COURSE SYLLABUS

Federal Incident Response Course (Self-Paced)

Build, execute, and continuously improve a federal incident response program, from detection and mandatory reporting to post-incident review and tabletop exercise design.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/federal-incident-response-course-self-paced

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

Course Outline

Module 1: Federal Incident Response Framework and Plan Development

- FISMA incident response requirements: plan maintenance, testing, and reporting obligations.
- NIST SP 800-61 Rev 2: incident response lifecycle, covering Preparation, Detection, Containment, Eradication, Recovery, and Post-Incident activity.
- US-CERT Binding Operational Directive 22-01 and incident category definitions: category codes, severity levels, and reporting thresholds.
- OMB M-21-31: logging requirements, event log retention, and investigative capability maturity tiers.
- IR plan required elements: scope, roles and responsibilities, communication procedures, and escalation criteria.

Module 2: Detection and Analysis – Identifying and Classifying Federal Incidents

- Detection sources: SIEM alerts, CDM dashboard anomalies, IDS/IPS signatures, user reports, and US-CERT notifications.
- Triage methodology: distinguishing events from incidents, and incidents from false positives.
- NIST incident categories applied to federal systems: CAT 1-6 category definitions and classification criteria.
- Incident severity matrix: impact assessment factors, including data sensitivity, system criticality, and operational impact.
- Threat hunting fundamentals: proactive detection techniques for nation-state TTPs in federal network environments.

Module 3: Containment Strategy and Technical Response

- Short-term containment: isolating affected systems without destroying evidence or disrupting mission operations.
- Long-term containment: maintaining operational continuity while an incident is investigated.
- Ransomware response: initial containment, backup verification, and communication to leadership during an active attack.
- Credential compromise response: forced password resets, session revocation, and re-authentication strategy.
- Network segmentation as containment: emergency firewall rule changes and inter-agency coordination for shared infrastructure.

Module 4: Digital Forensics and Evidence Preservation for Federal Incidents

- Federal forensic standards: NIST SP 800-86 and evidence preservation chain-of-custody requirements.
- Memory acquisition and disk imaging: when to capture volatile data before containment and how to do it correctly.
- Cloud forensics: evidence collection from cloud environments, including snapshots, audit logs, and provider cooperation.

- Log evidence standards under OMB M-21-31: required log sources, retention requirements, and log integrity.
- Legal referral preparation: when to contact OIG, FBI, or US Secret Service and what evidence package to prepare.

Module 5: US-CERT Mandatory Reporting and Inter-Agency Coordination

- US-CERT reporting timelines: 1-hour, 24-hour, and 72-hour notification requirements by incident category.
- Completing the US-CERT incident report: required fields, impact assessment, and what unreported incidents generate as a FISMA finding.
- CISA coordination during significant incidents: National Cyber Incident Scoring System and federal response coordination.
- Reporting to agency leadership and OMB: breach reporting under OMB M-17-12 and PII incident protocols.
- Congressional notification: when and how agencies notify oversight committees of significant incidents.

Module 6: Eradication, Recovery, and Restoration Procedures

- Eradication steps: removing malware, closing access vectors, and patching exploited vulnerabilities before restoration.
- Recovery sequence: restoring from known-good backups, verifying integrity, and validating system functionality.
- Return-to-operations criteria: what security validation is required before a recovered system is reconnected.
- Ransomware recovery: negotiation considerations, decryption tool availability, and data restoration from backups.
- Recovery documentation: what must be recorded for FISMA reporting, insurance claims, and lessons-learned review.

Module 7: Post-Incident Review and Lessons Learned Integration

- Post-incident review (PIR) methodology: blameless review vs. root cause accountability.
- Required PIR elements under NIST 800-61: timeline reconstruction, contributing factors, and corrective actions.
- Connecting PIR findings to security control improvements: how incident analysis informs RMF authorization updates.
- Metrics for IR program improvement: mean time to detect (MTTD), mean time to respond (MTTR), and reporting timeliness.
- Integrating lessons learned into the IR plan: version control, tabletop exercise design, and training updates.

Module 8: Tabletop Exercise Design and Capstone

- Tabletop exercise design principles: scenario realism, inject sequencing, and measuring plan effectiveness.
- Exercise types: discussion-based (tabletop) vs. operations-based (functional, full-scale), and when to use each.
- Scenario selection: choosing exercise scenarios that test the highest-risk gaps identified in IR plan reviews.
- FEMA and HSEEP standards for federal exercise design and documentation.
- Debrief methodology: capturing lessons learned and generating improvement plans from exercise outputs.