Welcome!

Schedule for the Session

10 min: Introduction and Welcome

- Introduction
- Welcome

20 min: Topic Presentation

- Presentation by RTI and NCSES: Defining the Cybersecurity Workforce

25 min: Small Group Discussions

- Breakout discussions

5 min break

25 min: Panel Discussion

- Rodney Petersen from the National Institute of Standards and Technology
- Marinda Hamann from ISC2
- Melissa Dark from Dark Enterprises

20 min: Q&A with Panel and NCSES

5 min: Concluding Remarks

Logistics

- We will have two opportunities for your input
  - o Small group sessions
  - o Q&A using the Zoom function
- We will be collecting transcripts from the small group sessions
- This presentation is being recorded and will be made available publicly on the CWDI website
  - o Recording + Slides will be on website
- We will be monitoring for and removing bots and AI notetakers.

Introduction to The Cybersecurity Workforce Data Initiative Workshop 1: Definitions

John Finamore
Chief Statistician
National Center for Science and Engineering Statistics
U.S. National Science Foundation

Cybersecurity
Workforce
Data Initiative

RTI INTERNATIONAL

National Center for Science and Engineering Statistics

Measuring America's progress in science, technology, and innovation

Part of the National Science Foundation (NSF)

One of 13 principal federal statistical agencies

Overseen by the U.S. Chief Statistician within the Office of Management and Budget (OMB)

MANDATE

Serve as a central **Federal clearinghouse** for the collection, interpretation, analysis, and dissemination of **objective data** on the **U.S. science and engineering enterprise**

Section 505 of the America COMPETES Reauthorization Act of 2010

Why a working definition of the cybersecurity workforce is necessary and complicated

- The CHIPS and Science Act of 2022 section 10317
- Numerous frameworks and definitions of the cybersecurity workforce exist
- Cybersecurity activities span a range of work roles, occupations, and industries

Goals of today's workshop

1. Hear the CWDI's proposed definition of the cybersecurity workforce
2. Discuss the working definition
3. Connect with other organizations working to advanced the cybersecurity workforce
4. Provide feedback to the CWDI to inform our determination of an appropriate and feasible approach to measuring the cybersecurity workforce

Cybersecurity Workforce Data Initiative Workshop I Defining the Cybersecurity Workforce

May 7, 2024

Michael Hogan

Economist, RTI International

NSF NCSES Cybersecurity Workforce Data Initiative

RTI INTERNATIONAL

About Us

RTI is an independent nonprofit research institute dedicated to improving the human condition.

RTI Research Team

Michael Hogan

Alison Bean de Hernandez

Patrick McHugh

Caren Arbeit

Pearl Sullivan

Kaitlin Lilienthal

cwdi@rti.org

NCSES CWDI Working Group

Amber Levanon Seligson

Kelly Phou

Gigi Jones

Shelley Feuer

Julia Milton

Vrinda Nair

Daniela Oliveira

Danielle Taylor

NCSES-CWDI@nsf.gov

Agenda

- Background
- Project timeline
- Definitions of the Cybersecurity Workforce
  - o Federal efforts
  - o The NICE Framework and its uses
  - o Global frameworks
- Our proposed definition
  - o Challenges
- Key takeaways and next steps

Background on the CWDI

- Mandated by the CHIPS and Science Act of 2022
  - Led by the National Center for Science and Engineering Statistics (NCSES)
  - Cybersecurity Workforce Data Initiative (CWDI)

- The goal of the CWDI is to assess the feasibility of producing nationally representative estimates and statistics on the cybersecurity workforce in the United States.

Project Timeline

Project kickoff and background research
- October- December 2023

Evaluate definitions, conduct interviews
- Jan-Apr 2024

Identify knowledge gaps, conduct interviews
- Jan-Apr 2024

Assess existing data on supply and demand
- Feb-May 2024

Evaluate Federal Data Sources
- Feb-May 2024

Evaluate nonfederal administrative data sources
- May-Jul 2024

Workshop 1
Definitions
May 7, 2024

Workshop 2
Knowledge Gaps
May 23, 2024

Workshop 3
Supply & Demand
June 11, 2024

We are here!

Workshop findings and recommendations to NCSES September 2024

Potential pilot survey 2025

Definitions Objective

*Our objective is to **understand how the cybersecurity workforce is currently defined** and **propose a definition** for the CWDI.*

Methods

To compile this information, our team

- Completed a **literature review** of existing federal, international, and private sector frameworks and data sources of the cybersecurity workforce;
- Conducted 15 **interviews** with 22 federal, private, and academic experts and stakeholders in the cybersecurity field;
- **Analyzed existing data** including traditional federal labor market data, education data, and data from nongovernment and administrative sources.

Background on Federal Efforts to Understand the Cybersecurity Workforce

- The federal government has been instrumental in **developing the cybersecurity field** as well as **understanding** it.

- The White House, Congress, and various agencies have published strategic cybersecurity strategies and cybersecurity workforce strategies since 2000.

- Initial focus was on national security and defense applications, and has broadened to understand the whole sector, including the **2023 White House Strategy** and **2024 NICE Framework Updates**

Timeline of Select Federal Efforts

Year	Agency	Initiative
2001	NSF/OPM/DHS	CyberCorps Scholarship for Services first cohort
2007	NSA	NSA IT Security Essential Body of Knowledge
2008	White House	The National Comprehensive Cybersecurity Initiative
2009	White House	White House Cyberspace Policy Review
2010	White House	National Security Presidential Directive 54 creates process to establish National Initiative for Cybersecurity Education (NICE) Framework
2011	OPM	Office of Personnel Management Competency Model for Cybersecurity
2012	NIST	First version of the NICE framework released
2014	Congress	Cybersecurity Enhancement Act
2014	NIST	Second version of the NICE framework released
2015	Congress	Federal Cybersecurity Workforce Assessment Act
2016	White House	Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
2017	NIST	Third version of the NICE framework released
2018	NSA	Supporting the Growth and Sustainment of Nation's Cybersecurity Workforce
2019	White House	Executive Order 13870: America's Cybersecurity Workforce
2020	NIST	Revised NICE framework released
2020	NSA	CISA Growth and Sustainment of Nation's Cybersecurity Workforce
2021	White House	Executive Order on Improving the Nation's Cybersecurity
2022	Congress	CHIPS and Science Act mandates CWDI
2023	**White House**	**National Cyber Workforce and Education Strategy**
2024	**NIST**	**Revisions to NICE framework**

Cybersecurity Workforce in the NICE Framework

- "The NICE Framework considers the cybersecurity workforce as those **whose primary focus is on cybersecurity** as well as those in the workforce who need specific **cybersecurity-related knowledge and skills** in order to perform their work in a way that enables organizations to properly manage the cybersecurity-related risks to the enterprise."

Source: NICE Framework 2023 One-Pager

Strengths of the NICE framework

The NICE Framework is driven by knowledge, skills, and work roles in cybersecurity. It:

- Establishes the core competencies and work functions common to most cybersecurity positions.
- Reflects the lack of a clear boundary around the periphery of the cybersecurity workforce.
- Permits flexible and scalable use.
- Facilitates workforce planning for federal agencies.

Federal use of the NICE Framework

Federal agencies draw on the NICE Framework to

- Create a **common language** for cybersecurity work
- Identify **job titles**, **specialty areas**, and work roles
- Standardize occupational series and grade levels (OPM)
- Enhance interoperability by establishing core skills and knowledge needed (DOD)

However, the NICE Framework is limited as it

- Does not translate directly to labor market data from federal survey providers

Connected to NICE Framework	Not Connected to NICE Framework
Federal Employers • OPM • DOD • DHS Federal Cybersecurity Centers of Excellence • NICCS • NCAE	Federal statistical data providers • BLS • Census Bureau • U.S. Department of Education • NSF NCSES

Cybersecurity as an Activity or Occupation

The NICE Framework emphasizes cybersecurity as a work **activity** by defining knowledge and skills in cybersecurity that can cut across job roles and functions.

- This enables the framework to be applied more broadly and cover both core cybersecurity workers and those who perform cybersecurity tasks as a part of a larger role.

Alternatively, European and UK frameworks define **occupations** in cybersecurity.

- This allows for clear definitions of who is included in the workforce and what skills are required to succeed within the workforce.

NICE Framework: 2024 Updates

European and UK Frameworks

Cybersecurity as a Work Activity or Occupation

The NICE Framework (left) and European Cybersecurity Skills Framework (right) offer two ways of understanding cybersecurity workforce.

Examples of work activities and occupations show how this can be interpreted.

Sources: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Work Activity *Examples – NICE Framework*	Occupation *examples – ECSF*
Oversight & Governance	Cyber Incident Responder
Design & Development	CISO
Implementation & Operation	Legal, Policy, and Compliance Officer
Protection & Defense	Cyber Threat Intelligence Specialist
Investigation	Cybersecurity Architect
Cyberspace Intelligence	Cybersecurity Auditor
Cyberspace Effects	Cybersecurity Educator

CWDI working definition (Part 1)

The cybersecurity workforce includes a **core set of cybersecurity occupations focused on cybersecurity**. Workers in other occupations where their **primary**, or **secondary work activities** include cybersecurity are also part of the core cybersecurity workforce.

The cybersecurity involved and adjacent workforce include those occupations where cybersecurity is a work activity, but not primary or secondary.

Combines definitions of occupations + activities

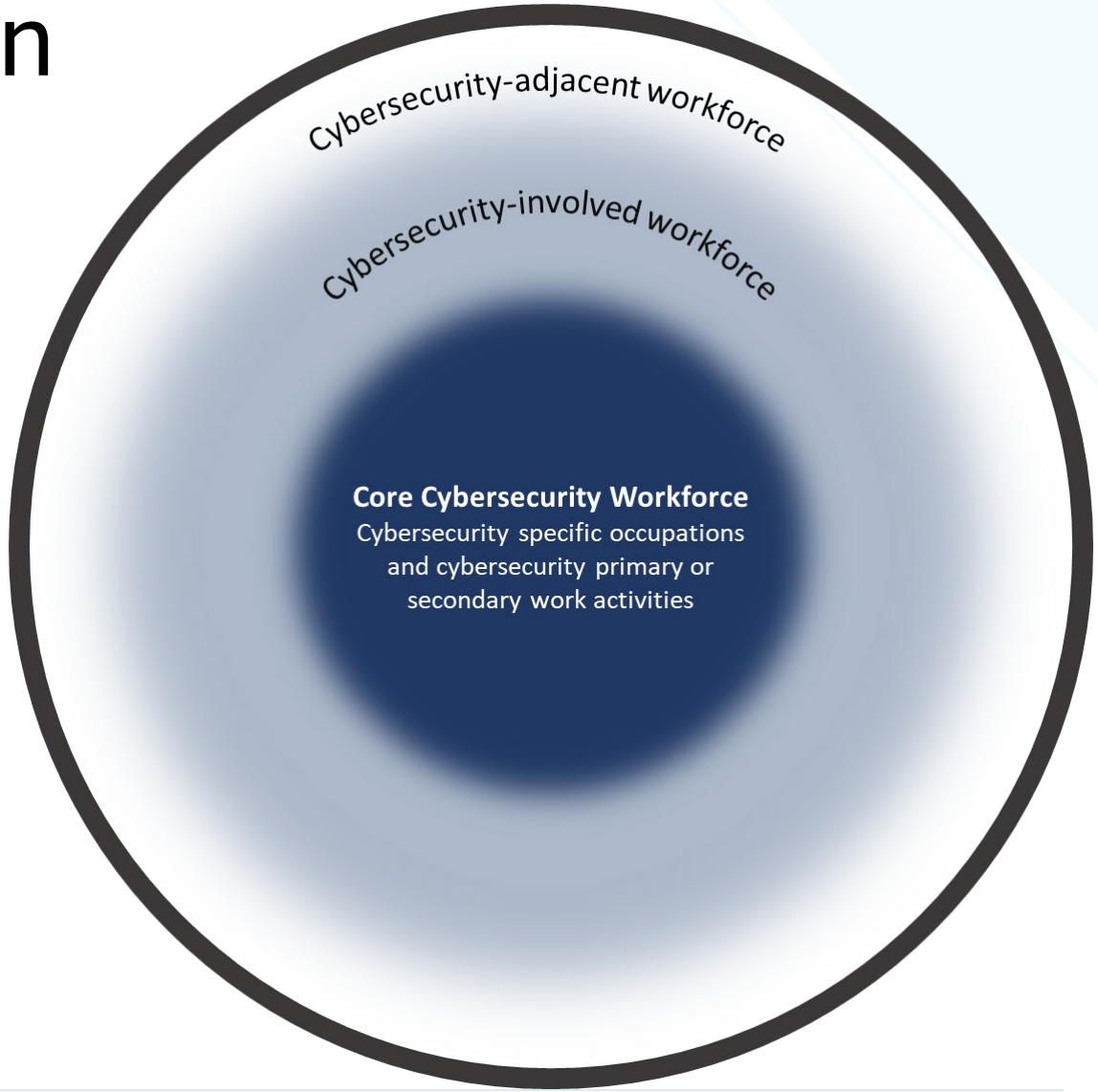
CWDI working definition (part 2)

Cybersecurity Core	Cybersecurity Involved	Cybersecurity Adjacent
Cybersecurity is the **primary work activity** and is **explicitly at the core** of the occupation. • Cybersecurity analysts, engineers • Penetration testers • CISOs Cybersecurity as a **primary or secondary work activity** • Cybersecurity lawyers • Database architects • Systems engineers • Software developers	Cybersecurity is an **explicit or other work activity**, but where an employee may not rank it as a primary or secondary part of their regular work roles. • Other computer and tech • Engineering • Financial and business • Legal and management • Military, protective services • Office support	Roles where cybersecurity is not an explicit work activity but where there are **cybersecurity implications** or a small number of required tasks, knowledge, and/or skills from the NICE Framework central to the occupation.

CWDI working definition (part 3)

The line between the core and cybersecurity-involved occupations is blurry and not easily defined by existing frameworks or data

For example, some web developers do cybersecurity work activities on a daily basis, while others more sporadically. Current taxonomies and data make it difficult to determine the difference.



Challenges for Defining the Workforce

- Job functions and skills vary based on how much cybersecurity-specific work someone is expected to do.
- Made up of a large number of job titles or occupation codes as one job title or SOC code cannot capture the diversity of the workforce.
  - Example – **cybersecurity lawyers** are a specific subset of lawyers in SOC classifications, but overlap with other lawyers
- Tied to many industries with different goals, challenges, and roles.
- Not defined by a single educational program of study or credentialing background.
- Technology evolves faster than traditional workforce data.

Key Takeaways

- There is not a single, widely used definition of who composes the cybersecurity workforce.
- Cybersecurity jobs are defined by work roles, tasks, knowledge, and skills that cut across job titles and industries and evolve quickly to keep pace with technology.
- Our proposed definition bridges the gap between differing frameworks and definitions of cybersecurity by establishing a core workforce and adjacent workforce, blending occupations and activities in cybersecurity.

Next Steps

Two upcoming workshops

- **May 23,** Knowledge Gaps
- **June 11**, Supply and demand

Workshop recommendations to NCSES in **September 2024,** to inform a potential **pilot study in FY 2025**.

More Information

- Learn more about the CWDI here: https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative
- Read the full report at: https://ncses.nsf.gov/760/assets/0/files/ncses-cwdi-working-definitions.pdf
- Agenda for upcoming workshops: https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative/workshops
- Reach us at NCSES-CWDI@nsf.gov and CWDI@rti.org

Transition into Small Group Discussions

Questions for Small Group Discussion

- What delineates a cybersecurity vs. non-cybersecurity job?
  - Do you consider cybersecurity to be an occupation, job title, or work activity?
  - How do you distinguish between cybersecurity and cyber jobs?

- What type of definition would be useful to you and why?
  - Would a more broad or more narrow definition be useful to you and why?
  - How would this help improve statistics on the workforce?
  - What are the strengths and drawbacks to these approaches?

- How can the current definition(s) be improved?
- What are the skills, credentials, and/or experience required for a cybersecurity job and how have those evolved over the last five years?
  - How does this impact the definition? Has the definition changed?

Break

Poll Question

Panel Discussion

Rodney Petersen
NIST

Marinda Hamann
ISC2

Melissa Dark
DARK Enterprises

Jennifer Ozawa
RTI
Moderator

CWDI working definition for Panelists

The cybersecurity workforce includes a **core set of cybersecurity occupations focused on cybersecurity**. Workers in other occupations where their **primary**, or **secondary work activities** include cybersecurity are also part of the core cybersecurity workforce.

The cybersecurity involved and adjacent workforce include those occupations where cybersecurity is a work activity, but not primary or secondary.

Combines definitions of occupations + activities

CWDI Working Definition for Panelists (Part 2)

Cybersecurity Core	Cybersecurity Involved	Cybersecurity Adjacent
Cybersecurity is the **primary work activity** and is **explicitly at the core** of the occupation. • Cybersecurity analysts, engineers • Penetration testers • CISOs Cybersecurity as a **primary or secondary work activity** • Cybersecurity lawyers • Database architects • Systems engineers • Software developers	Cybersecurity is an **explicit or other work activity**, but where an employee may not rank it as a primary or secondary part of their regular work roles. • Other computer and tech • Engineering • Financial and business • Legal and management • Military, protective services • Office support	Roles where cybersecurity is not an explicit work activity but where there are **cybersecurity implications** or a small number of required tasks, knowledge, and/or skills from the NICE Framework central to the occupation.

Panel Questions

- What is your reaction to the proposed definition for the cybersecurity workforce in the CWDI? How does it reflect your thinking on the workforce?
- What are some potential challenges you see with taking this approach of a workforce that is defined by both occupations and work activities?
- Where is your biggest need or biggest missing piece in understanding the cybersecurity workforce today? How has that changed in the last five years?
- How can the CWDI best address your cybersecurity workforce data needs and those of your organization?

Thank you!

Next Steps

- Two upcoming workshops
  - o **May 23,** Knowledge Gaps
  - o **June 11**, Supply and Demand

- Send workshop feedback for consideration to NCSES by **Friday June 28, 2024**

- We are developing a report about the workshops by October 2024

- To send feedback or ask questions: NCSES-CWDI@nsf.gov