The NICE Framework:
Preparing a Job-Ready Cybersecurity Workforce
NIST SP 800-181r1

Karen A. Wetzel, Manager of the NICE Framework
karen.wetzel@nist.gov
Today’s Agenda

• Today’s Cybersecurity Workforce
• What is a Workforce Framework?
• NICE Workforce Framework for Cybersecurity
• Using the NICE Framework to Address Challenges
NICE Strategic Plan and Implementation Plan
(2021-2025)

- **Career Discovery**: Promote the Discovery of Cybersecurity Careers and Multiple Pathways
- **Learning Process**: Transform Learning to Build and Sustain a Diverse and Skilled Workforce
- **Talent Management**: Modernize the Talent Management Process to Address Cybersecurity Skills Gaps
- **NICE Framework**: Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)
- **Research**: Drive Research on Effective Practices for Cybersecurity Workforce Development
NICE Framework Focus: Who and How

NIST Cybersecurity Framework (CSF): Standards, guidelines and best practices to manage cybersecurity risk
www.nist.gov/cyberframework

NICE Framework: Education, Training, and Workforce

Where They Connect: How
Cybersecurity Workforce Challenges

- Aging workforce
- Growing demand
- Low retention
- Low availability of entry points for new workers
- Low diversity
- Highly experienced and skilled workforce requirements
Cybersecurity Workforce Opportunities

- Demand for workers is high
- Work is well paying
- Mission is attractive
- Positions can often accommodate remote work
- Multiple career pathways
A Playbook for Workforce Frameworks


Benefits of a Workforce Framework

Workforce Framework Uses

Workforce Framework Components

Supporting Resources
Workforce Frameworks: Example Uses

• Promote cybersecurity career awareness in K12 and beyond
• Create curriculum to prepare an effective workforce and highlight connection to jobs
• Assess current cybersecurity workforce and prepare for future needs
• Identify job requirements, write job descriptions, and assess candidates
• Support continuous learning, career pathways, and career development
Workforce Framework Attributes

Agility
People, processes, and technology mature and must adapt to change. A workforce framework enables organizations to keep pace with a constantly evolving ecosystem.

Flexibility
There is no one-size-fits-all solution to common challenges. A workforce framework enables organizations to account for their unique operating context.

Interoperability
Solutions to common challenges may be unique, but they must agree upon consistent use of terms. A workforce framework enables organizations to exchange workforce information using a common language.

Modularity
In addition to cybersecurity, organizations manage other risks within the enterprise. A workforce framework enables communication about these other workforces within the enterprise and across sectors.
Adapting the Framework: Local Factors

- Workforce Needs
- Technology
- Threat Landscape
- Industry Standards
- Government & Regulation
The NICE Framework
Workforce Framework for Cybersecurity (NICE Framework)

A common, consistent vocabulary to clearly share information about what a workforce needs to know

A modular, building-blocks approach based on Task, Knowledge, and Skill (TKS) statements

The concepts of work and learner can be applied to any organization

Enables the establishment of regular processes

For use in career awareness, education and training, hiring and career development, & workforce planning and assessment

www.nist.gov/nice/framework
Who is the NICE Framework For?

**EMPLOYERS**
- Track workforce capabilities
- Create job descriptions
- Develop employees
- Provide career pathways

**LEARNERS**
- Learn about the variety of cybersecurity work roles
- Develop knowledge and skills in a defined area of expertise
- Apply learning and demonstrate capability

**EDUCATION, TRAINING, AND CREDENTIAL PROVIDERS**
- Develop learning courses and programs
- Align teaching with the NICE Framework
- Conduct performance-based assessments

GOVERNMENT • INDUSTRY • ACADEMIA
NICE Framework Components

TKS Statements, Work Roles, and Competency Areas
NICE Framework Building Blocks:
Task, Knowledge, and Skill (TKS) Statements

TKS Definitions
- **Task**: An activity that is directed toward the achievement of organizational objectives.
- **Knowledge**: A retrievable set of concepts within memory.
- **Skill**: The capacity to perform an observable action.
Using the NICE Framework: **Building Block Applications**

**WORK ROLES**
- Groupings of Task statements
- Work an individual or team is responsible for

**COMPETENCY AREAS**
- Groupings of related Knowledge and Skill statements
- Correlate with capability to perform Tasks in a domain

**TEAMS**
- Created Using Competency Areas or Work Roles
**NICE Framework Work Role Categories**

and example roles*

- **OG** 
  - OVERSIGHT & GOVERNANCE
  - Security Architect, Systems Development

- **DD** 
  - DESIGN & DEVELOPMENT
  - Database Administration, Network Management

- **IO** 
  - IMPLEMENTATION & OPERATION
  - Defensive Cybersecurity, Incident Response

- **PD** 
  - PROTECTION & DEFENCE
  - Cyber Operations, Target Development

- **CE** 
  - CYBERSPACE EFFECTS
  - All-Source Analysis, Intelligence Planning

- **IN** 
  - INTELLIGENCE
  - Cybercrime Investigation, Digital Evidence Forensics

*This diagram is based on proposed updates to the Work Roles and feedback from public comments. Not final.*
Occupations, Jobs, and Work Roles

**Work Role:**
A grouping of work for which someone is responsible or accountable

**Work Roles:**
- Are not synonymous with job titles or occupations
- May apply to many varying job titles
- Can be combined to create a particular job

**Consist of:**
- Tasks that constitute the work to be done
## NICE Framework

### Work Role Examples

<table>
<thead>
<tr>
<th>Incident Response</th>
<th>Systems Management</th>
<th>Threat Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category: Protection and Defense</td>
<td>Category: Oversight and Governance</td>
<td>Category: Protection and Defense</td>
</tr>
<tr>
<td>Responsible for investigating, analyzing, and responding to network cybersecurity incidents.</td>
<td>Responsible for the cybersecurity of a program, organization, system, or enclave.</td>
<td>Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat and warning assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.</td>
</tr>
<tr>
<td>• 17 Tasks</td>
<td>• 53 Tasks</td>
<td>• 29 Tasks</td>
</tr>
<tr>
<td>• 40 Knowledge/Skill/Ability</td>
<td>• 59 Knowledge/Skill/Ability</td>
<td>• 32 Knowledge/Skill/Ability</td>
</tr>
</tbody>
</table>

### Example Tasks (Systems Management)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0213</td>
<td>Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.</td>
</tr>
<tr>
<td>T0219</td>
<td>Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.</td>
</tr>
<tr>
<td>T0254</td>
<td>Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.</td>
</tr>
<tr>
<td>T0263</td>
<td>Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.</td>
</tr>
</tbody>
</table>
NICE Framework Competency Areas

Clusters of related Knowledge and Skill statements that correlate with one’s capability to perform Tasks in a particular domain.

Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner’s capabilities in the domain.

- **Name:** Clearly signals the area that will be described.
- **Description:** Provides simple and clear language that focuses on the learner
- **Associated TKS Statements**
NICE Framework Competency Areas: Preparing a Job-Ready Workforce

- Competency Areas and the NICE Framework
- Competency Area Development
- Example Uses

https://csrc.nist.gov/publications/detail/nistir/8355/final
NICE Framework Competency Areas May...

• Be additive to one or more Work Roles
• Be used independently of Work Roles
• Represent domains that span multiple Work Roles
• Represent emerging domains that do not yet have established Work Roles

In addition, Competency Areas:
Do not duplicate existing Work Roles
### Proposed NICE Framework Competency Areas

15 Competency Areas, representing:
Fundamental Areas • Emerging Areas • Unique Domains

| 1. Access Controls          | 9. Data Security       |
| 2. AI Security             | 10. DevSecOps          |
| 5. Communications Security | 13. OT Security         |
| 7. Cybersecurity Fundamentals | 15. Supply Chain Security |
| 8. Cybersecurity Leadership|                        |
Applying Competency Areas: Additive to Work Role(s)

- When additional capabilities are necessary for a particular Work Role at your organization, the Competency Area can be added to supplement that role.
- A position responsible for more than one Work Role may need the Competency Area across the multiple roles.
- An organization may want a candidate to demonstrate capability in a defined Competency Area for particular Work Roles.

Example:
Cloud Security Competency Area + Security Architecture Work Role
Applying Competency Areas: Span Multiple Work Roles

- To improve communication and coordination in a specific sector or domain
- For staff who don’t work in cybersecurity but need cybersecurity expertise to mitigate risks
- A starting place to shift into cybersecurity

Example:
OT Cybersecurity Competency Area needed by:
- Facilities Managers
- Information Systems Security Developers
Applying Competency Areas: Independent, Emerging Domains

- A starting place for learning about cybersecurity work
- A way to shift to a different or related area of cybersecurity
- A way to develop higher-level expertise in an area
- A way to represent emerging domains prior to Work Role consensus

Examples:
- Cybersecurity Fundamentals
- Secure Programming
- AI Cybersecurity
Competency Areas Authoring Guide

- What are Competency Areas?
- Competency Areas and Work Roles
- How to Draft Competency Areas

Benefits of a Workforce Framework
Workforce Framework Uses
Workforce Framework Components
Supporting Resources

Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework

**Recommendations**

1. Establish a **workplace-focused NICE Framework proficiency scale** to be applied to Competency Areas and Work Roles.

2. Encourage the NICE Modernize Talent Management Working Group to establish a Project Team for NICE Strategic Plan Goal #3: Align qualification requirements according to proficiency levels.

3. Engage stakeholders and subject matter experts to develop statements of proficiency to apply to NICE Framework.

---

**Key Characteristics of Workplace Proficiency Scales**

- **Demonstrative**: How capability is evidenced
- **Supervision**: Amount and type for the level
- **Professional Skills**: Soft skills, employability skills...
Example Use: Hiring

Common Challenges
- Unclear workforce needs
- Working without a detailed position description
- Conducting a candidate search with unrealistic goals
Do we have the right people on our cybersecurity team?

**Solution:** Conduct a workforce assessment using the NICE Framework

- Determine needed Work Roles
- Assess current cybersecurity staff in needed Competency areas
- Identify gaps and provide requisite training
How can we be sure to hire the right candidate?

**Solution:** Use the NICE Framework to...

- Identify Competencies & Work Roles the new hire will be responsible for
- Use language from the NICE Framework in your job description
- Assess candidates for needed knowledge and skills
I’m looking to shift to a new cybersecurity role in my organization but want to make sure I’m prepared.

**Solution:** Upskill and reskill with the NICE Framework

- Use related Work Roles in career pathing
- Clearly communicate organizational needs
- Identify areas of strength and weakness – and then focus on areas that need work
IT Cybersecurity Specialist

Typical work assignments include:

• Ensures that the implemented security safeguards are adequate to assure the integrity, availability and confidentiality of the information being processed, transmitted or stored consistent with the level of sensitivity of that information.

• Plans the work to be accomplished by subordinate civilian and contractor; sets and adjust short-term priorities, and prepare schedules for completion of work; assigns work to subordinates based on priorities, selective consideration of the difficulty, requirements of assignments, and the capabilities of employees.

• Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams.

• Analyzes policy and recommends improvements.

• Serves as an expert consultant evaluation for functional teams, to assist them in anticipating, identifying, evaluating, mitigating and minimizing risks associated with IT systems vulnerabilities.
NICE Framework Resource Center

• Getting Started & FAQ
• Documents & Data
• Translations
• Playbook for Workforce Frameworks
• Success Stories (Case Studies) and Framework in Focus (Practitioner Interviews)
• Resources for Employers, Education & Training Providers, and Learners
• Coming Soon: Employers Guide to Developing Job Descriptions
• Planned: Usage Guides, Job Profiles, Career Pathways, Proficiency Levels

NICE Framework Tools

• CyberSeek: An interactive cybersecurity jobs heat map across the U.S. by state and metropolitan areas and career pathway tool.
• NICE Framework Tool & Keyword Search: Enables browsing and searching.
• NICE Framework Mapping Tool: Answer questions about your federal cybersecurity-related position and the tool will show you how it aligns to the NICE Framework and what can be done to strengthen your cybersecurity team.
• NICCS Education and Training Catalog: Cybersecurity professionals across the nation can find over 6,000 cybersecurity-related courses aligned with the NICE Framework.
• NICCS Cyber Career Pathways Tool: Includes common relationships between roles as well as frequently used titles in each role. (Federal)
• NICE Challenge Project: Real-world cybersecurity challenges within virtualized business environments to provide students with workforce experience before entering the workforce.
Cyber Seek Cybersecurity Career Pathway: Cybersecurity Analyst

### Cybersecurity Analyst

**Average Salary:** $107,517

**Common Job Titles:**
- Cybersecurity Analyst
- Information Security Analyst
- Security Analyst
- IT Security Analyst
- Cyber Threat Analyst

**Requested Education (%)**
- Sub-Bac: 12%
- Bachelor's Degree: 70%
- Graduate Degree: 17%

**Total Job Openings:** 27,091

#### Top Future Skills Requested

- **Skills**
  - Public Cloud Security: 121%
  - Comprehensive Software Security: 114%
  - Threat Hunting: 105%
  - Security Information and Event Management (SIEM): 60%
  - Threat Intelligence & Response: 53%

- **5-Year Projected Growth**
  - Security Provision: 55%
  - Operate and Maintain: 45%
  - Protect and Defend: 40%
  - Analyze: 40%
  - Investigate: 35%
  - Oversee and Govern: 30%
  - Collect and Operate: 25%

#### Top Certifications Requested

- Certified Information Systems Security Professional (CISSP)
- GIS Certification
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager

#### Top Skills Requested

1. Cyber Security
2. Computer Science
3. Vulnerability
4. Auditing
5. Incident Response
6. Risk Analysis
7. Firewall
8. Risk Management
9. Cyber Threat Intelligence

---

[Image of Cybersecurity Analyst career map and skill set chart]
NICCS Pathways Tool: Cyber Defense Analyst
Engage with NICE

• NICE Framework Users Group
  o Sharing and learning how to apply and use the NICE Framework

• NICE Interagency Coordinating Council
  o Open to all federal employees with responsibilities to grow and sustain the Nation’s cybersecurity workforce
  o Monthly meetings (next call: July 13, 2023)

• NICE Community Coordinating Council
  o Public and private sector participants
  o Monthly meetings (next call: May 24, 2023)

• Calls for Comments, Workshops, Webinars, Conferences

October 16-21: Cybersecurity Career Week
September 6: #ChooseCyber - Insider Tips for Cybersecurity Career Week 2023
September 20: The Impact of Generative Artificial Intelligence on Education and Workforce
Questions?

- www.nist.gov/nice/framework
- NICEframework@nist.gov
- karen.wetzel@nist.gov