CyberKnights™

NICE Skills Assessment, Development and Talent Portal

CyberKnights™

What is the National Initiative for Cybersecurity Education (NICE)?

- **A partnership among government, academia, and the private sector focused on education, training, and workforce development**
- **Will strengthen the cybersecurity posture of organizations through adoption of standards and best practices**

CyberKnights

NICE Goals

1. Promote the Discovery of Cybersecurity Careers and Multiple Pathways
2. Transform Learning to Build and Sustain a Diverse and Skilled Workforce
3. Modernize the Talent Management Process to Address Cybersecurity Skills Gaps
4. Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)
5. Drive Research on Effective Practices for Cybersecurity Workforce Development

CyberKnights

The NICE Framework mapped to certification programs

- provide hands-on learning and performance-based assessments
- validate competencies to perform work roles
- supply learners with portable and stackable credentials
- ensure continued competence in an evolving field through renewal requirement

COMPARED TO

beginner-level salaries in IT, the salary premium for specializations such as Security and Network Technologies is:

10% higher with an intermediate certification (e.g. Security+)
26% higher with an advanced certification (e.g. CISSP)
45%+ higher with an expert certification (e.g. CISM)[1]

IN THE U.S.

the difference between salaries of certified and noncertified IT staff is nearly **$8,400** or **11.7%.**[2]

ON A NATIONAL LEVEL

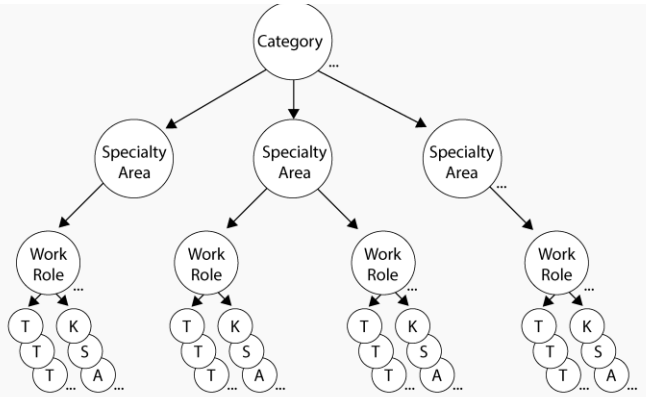
there are approximately **215,371 job openings** requesting certifications such as Security+, CIPP, CISSP, GIAC, CISA, and CISM as of 2018.[3]

The NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

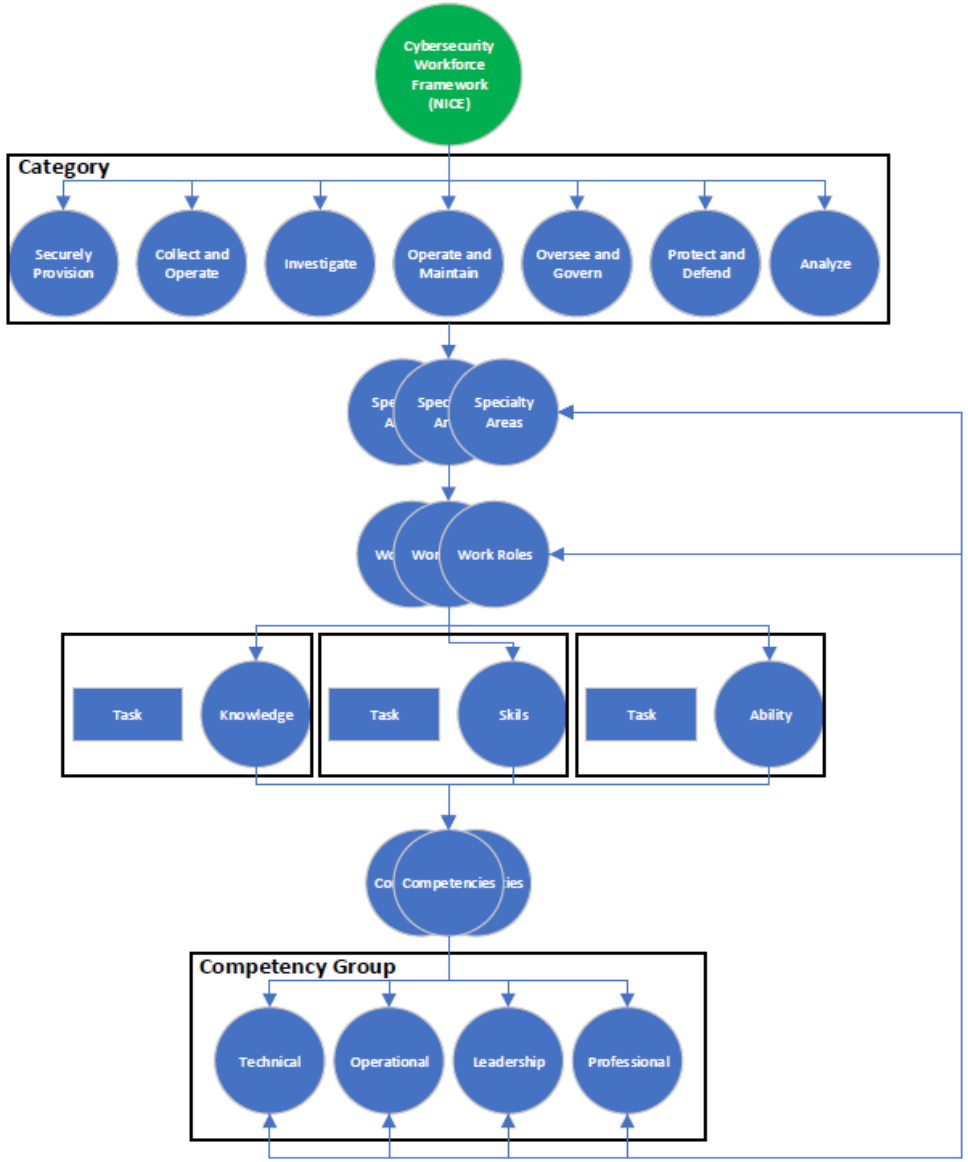
WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role



TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

CyberKnights™



CyberKnights™

Securely Provision- Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

Specialties		Work Roles
• **Risk Management** Oversees, evaluates, and supports processes necessary for existing and new information technology (IT) systems to meet the organization's cybersecurity and risk requirements.	⟷	Authorizing Official/ Designating Representative Security Control Assessor
• **Software Development** Develops and codes new (or modifies existing) computer applications software, or specialized utility programs.	⟷	Software Developer Secure Software Assessor
• **Systems Architecture** Develops system concepts and translates law and regulation conditions into system and security designs and processes.	⟷	Enterprise Architect Security Architect
• **Systems Development** Works on phases of the systems development life cycle.	⟷	Systems Developer Information Systems Security Developer
• **Systems Requirements Planning** Consults with customers to gather and evaluate functional requirements and translates them into technical solutions.	⟷	Systems Requirements Planner
• **Technology R&D** Conducts technology assessment and integration processes.	⟷	Research and Development Specialist
• **Test and Evaluation** Develops and conducts tests of systems to evaluate compliance with specifications and requirements.	⟷	System Testing and Evaluation Specialist

CyberKnights™

Collect and Operate- Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

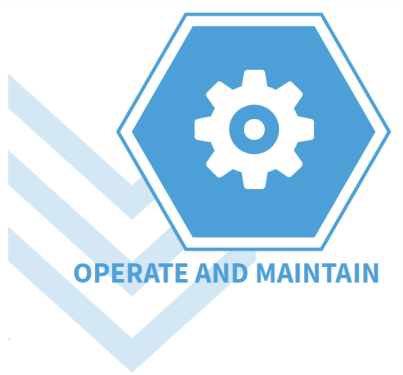
Specialties		Work Roles
• **Collection Operations** Executes collection using appropriate strategies within the priorities established through the collection management process.	⟷	All Source-Collection Manager All Source-Collection Requirements Manager
• **Cyber Operational Planning** Performs in-depth joint targeting and cybersecurity planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.	⟷	Partner Integration Planner Cyber Intel Planner Cyber Ops Planner
• **Cyber Operations** Performs activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support various other intelligence activities.	⟷	Cyber Operator

CyberKnights™

Investigate- Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Specialties		Work Roles
• Cyber Investigation Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include, but not limited to, interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.	⟷	Cyber Crime Investigator
• Digital Forensics Collects, processes, preserves, analyzes, and presents evidence in support of network vulnerability and/or criminal, fraud, counterintelligence, or law enforcement investigations.	⟷	Law Enforcement/Counterintelligence Forensics Analyst Cyber Defense Forensics Analyst

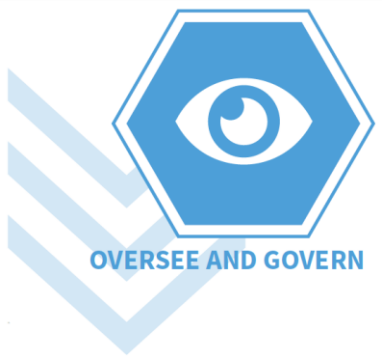
CyberKnights™



Operate and Maintain- Provides the support, administration, and maintenance necessary for effective and efficient information technology (IT) system performance and security.

Specialties	Work Roles
• **Customer Service and Technical Support** Addresses problems; installs, configures, troubleshoots, and provides maintenance and training in response to customers.	Technical Support Specialist
• **Data Administration** Develops and administers databases and/or management systems that allow for the storage, query, protection and utilization of data.	Database Administrator Data Analyst
• **Knowledge Management** Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.	Knowledge Manager
• **Network Services** Installs, configures, tests, operates, maintains, and manages networks and their firewalls.	Network Operations Specialist
• **Systems Administration** Installs, configures, troubleshoots, and maintains server configurations for confidentiality, integrity, and availability.	System Administrator
• **Systems Analysis** Studies an organization's current computer systems and procedures, and designs information systems solutions to help the organization operate more securely, efficiently, and effectively.	Systems Security Analyst

CyberKnights



Oversee and Govern- Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Specialties	Work Roles
• **Cybersecurity Management** Oversees the cybersecurity program of an information system network, or other area of responsibility.	Information Systems Security Manager Communications Security (COMSEC)
• **Executive Cyber Leadership** Supervises, manages, and/or leads work and workers performing cyber and cyber-related and/or cyber operations work.	Executive Cyber Leadership
• **Legal Advice and Advocacy** Provides legal advising to leadership and staff on a variety of relevant topics. Advocates legal and policy changes, and makes a case on behalf of client via legal briefs and proceedings.	Cyber Legal Advisor Privacy Officer/Privacy Compliance Manager
• **Program/Project Management and Acquisition** Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs.	Program Manager IT Project Manager Product Support Manager IT Investment/Portfolio Manager IT Program Auditor
• **Strategic Planning and Policy** Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives	Cyber Workforce Developer and Manager Cyber Policy and Strategy Planner
• **Training, Education, and Awareness** Conducts training of personnel. Develops and delivers and/or evaluates training courses, methods, and techniques.	Cyber Instructional Curriculum Developer Cyber Instructor

CyberKnights™

Protect and Defend- Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.

Specialties		Work Roles
• **Cyber Defense Analysis** Uses defensive measures and information collected from a variety of sources to identify, analyze and report events that occur or might occur within the network to protect information, information systems, and networks from threats.	⟷	Cyber Defense Analyst
• **Cyber Defense Infrastructure Support** Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities.	⟷	Cyber Defense Infrastructure Support Specialist
• **Incident Response** Responds to crises or urgent situations to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activity.	⟷	Cyber Defense Incident Responder
• **Vulnerability Assessment and Management** Conducts assessments of threats and vulnerabilities; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	⟷	Vulnerability Assessment Analyst

CyberKnights™

Analyze- Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Specialties		Work Roles
• **All-Source Analysis** Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.	⟷	All-Source Analyst Mission Assessment Specialist
• **Exploitation Analysis** Analyzes collected information to identify vulnerabilities and potential for exploitation.	⟷	Exploitation Analyst
• **Language Analysis** Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.	⟷	Multi- Disciplined Language Analyst
• **Targets** Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.	⟷	Target Developer Target Network Analyst
• **Threat Analysis** Identifies and assesses the capabilities and activities of cybersecurity criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.	⟷	Threat/Warning Analyst

CyberKnights™

Competencies

- Asset/Inventory Management
- Collection Operations
- Computer Forensics
- Computer Languages
- Computer Network Defense
- Computers and Electronics
- Data Analysis
- Data Management
- Database Administration
- Database Management Systems
- Encryption
- Enterprise Architecture
- Identity Management
- Incident Management
- Information Assurance
- Information Management
- Information Systems/Network Security
- Infrastructure Design
- Intelligence Analysis
- Knowledge Management
- Mathematic Reasoning
- Modeling and Simulation
- Network Management
- Operating Systems
- Operations Support
- Problem Solving
- Requirements Analysis
- Software Development
- Software Testing and Evaluation
- System Administration
- Systems Integration
- Systems Testing and Evaluation
- Target Development
- Technology Awareness
- Telecommunications
- Threat Analysis
- Vulnerabilities Assessment
- Web Technology

CyberKnights™

Competencies

- Business Continuity
- Client Relationship Management
- Contracting/Procurement
- Data Privacy and Protection
- External Awareness
- Legal, Government, and Jurisprudence
- Organizational Awareness
- Policy Management
- Process Control
- Risk Management
- Third Party Oversight/Acquisition Management

CyberKnights™

Competencies

- Project Management
- Strategic Planning
- Teaching Others
- Workforce Management

CyberKnights™

Competencies

- Conflict Management
- Critical Thinking
- Interpersonal Skills
- Oral Communication
- Presenting Effectively
- Written Communication

CyberKnights

What is CyberKnights?

A portal design based on the NICE Framework taxonomy to establish:


A skills portfolio


Assess current soft and hard skills


Identify skills gaps


Identify pathways to obtain additional skills

CyberKnights

Portal Architecture

National Initiative for Cybersecurity Education Framework

Taxonomy based on Knowledge, Skills, and Abilities

Individual Practitioners (all levels)
(Students/Interns/Apprentices/Employees)

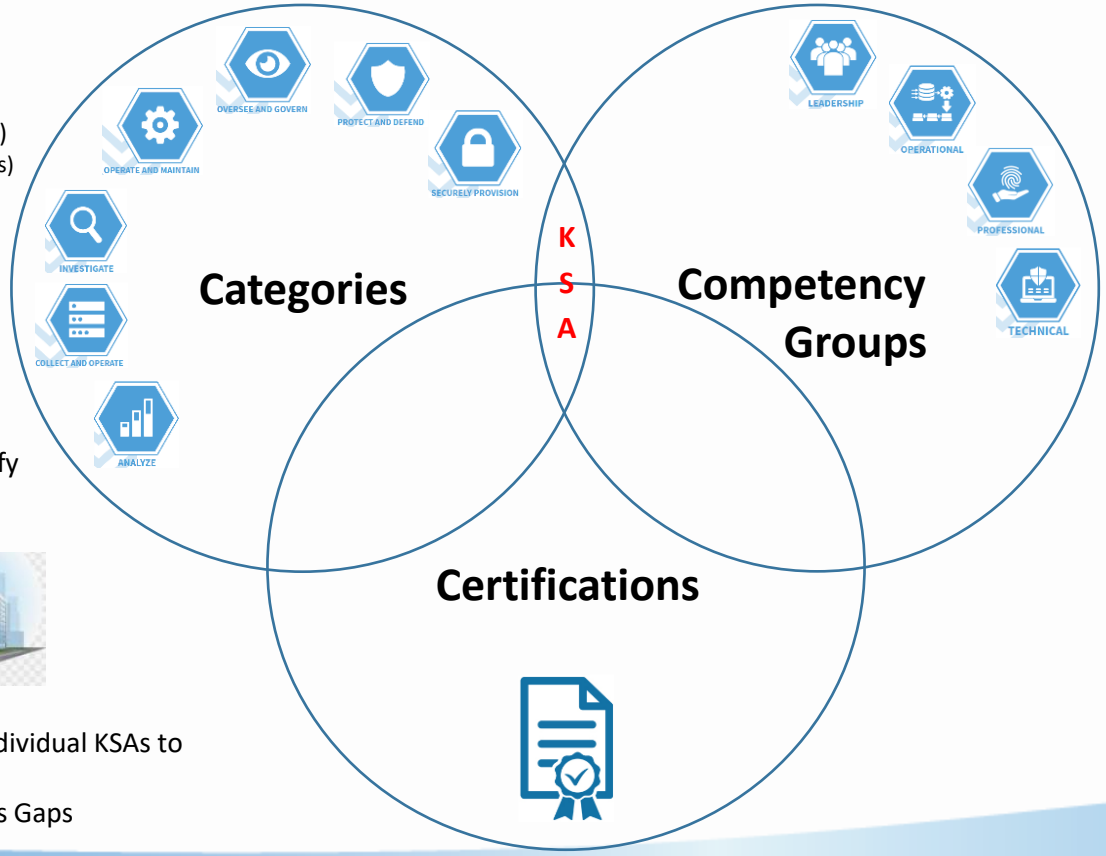
- Understand NICE KSAs and Competencies

Employers

- Use existing work roles or modify to fit needs of employer work roles

Employers

- Track alignment of Individual KSAs to Job KSAs
- Identify/Manage Skills Gaps



Employees / Employers

- Career path interest
- Increase retention

Educators

- Offer pathways to acquire work role KSAs
- View employer most-requested KSAs to keep curriculum aligned

CyberKnights

Roles-based Portal

Individual Role

- job seekers/students/interns/apprentices/professionals/employees
- want to establish a skills portfolio
- want to be vetted cybersecurity practitioners

Employer Role

- can post a position for system to match talent
- can take inventory of employees' cybersecurity skills
- can identify skills gaps and develop upskill plans
- system can match internal and/or external talent to skills gaps
- perform operational assessments to identify risk and find talent to mitigate

Educators Role

- visibility into the skills employers are requiring
- keep curriculum current to address the skills gap
- be visible to employers with courses/curriculum
  - skills gap remediation options
  - apprenticeships

CyberKnights™

www.cyberknights.us