

Cybersecurity for Federal HR: People Data and the Cyber Workforce Course

Protect the personnel data your HR office holds and code cyber workforce positions to meet federal reporting rules.

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/cybersecurity-for-federal-hr-course>



support@graduateschool.edu • [\(888\) 744-4723](tel:(888)744-4723)

Course Outline

Module 1: Federal HR Data: What It Is and Why It's a Target

- Lessons:
 - What Counts as Federal Personnel Data
 - Why HR Systems Are a High-Value Target
 - A Look at Federal HR Systems and Where Data Lives
- Applied activity: Learners review a short, described list of data fields in a personnel file and sort them into PII, sensitive PII, and non-sensitive categories, explaining one reason each sensitive item would be valuable to an attacker.

Module 2: Protecting Personnel Data: Rules, Roles, and Practices

- Lessons:
 - The Privacy Act and What It Requires of HR
 - Access Controls and the Need to Know Principle
 - Everyday Habits That Protect Personnel Data
- Applied activity: Learners review a short scenario in which a colleague from another office asks for access to a personnel file and decide, using the need to know principle, whether and how to grant it.

Module 3: The Federal Cyber Workforce Framework: NICE and DCWF

- Lessons:
 - Why the Federal Government Standardized Cyber Work Roles
 - The NICE Framework: Categories, Work Roles, and What Happened to Specialty Areas
 - The DoD Cyber Workforce Framework: NICE in Practice
- Applied activity: Learners are given a short position description and match it to the NICE Framework category and work role it most likely belongs to.

Module 4: Coding and Recruiting for Cyber Roles: HR's Part in Workforce Readiness

- Lessons:
 - Coding a Position with the Right Work Role
 - Writing Position Descriptions That Attract Cyber Talent
 - Common Coding and Recruiting Mistakes
- Applied activity: Learners review a short, generic position description for a cyber role and identify what is missing or vague, then suggest a specific work role code and a revision that would better attract qualified candidates.