

# CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER



01000011  
01011001  
01000010  
01000101  
01010010

## Report Roundup Learning from Good Ideas



***The State of Cybersecurity Education in K-12 Schools***

JULY 2020

# Building a Cybersecurity Workforce

## Educational Resources and Professional Development

- CYBER.ORG courses integrate foundational concepts like **programming, cyber hygiene, and security vulnerabilities** into core STEM classes and specialized cyber pathways
- Students from CYBER.ORG partner schools were **4 times** more likely to **pursue a cyber degree program**
- **92%** of active CYBER.ORG teachers said that the program is effective at **helping students understand cyber career pathways**
- **93%** of active CYBER.ORG teachers said that the program was **effective in promoting student achievement**
- Classroom teachers as force multipliers, training them to build the cybersecurity workforce of the future.



*"[Using the curricula], our instructional teams have worked to embed **real-world cybersecurity topics and careers** within our core curriculum – across all subject areas."*

- Middle School Principal

**19,700+**

TEACHERS ACCESSING CURRICULA  
SINCE 2014

**20**

CYBER-INTEGRATED K-12 COURSES  
DEVELOPED  
SINCE 2012

**13,630**

TEACHERS TRAINED SINCE 2015

**432**

TEACHER EVENTS LED SINCE 2015

**61%**

TEACHER PARTICIPANTS FROM TITLE  
1 SCHOOLS



**CYBER.ORG**

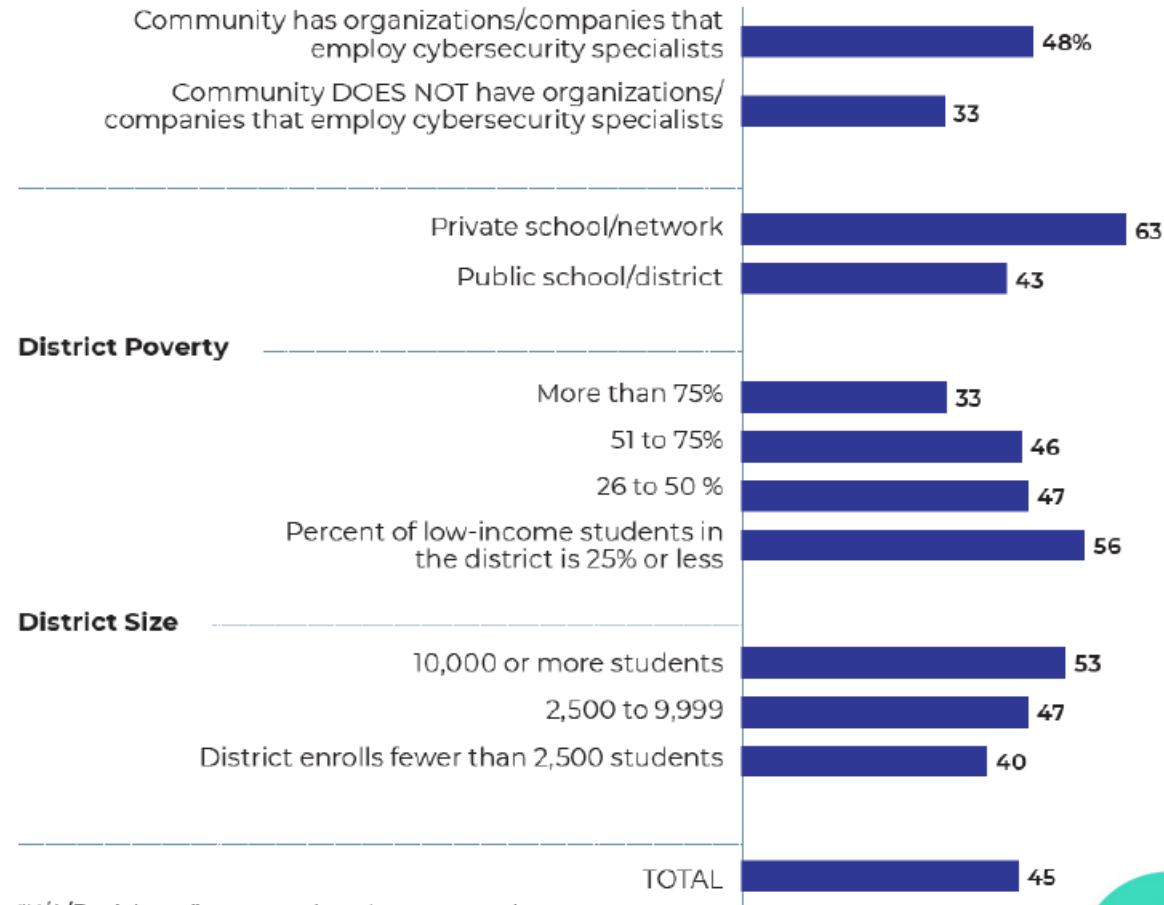
# CYBER.ORG: Building a Cybersecurity Workforce

## Key Findings

### Key Take-Aways

- Less than half of educators surveyed (45%) say students are taught cybersecurity;
- Access to cybersecurity education resources is not consistent across communities and educational settings;
- Cybersecurity education is more available to the higher socioeconomic regions of the country, leaving out students in rural, low-income areas.

### Percent of survey respondents who say their students currently receive cybersecurity education



"N/A/Don't know" responses have been removed.



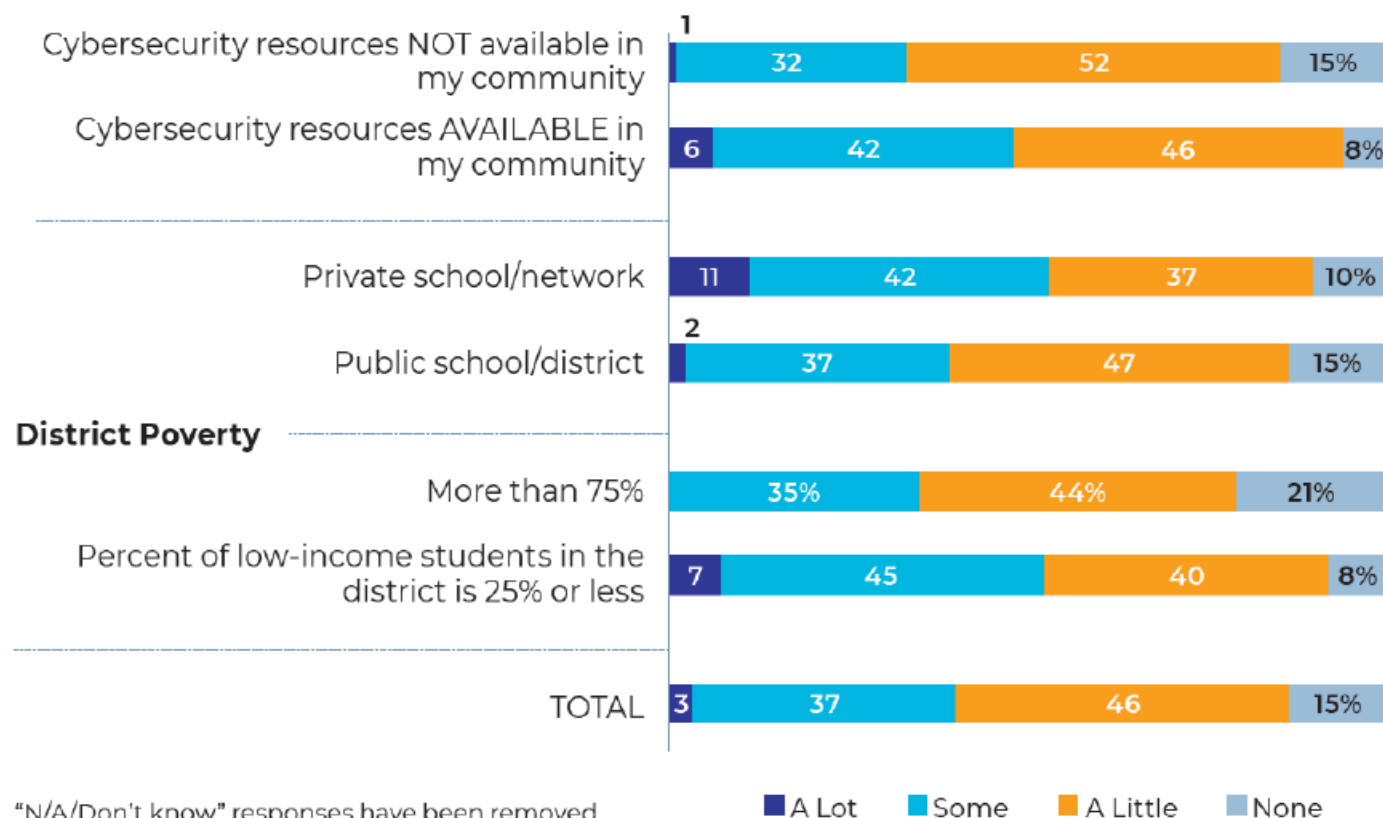
# CYBER.ORG: Building a Cybersecurity Workforce

## Key Findings

### Key Take-Aways

- Most students know little or nothing about Cybersecurity;
- Student and educator knowledge of cybersecurity are correlated;
- Disparity of cybersecurity educational opportunities is significant, exponential in cybersecurity deserts.

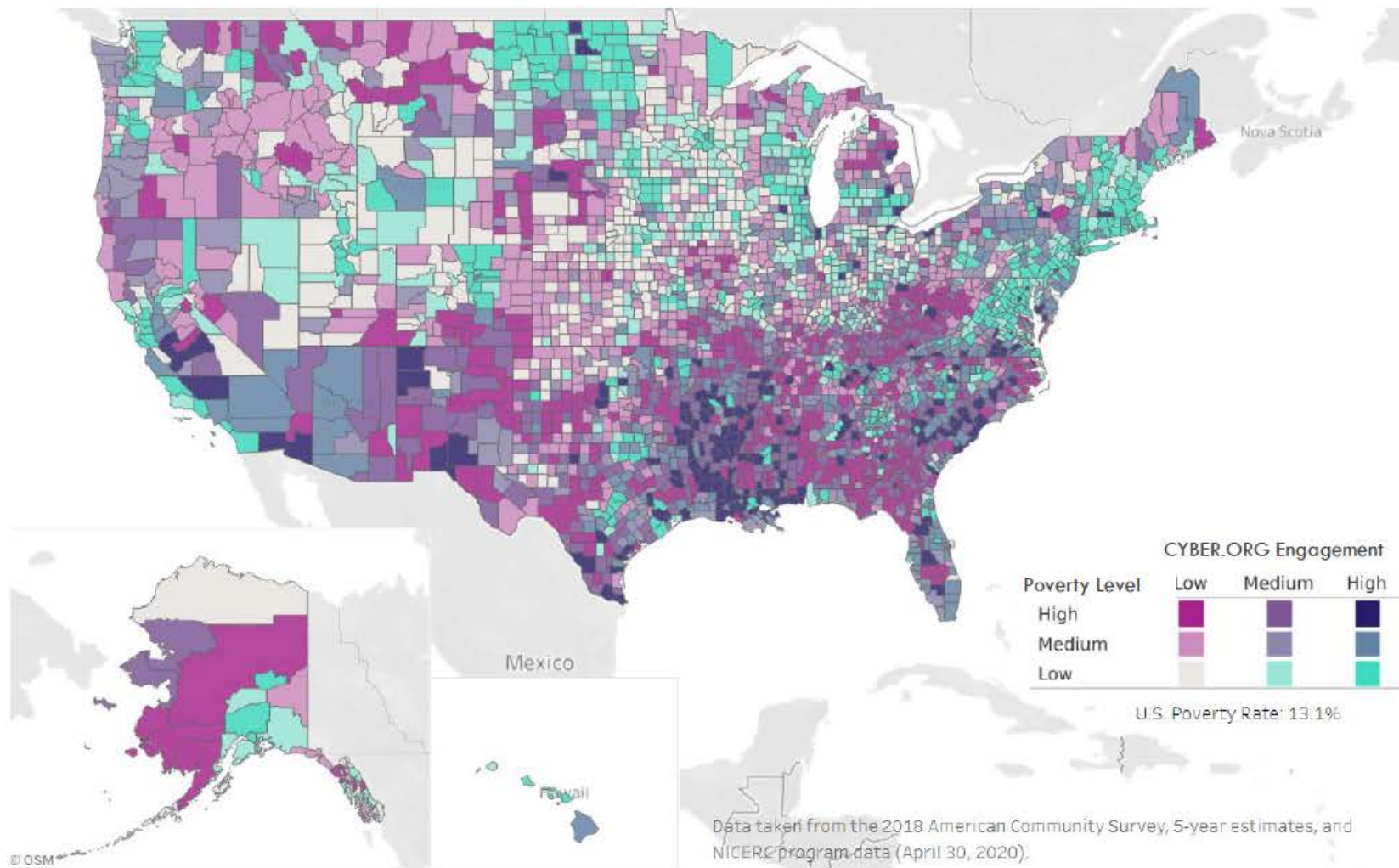
### How much do your students know about cybersecurity education?





# CYBER.ORG

## Impact Compared to Socioeconomic Level



# CYBER.ORG: Building a Cybersecurity Workforce

## Calls to Action



- Ensuring access to cybersecurity education in cybersecurity deserts;
- Raising basic levels of knowledge about cybersecurity education;
- Increasing the number of schools offering cybersecurity education;
- Enhancing educational offerings;
- Informing students about cybersecurity careers.



# CYBER.ORG

THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER



01000011  
01011001  
01000010  
01000101  
01010010

<https://cyber.org/stateofcybersecurity>



**Kevin Nolten**

CYBER.ORG

[Kevin.Nolten@cyber.org](mailto:Kevin.Nolten@cyber.org)



*Safa Shahwan Edwards*  
*Associate Director, Cyber Statecraft Initiative*  
*Program Director, Cyber 9/12 Strategy Challenge*



# About Cyber 9/12

- Established in 2012
- Cyber crisis simulation and scenario exercise



# About Cyber 9/12

- Tackle cyber skills shortage
- Diversity challenges
- Competitions in 5 countries
- NextGen Fund



# Connections to NICE Strategic Plan

- Pursue Action
- Challenge Assumptions
- Stimulate Innovation
- Foster Communication
- Facilitate Collaboration
- Model Inclusion

# NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES (NICCS)



Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020



# About NICCS

Since 2013, NICCS has been a national hub for cybersecurity education, careers, and training.

NICCS provides tools and resources for current and future cybersecurity professionals to ensure the nation's workforce has the appropriate training and education in the cybersecurity field.

Our offerings are mapped to the [National Initiative for Cybersecurity Education \(NICE\) Cybersecurity Workforce Framework](#).



Official website of the Cybersecurity and Infrastructure Security Agency [Here's how you know](#)

**NICCS™**  
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Training ▾ Formal Education ▾ Workforce Development ▾ About NICCS ▾ | 🔍



**Women In Cybersecurity**

Training Catalog



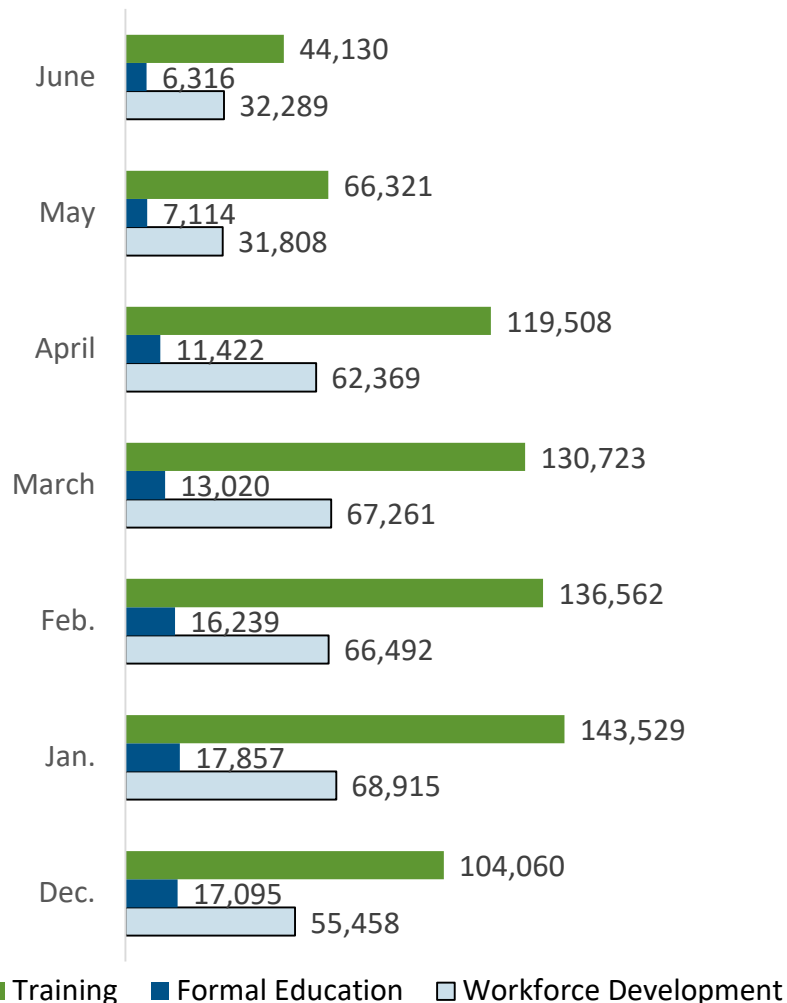
The NICCS Training Catalog provides a robust listing of cybersecurity and cybersecurity-related training courses offered in the U.S. The Training Catalog contains over 5,000 courses, with more courses being added every day!

[Read More](#)

Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020

# NICCS Pageviews by Website Sections June 2020

## Main Section: Page views



## TRAINING – 44,130

### TOP 5 Training Pageviews

5,400	NICCS Education and Training Catalog landing page
4,381	Training Landing page
4,380	FedVTE page
1,696	Veterans
914	McAfee Institute Course – Certified Open Source Intelligence

## FORMAL EDUCATION – 6,316

### TOP 5 Formal Education pageviews

2,153	Students, Launch your Cyber Career page
1,541	CyberCorp: Scholarship for Service page
1,467	Cybersecurity in the Classroom page
761	National Centers of Academic Excellence (CAE) page
350	Formal Education landing page

## WORKFORCE DEVELOPMENT – 30,033

### TOP 5 CONTENT Workforce Development Pageviews

8,978	NICE Cybersecurity Workforce Framework landing page
1,689	NICE Cybersecurity Workforce Framework Work Roles page
1,005	NICE Framework Mapping Tool page
910	Cybersecurity Resources page
742	Workforce Development landing page

Mauro  
Training  
Agency  
2020

# NICCS Top Content Searches/Downloads June 2020

## TRAINING

### TOP 5 TRAINING COURSES SEARCHED

916	Certified in Open Source Intelligence (C OSINT) (McAfee Institute)
626	Certified Digital Forensics Examiner (CDFE) (Mile2)
615	Cybersecurity Fundamentals Online Course (ISACA)
562	HIPAA Compliance Officer Training Certified HIPPA Privacy Security Expert (Supremus Group)
557	ASAE v2.0 – ASA Essentials v2.0 (Global Knowledge)

## FORMAL EDUCATION

### TOP 5 CYBER CAREER PROFILES SEARCHED

263	Vulnerability Assessment Analyst
212	Information Systems Security Manager
209	Cyber Forensics Expert
196	Cryptographer
188	Cyber Security Engineer

## Downloads

### TOP 5 DOWNLOADED RESOURCES

1,054	FedVTE Veterans Cybersecurity Guide_20190531
343	Cybersecurity Workforce Development Toolkit
332	Using the NICE Framework
263	Vulnerability Assessment Analyst
225	FedVTE Championcommsmanual

## WORKFORCE DEVELOPMENT NICE CYBERSECURITY WORKFORCE FRAMEWORK

### TOP 5 SPECIALITY AREAS SEARCHED

736	Digital Forensics
700	All Source Analysis
517	Cyber Investigation
507	Cyber Defense Analysis
454	Cybersecurity Management

### TOP 5 WORK ROLES SEARCHED

233	Cyber Defense Analyst
100	Cyber Defense Forensics Analyst
99	Cyber Defense Incident Responder
93	Information Systems Security Manager
88	Vulnerability Assessment Analyst

Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020



# NICCS – Education and Training Catalog

The [NICCS Education and Training Catalog](#) is a central location where the public can access over 5,000 cybersecurity focused courses. These courses are delivered by accredited universities, [National Centers of Academic Excellence](#), federal agencies, and other training providers.

Each course is mapped to the [NICE Cybersecurity Workforce Framework](#), which was developed to encourage a cybersecurity workforce standard.

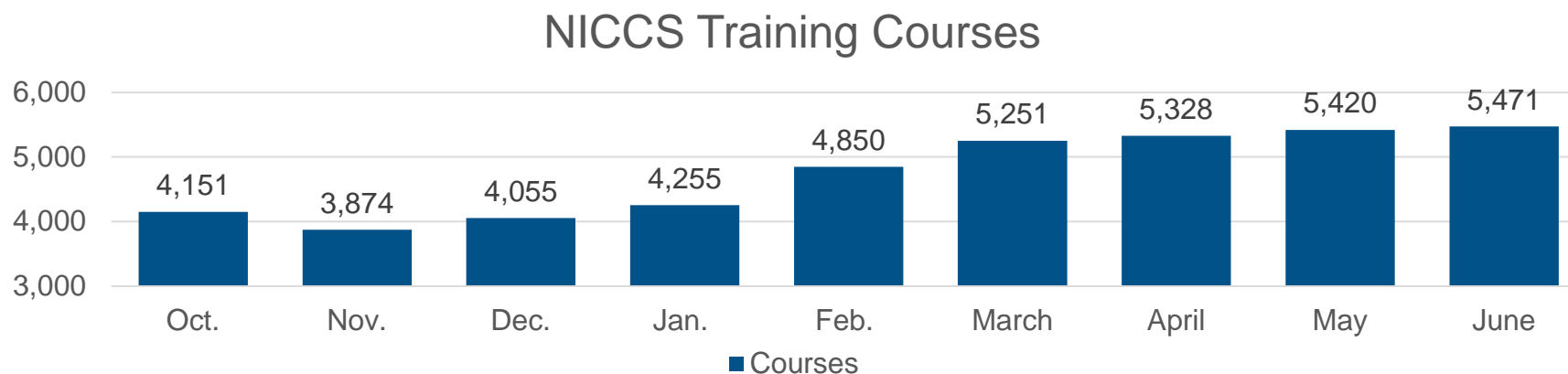
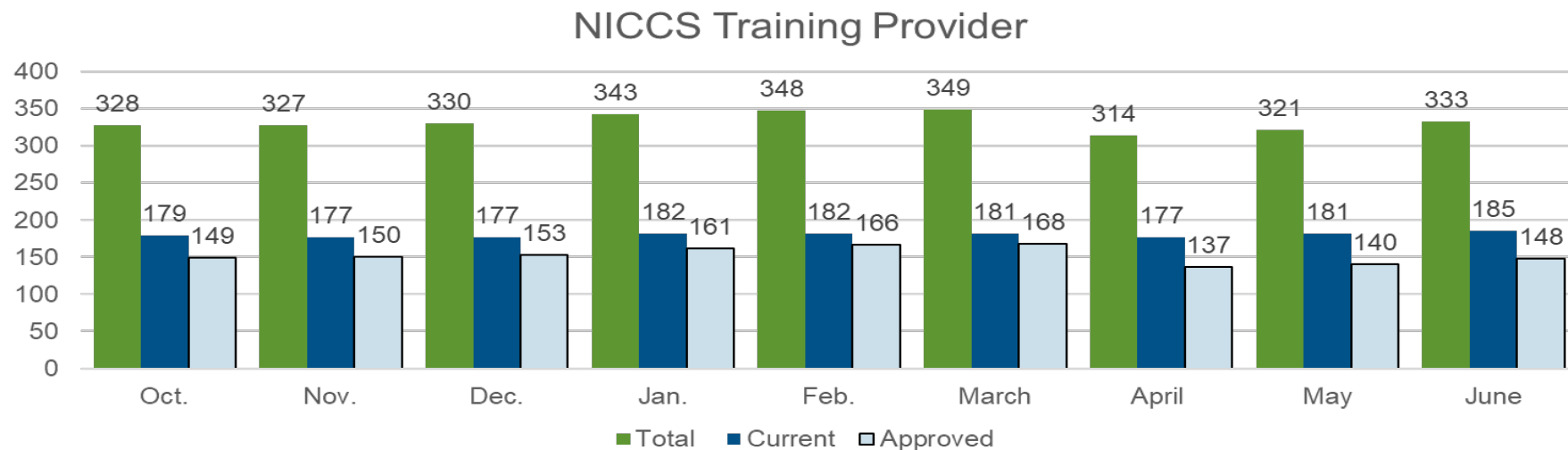


A screenshot of the NICCS Education and Training Catalog website. The header includes the NICCS logo and navigation links for Training, Formal Education, Workforce Development, and About NICCS. The main content area is titled "NICCS Education and Training Catalog" and includes a "Become a Provider" button. Below this is a map of the United States with yellow circles indicating the number of courses available in various regions. A search bar is located below the map, with fields for Keyword, Location (Zip Code, City, State or Address), and Distance (Enter miles). There are also dropdown menus for Specialty Area, Provider, and Proficiency Level, and checkboxes for National CAE Designated Institution and Available Delivery Methods (Classroom, Online, Instructor-Led, Online, Self-Paced). A "Search" button is at the bottom of the search section.

Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020



# NICCS – Training Catalog Metrics



# NICCS – Training Catalog Metrics

As of June 2020

## TOP TRAINING PROVIDERS VIEWED

- McAfee Institute
- Mile2
- FedVTE
- itSM Solutions LLC
- Lunarline Inc.

## TOP 5 TRAINING COURSES VIEWED

- Certified in Open Source Intelligence (C|OSINT) (McAfee Institute)
- Certified Digital Forensics Examiner (CDFE) (Mile2)
- Cybersecurity Fundamentals Online Course (ISACA)
- HIPAA Compliance Officer Training Certified HIPPA Privacy Security Expert (Supremus Group)



Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020

# NICCS – Cyber Career Pathways Tool

The [Cyber Career Pathways](#) tool presents a new and interactive way to explore work roles within the NICE Cybersecurity Workforce Framework.

This tool will:

- depicts the cyber workforce according to five distinct, yet complimentary skill communities.
- highlights core attributes among each of the 52 work roles, the foundational units of job descriptions in the NICE Framework
- offers actionable insights for employers, professionals, and individuals considering a career in cyber.



NICCS™  
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Official website of the Cybersecurity and Infrastructure Security Agency [Here's how you know](#)

Training ▾ Formal Education ▾ Workforce Development ▾ About NICCS ▾

[Home](#) » [Workforce Development](#) » Cyber Career Pathways

## Cyber Career Pathways

Welcome to the Cyber Career Pathways tool!

This tool presents a new and interactive way to explore work roles within the NICE Cybersecurity Workforce Framework. It depicts the Cyber Workforce according to five distinct, yet complimentary skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber.

To start, select a work role below, or enter keywords in the search bar.

**All** Core Relationships  
Toggle the top 5 relationships based on all or core shared Tasks and KSAs.

Select a work role ▾  
Begin typing to search work role names.

The diagram illustrates the Cyber Workforce as a large oval containing five overlapping circles representing skill communities: IT (blue), Cybersecurity (green), Cyber Effects (orange), Intel (Cyber) (yellow), and Intelligence (grey). Below these circles is a purple bar labeled "Cross Functional" containing four boxes: Lifecycle Management, Talent Management, Strategic Management, and Legal/Law Enforcement. An information icon (i) is located in the top right corner of the diagram area.

Nancy Limauro  
Cyber Defense Education and Training  
Cybersecurity and Infrastructure Security Agency  
July 22, 2020



**CISA**  
CYBER+INFRASTRUCTURE



## Successful Strategies for Cybersecurity Hiring: for Human Resources and hiring professionals

The [shortage of cybersecurity talent](#) can make it challenging for organizations and Human Resource departments to hire and retain a skilled cybersecurity workforce. Additionally, organizations need to build a human capital pipeline that brings new candidates into the field, and [increases representation from under-represented populations](#). Adoption of one or more of the following strategic concepts may allow a hiring manager to reduce time-to-hire, identify gaps in their cybersecurity workforce, develop career pathways and diversify their teams. Resources for a deeper understanding of these ideas may be found on the reverse of this document.

### Assess the Current Cybersecurity Environment

Every individual has a work role in organizational cybersecurity. Organizations can use the NICE guidebook, [Cybersecurity is Everyone's Job](#) to identify work roles by business function, defining each role and function as a part of the cybersecurity workforce.

Use Knowledge, Skills and Abilities tools, like the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce [Framework](#), the Department of Labor's [O\\*Net](#) tool and the [Cyberseek.org](#) website to evaluate workforce needs. This may help to improve the overall understanding of cybersecurity work in an organization.

Create a demographic profile of the cybersecurity workforce and determine if staffing is designed to support diversity objectives. Assess the time it takes to hire new personnel (time-to-hire) and annual retention rates. Evaluate salaries, using tools like the Department of Labor [BLS Wage](#) data by Area and Occupation, against competitive data for the local job market and national averages.

### Review Job Requirements

Using the NICE Framework, describe the necessary Tasks, and related Knowledge, Skills and Abilities to build job descriptions aligned to business needs. [Organizations](#) are re-evaluating requirements such as college degrees, advanced certifications and experience requirements that might unnecessarily discourage otherwise qualified talent from applying or being considered. [The U.S. Bureau of Labor Statistics](#) uses a system to assign categories for entry-level education, work experience in a related occupation, and typical on-the-job training to each occupation.

### Standardize Cybersecurity Job Titles

Cyber Threat Hunter? Information Security Analyst? Job titles are different across industry, academia, and government. The NICE Cybersecurity Workforce Framework and the Department of Labor's O\*Net tool can help provide some examples; review the Cyberseek website to see other common titles in use.

### Remove Hidden Bias in Position Descriptions and Hiring

Seek to [remove language from job advertising and position descriptions](#) that may discourage [diverse candidates](#) from applying for open positions, i.e. the use of masculine gendered nouns or references to military-style approaches. This can be difficult to recognize without guidance from experts or the use of text-based tools that both spot biased or coded terminology and offer suggestions to use in their place.

[SHRM.org](#) identifies masking strategies and blind interview steps to strip identifying information from resumes and job applications before sharing with the hiring teams. Invite a diverse team from across your organization to assist in panel-style reviews of candidates.

#### Be [Candidate Centric](#) in Hiring

Make the application process a candidate-centric experience. Consider posting information on your Career portion of the organization website that describes the steps in the hiring process, what interactions the candidate may expect to have, examples of interview questions per department or position. Ask for and include anonymized candidate feedback.

#### Screen for Talent with Aptitude or Skill Assessment Tools

##### [Critical Thinking](#)

Critical Thinking Asking Who, What, When, Where, Why and How questions, at the appropriate level can help candidates show analytical, interpretation, evaluation, problem solving and communication skills.

#### Interviewing CyberSecurity candidates

Finding the right candidate for cybersecurity positions can be a challenge. HR managers and IT professionals can work together to balance performance-based questions with education, skills and organizational culture assessments.

Verbal and Written communication skills assessment: Re-evaluate the importance of soft skills in cybersecurity positions. Interviews should allow candidates to display [soft skills](#) as well as hard skills.

*Ex question:* Can you give an example of how you explained a technical problem to a non-technical person?

[Unicorns](#) are rare—don't build job descriptions and interviews based on all or nothing criteria. Guidelines like the Aspen CyberSecurity Groups [Principles](#) for Growing and Sustaining the Nation's Cybersecurity Workforce, offer insights and guidelines to help build organizational pipelines for the cybersecurity workforce.



**THE 2020 NICE K12 CYBERSECURITY EDUCATION  
VIRTUAL CONFERENCE**

**CONFERENCE MOVED TO VIRTUAL EVENT:** In an effort to be mindful of the disparate impacts of COVID-19, and based on the conference's continued commitment to equity and inclusion, the 2020 NICE K12 Cybersecurity Education Conference will be reimagined to bring the community spirit and networking energy to an inspiring and engaging online space.

**AGENDA & PRESENTERS:** Proposal review sub-committee in process of ranking proposals. Presenter roster & draft agenda is in process.

**COMMITTEE & SUB-COMMITTEE:** Working to plan engagement & networking activities.

**REGISTRATION DATE & PRICE:** Tentative early bird registration AUGUST 18. Tickets will be \$150 early bird, \$175 regular price

**CONFERENCE VIRTUAL PLATFORM:** Narrowed down to either Whova or Socio.

**Join the event email list for announcements:**

**[k12cybersecurityconference.org](https://k12cybersecurityconference.org)**