What’s New – Revisions to the NICE Framework

July 15, 2020
Timeline of Framework Updates

Engagement with Key Stakeholders
*Pre-November 2019*

Webinar to Describe Process and Request for Comments
*December 2019*

Adjudicate Comments Received
*January-February 2020*

First Draft of Changes for Comments
*July 2020*

- Updates to Tasks, Knowledge, Skills, and Abilities, *November 2019-2021*
  - Announcement of Request for Comments
    *November 2019*
  - Request for Comments Deadline
    *January 2020*
  - Consultative Process
    *March-May 2020*
  - Final Draft of Changes
    *November 2020*
Attributes of the New Revision

• **Agility**— The NICE Framework enables organizations to keep pace with a constantly evolving ecosystem.

• **Flexibility**— The NICE Framework enables organizations to account for the organization’s unique operating context.

• **Interoperability**— The NICE Framework enables organizations to exchange workforce information using a common language.

• **Modularity**— The NICE Framework enables organizations to communicate about other workforces within an enterprise (e.g., Privacy, Artificial Intelligence, etc.).
Feature: “The Work” and “The Learner”

Describes the work

Task

Describes the learner

Knowledge

Skill
Feature: Building Blocks

• Task: an activity that is directed toward the achievement of objectives
• Knowledge: a retrievable set of concepts within memory
• Skill: the capacity to perform an observable action
Feature: Work Roles

Includes:
- Name
- Description

Work Role

Describes the work

Task

Task

Task
Feature: Work Roles

Includes:
- Name
- Description

Describes the work
Pam Frugoli
Senior Workforce Analyst
Employment and Training Administration
U.S. Department of Labor
Use of NICE Framework by Private Sector and Role of Employment and Training Administration

- The Employment and Training Administration (ETA) and industry partners collaborate to develop and maintain dynamic models of the foundation and technical competencies needed in various industries and sectors of the American economy.

- The goal is to promote an understanding of the skill sets and competencies that are essential to educate and train a globally competitive workforce.

- The models are a resource to inform collaboration among industry leaders, educators, economic developers, and public workforce investment professionals to:
  - Identify specific employer skill needs
  - Develop competency-based curricula and training models
  - Develop industry-defined performance indicators, skill standards, or certifications
  - Develop resources for career exploration and guidance
DOL-sponsored online resources

Occupational Information Network (O*NET) system

Competency Model Clearinghouse
## O*NET Focus on Careers and Occupations

<table>
<thead>
<tr>
<th>O*NET</th>
<th>NICE Cybersecurity Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>974</strong> Occupations</td>
<td><strong>52</strong> Work Roles</td>
</tr>
<tr>
<td><strong>41</strong> Knowledge Areas</td>
<td><strong>614</strong> Knowledge statements</td>
</tr>
<tr>
<td><strong>35</strong> Skills</td>
<td><strong>359</strong> Skills</td>
</tr>
<tr>
<td><strong>55</strong> Abilities</td>
<td><strong>119</strong> Abilities</td>
</tr>
<tr>
<td><strong>19,566</strong> Tasks</td>
<td><strong>928</strong> Tasks</td>
</tr>
</tbody>
</table>

The NICE Framework is an unparalleled **in-depth** resource
O*NET Profile for Information Security Analysts

Wages & Employment Trends
- Median wage (2018): $90,730 yearly / $43.17 hourly
- State wages: Select a State
- Local wages: Zip Code
- Employment (2018): 112,360 workers
- Projected growth (2018-2028): Much faster than average (11% or higher)
- Projected job openings (2018-2028): 12,080
- State trends: Select a State
- Top industries (2018): Professional, Scientific, and Technical Services

Sources of Additional Information
- The U.S. Department of Labor's O*NET program, which provides comprehensive information on the occupational requirements, working conditions, training, education, and outlook for each occupation.
- The National Initiative for Cybersecurity Education (NICE) Framework, which outlines the skills, knowledge, and abilities needed for cybersecurity professionals.
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides a common language for describing cyber risk and setting expectations for cybersecurity performance.
- The Certified Information Systems Security Professional (CISSP) certification program, which prepares professionals for roles in information security.
- The Cybersecurity Workforce Development Network, which connects employers and educational institutions to ensure that the cybersecurity workforce is adequately trained.

Disclaimer: Data is subject to change and should be verified with the latest sources provided.
Feature: Competencies

Describes the learner

Knowledge

Competency

Skill
Socializing the NICE Framework to a Wider Audience

How To

- Download the industry model and worksheets in several formats
- Instructions to view the model online

General Information

- The "Build-Block" tool
- Frequently Asked Questions

https://www.careeronestop.org/CompetencyModel/Competency-Models/cybersecurity
Q & A
Matthew Isnor
Senior Program Lead
Cyber Workforce Development
Department of Defense, OCIO
DoD Cyberspace Workforce Framework (DCWF)

Establishes an authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator.

Develops qualification requirements for cyber work roles outlined in DoD Manual 8140.XX.

Facilitates uniform identification, tracking, and reporting required by the Federal Cybersecurity Workforce Assessment Act (FCWAA).

The DCWF has been adapted at the national level in NIST Special Publication 800-181.

Used to develop an international framework under the NATO Multinational Cyber Defense Training & Education Project.
The 8140 issuances will establish enterprise baseline standards and requirements according to DCWF work role(s).

Components will be expected to add additional requirements to enhance readiness based on environment specific factors.

This structure will enable reciprocity while enhancing interoperability and cyber readiness.

Establish enterprise baseline standards and requirements according to NICE Framework Series requirements.
Lisa Dorr, Senior Talent Manager

Department of Homeland Security Office of the Chief Human Capital Officer

- Cybersecurity and Intelligence Talent Experience (CITE) Division
- Cybersecurity Talent Management System (CTMS) Innovations Team
- Senior Talent Manager for Strategic Analysis & Change Management and Talent Engagement & Development
Federal Cybersecurity Workforce Trends

Workforce Trends

1. Government work is increasingly knowledge work, requiring complex problem-solving and unpredictable application of skills
2. Jobs are becoming increasingly non-standard and complex
3. Employee expectations no longer always map to the 30-year federal career
4. Highly-competitive labor markets exist in which the Federal Government is only one employer

Practices to Revisit

1. Position classification from the first half of the 20th century cannot describe cybersecurity work or talent
2. Self-rating and brief interviews cannot measure cybersecurity expertise
3. Rigid, tenure-based approaches to pay and career progression are not competitive
# DHS Cybersecurity Talent Management System

## Background
Congress granted the Secretary broad authority to establish an alternative personnel system to recruit and retain cybersecurity talent

- Passed as part of the December 2014 Border Patrol Agent Pay Reform Act
- Broad authority with some restrictions and requirements, including producing regulation
- Similar language to authorities for personnel systems in Department of Defense and Intelligence Community

## Challenge
Simply eliminating a step in the hiring process or adding a pay grade will not make DHS competitive, especially given the global shortage for cybersecurity talent

- Department’s cybersecurity human capital challenges are about more than just pay
- The world of work—especially cybersecurity work—continues to evolve
- Conventional civil service approaches, including position-based hiring and pay, are showing their age

## Solution
DHS is preparing to launch the CTMS and Cybersecurity Service (DHS-CS) to better manage cybersecurity talent in the 21st century

- Modernize talent management to align to and keep pace with cybersecurity work
- Take a comprehensive, mission-focused approach to recruit and retain talent
- Understand and customize leading private and public sector practices for DHS

## Methodology
Sourced input from key DHS cybersecurity and human capital stakeholders + Reviewed all major federal personnel transformations since the 1970s + Benchmarked leading private sector practices, including those for hiring assessment and compensation + Engaged with human capital experts from the Office of Personnel Management and the Intelligence Community
Ken Vrooman, Senior Advisor

Cybersecurity and Infrastructure Security Agency

- Cyber Defense Education and Training sub-division
- Acting Branch Chief for the Curriculum, Evaluation and Support Branch
As the Nation’s Risk Advisor, CISA leads the effort to ensure there is an appropriate staffing of cybersecurity professionals to address the increasing demand of protecting the government, critical infrastructures, SLTT, and public/private partners.

To accomplish this, CISA is standing up the Cyber Defense Education & Training (CDET) Subdivision to consolidate and expand the agency’s ability to address this workforce shortage crisis.

**CDET Mission**

Educating the Nation to Address Cybersecurity Challenges

**CDET Vision**

Sustain an Adaptive Cybersecurity Workforce as a National Asset
NICE Framework is the Core

- **K-12**: 17 K-12 courses integrated across multiple disciplines to promote innovative learning.
- **CAE/SFS**: Knowledge units mapped to Framework competencies results in greater likelihood of success in future work.
- **PDs/workforce**: Suite of tools designed to increase efficiency and effective workforce planning and recruitment.
- **Training**: Training courses mapped to Framework for easier professional development.
- **National alignment**: Creates a standardized lexicon and understanding of work, competencies, and behavioral indicators.
## Feature: Building Teams with Work Roles

<table>
<thead>
<tr>
<th>Lifecycle Phase</th>
<th>Work Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td>Security Architect</td>
</tr>
<tr>
<td>Build</td>
<td>Software Developer</td>
</tr>
<tr>
<td>Deploy</td>
<td>Network Operations Specialist</td>
</tr>
<tr>
<td>Operate</td>
<td>Customer Support Specialist</td>
</tr>
<tr>
<td>Maintain</td>
<td>Database Administrator</td>
</tr>
<tr>
<td>Decommission</td>
<td>Communications Specialist</td>
</tr>
</tbody>
</table>
Feature: Building Teams with Competencies

• Example: Red Team
  – Competency: Engagement Planning
  – Competency: Rules of Engagement
  – Competency: Pen Testing
  – Competency: Data Collection
  – Competency: Vulnerability Exploitation
Q & A
Thank You for Joining Us!

**Upcoming Webinar:** *Educating Youth for a Cybersecurity Future*

**When:** Wednesday, September 16, 2020, at 2:00 p.m. EDT