive Threat Briefing provides senior leaders with critical insights into the latest cyber threats targeting organizations, highlighting emerging attack vectors, trends, and key vulnerabilities. Led by the State Cybersecurity Office, this session will equip executives with the knowledge and tools to make informed decisions on cybersecurity strategy, risk management, and organizational preparedness. Attendees will gain actionable intelligence to safeguard their enterprises against sophisticated threats, all while fostering a culture of resilience at the leadership level.
Min. Requirements	No minimum skills required.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K1139: Knowledge of cybersecurity threats and vulnerabilities • T1456: Determine the impact of threats on cybersecurity

NIST SP 800-37, Risk Management Framework (RMF)

Date	10/22/25
Time	9:00 a.m. - 12:00 p.m.
Targeted Audience	IT Staff, Non-technical Staff (max 100)
Location	Virtual
Registration	https://forms.office.com/g/nK1rB9q2Sn
Presenter Name	Ray Girdler
Session Title	NIST SP 800-37, Risk Management Framework (RMF)
Session Description	**NIST SP 800-37, Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy** The purpose of this course is to provide people *new to risk management* with an overview of a methodology for managing organizational risk in accordance with NIST Special Publication (SP) 800-37, Revision 2. For individuals with experience with NIST SP 800-37, Revision 1, this course explains updates to the RMF in Revision 2, including the integration of privacy and supply chain risk management into this holistic process. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. This course describes at a high level the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.
Min. Requirements	No minimum skills required.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0734: Knowledge of Risk Management Framework (RMF) requirements

NIST SP 800-53, 800-53A, & 800-53B

Date	10/29/25
Time	9:00 a.m. - 12:00 p.m.
Targeted Audience	IT Staff, Non-technical Staff (max 100)
Location	Virtual
Registration	https://forms.office.com/g/xE0b29RuAG
Presenter Name	Ray Girdler
Session Title	NIST SP 800-53, 800-53A, & 800-53B
Session Description	**NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations** NIST SP 800-53 provides a comprehensive catalog of outcome-based security and privacy controls. This course introduces the structure and organization of the security and privacy controls in Revision 5 of the catalog. It also describes key considerations for the implementation of controls as part of an organization-wide risk management program. **NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations** NIST SP 800-53A introduces an control assessment methodology and set of assessment procedures for the SP 800-53 controls. This course introduces the structure and organization of the Revision 5 assessment procedures. It also describes, a methodology to build and tailor effective assessment plans, and how to report, analyze, and manage assessment results as part of an organization-wide risk management program. **NIST SP 800-53B, Control Baselines for Information Systems and Organizations** NIST SP 800-53B establishes security and privacy control baselines for systems and organizations, and provides tailoring guidance for those baselines. This course introduces the structure and organization of the SP 800-53B security and privacy control baselines, and guidance on tailoring and development of control overlays to facilitate control baseline customization for specific communities of interest, technologies, and environments of operation. *Note SP 800-53B is a companion document to SP 800-53 Revision 5.*
Min. Requirements	No minimum skills required.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K1077: Knowledge of data security controls • K1084: Knowledge of data privacy controls • K1212: Knowledge of security controls • S0667: Skill in assessing security controls • S0569: Skill in designing security controls

FEMA ICS-100.C: Introduction to the Incident Command System (ICS)

Date	11/12/25
Time	9:00 a.m. – 11:00 a.m.
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership (max 100)
Location	Virtual
Registration	https://forms.office.com/g/6VksWHX1K3
Presenter Name	Ray Girdler
Session Title	Introduction to the Incident Command System (ICS)
Session Description	ICS 100, Introduction to the Incident Command System, provides the foundation for ICS training by covering its history, features, principles, and organizational structure, as well as its relationship to the National Incident Management System (NIMS). By the end of the course, you will be able to explain ICS principles and structure; describe NIMS management characteristics; outline ICS functional areas and key leadership roles; and apply NIMS management characteristics to various roles and disciplines.
Min. Requirements	No minimum skills required. The target audience includes persons involved with emergency planning, and response or recovery efforts.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0724: Knowledge of incident response principles and practices • K0824: Knowledge of incident response roles and responsibilities

FEMA ICS-200.C: Basic Incident Command System for Initial Response

Date	11/19/25
Time	8:30 a.m. – 12:30 p.m.
Targeted Audience	IT Staff, Non-technical Staff, Senior Leadership (max 100)
Location	Virtual
Registration	https://forms.office.com/g/DH9SuT4Yb4
Presenter Name	Ray Girdler
Session Title	Basic Incident Command System for Initial Response
Session Description	IS-200, Basic Incident Command System for Initial Response, is designed for personnel likely to assume supervisory roles within ICS. The course reviews ICS in the context of initial response, builds on foundational ICS knowledge, and supports higher-level training. Participants learn how NIMS management characteristics apply to Incident and Unified Command, delegation of authority, ICS organizational components and tools, briefing types, and transfer of command procedures, as well as how to use ICS to manage incidents and events.
Min. Requirements	No minimum skills required. Intended for supervisory-level personnel involved in emergency planning, response, or recovery.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • T0510: Coordinate incident response functions

NIST SP 800-37, Risk Management Framework (RMF)

Date	12/03/25
Time	9:00 a.m. - 12:00 p.m.
Targeted Audience	IT Staff, Non-technical Staff (max 100)
Location	Virtual
Registration	https://forms.office.com/g/83mtNLFfyj
Presenter Name	Ray Girdler
Session Title	NIST SP 800-37, Risk Management Framework (RMF)
Session Description	**NIST SP 800-37, Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy** The purpose of this course is to provide people *new to risk management* with an overview of a methodology for managing organizational risk in accordance with NIST Special Publication (SP) 800-37, Revision 2. For individuals with experience with NIST SP 800-37, Revision 1, this course explains updates to the RMF in Revision 2, including the integration of privacy and supply chain risk management into this holistic process. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. This course describes at a high level the importance of establishing an organization-wide risk management program, the information security legislation related to organizational risk management, the steps in the RMF, and the NIST publications related to each step.
Min. Requirements	No minimum skills required.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0734: Knowledge of Risk Management Framework (RMF) requirements

NIST SP 800-53, 800-53A, & 800-53B

Date	12/10/25
Time	9:00 a.m. - 12:00 p.m.
Targeted Audience	IT Staff, Non-technical Staff (max 100)
Location	Virtual
Registration	https://forms.office.com/g/xE0b29RuAG
Presenter Name	Ray Girdler
Session Title	NIST SP 800-53, 800-53A, & 800-53B
Session Description	**NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations** NIST SP 800-53 provides a comprehensive catalog of outcome-based security and privacy controls. This course introduces the structure and organization of the security and privacy controls in Revision 5 of the catalog. It also describes key considerations for the implementation of controls as part of an organization-wide risk management program. **NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations** NIST SP 800-53A introduces an control assessment methodology and set of assessment procedures for the SP 800-53 controls. This course introduces the structure and organization of the Revision 5 assessment procedures. It also describes, a methodology to build and tailor effective assessment plans, and how to report, analyze, and manage assessment results as part of an organization-wide risk management program. **NIST SP 800-53B, Control Baselines for Information Systems and Organizations** NIST SP 800-53B establishes security and privacy control baselines for systems and organizations, and provides tailoring guidance for those baselines. This course introduces the structure and organization of the SP 800-53B security and privacy control baselines, and guidance on tailoring and development of control overlays to facilitate control baseline customization for specific communities of interest, technologies, and environments of operation. *Note SP 800-53B is a companion document to SP 800-53 Revision 5.*
Min. Requirements	No minimum skills required.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K1077: Knowledge of data security controls • K1084: Knowledge of data privacy controls • K1212: Knowledge of security controls • S0667: Skill in assessing security controls • S0569: Skill in designing security controls

NCPC Cybersecurity Proactive Defense (CPD)

Date	12/15/25 - 12/18/25 (4 days)
Time	8:00 a.m. - 5:00 p.m.
Targeted Audience	Technical staff in critical infrastructure responsible for securing networks and responding to cyber attacks. (max 35)
Location	Little Rock, AR (in-person)
Registration	https://cybersecuritydefenseinitiative.org/courses/cpd-course-little-rock/
Presenter Name	National Cybersecurity Preparedness Consortium (NCPC)
Session Title	Comprehensive Cybersecurity Defense
Session Description	Cybersecurity Proactive Defense (CPD) is an **advanced-level course** designed for technical personnel who monitor and protect our nation's critical cyber infrastructure. *This is the first time CPD has been offered through the Cyber Center of Excellence.* This course prepares cyber defenders to recognize their own weaknesses by providing advanced attack vectors, sequential and escalating attack steps, and hands-on attack execution experience. CPD provides context behind a cyberterrorism attack by illustrating each attack step, the tools used to conduct the step, and the resulting impact on targeted systems. **Course Objectives** Upon successful completion of this course, participants will be able to: • The cyber-attack sequence from initial reconnaissance to eventual execution and exfiltration • To perform a functional penetration test of various cyber environments, to include both identifying deficiencies and subsequent mitigation steps • To recognize when your environment has been targeted by cyber-attack tools by performing post-test analysis at the conclusion of the planned penetration test
Min. Requirements	This is an advanced-level hands-on course where specific network and security knowledge and experience are required. Participants should have two years of experience in network or system administration or cybersecurity, a strong understanding of networking and operating systems, and basic knowledge of cyber incident response.
NICE Framework	https://niccs.cisa.gov/workforce-development/nice-framework • K0844: Knowledge of cyberattack stages • S0925: Skill in developing and analyzing attack paths • T1359: Perform penetration testing • T1192: Conduct analysis of computer network attacks