COURSE SYLLABUS

Federal Incident Response for Agency Practitioners Course

Run a federal incident response program end to end, organized the way NIST now organizes it: from governance and readiness, through detection and the one-hour CISA notification clock, to recovery and continuous improvement.

Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/federal-incident-response-for-agency-practitioners



support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1. Program Governance and Risk Management Strategy

The federal IR landscape, the IR charter and CSIRC/SOC standup, roles and a RACI matrix, program maturity and metrics

Module 2. Risk-Informed Readiness

Asset and risk awareness that tunes an IR program to the agency's real exposure, and the preventive controls and workforce readiness that keep detection and response from being overwhelmed

Module 3. Detection and Classification

Detection sources and the 2026 logging baseline, triage and NCISS scoring, determining major-incident status, applied classification exercise

Module 4. Containment and Eradication

Containment strategy, coordinating across on-premises, cloud and OT environments, evidence preservation and chain of custody, root cause analysis and eradication

Module 5. Incident Reporting, Notification and Communication

The one-hour CISA notification, the seven-day congressional notification and annual FISMA reporting, PII and breach-specific notification, and a horizon scan of pending rules

Module 6. Restoration and Recovery Communication

Phased restoration and return-to-operations sign-off, aligning recovery with binding remediation deadlines, and keeping leadership and oversight informed

Module 7. Post-Incident Review and Lessons Learned

After-action methodology, root-cause-to-control mapping, closing the loop back into governance and readiness

Module 8. Tabletop Exercise Design

Exercise design fundamentals and MSELs, building realistic scenarios, facilitation and evaluation, and a design workshop

Module 9. Capstone Simulation and Program Self-Assessment

A full-lifecycle simulated incident worked through every Function in sequence, then a program self-assessment and 90-day action plan