National Initiative for Cybersecurity Education (NICE)
Workforce Framework for Cybersecurity

Danielle Santos, Karen Wetzel

March 10, 2022
NICE Strategic Plan and Implementation Plan (2021-2025)

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

Promote the Discovery of Cybersecurity Careers and Multiple Pathways

Transform Learning to Build and Sustain a Diverse and Skilled Workforce

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)

Drive Research on Effective Practices for Cybersecurity Workforce Development

www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
Expand Use of the (NICE Framework)

*Workforce Framework for Cybersecurity*

- Document and Disseminate Successful Uses
- Align NICE Framework with Other Cybersecurity and Privacy Guidance
- Establish a Process for Reviews and Updates
- Explore Tools to for Access and Interoperability
- Identify Work Subject to Automation
- Expand International Outreach
NICE Workforce Framework for Cybersecurity

✔ A common, consistent lexicon to clearly share information about cybersecurity work
✔ Direct information about what a workforce needs to know
✔ A workforce skilled in cybersecurity, not only a cybersecurity workforce
✔ Enables the establishment of regular processes
✔ For use in career awareness, education and training, hiring and career development, workforce planning and assessment
NICE Framework Evolution

- **2017**: NIST 800-181: A National Framework
  - What started as an effort to align the federal cyber workforce is intentionally expanded as a national framework.

- **2020**: NIST 800-181: First Revision
  - Name changed in recognition that cybersecurity is a concern across the workforce; other community-suggested adjustments streamline use and increase efficacy.

- **2021**: NICE Framework Data Review
  - Beginning of data review to align with the 2020 revision and TKS Authoring Guide; identifying and addressing gaps; and community engagement throughout.

- **2022**: Continued Growth
  - Competency areas list
  - Task review and alignment
  - Machine-readable
  - Public comments
  - Accessible platform

NIST 800-181: A National Framework

NIST 800-181: First Revision

NICE Framework Data Review

Continued Growth

NICE Framework Evolution
Flexibility
There is no one-size-fits-all solution to common challenges. The NICE Framework enables organizations to account for their unique operating context.

Agility
People, processes, and technology mature and must adapt to change. The NICE Framework enables organizations to keep pace with a constantly evolving ecosystem.

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

Modularity
In addition to cybersecurity, organizations manage other risks within the enterprise. The NICE Framework enables communication about these other workforces (e.g., privacy) within the enterprise and across sectors.
Where We Have Been...

- **Dec 2020**: Revised NICE Framework Published
- **Jan 2021**: NICE Framework Users Group, Success Stories Launched
- **Mar 2021**: TKS Authoring Guide, 1st Draft Competencies NISTIR
- **Mar – Aug 2021**: NICE Community Workshops: Competencies, Education/Training, OT, Awareness
- **Sep 2021 – Mar 2022**: KSA Statement Review & Updates
- **Dec 2021**: Request for Comments: 2nd Draft Competencies NISTIR, Public Comment Process, Refactored Ability Statements
- **Jan – Mar 2022**: Stakeholder Conversations
Where We Are Going.
NICE Framework: Updates

• December 2020: Revision
  – Workforce Framework for Cybersecurity
  – Introduction of Competencies
  – Deprecation of Ability Statements, Specialty Area

• March 2021: Draft Competencies NISTIR, List

• December 2021: Ability Statements Refactored

• March 2022: Knowledge and Skill Statement Updates

• Spring 2022: Work Roles & Categories

• Fall/Winter 2022: Tasks and K&S Alignment
NICE Framework: Why Competencies?

- **Evolving Recruiting Practices**
  - Shift from [only] degree-based to [also] competency-based hiring
  - Broader, more qualified applicant pool
  - Candidates for new and emerging technologies, threat vectors, capabilities

- **Assessment-based hiring and promotion**

- **Identify current gaps and anticipate future needs**

- **Align education and training to organizational goals**

NDAA Cybersecurity Proficiencies Report (June 2022)
- scope and sufficiency of current efforts
- recommend effective methods
Competency Areas
- Learner focused
- Help address employer needs
- Assessment is typically based on the area as a whole

Work Roles
- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the task level
NICE Framework Competency Areas

What are they?
Measurable clusters of related Task, Knowledge, or Skill (TKS) statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

✔ Title: Clearly signals the area that will be described.
✔ Description: Provides simple and clear language that focuses on the learner
✔ Associated TKS Statements

2nd Draft NISTIR 8355
NICE Framework Competencies: Assessing Learners for Cybersecurity Work
https://doi.org/10.6028/NIST.IR.8355-draft2
Identifying NICE Framework Competency Areas

01  2011 OPM Competency Model for Cybersecurity

02  Comparison to NICE Framework Work Roles & Specialty Areas

03  Review and alignment with CSF, RMF, certifications, & other related resources
NICE Framework: New Platform

Phase I:
• Browsable
• Searchable
• Exportable
• Machine-readable

Future Phases:
• Tool development and support
• Customizable
• Connection with other workforce frameworks, related NIST content (PWF, RMF, CSF, etc.)
• Integrated mappings (OPM codes, etc.)
NICE Framework: Public Commenting Tool

Who: Public stakeholders and subject matter experts
What: NICE Framework data
When: Open throughout the year; defined review and publication periods

- Additive to existing update processes (calls for comment, SME/stakeholder engagement, etc.)
- NIST principles for standards and guidelines development

Submission  Review  Sandbox  Release
What to Expect in 2022

- March: Knowledge and Skill statements out for comment
- April/May: Updated Competency Areas list for comment
- April/May: Cybersecurity awareness role for comment
- May/June: OT content integration for comment
- June: NDAA Proficiencies Report
- June: Updated Work Roles and Categories for comment
- June: Online platform (phase 1)
- Fall/Winter: Task review & TKS alignment
- Winter: Public comment platform
- 2022: Resource development
- 2022: Resource Center updates
NICE Framework Resource Center

Current Version & Latest Updates

- NIST Special Publication
- NICE Framework Data
- Supplemental Materials
  - Playbook for Workforce Frameworks
  - TKS Authoring Guide
  - Data Update Process (draft)

Tools

Resources by Audience

Example Applications and Uses
Example Applications and Uses

Success Stories

NICE FRAMEWORK SUCCESS STORY
Comic-EE
Secure Decisions
Cybersecurity Education and Evaluation

The voluntary Workforce Framework for Cybersecurity (NICE Framework) was developed through a collaborative process by industry, academic, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE
Secure Decisions was created as a division of Applied Visions, Inc. to conduct research and development and develop innovative technologies in cybersecurity, including application security, cybersecurity education, network defense, and infrastructure protection. Secure Decisions develops cutting-edge technologies focused on improving the human decision-making in cybersecurity. A small business based in Northport, NY, our cybersecurity education research projects have been funded by customers such as the U.S. Air Force Research Laboratory, U.S. Department of Homeland Security, and National Science Foundation.

DRIVERS
- Secure Decisions received a grant from Department of Homeland Security, Science & Technology Directorate, Cyber Security Division to create novel cybersecurity education technology. Our idea was to use graphic storytelling: creating branching web comics aligned with instructional goals: readers of the comic are asked to make choices for a character; these choices lead to different scenes that illustrate the consequences (good or bad) of that choice.
- To enable this approach, Secure Decisions created a lesson plan; visually laying out a storyboard of that script scene by scene; and, finally, converting the storyboards to full color comic panels and publishing the comics.
- Customers wanted to also use branching web comics to evaluate cybersecurity knowledge of the workforce. Comics need only an HTML5-compliant browser — no expensive labs, environments, or software for clients to download.

Framework in Focus Interviews

Comic-EE approach

Figure 1: Comic-EE approach

PROCESS
Comic-EE already used a hierarchical approach to scaffold authors through the process of creating a lesson plan, the first
NICE Interagency Coordinating Council
Open to all federal employees with responsibilities to grow and sustain the Nation’s cybersecurity workforce from the Executive Offices of the President and other federal departments, agencies, or bureaus

NICE Community Coordinating Council
Open to all public and private sector participants interested in pursuing actions that advance cybersecurity education, training, and workforce development.

– NICE Framework Feature (monthly meeting topic)
– NICE Framework Users Group

As needed meetings with stakeholders
International Engagement

Translations
• Spanish
• Portuguese
• Others in progress

Activities
• Ongoing meetings
• International Cybersecurity Competition and US Cyber Team
• Regional Initiative for Cybersecurity Education (RICET)
• George C Marshall Center: International Workshops on Cybersecurity Education and Workforce Development Capacity Building (2 workshops)
Other Ways to Get Engaged

**EVENTS**

- NICE Webinars (monthly)
- Annual NICE Conference & Expo (Jun 6-8 - Atlanta, GA)
- Cybersecurity Career Awareness Week (Oct 17-22)
- NICE K12 Cybersecurity Education Conference (Dec 5-7 - St. Louis, MO)
- Federal Cybersecurity Workforce Summit and Webinar Series (Apr 26)
- Federal Information Security Educators (FISSEA) (quarterly)

**FEEDBACK LOOPS**

- Public Comment Periods
- NICE Framework Users Group
Thank You

www.nist.gov/nice/framework

karen.wetzel@nist.gov
danielle.santos@nist.gov

Upcoming Webinar:

The NICE Framework at Work - Use Cases from Industry

March 16, 2022
2:00-2:25pm ET

nist.gov/nice/webinars