Cybersecurity

## Competency development areas in cybersecurity

* AI for Cybersecurity: Basic concepts and applications of artificial intelligence and machine learning in the field of cybersecurity. Threat Detection and Analysis: Utilizing AI techniques to detect and analyze cyber threats.
* Emerging Technologies and Threats: Emerging cybersecurity technologies, trends, and threats such as Artificial Intelligence (AI) in cybersecurity, Internet of Things (IoT) security, Blockchain security, and cloud-native security.
* Federal Risk and Authorization Management Program (FedRAMP): Based on the FedRAMP framework, which provides a standardized approach to assessing and authorizing cloud service providers for federal government use. Understand the security requirements and processes involved in FedRAMP compliance.
* Security Assessment and Authorization: The process of conducting security assessments and authorizations for federal systems and applications. Understand the roles and responsibilities of federal employees in the SA&A process.
* Federal Information Security Management Act (FISMA) Compliance: The requirements and guidelines outlined by FISMA for federal information security.
* Cyber Threat Intelligence: Methods for gathering, analyzing, and interpreting threat intelligence data to identify potential cyber threats and vulnerabilities.
* Security Governance and Compliance: The frameworks, policies, and standards governing cybersecurity practices, such as the NIST Cybersecurity Framework, ISO 27001, and regulatory compliance requirements like GDPR or HIPAA.
* Cloud Security: Security considerations and controls specific to cloud computing environments. Shared responsibility models, cloud security architecture, and cloud provider security features.

## Online training resources

* CompTIA: CompTIA offers online training resources and certifications in cybersecurity. They cover topics like cybersecurity fundamentals, network security, and security management. Their certifications, such as Security+ and CySA+, are highly regarded in the industry. ([comptia.org/training/certmaster-learn/security](https://www.comptia.org/training/certmaster-learn/security)).
* SANS Cyber Aces Online: SANS Cyber Aces Online provides free foundational cybersecurity training, including modules on networking, operating systems, and cybersecurity principles. This resource is suitable for beginners looking to build a solid cybersecurity knowledge base. (sans.org/cyberaces/).
* National Initiative for Cybersecurity Careers and Studies (NICCS): NICCS provides a catalog of cybersecurity training resources, including online courses, virtual labs, and webinars. Their catalog can be searched for relevant training based on specific cybersecurity interests and skill level. (niccs.cisa.gov/education-training/catalog).

## Online training resources in cybersecurity specifically tailored for federal employees:

* Federal Cyber Defense Skilling Academy: An intense, full-time, three-month accelerated training program, which helps civilian federal employees develop their cyber defense skills through training in the baseline knowledge, skills and abilities of a Cyber Defense Analyst (CDA). (cisa.gov/resources-tools/programs/federal-cyber-defense-skilling-academy).
* Federal Virtual Training Environment (FedVTE): Self-paced courses on cybersecurity-related topics that are free to government employees, federal contractors, military, veterans and the public. (niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte).