

# NICE Webinar Series

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



How You Can Influence an Update to the NICE Framework

December 3, 2019



**1.** Improves communication about how to identify, recruit, develop, and retain cybersecurity talent.

**2.** Categorizes, organizes, and describes cybersecurity work.

**3.** Can be used by educators, students, employers, employees, training providers, policy makers, and more.

**4.** [nist.gov/nice/framework](https://nist.gov/nice/framework)

Throughout the NIST SP 800-181, the NICE Framework, the combined terms “cybersecurity workforce” is shorthand for a workforce with work roles that have an impact on an organization’s ability to protect its data, systems, and operations.

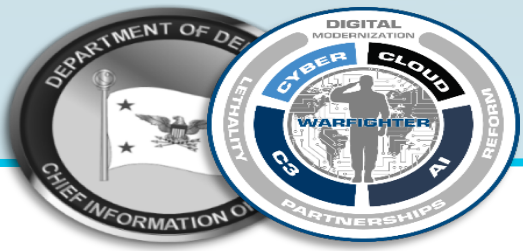
Action from the Report to the President on Growing and Sustaining the Nation’s Cybersecurity Workforce:

Action 1.3.3 To reduce confusion and ensure alignment, federal departments and agencies should strive to standardize around the use of a single definition of “cybersecurity workforce” based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.



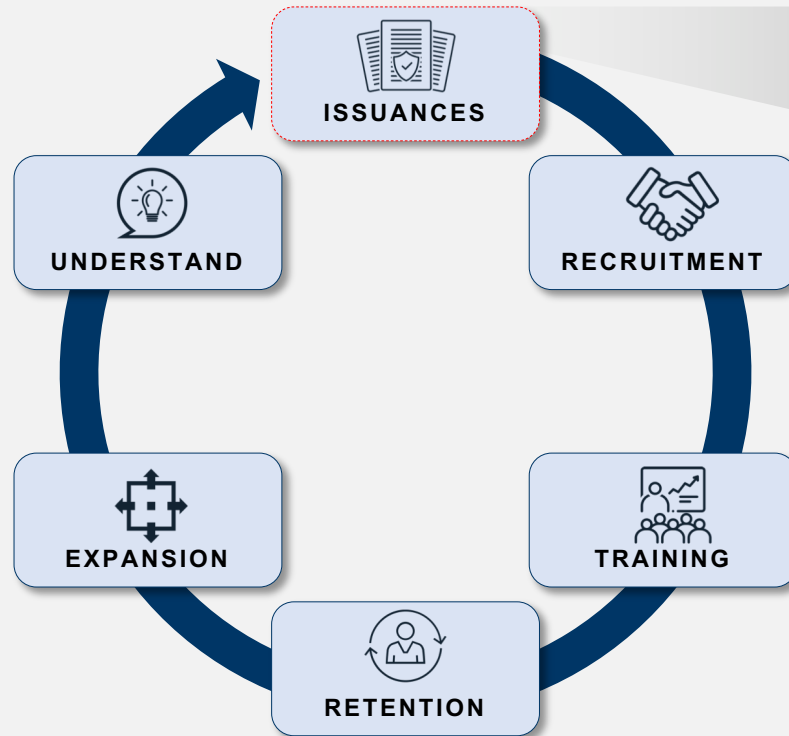
## Building Blocks for a Capable and Ready Cybersecurity Workforce





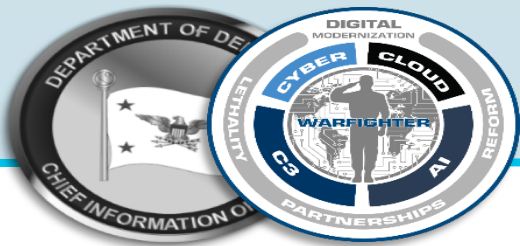
# DoD Cyber Strategy 2018 – Workforce Elements

The DoD Cyber Strategy 2018 serves as overarching guidance for transforming the Department's cyber capabilities. Line of Effort (LOE) 8 of the Strategy Implementation Plan is focused on sustaining a ready cyber workforce and includes nine objectives to recruit, develop, and retain cyber personnel in a competitive national environment.



**LOE 8-1:**  
Enhance cyber workforce capabilities to be come a more agile, lethal, and effective force

A critical workforce element of the DoD Cyber Strategy is LOE 8, objective 1, which requires the development of cyber workforce policies that provide guidance for the management of the DoD cyber workforce according to the DoD Cyber Framework (DCWF). The DCWF and 8140 policy series provide for the standardized, identification, tracking, development, qualification and reporting of the DoD cyber workforce.

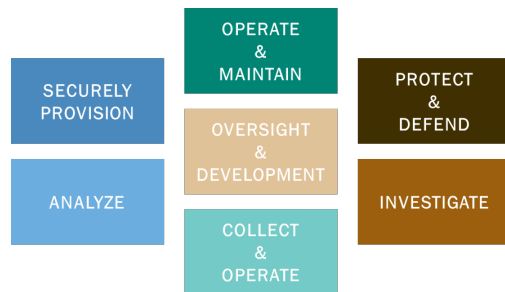


# DoD Cyber Workforce Framework (DCWF)

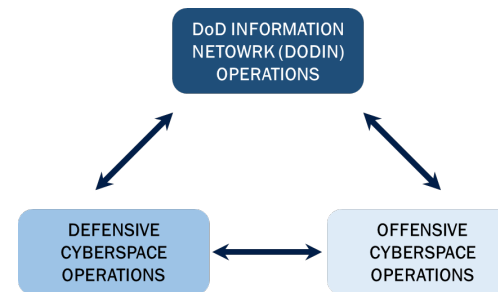
## OVERVIEW

- On behalf of the Department, the DoD CIO led the development of the DoD Cyber Workforce Framework (DCWF) to establish a authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator.
- The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Framework (NCWF) and the DoD Joint Cyberspace Training & Certification Standards (JCT&CS).
- The DCWF contains 54 work roles divided between 32 specialty areas which are organized within 7 distinct categories

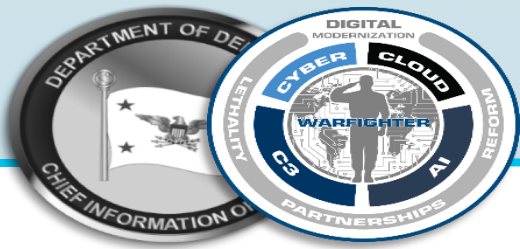
### NICE Cybersecurity Workforce Framework



### USCYBERCOM JCT&CS – JP 3-12 Lines of Operation



- ❖ The DCWF has been adapted at the national level in NIST Special Publication 800-181, and was used to develop an international framework under the North Atlantic Treaty Organization (NATO) Multinational Cyber Defense Training & Education Project.
- ❖ The DCWF is being used to facilitate the uniform identification, tracking, and reporting required by the Federal Cybersecurity Workforce Assessment Act (FCWAA); develop qualification requirements for cyber work roles outlined in DoD Manual 8140.XX; and support a number of other DoD-wide workforce management & planning activities.



# DoD 8140 Issuances: Policy to Enable Workforce

## DoD Cyber Strategy 2018 – LOE 8

### DoD Directive 8140.01

*Cyberspace Workforce Management*

- ❖ DoD Directive 8140, signed August 2015, establishes a definition for the cyber workforce and outlines Component roles and responsibilities for the management of the DoD cyber workforce.
- ❖ **NOTE: 8570.01-M is still in effect** until such a time as it is replaced.

### [DRAFT]: DoD Instruction 8140

*Cyberspace Workforce Identification, Tracking & Reporting*

**DoD Cyber Workforce Framework**  
(Authoritative Lexicon of Cyber Work Roles)

- ❖ DoD Instructions 8140 (*currently in draft*) will cover the identification, tracking, and reporting of the cyber workforce in accordance with the DCWF.

### [DRAFT]: DoD Manual – *Cyber Workforce Qualification and Management Program*

**Qualifications Model:** *Establishes qualification criteria for each DCWF work role.*

Education

Training

Certifications

On-the-Job  
Qualification

Continuous  
Professional  
Development



# NICE CYBERSECURITY WORKFORCE FRAMEWORK

Benjamin Scribner

Email: [Benjamin.Scribner@cisa.dhs.gov](mailto:Benjamin.Scribner@cisa.dhs.gov)

[niccs.us-cert.gov](https://niccs.us-cert.gov)



**CISA**  
CYBER+INFRASTRUCTURE

# Career information from the U.S. Department of Labor

The screenshot shows the O\*NET OnLine website. At the top left is the O\*NET logo and the text "O\*NET OnLine". To the right is an "Occupation Quick Search" bar. Below the logo are navigation links: "Help", "Find Occupations", "Advanced Search", "Crosswalks", "Share", and "O\*NET Sites". A large banner features a construction crane with the text "Build your future with O\*NET OnLine." and a "What is O\*NET?" button. Below the banner are three search options: "Occupation Search" with a search bar, "Find Occupations" with a "Browse" button, and "Advanced Search" with a "Browse by O\*NET Data" dropdown. On the right side, there are several promotional boxes: "What's New?" with a "Learn More" button, "I want to be a..." with a "Find It Now" button, "ATTN: VETERANS" with a "Get Started" button, and "Hot Technologies" with a "Learn More" button.

<https://www.onetonline.org/>

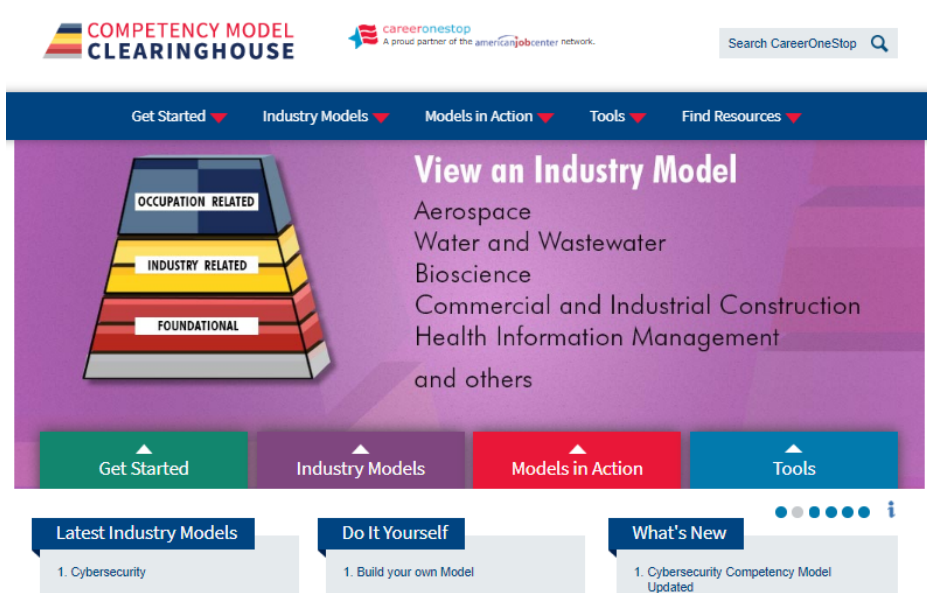
The screenshot shows the MY NEXT MOVE website. At the top is the "MY NEXT MOVE" logo and navigation icons for "HOME", "SEARCH", "INDUSTRIES", and "INTERESTS". The main heading is "What do you want to do for a living?". Below this is a row of three cards: "I want to be a..." with a "Search careers with key words" button, "I'll know it when I see it." with a "Browse careers by industry" button, and "I'm not really sure." with a "Tell us what you like to do" button. At the bottom, there are two more sections: "Still not sure? Check out careers in these groups:" with buttons for "Bright Outlook", "Interests", and "Job Prep"; and "Are you a veteran looking for work?" with a link to "My Next Move for Veterans".

<https://www.mynextmove.org/>

FIND THE APPRENTICESHIP THAT'S RIGHT FOR YOU [APPRENTICESHIP.GOV](https://www.apprenticeship.gov)

# Competency Model Clearinghouse

## 26 Sector-specific industry competency models



**COMPETENCY MODEL CLEARINGHOUSE**

careeronestop  
A proud partner of the americanjobcenter network.

Search CareerOneStop

Get Started Industry Models Models in Action Tools Find Resources

**View an Industry Model**

OCCUPATION RELATED  
INDUSTRY RELATED  
FOUNDATIONAL

Aerospace  
Water and Wastewater  
Bioscience  
Commercial and Industrial Construction  
Health Information Management  
and others

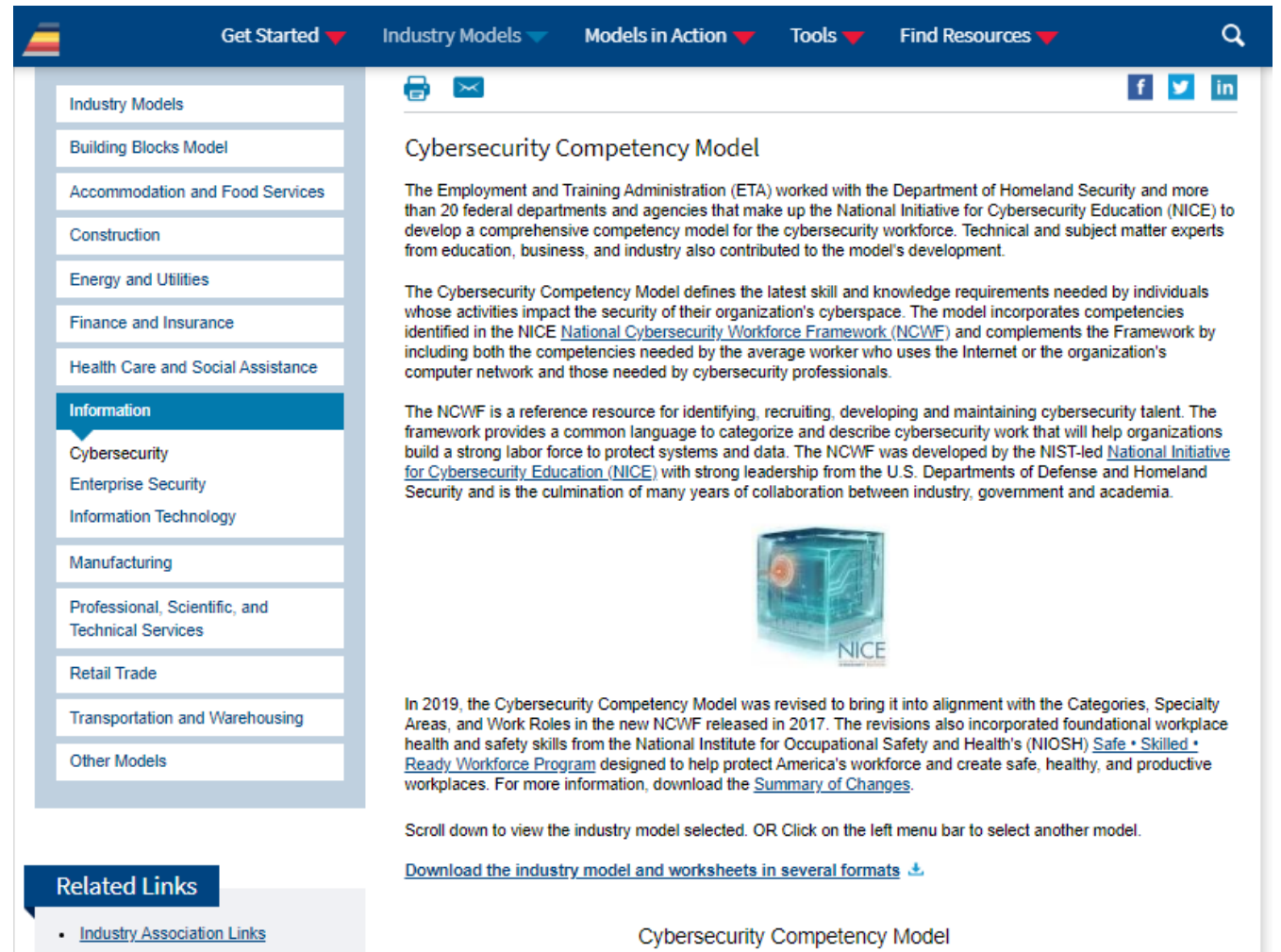
Get Started Industry Models Models in Action Tools

Latest Industry Models  
1. Cybersecurity

Do It Yourself  
1. Build your own Model

What's New  
1. Cybersecurity Competency Model Updated

[www.CareerOneStop.org/CompetencyModel](http://www.CareerOneStop.org/CompetencyModel)



Get Started Industry Models Models in Action Tools Find Resources

Industry Models

Building Blocks Model  
Accommodation and Food Services  
Construction  
Energy and Utilities  
Finance and Insurance  
Health Care and Social Assistance  
Information  
Cybersecurity  
Enterprise Security  
Information Technology  
Manufacturing  
Professional, Scientific, and Technical Services  
Retail Trade  
Transportation and Warehousing  
Other Models

**Cybersecurity Competency Model**

The Employment and Training Administration (ETA) worked with the Department of Homeland Security and more than 20 federal departments and agencies that make up the National Initiative for Cybersecurity Education (NICE) to develop a comprehensive competency model for the cybersecurity workforce. Technical and subject matter experts from education, business, and industry also contributed to the model's development.

The Cybersecurity Competency Model defines the latest skill and knowledge requirements needed by individuals whose activities impact the security of their organization's cyberspace. The model incorporates competencies identified in the NICE [National Cybersecurity Workforce Framework \(NCWF\)](#) and complements the Framework by including both the competencies needed by the average worker who uses the Internet or the organization's computer network and those needed by cybersecurity professionals.

The NCWF is a reference resource for identifying, recruiting, developing and maintaining cybersecurity talent. The framework provides a common language to categorize and describe cybersecurity work that will help organizations build a strong labor force to protect systems and data. The NCWF was developed by the NIST-led [National Initiative for Cybersecurity Education \(NICE\)](#) with strong leadership from the U.S. Departments of Defense and Homeland Security and is the culmination of many years of collaboration between industry, government and academia.

In 2019, the Cybersecurity Competency Model was revised to bring it into alignment with the Categories, Specialty Areas, and Work Roles in the new NCWF released in 2017. The revisions also incorporated foundational workplace health and safety skills from the National Institute for Occupational Safety and Health's (NIOSH) [Safe • Skilled • Ready Workforce Program](#) designed to help protect America's workforce and create safe, healthy, and productive workplaces. For more information, download the [Summary of Changes](#).

Scroll down to view the industry model selected. OR Click on the left menu bar to select another model.

[Download the industry model and worksheets in several formats](#)

**Related Links**

- [Industry Association Links](#)

Cybersecurity Competency Model

# The Occupational Information Network (O\*NET) is an *entry-point* into the *World of Work*

- Descriptive career and occupational information resource
- Provides comprehensive coverage of over 900 occupations across all sectors of the economy
- Includes Knowledge, Skills, Abilities, Tasks, and Detailed Work Activities (along with other descriptors)
- O\*NET websites are used by tens of millions of users annually

# The value of links from DOL information to more detailed frameworks

We seek increased linkages and interoperability between systems like O\*NET and industry competency models to even more detailed sector-specific systems, such as the NICE Cybersecurity Framework

- For when learners and job-seekers move *beyond* the entry point of a career to being serious about a specific field and job, such as one in cybersecurity

# 3 new Cyber occupations will be included in O\*NET in the November 2020 release

## Corresponding to 3 Work Roles from the NICE Cybersecurity Framework

- 15-1299.04 Penetration Testers
- 15-1299.06 Information Security Engineers
- 15-1299.06 Digital Forensics Analysts

The screenshot shows the 'MY NEXT MOVE' website page for 'Information Security Analysts'. The page includes a navigation bar with 'HOME', 'SEARCH', 'INDUSTRIES', and 'INTERESTS' icons. Below the title, there is a 'Print' and 'Share' button. A 'Watch Career Video' button is also present. The main content area is divided into several sections: 'What they do', 'On the job, you would', 'KNOWLEDGE', 'SKILLS', 'ABILITIES', 'PERSONALITY', and 'TECHNOLOGY'. Each section contains a list of specific tasks, skills, or knowledge areas relevant to the occupation.

**MY NEXT MOVE** o-net in-it

**Information Security Analysts** Print Share

**Also called:** Information Security Officer, Information Systems Security Officer, Information Technology Specialist, Network Security Analyst

[Watch Career Video](#)

**What they do:**  
Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.

**On the job, you would:**

- Develop plans to safeguard computer files against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs.
- Monitor current reports of computer viruses to determine when to update virus protection systems.
- Encrypt data transmissions and erect firewalls to conceal confidential information as it is being transmitted and to keep out tainted digital transfers.

**KNOWLEDGE**

- Engineering and Technology**
  - computers and electronics
  - product and service development
- Arts and Humanities**
  - English language
- Business**
  - management
  - customer service
- Communications**
  - telecommunications

**SKILLS**

- Basic Skills**
  - reading work related information
  - thinking about the pros and cons of different ways to solve a problem
- Problem Solving**
  - noticing a problem and figuring out the best way to solve it
- People and Technology Systems**
  - figuring out how a system should work and how changes in the future will affect it
  - thinking about the pros and cons of different options and picking the best one

**ABILITIES**

- Verbal**
  - listen and understand what people say
  - read and understand what is written
- Ideas and Logic**
  - make general rules or come up with answers from lots of detailed information
  - notice when problems happen
- Visual Understanding**
  - see hidden patterns
  - quickly compare groups of letters, numbers, pictures, or other things

**PERSONALITY** **TECHNOLOGY**

People interested in this work like activities that include **data\_detail**. You might use software like this on the job:

# Q & A

# NICE Cybersecurity Workforce Framework Resource Center

## Introducing a new website!

...to help provide information and resources on consulting and implementing a national-focused resource that categorizes and describes cybersecurity work.

[nist.gov/nice/framework](https://nist.gov/nice/framework)

**NIST**  
Applied Cybersecurity Division / National Initiative for Cybersecurity Education (NICE)

### NICE CYBERSECURITY WORKFORCE FRAMEWORK RESOURCE CENTER

The NICE Cybersecurity Workforce Framework is a national-focused resource that categorizes and describes cybersecurity work.

- About
- Current Version
- Resources
- Uses
- Related Programs

CONNECT WITH US

**REQUEST for COMMENTS**

The public is invited to provide comments by Jan. 13, 2020, for consideration in planned updates to the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181.

[Learn More](#)

The NICE Cybersecurity Workforce Framework (NICE Framework), [NIST Special Publication 800-181](#), is a national-focused resource that categorizes and describes cybersecurity work. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. The NICE Framework is intended to be applied in the public, private, and academic sectors.



NICE Framework For...



# Review and Updates to the NICE Cybersecurity Workforce Framework



**We're seeking input on updates to the  
NICE Cybersecurity Workforce Framework**

*Improvements to the NICE Framework*

*Awareness, Applications, and Uses of the NICE  
Framework*

---

The public is invited to provide  
input by January 13, 2020.

[NICEFramework@nist.gov](mailto:NICEFramework@nist.gov)

See Full Announcement

## Improvements to the NICE Framework (12)

- Components that have been most useful and why
- Components that should be static v. dynamic
- Changes to scope and major components
- Benefits or challenges in using the NICE Framework with other standards or resources

## Awareness, Applications, and Uses of the NICE Framework (10)

- How you learned about the NICE Framework
- How you are using or referencing the NICE Framework
- Tools and Resources that have been created
- Tools and Resources that are needed

[See Full Announcement](#)

# Timeline for Review and Updates to NICE Framework

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  
*June 2020*



Announcement of Request for Comments  
*November 2019*



Request for Comments Deadline  
*January 2020*



Consultative Process  
*March-May 2020*



Final Draft of Changes  
*November 2020*



Updates to Tasks, Knowledge, Skills, and Abilities , *November 2019-2021*



**NICE** | Conference  
and Expo  
**2020**



**SAVE  
THE  
DATE**

Hilton Atlanta  
November 16-18, 2020

Hosted by

**FIU** | FLORIDA  
INTERNATIONAL  
UNIVERSITY

 **NEW  
AMERICA**

# Timeline for Review and Updates to NICE Framework

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  
*June 2020*



Announcement of Request for Comments  
*November 2019*



Request for Comments Deadline  
*January 2020*



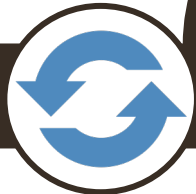
Consultative Process  
*March-May 2020*



Final Draft of Changes  
*November 2020*



Updates to Tasks, Knowledge, Skills, and Abilities , *November 2019-2021*



# Q & A

# Thank You for Joining Us!

**Upcoming Webinar:** Shopping Safely Online and the Work of Cybersecurity Awareness and Behavior Change

**When:** December 18, 2019 at 2pm EST

**Register:** <https://nist-nice.adobeconnect.com/webinardec19/event/registration.html>

[nist.gov/nice/webinars](https://nist.gov/nice/webinars)