Department of Defense Chief Information Officer: Cybersecurity Education Developments

Patrick Johnson
Director of Workforce Innovation Directorate
DoD CIO

GROWING THE NEXT GENERATION OF CYBER TALENT

Patrick Johnson

Director, Workforce Innovation Directorate

DoD CIO

September 2023

AGENDA

- Mission Statement
- DoD CWF Strategy Implementation Plan
- Cultivating Tomorrow's Talent Pool
- Cyber Academic Engagement Central Program Office
- What is the DoD Cyber Scholarship Program?
- DoD 8140 Qualification Model Example
- DoD Foundational Qualification Option: Education
- Questions

MISSION STATEMENT

The Department of Defense is one of the Nation's largest employers with approximately:

- 1.3 million active-duty service members
- 750,000 National Guard and Reserve service members
- 750,000 civilian personnel
- 600,000 contractors

Growing Our Talent:

To remain the strongest fighting force in the world, we must **recruit** and **retain** the best of America. That means we must continue:

- Building pathways of opportunity for all qualified American's.
- Deepening the Department's partnerships with America's best universities.
- Continuing to invest in training and education and create programs that focus on science, technology, engineering, and math.
- Providing exceptional opportunities for service and professional development for our total force.

DoD CWF STRATEGY IMPLEMENTATION PLAN

CWF Strategy

- Aims to provide the tools, resources, policies and programs that enable the Department's cyber workforce stakeholders to **identify, recruit, develop** and **retain** a more agile and effective cyber workforce.

Implementation Plan

- Sets the foundation for how the Department will execute the 22 objective and 38 initiatives aligned with the 4 overarching goals in the CWF Strategy.

- Identification
- Recruitment
- Development
- Retention

GOAL 1: Execute consistent capability assessment and analysis processes to stay ahead of force needs.

GOAL 2: Establish an enterprise-wide talent management program to better align force capabilities with current and future requirements.

GOAL 3: Facilitate a cultural shift to optimize Department-wide personnel management activities.

GOAL 4: Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

CULTIVATING TOMORROW'S TALENT POOL

CWF Strategy Goal 4:

- Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

Objective 4.3:

- Enhance collaboration with academia to cultivate a talent pipeline and support important areas of research.

Initiative 4.3.1:

- Establish a centralized program office to manage cyber-focused student and employee developmental programs across the Department.

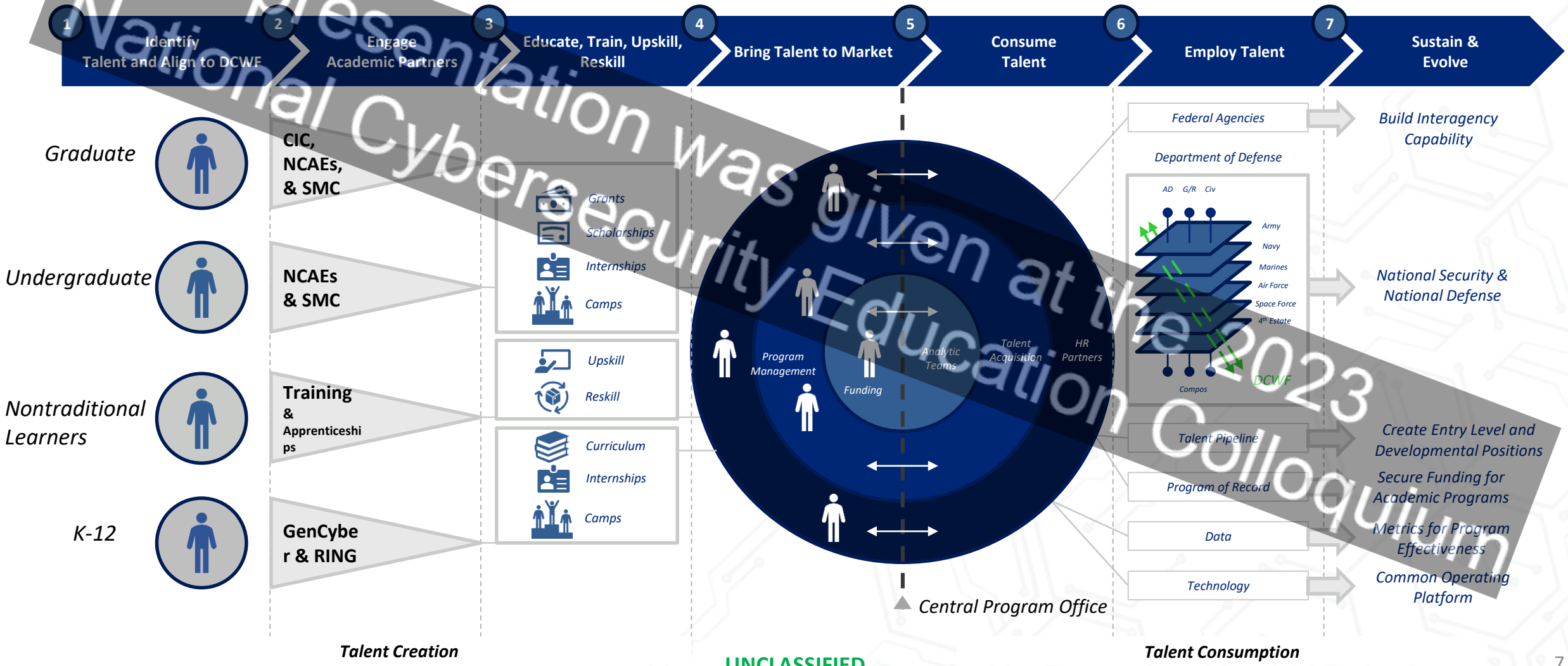
Initiative 4.3.2:

- Ensure NCAE-C curriculum aligns with Department-wide cyber standard.

Initiative 4.3.3:

- Increase return on investment of scholarship programs and effectively track participation to customize recruitment and outreach efforts.

CYBER ACADEMIC ENGAGEMENT CENTRAL PROGRAM OFFICE



WHAT IS THE DoD CYBER SCHOLARSHIP PROGRAM?

The DoD Cyber Scholarship Program (DoD CySP)

(Formerly the Information Assurance Scholarship Program) is designed to encourage the recruitment of the nation's top cyber talent and the retention of DoD personnel who have skills necessary to meet DoD's cyber requirements and help secure our nation against the threats of information systems and networks.

Grants awarded for scholarships and capacity building to NCAE-Cs:

Scholarships

Recruitment: Targets students who are not current DoD or Federal employees and who are enrolled at designated CAEs; may be undergraduate or graduate students

Retention: Targets Military and Civilian DoD personnel for Associates or Graduate (Certificates, Masters, and PhD programs)

NCAE-Cs

National Centers of Academic Excellence in Cybersecurity (NCAE-C)

National Centers of Academic Excellence in Cyber Defense (CAE-CD)

National Centers of Academic Excellence in Cyber Defense Research (CAE-R)

National Centers of Academic Excellence in Cyber Operations (CAE-CO)

DoD 8140 QUALIFICATION MODEL EXAMPLE

(621) Software Developer				
		Basic	Intermediate	Advanced
Foundational Qualification Options	Education	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university
		OR	*OR*	*OR*
	Training	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository
		OR	*OR*	*OR*
	Personnel Certification	GSEC	CSSLP	CISSP-ISSAP
Foundational Qualification Alternative	Experience	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification	On-the-Job Qualification	Always Required	Always Required	Always Required
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Annual Maintenance	Continuous Professional Development	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.

DoD 8140 FOUNDATIONAL QUALIFICATION OPTION: Education

DoD CYBER EXCHANGE NIPR

DOD WORKFORCE INNOVATION DIRECTORATE

- 8140 Home
- Documents Library
- DoD Approved 8570 Baseline Certifications
- Frequently Asked Questions - FAQs
- Steps to Obtain a DoD 8570 Baseline Certification
- Summary of IA Workforce Qualification Requirements
- Help
- Workforce Innovation Directorate Home
- Qualifications Matrices

DoD 8140 Policy Requirements

Degree Achievement within 5 Years
Degree conferred within the past 5 years by an institution of higher education unless continuous work in a relevant discipline can be demonstrated.

Demonstration of Continuous Work
Considered documentation of employment covering any cyber work role with no more than three consecutive years lapse in cyber work.

DoD 8140 Qualification Approval Process

Academic Programs Mapped to DCWF Work Role Codes
Emphasis on ABET Accredited and CAE Designated Programs.
Example Programs: Computer Science, Cybersecurity, Data Science, Information Technology, Electrical Engineering, Information Systems, Software Engineering, Computer Engineering.

Basic, Intermediate, and Advanced Proficiency Levels for each Work Role Code
Associates, Bachelors, Masters, Doctoral Degrees, Masters Certificate mapped to proficiency level.

Survey on Cyber Education Requirements

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

Sponsor: Institute for Defense Analyses (IDA) (on behalf of the DoD)

Purpose: To gather perspectives on how to best educate the DoD's cyber workforce to protect the Nation from future cyber threats (findings will be included in a report requested by Congress).

Survey Question Focus:

- Student capacity in cyber programs of study
- Educator staffing levels
- Cyber education preferences and requirements
- Perceptions of future cyber threats
- The need for a National Cyber Academy

SHARE YOUR THOUGHTS ON CYBER EDUCATION BY TAKING A BRIEF SURVEY

(visit the URL or Scan the QR Code below)

https://idaorg.gov1.qualtrics.com/jfe/form/SV_251iRbldGNIdmUC

QUESTIONS

SCAN TO VIEW THE CYBER WORKFORCE STRATEGY

This presentation was given at the 2023 National Cybersecurity Education Colloquium

NCAE-C Grants Program

Alice Smitley
Grant Manager
NCAE-C Program Management Office

Early External Education in Cybersecurity (E^3C)

NCAE-C Grant Program

(Updates and Processes)

September 2023

Early External Education in Cybersecurity Grants

The **Early External Education in Cybersecurity program** at the National Security Agency offers three distinct grant programs available to various academic institutions and non-profits.

- National Centers of Academic Excellence in Cybersecurity Grants (NCAE-C)
- DoD Cyber Scholarship Program (DoD CySP)
- GenCyber

Metrics for 2023

- NCAE-C
  - 14 Grants
    - 14 Unique CAEs
- DoD CySP
  - 59 Grants/CAEs
- GenCyber
  - ~80 Grants
    - 65 CAEs

Guidelines for Grants

- Promote fairness across the CAE Community
- Provide access to all NCAE-Cs
- Eliminate the appearance of an unfair advantage
- Meet internal NSA financial goals
- Meet external DoD and Congressional Grants Management Policies
- Improve access to results and findings from grant activities

Contact with the Program Office - Acceptable

- Acceptable Contact:
  - Asking about specific forms
  - Asking about submission processes (format, page limits, etc.)
  - Asking for email addresses
  - Asking how to document an item in a proposal
  - Receiving permission from the Program Office employee to call them after hours on a topic not related to a specific grant or solicitation.
  - Emailing requesting a review of a press release
  - Emailing specific grant questions after award. Please contact the correct POC! NCAECgrants@nsa.gov; AskCySP@nsa.gov; GenCyber@nsa.gov

Any NCAE-C found calling a Program Office employee will automatically be disqualified from any and all grant solicitations.

Contact with the Program Office - Unacceptable

- Unacceptable Contact:
  - Calling the Program Office to ask if a project is “what we are looking for?”
  - Calling/emailing a Program Office employee on their personal number/email to ask if a project is what we are looking for
  - Calling to tell the employee what you plan to submit
  - Calling the Program Office during work hours/after hours to talk about plans to meet with your legislative representatives
  - Talking to a Program Office member during a conference to ask for a no-cost extension or budget modification

Any NCAE-C found calling a Program Office employee will automatically be disqualified from any and all grant solicitations.

Invoicing

- Grantees are required to submit an invoice at a minimum once every three months.
- Invoices with a covered period exceeding 6 months must include a justification.
- Any grantee that does not invoice at least once every three months may be placed on the Unliquidated Obligation List and could potentially lose funding.
- Failure to invoice properly will result in denial of no-cost extension and potential option year funding.
- Future government funding is affected by the amount of un-invoiced funding on active grants.

No-Cost Extensions

- Must be submitted in writing and emailed to either AskCySP@nsa.gov or NCAECGrants@nsa.gov.
  - May only request once
  - May only be for a maximum of 12 months
  - Grants that have not been invoiced at least 50% at the time of request will be denied.
  - Must be current on any and all reports.
- Only leads of coalition grants may request no-cost extensions
- GenCyber does not authorize no-cost extensions.

Budget Modifications

- Must be submitted in writing to the respective Grant Program Office
- You must show the "From By To"
  - From - What was the original amount?
  - By – What are you adding or subtracting?
  - To – What is the new amount?
- Budget changes must stay within the original scope of the grant
- Only Leads of coalition grants may request modifications

Dino Institute

MOD September 2023

Faculty and Staff							
Position:	**Name**	**Months**	**Rate**	**Total**	**MOD**	**New Total**	**Justification**
PI	Dr. Grant Seeker	10	$ 19,710.00	$ 197,100.00	$ (60,751.00)	$ 136,349.00	reduced to three (3) months at new salary & position
Admin	Helen Parr	12	$ 2,319.00	$ 27,828.00	$ (368.44)	$ 27,459.56	Reduced time to allow
Dino Institute Director	Dr. Helen Marsh	12	$ 19,550.00	$ 234,600.00	$ (54,050.00)	$ 180,550.00	Reduced Dr. Marsh time to allow for project turnover to Dr. Jones
New Project Director	Dr. I. Jones				$ 115,169.44	$ 115,169.44	Dr. Jones will start the project in Spring 2024
				$ 459,528.00		$ 459,528.00	

Options

- Options are not a guarantee
- Options may be awarded if it was included in the original proposed budget
  - We cannot go back and create an option.
- If funding is identified the following criteria has to be met before the option can be awarded:
  - Invoiced for at least 50% or more of the grant
  - Current on all reports
  - Current on invoicing

Issue Date	PoP	Option Eligibility
2022	1 year	2023
	2 years	2024
2023	1 year	2024
	2 years	2025
2024	1 year	2025
	2 years	2026
2025	1 year	2026
	2 years	2027

Reporting

- Each Grant program sets their reporting requirements
  - DoD CySP:
    - Mid-cycle report,
    - Final technical report, and
    - Final SF-425
  - NCAE-C:
    - Mid-cycle report,
    - Final technical report, and
    - Final SF-425
  - GenCyber:
    - Planning/Pre-Camp Outreach,
    - Camp Report,
    - Final Technical Report/Three lesson plans (with post-camp outreach),
    - Final SF-425

Additional Grant Information

- Grants are awarded to the institution and not specifically to the Principal Investigator.
  - It is the institution's responsibility to ensure that the grant is executed and grant funds are spent.
  - If a PI leaves the institution, the grant cannot follow the PI.
  - The institution may sub-contract with the PI to finish the grant.
- The NCAE-C Program Office cannot act as a pass-through for funding or receive earmarks.
  - All funding received by the NCAE-C Program Office for grants must be competed among all the NCAE-Cs.
  - OMB defines earmarks as funds provided by Congress for projects or programs where the congressional direction (in bill or report language) circumvents the merit-based or competitive allocation process, or specifies the location or recipient, or otherwise curtails the ability of the Administration to control critical aspects of the funds allocation process.

How Grants Are Reviewed? Part 1

- Check 1: Are all forms/documents included and in the correct format?
  - Yes – Proposal is moved to Check 2.
  - No – Proposal is rejected.
- Check 2: Is the NCAE-C Point of Contact identified in the proposal or has provided a letter of support?
  - Yes – Proposal is moved to Check 3.
  - No – Proposal is rejected.
- Check 3: Is the institution current on their NCAE-C designation and annual report (if required)?
  - Yes – Proposal is moved to Check 4.
  - No – Proposal is rejected.
- Check 4: Does the institution have current grants with NCAE-C or DoD CySP (GenCyber will be added to this mix in the future)?
  - Yes – Proposal is moved to Check 5.
  - No – Proposal is moved to the "ready for review pile"

How Grants Are Reviewed? Part 2

- Check 5: Since the institution has current/active grants, a review of each grant (up-to 5 years prior) is performed. Calculate point deductions from overall score.

Grant Number	Grant Amount	Invoice Amount	Remaining	Returned	Final SF425	Final Tech Report	% Expended Grant Funds	Outstanding Grant Funding	Outstanding Grant Reports	Returned money	Total
19 CySP	$ 798,000.00	$ 725,000.00	$ -	$ *73,000.00*	Y	Y	91%	0	0	-10	
20 CySP	$ 150,000.00	$ 139,435.57	$ -	$ *10,564.43*	Y	Due 12/16/2023	93%	0	0	-3	-3
20 NCAE-C	$ 199,999.00	$ 171,775.15	$ -	$ *28,223.85*	Y	Y	86%	0	0	-5	-5
21 CySP	$ 509,667.00	$ 413,665.75	$ 96,001.25	$ -	Due 03/30/2024	Due 03/30/2024	81%	0	0	0	0
21 NCAE-C	$ 1,678,112.40	$ 654,377.35	$ 1,023,735.05	$ -	Due 12/30/2023	Due 12/30/2023	39%	-5	0	0	-5
21 NCAE-C	$ 494,702.51	$ 159,293.56	$ 335,408.95	$ -	Due 03/30/2025	Due 03/30/2025	32%	-5	0	0	-5
21 NCAE-C	$ 464,152.89	$ 145,819.26	$ 318,333.63	$ -	Due 03/30/2025	Due 03/30/2025	31%	-5	0	0	-5
22 DoD CySP	$ 588,368.00	$ 207,837.85	$ 380,530.15	$ -	Due 03/09/2024	Due 03/30/2024	35%	-5	0	0	-5
22 NCAE-C	$ 2,236,000.00	$ 758,000.00	$ 1,478,000.00	$ -	Due 12/31/2024	Due 12/31/2024	34%	-5	0	0	-5
	$ 7,119,001.80	$ 3,375,204.49	$ 3,632,009.03	$ *111,788.28*				-25	0	-18	-43

How Grants Are Reviewed? Part 3

- Check 6: Provide all viable proposals to independent reviewers
  - Reviewers have approx. 30 days, unless a quick turn around is required.
- Check 7: Add scores and average the total.
- Check 8: Process point deductions from total score to obtain final score.
- Check 9: Rank order proposals by final score
- Check 10: Make announcements.

Individual feedback for GenCyber, DoD CySP, and NCAE-C grant submissions is not provided.

Proposal Review Deductions

- Amount of outstanding grant funding (failure to invoice) on current grants. Number of grants that have not been invoiced or remain at 50% or less at the mid-point of the period of performance. (***5 points for anything 50% or higher un-invoiced***)
- Number of outstanding grant or annual reports (NCAE-C, NCAE-C Grants, DoD CySP, and GenCyber) (***3 points for each missing report***)
- Amount of money returned on closed grants
  - ***0 points for anything under $500***
  - ***3 points for $501 to $10,000,***
  - ***5 points for $10,001 to $75,000,***
  - ***7 points for $75,001 to $100,000,***
  - ***10 points for $100,001 to $150,000,***
  - ***Automatic disqualification for any amount over $150,001***

Outstanding Grant Funding

Grant Name	Year	Awarded Amount	Uninvoiced Funds	Unused Amount	Grant Status
DoD CySP	2018	$ 6,327,213.00	$ -	$ 542,600.24	In Close Out
CRRC Grants	2019	$ 1,582,641.00	$ -	$ 83,125.35	In Close Out
DoD CySP	2019	$ 14,773,572.43	$ 149,734.30	$ 784,574.75	In Close Out
NCAEC-001	2020	$ 26,031,435.51	$ 6,327,371.42		Some Active Grants / Others Beginning Closeout
NCAEC-002	2020	$ 5,372,756.23	$ 2,439,621.70	$ 252,625.49	Beginning Close-Out
NCAEC-003	2020	$ 35,151,632.80	$ 8,994,280.13	$ 147,821.15	Some Active Grants / Others Beginning Closeout
NCAEC-004	2020	$ 19,794,352.00	$ 9,632,538.62		Grants are Active
DoD CySP	2020	$ 18,685,560.54	$ 846,376.82	$ 965,445.11	Beginning Close-Out
NCAEC-001	2021	$ 24,585,033.97	$ 15,052,939.86	$ -	Grants are Active
NCAEC-002	2021	$ 9,340,187.89	$ 6,237,006.33	$ -	Grants are Active
NCAEC-003	2021	$ 28,499,999.00	$ 18,936,498.58	$ -	Grants are Active
NCAEC-004	2021	$ 149,880.00	$ 73,684.27	$ -	Grant is Active
DoD CySP	2021	$ 13,660,478.25	$ 821,623.35	$ 390,607.36	Beginning Close-Out
NCAEC-001	2022	$ 43,992,907.83	$ 31,034,193.04	$ -	Grants are Active
NCAEC-002	2022	$ 1,013,282.00	$ 720,333.16	$ -	Grants are Active
NCAEC-003	2022	$ 7,798,980.00	$ 4,953,535.56	$ -	Grants are Active
NCAEC-004	2022	$ 13,999,803.00	$ 13,280,631.06	$ -	Grants are Active
DoD CySP	2022	$ 12,831,826.65	$ 4,268,472.66	$ -	Grants are Active
		$ 283,591,542.10	$ 123,768,840.86	$ 3,166,799.45	

Referencing Your Grant

- XYZ University received a $X00,000.00 a grant (H98230-XX-1-0XXX), from the National Centers of Academic Excellence in Cybersecurity (located within the National Security Agency) to fund ABC Project
- A two-year, $000,000.00 grant (H98230-XX-1-0XXX) from the National Centers of Academic Excellence in Cybersecurity, which is part of the National Security Agency; will support project ABC.
- This research was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-XX-1-0XXX), which is part of the National Security Agency.
- Students supported through a grant from the DoD Cyber Scholarship Program.
- This research was funded by a grant from the DoD Cyber Scholarship Program, which is funded by the Department of Defense and managed by the National Security Agency
- XYZ Camp was funded via a grant from the GenCyber Program which is housed with the National Centers of Academic Excellence in Cybersecurity and is co-sponsored by the National Security Agency and National Science Foundation.
- This activity was supported by a GenCyber Program grant in the amount of $XXX,000.00

Events/Briefings, etc.

- NCAE-Cs, regardless of grant status, should not brief the NCAE-C, DoD CySP, or GenCyber on a programmatic level. NCAE-Cs should request a program office speaker to provide an overview at events.
- NCAE-C, DoD CySP, and GenCyber grantees are encouraged to present their projects or experiences.
- The NCAE-C, DoD CySP, or GenCyber program offices should not be planning events that were funded as part of your grant award. Program Office individuals may advise on the agenda and provide suggestions on speakers, but they should not be managing the entire agenda or provide support staff.
- The NCAE-C Program Office kindly asks that you provide a heads-up when an event includes one of the federal partners.

Contact/Questions

- NCAE-C Grants: NCAECGrants@nsa.gov
- DoD CySP: AskCySP@nsa.gov
- GenCyber: GenCyber@nsa.gov
- NCAE-C Program Office: CAEPMO@nsa.gov
- Maryland Procurement Office Help Desk – 410-854-5445 (M-F, 8-4PM EST)
- NSA Contract Closeout: Contract_Closeout@nsa.gov

Survey on Cyber Education Requirements

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

Sponsor: Institute for Defense Analyses (IDA) (on behalf of the DoD)

Purpose: To gather perspectives on how to best educate the DoD's cyber workforce to protect the Nation from future cyber threats (findings will be included in a report requested by Congress).

Survey Question Focus:

- Student capacity in cyber programs of study
- Educator staffing levels
- Cyber education preferences and requirements
- Perceptions of future cyber threats
- The need for a National Cyber Academy

SHARE YOUR THOUGHTS ON CYBER EDUCATION BY TAKING A BRIEF SURVEY

(visit the URL or Scan the QR Code below)

https://idaorg.gov1.qualtrics.com/jfe/form/SV_251iRbldGNIdmUC

Robust Software Development: RFI

The NCAE-C Grant Program Office, in conjunction with the NSA's Cybersecurity Directorate, is seeking voluntary information about your secure coding, secure programming, or secure software development offerings on campus. Please respond back to the NCAEC Grant Program Office at NCAECGrants@nsa.gov by September 29 via email and answer the following questions:

- Do you offer classes in secure coding, secure programming, or secure software development? (Yes or No)
- If yes, please list those classes: (*Designator and formal name; example: CMSC 150 Introduction to Security*)
- Do you utilize any commercial or open-source software analysis tools in your curriculum? (Yes or No)
- If yes, please list the tools you use, and describe in a brief statement how you use these tools in your curriculum.

Please understand that this RFI is completely voluntary. Participation does not impact an institution's NCAE-C designation and/or future grant opportunities or funding.

Rita Doerr will be hosting a session on Thursday 21 Sept, in room M201.
Please visit if you have more questions

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Dual Credit and RING

Dr. John Sands
Department Chair of the Computer Integrated Technologies Department
Moraine Valley Community College

Dual Credit and RING

National Cybersecurity Educational Colloquium (NCEC)
September 19th, 2023

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Dr. John Sands

PI, Education Pathway National Center

Moraine Valley Community College

Jesse Hairston

Co-PI, Education Pathway National Center RING

University of Alabama Huntsville

Michael Qaissaunee

Co-PI, Education Pathway National Center

Brookdale Community College

Kyle Jones

Co-PI, Education Pathway National Center

Sinclair Community College

Educational Pathways National Center (EPNC)

- **Promote the RING curriculum and education-to-career pathways (CAE)**
  - Implement RING in local communities and statewide
  - Track student enrollment
- **Work with EPNC to establish RING infrastructure**
  - Implement extra-curricular activities (clubs, honor society)
  - Provide range access for RING
  - Develop industry partnerships
- **Scale EPIs Model Nationally**
  - Expand capacity
  - Increase cybersecurity pathway diversity
  - Expand post-secondary and secondary educational partners
  - Expand the number of EPIs

Successful CyberSecurity POS Pathways

Using Perkins V Key Elements

EPNC Road Map

Advising	• Support Academic Advisors and Career Councilors
Curriculum	• Engage Students With Relevant & Rigorous Content
DEI	• Support under-represented Institutions & Bridge Digital Divide
Career Awareness	• Embed career awareness tools and opportunities in curriculum.
Articulation	• Establish Formal Pathways K12-CAEs: Dual Credit/Enrollment
Faculty Development	• Provide Continuous Faculty Development and Support

EPNC
EDUCATION PATHWAY NATIONAL CENTER

Academic Advising

Awareness Events

Engagement

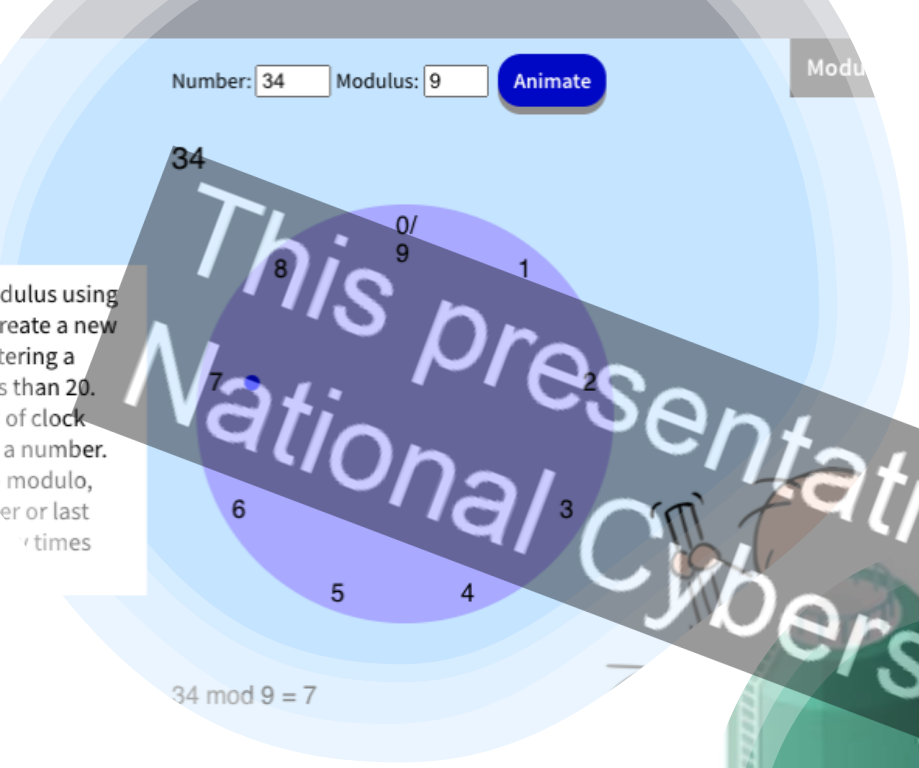
Cybersecurity Careers Toolkit

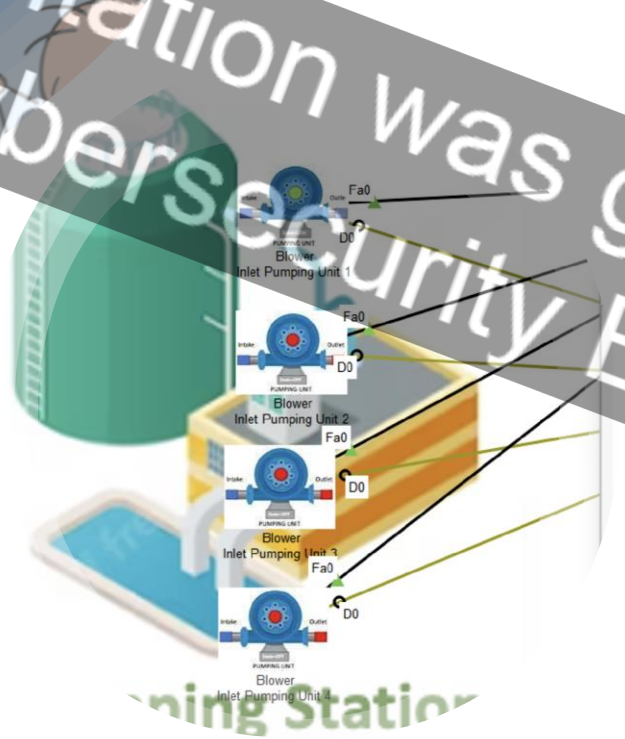
Curriculum (RING)

Rigorous

Relevant

Engaging



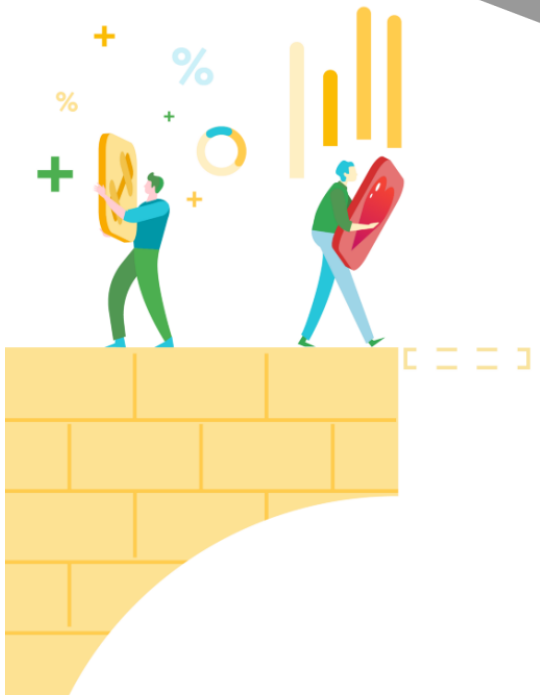


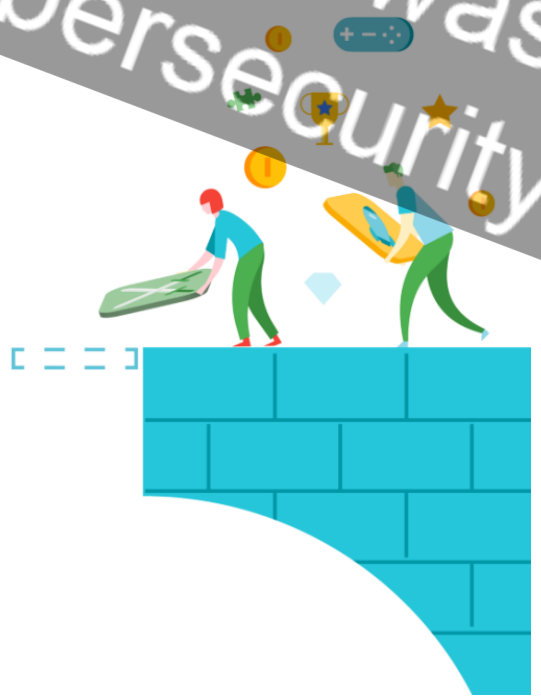
E-Mate Interactive Activity

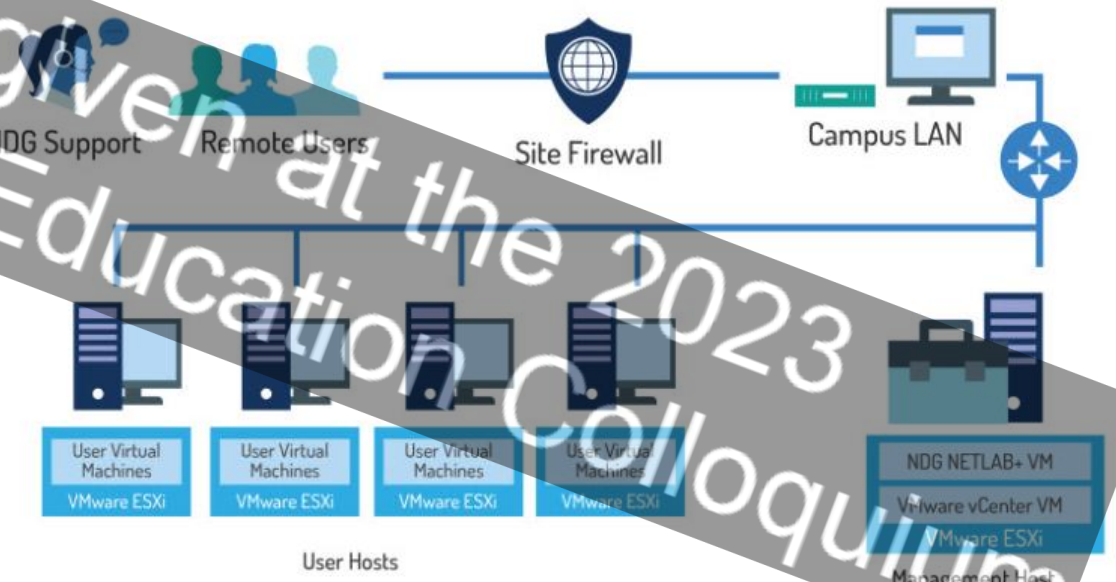
RING REGIONS INVESTING IN THE NEXT GENERATION

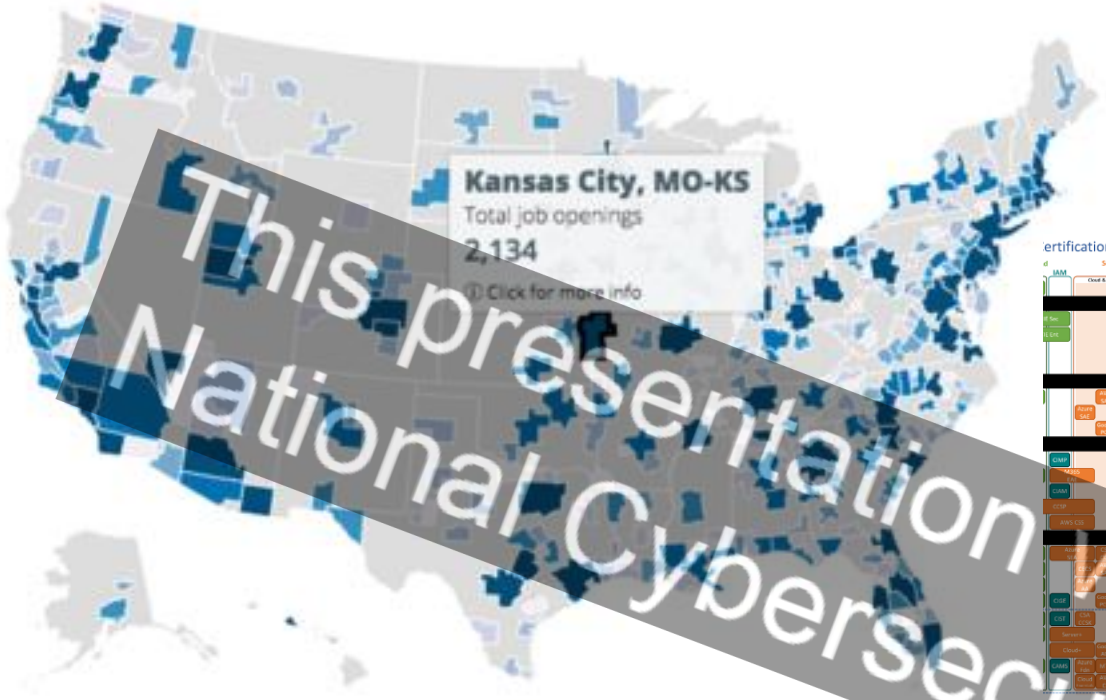
Diversity, Equity, and Inclusion

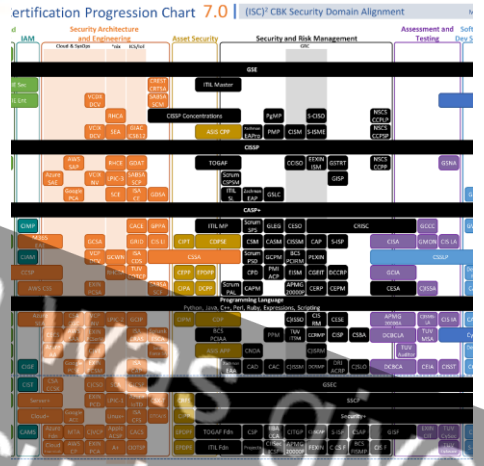
Bridge	Promote	Provide
Bridge Digital Divide	Promote Career Opportunities	Provide Resources & Support











Career Awareness

Knowledge and Skills	Credentials	Careers	Academic Plan
CAE Knowledge Units Critical Concepts Hands-on Experience Competencies	Degrees/Certificates Industry Certifications Workforce Experiences	Work Roles Nature of Work Compensation	HS Courses College Degrees/Cert Certifications CAE Programs

Knowledge and Skills	Credentials	Careers	Academic Plan
CAE Knowledge Units Critical Concepts Hands-on Experience Competencies	Degrees/Certificates Industry Certifications Workforce Experiences	Work Roles Nature of Work Compensation	HS Courses College Degrees/Cert Designing Articulation programs Perkins V – Reforms and Certifications

Articulation

Types of Articulation Programs

- Dual Credit
  - Early College
  - TechPrep
  - Dual Enrollment
- Advanced Placement AP
  - Life Experience

Faculty Development

Credentials

RING
Security+
CEH
CISA/CISM
CISSP

Technologies

Wireless Security
Docker and Containers
Adjure vs ACS
Arduino Certification

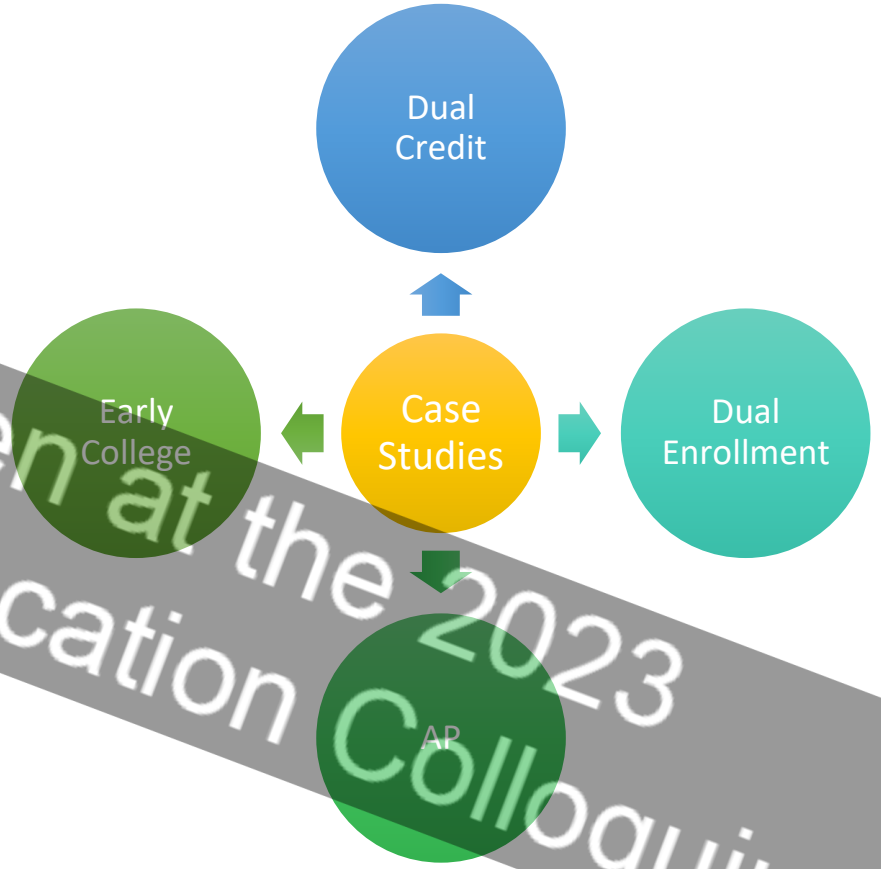
Cybersecurity Trends

Artificial Intelligence
CMMC
IT Merging with OT
Python Scripting

Non Faculty

Cybersecurity Careers
Certifications
CAE Programs

Articulation Case Studies in the CAE Community



CAE IN CYBERSECURITY COMMUNITY

Dual Credit	Dual Enrollment	Early College	Advanced Placement
IHSD 218 Students can earn 13 credits in the MVCC Information Security AAS • LAN101 Career Awareness • LAN111 Hardware • LAN112 Software / APPS • LAN121 Networking • LAN143 Security+		IHSD 218 Students can earn 13 credits in the MVCC Information Security AAS	

NCAE-C Education Pathway National Center

Questions / Comments ?

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Break

10:00 - 10:15 am

This presentation was given at the 2023 National Cybersecurity Education Colloquium

NCAE-C Strategy and Re-designation Requirements

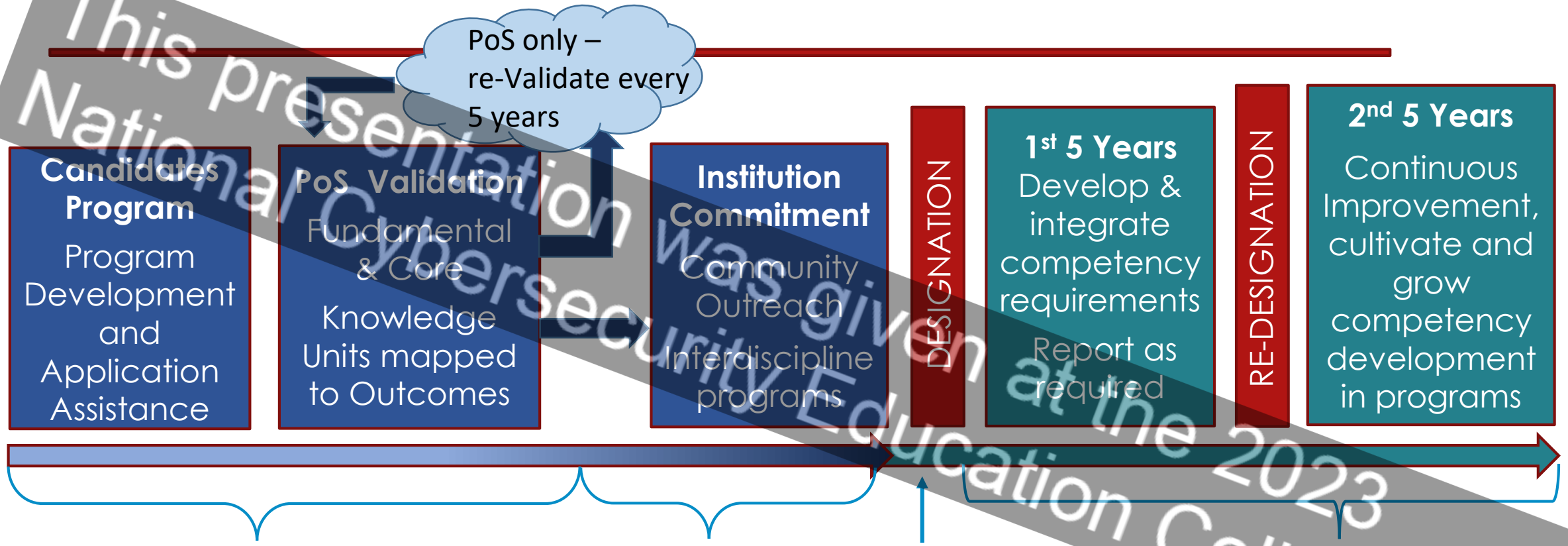
Lynne Clark

This presentation was given at the 2023 National Cybersecurity Education Colloquium

NCAE-C Redesignation Requirements

National Cybersecurity Education Colloquium

Program Progression



<u>Candidates and Peer Review programs manage</u>

PoS Validation is focused on ensuring academic outcomes are aligned to NCAE-C KU outcomes and either NICE Framework or NCWF work roles

Designation endorses institution's commitment to support the program, sustainability, academic quality

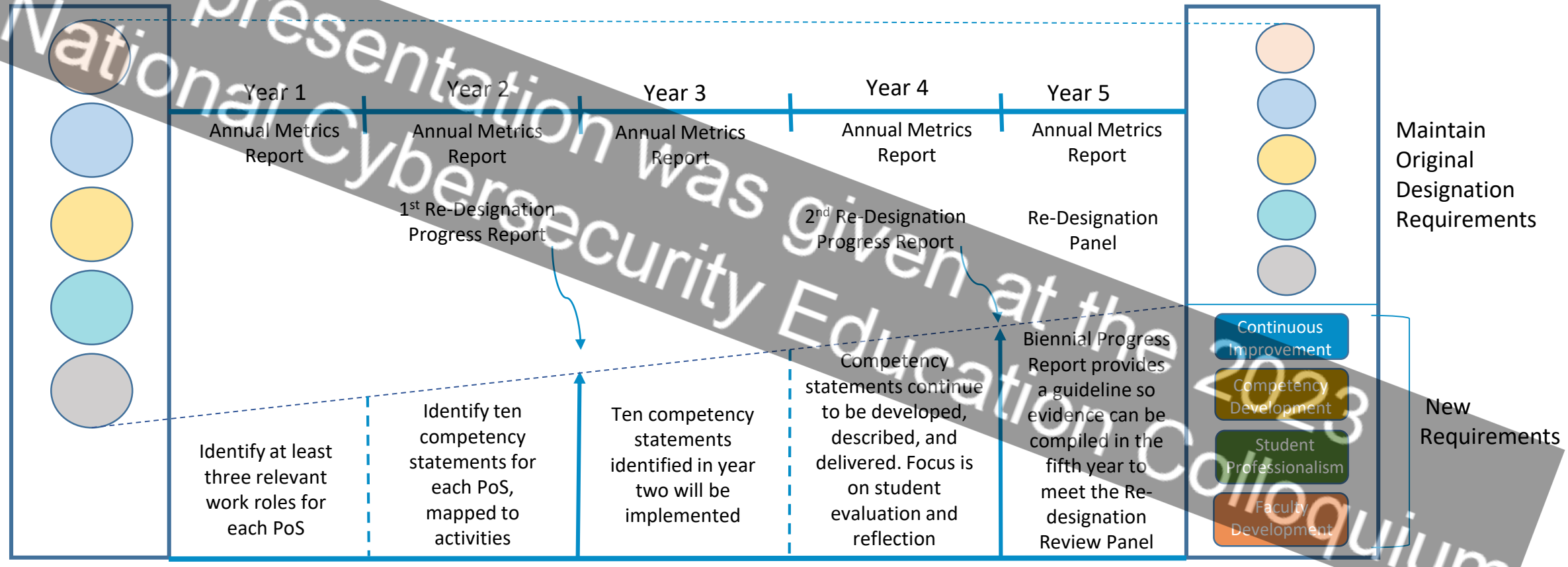
<u>PMO manages</u>

Re-designation confirms continuing original requirements PLUS continuous improvement and implementation of competency development integration into PoS

Competency Development

- Measure individual student professional development and competency – document
- Evidence institution's investment in student development/competency
- Faculty development

Re-Designation Objective Process

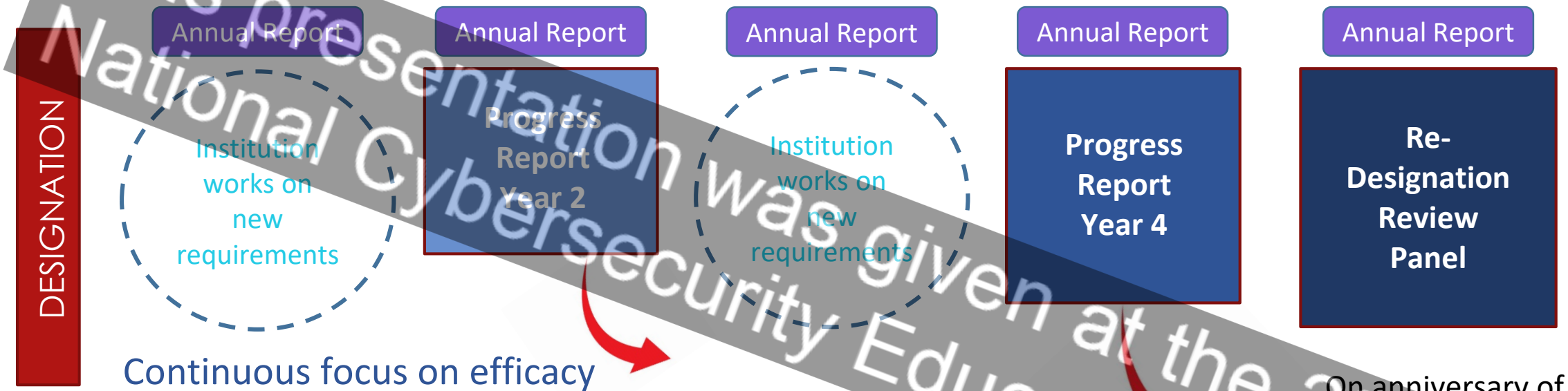


Designation

Designated institutions expand competency development, student professionalism and faculty development efforts and demonstrate continuous improvement of the PoS and institution

Re-Designation

Biennial Progress Reports Build Re-designation



Continuous focus on efficacy
Re-designation builds throughout the five years

On anniversary of 4th year the institution is assigned to a review cycle so that the institution is re-designated by the 5th anniversary

- At the time of Designation, the PMO will assign a Biennial Re-Designation Progress Report due date
- PMO staff will review reports and provide feedback
  - Will address insufficient items, work with schools as appropriate
  - Will work with schools to identify trends and best practices

Reporting Process = Re-designation Preparation

Annual Status Report

Annual Metrics Report and Review of Original Designation Requirements

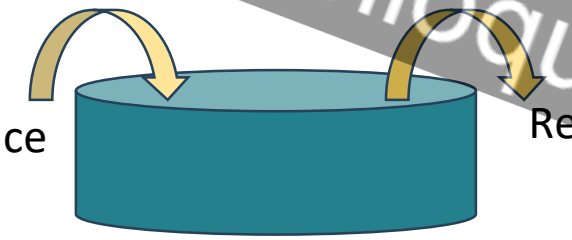
- Students enrolled per degree/certificate per PoS
- Students completed or graduated per PoS
- Faculty changes associated with the PoS
- Yes/No on currency summary of PoS Validation and Designation requirements
- Explanation of any “no” answers and plan for correction

Biennial Re-designation Progress Report

Continuous Improvement, Competency Development, Student Professionalism, Faculty Development

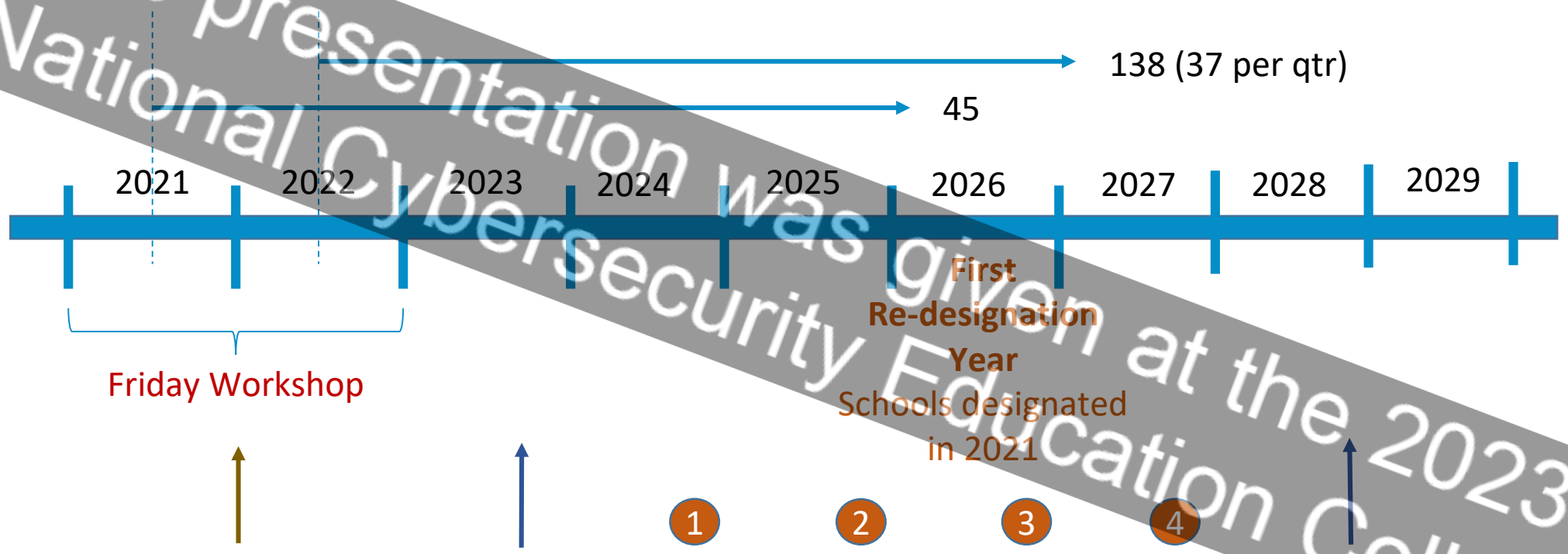
- Yes/No on specific requirements
- Explanation of “no” answers, plan for implementation
- Due dates assigned in designation letter

Self-reporting; Save documentation/evidence in repository



Re-designation Package

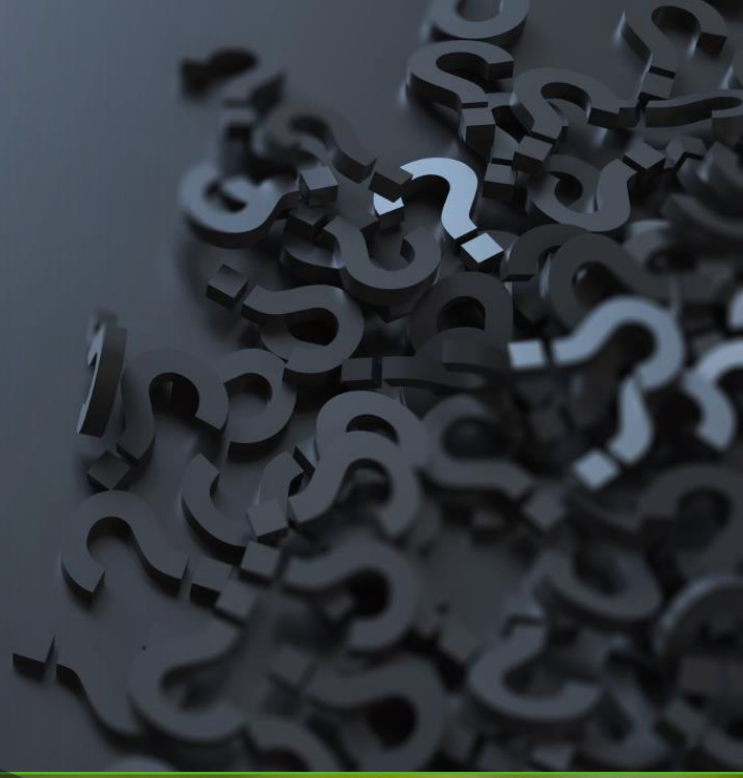
Starting Point for New Process



Began designating CAE-CD schools in the new tool

Schools designated or re-designated in 2023 will be the first to have a full four years to prepare for re-designation in Year 5

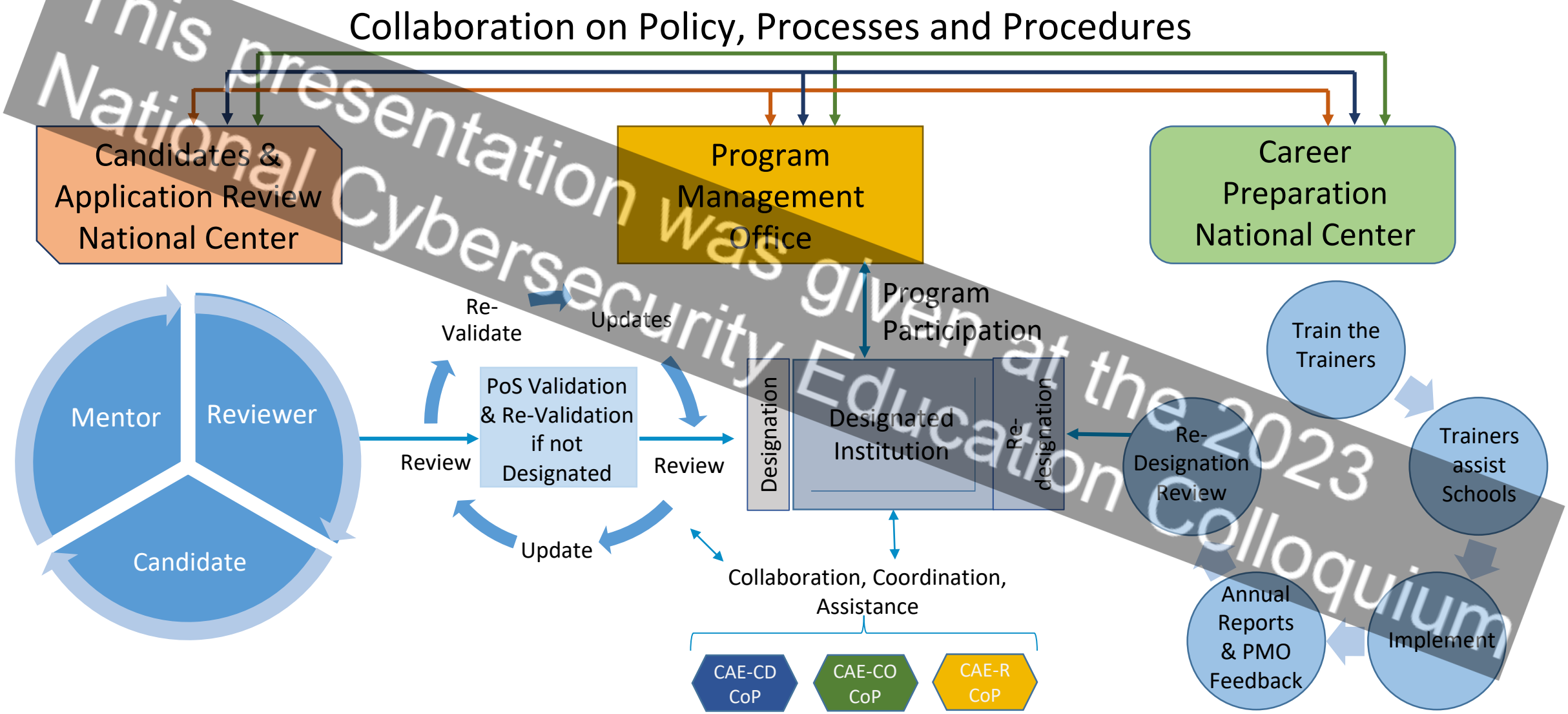
Questions ?



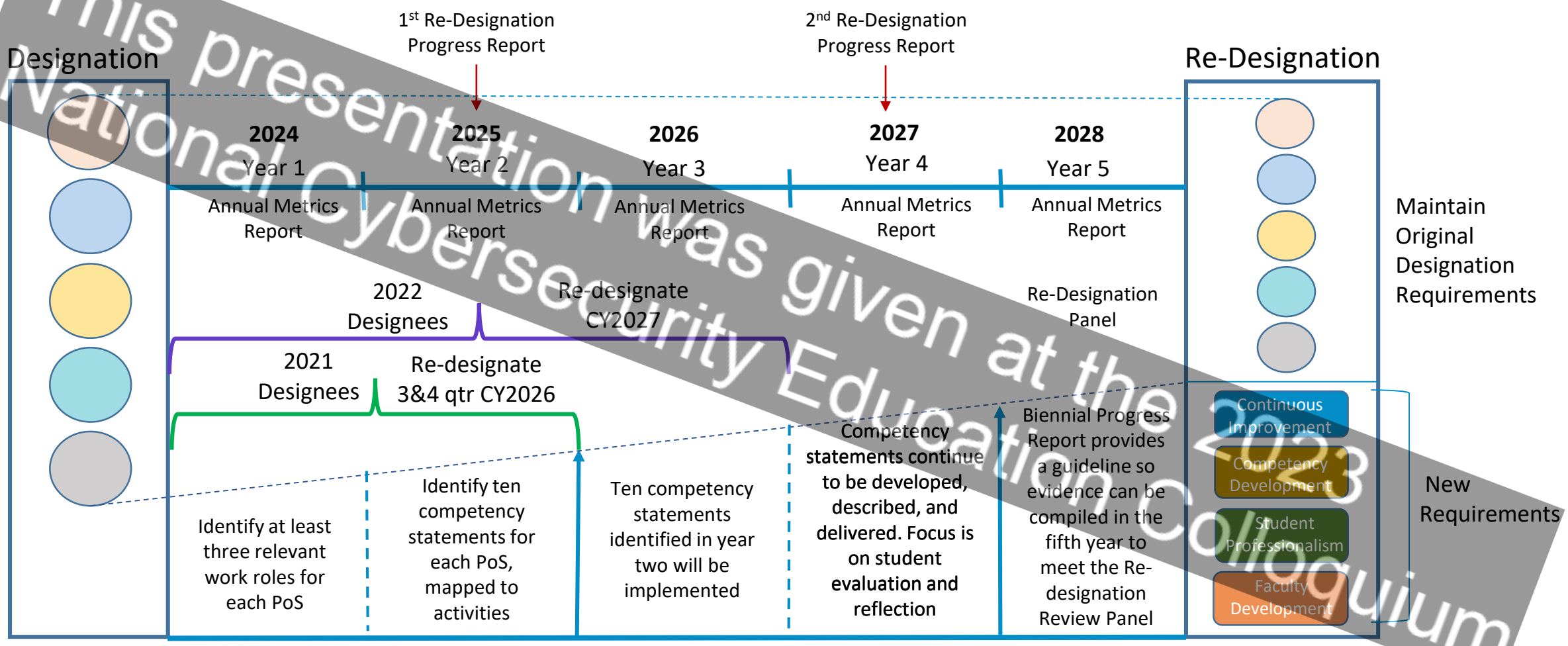
This presentation was given at the 2023 National Cybersecurity Education Colloquium

NCAE-C Redesignation Requirements Implementation

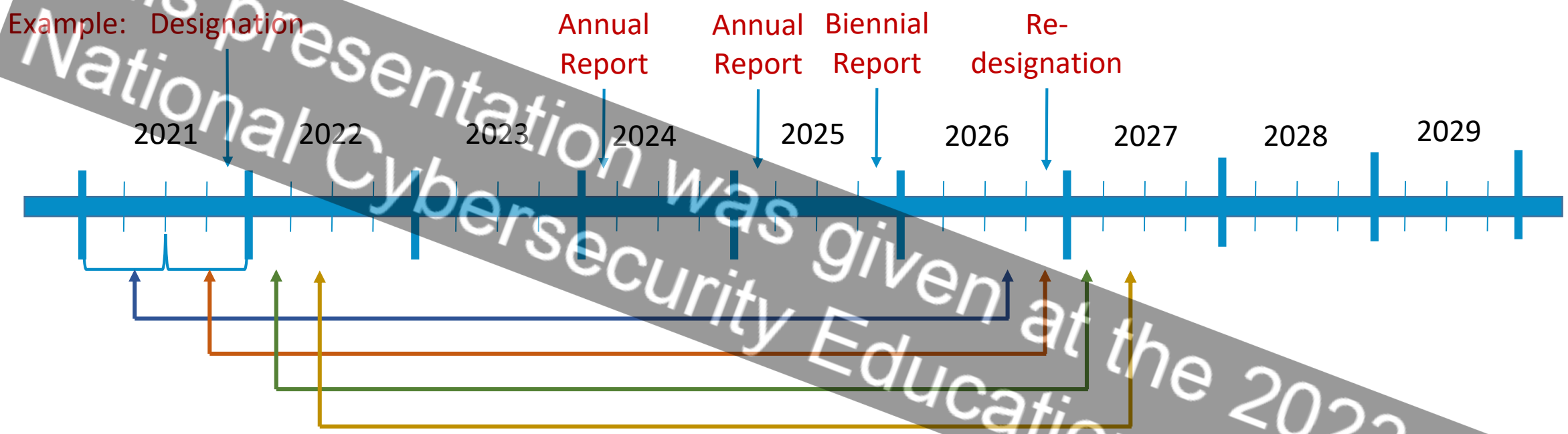
Lifetime Validation & Designation Process



Re-Designation "Grandfather" Schedule

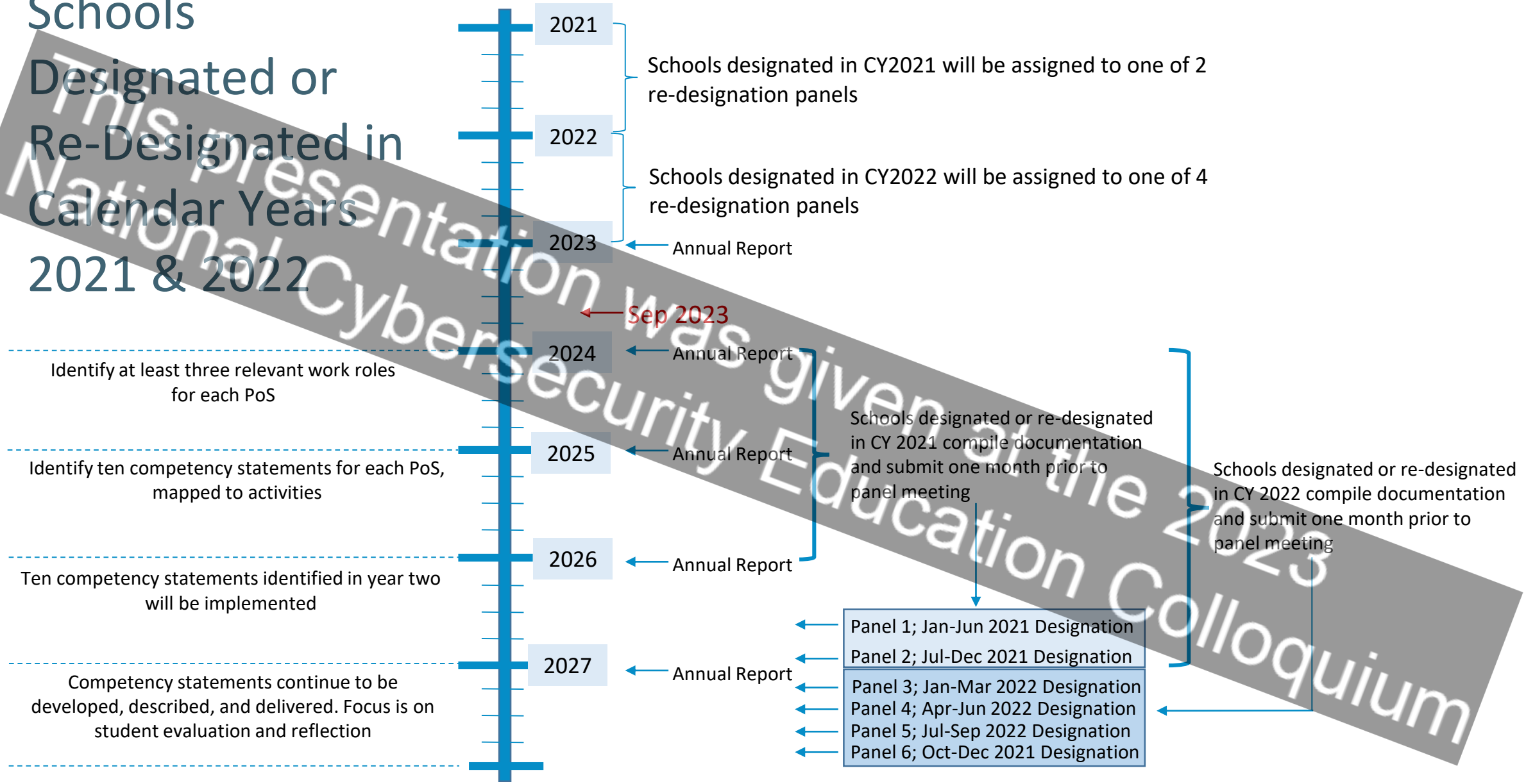


Implementation

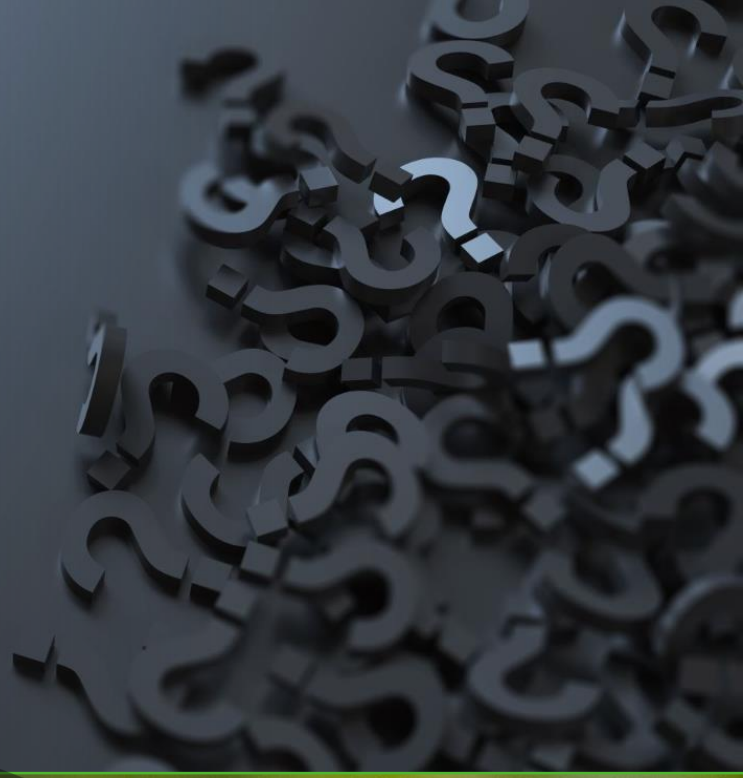


- Designation first half of 2021, re-designate in 3rd quarter 2026
- Designation second half of 2021, re-designate in 4th quarter 2026
- Designation first quarter 2022, re-designate 1st quarter 2027
- Designation second quarter 2022, re-designate 2nd quarter 2027
- etc

Schools Designated or Re-Designated in Calendar Years 2021 & 2022

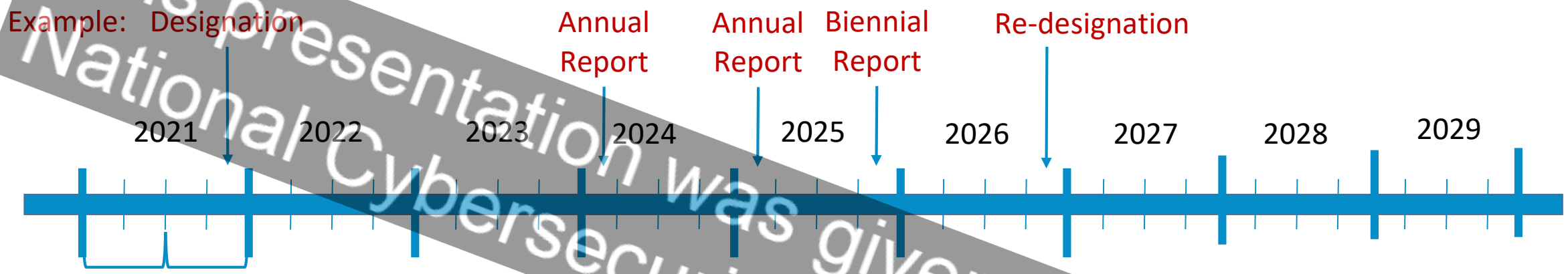


Questions ?

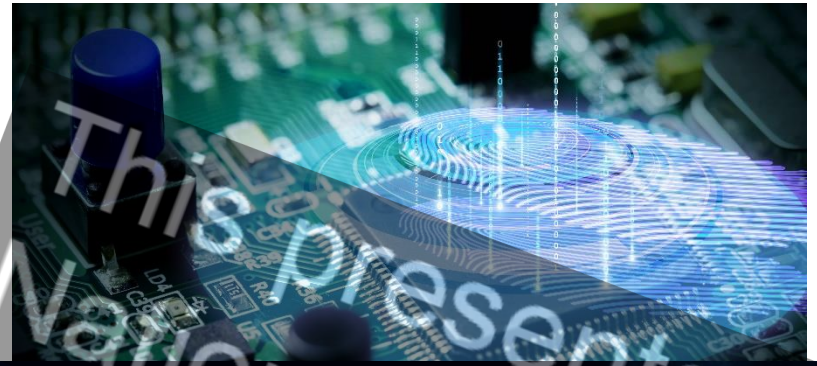


This presentation was given at the 2023 National Cybersecurity Education Colloquium

Implementation



- Designation first half of 2021, re-designate in 3rd quarter 2026
- Designation second half of 2021, re-designate in 4th quarter 2026
- Designation first quarter 2022, re-designate 1st quarter 2027
- Designation second quarter 2022, re-designate 2nd quarter 2027
- etc



This presentation was given at the 2023 National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium

NCAE-C and the National Cyber Workforce Education Strategy

No Photography

Albert Palacios
Director of Cyber Education
Office of the National Cyber Director

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Introduction to Workshops

Dr. Sharon Hamilton, Norwich University
Dr. Zoe Fowler, Norwich University
Dr. Vincent Nestler, California State University, San Bernardino
Dr. John Sands, Moraine Valley Community College

This presentation was given at the 2023 National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Lunch

12:00 - 12:45 pm

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Networking and Exhibits

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Break

1:30 - 1:45

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Career Preparation National Center Workshop

Dr Vincent Nestler

CSUSB

Dr. Zoe Fowler

Building and evidencing competencies in the cybersecurity classroom

Dr. Vincent Nestler

Dr. Zoe Fowler

Tuesday September 19 2023, NCEC

CALIFORNIA STATE UNIVERSITY SAN BERNARDINO

NORWICH UNIVERSITY

Careers Preparation National Center

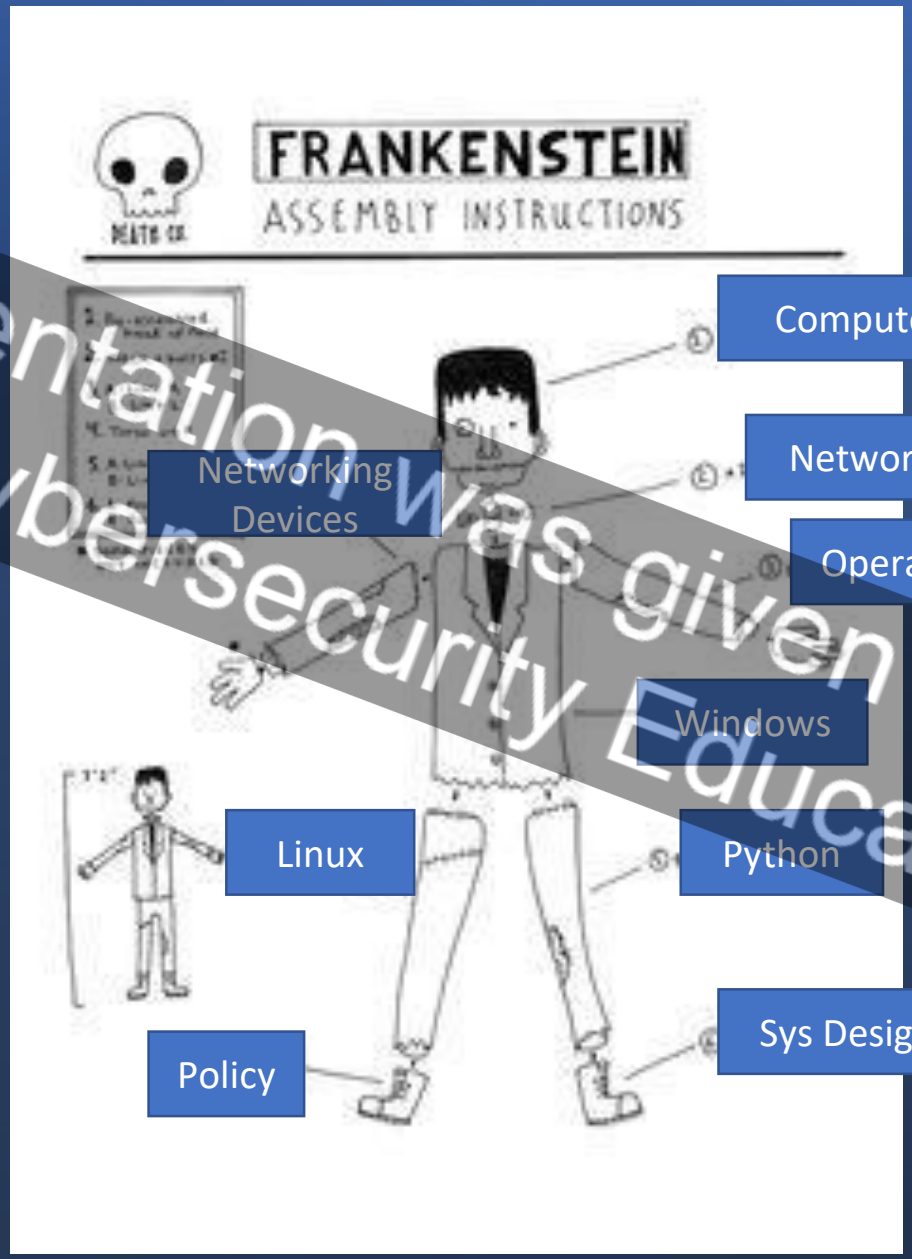
Overview of session

This presentation was given at the 2023 National Cybersecurity Education Colloquium

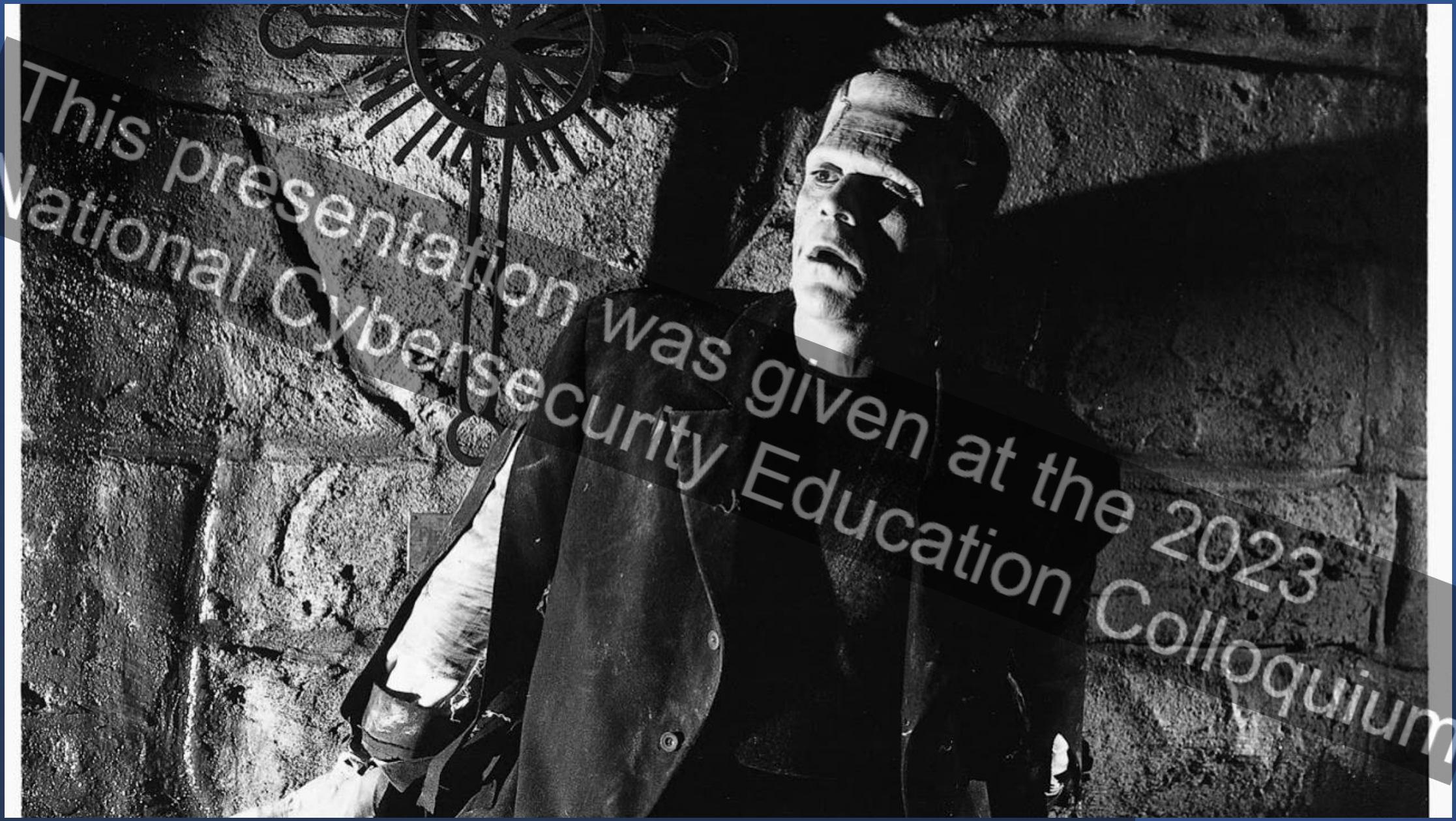
- The problem: Frankenstein's monster
- Step 1: start with the work role
- Step 2: learning your ABCDEs
- Step 3: Inputs and outputs
- Spreading the word

Educating Frankenstein's Monster

- Computer Skills
- Networking Skills
- Operating Systems
- Network Devices
- Windows
- Linux
- Coding and Scripting
- Etc.

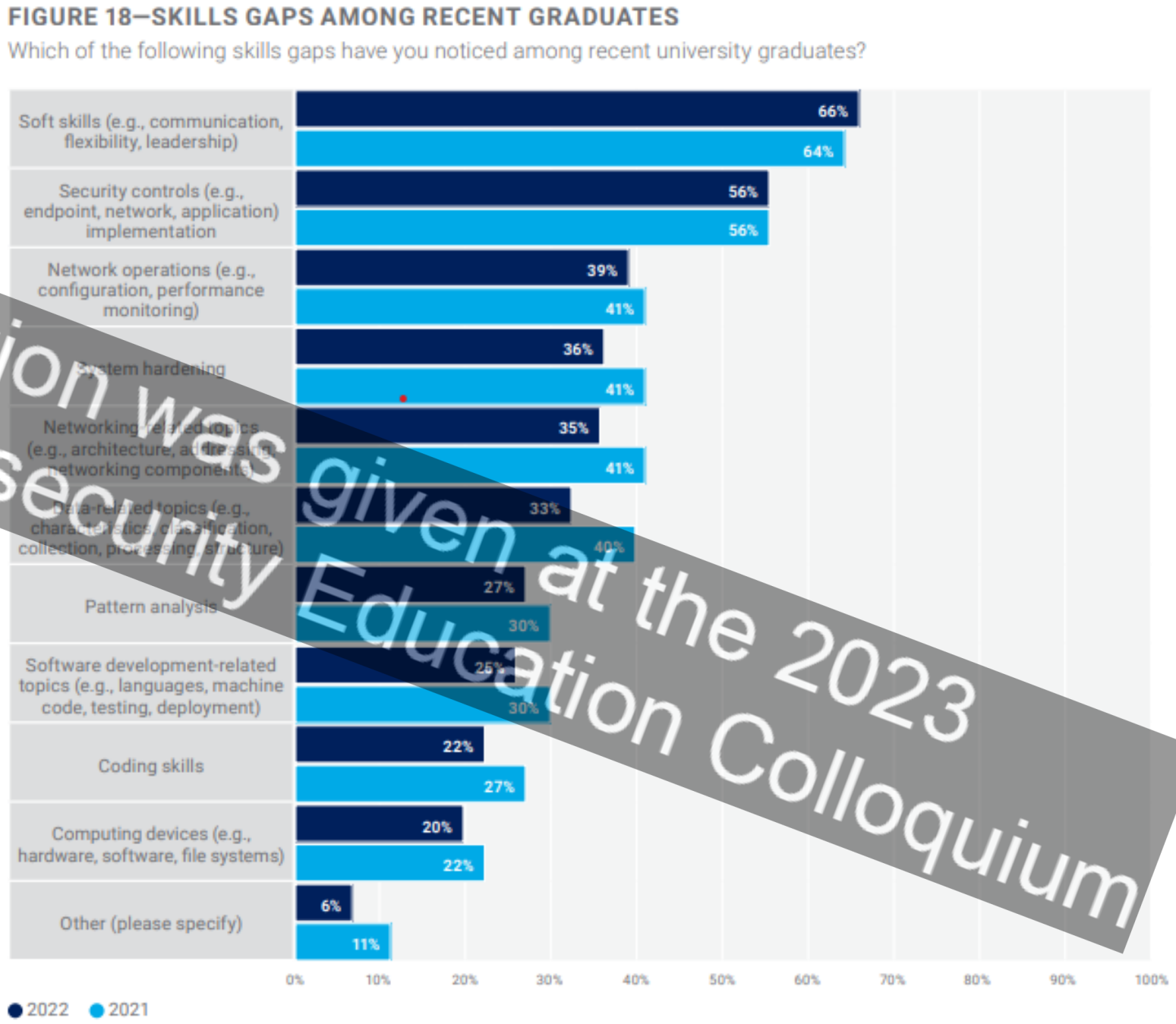



This presentation was given at the 2023
National Cybersecurity Education Colloquium


This presentation was given at the 2023
National Cybersecurity Education Colloquium

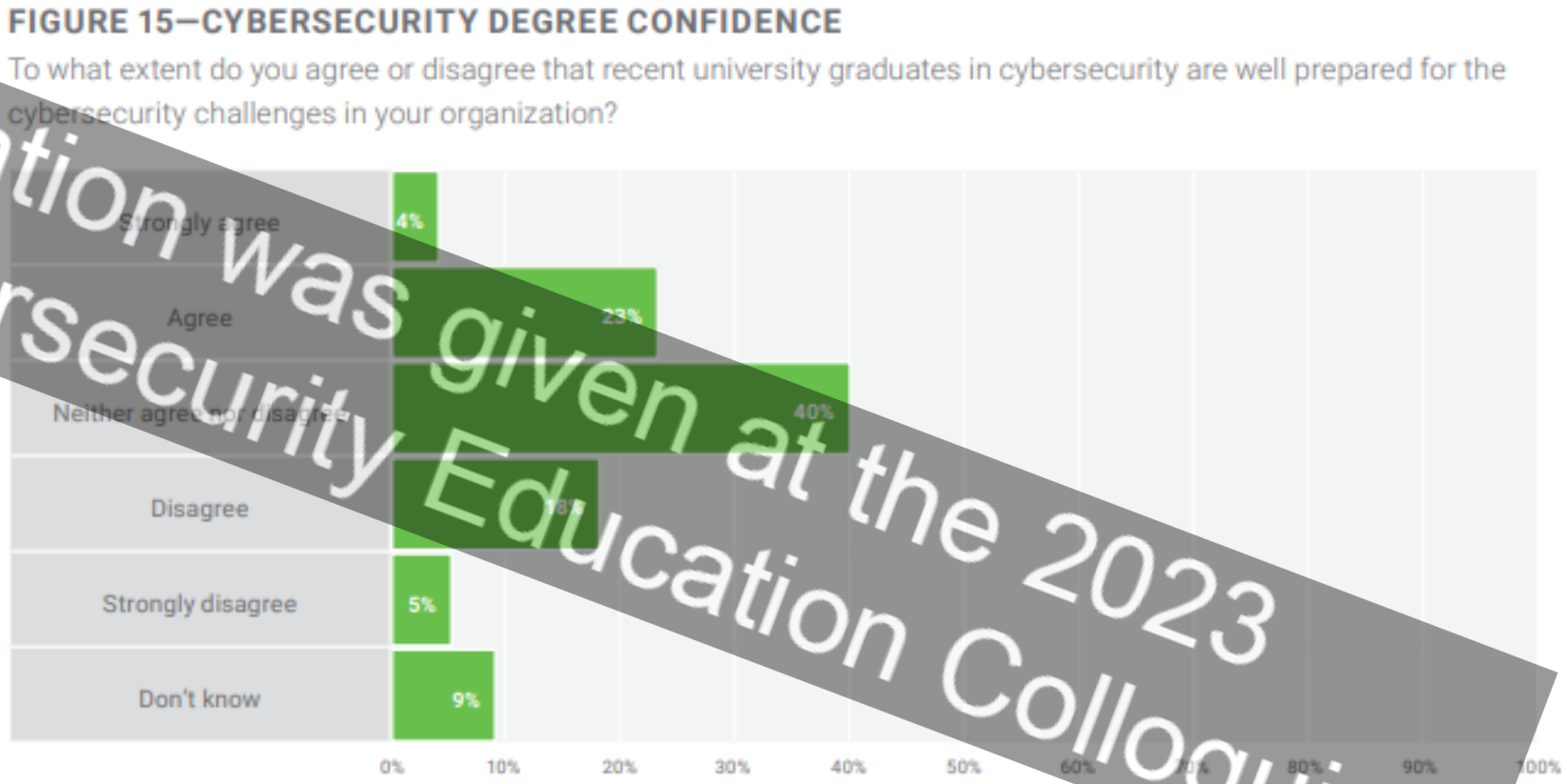
The Skills Gap Stats

From ISACA - State of Cyber Security 2022



The Skills Gap Stats

From ISACA - State of Cyber Security 2022



Reasons for this disconnect pt.1

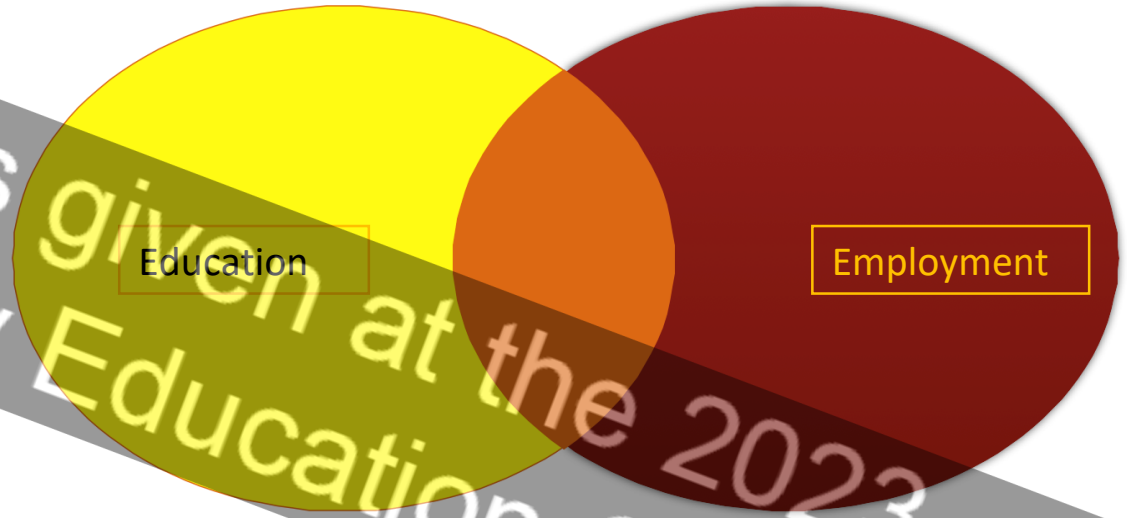
- Challenge of providing a contextualized learning experience both in terms of a realistic work environment with realistic tasks to be accomplished.
- Students graduate with component skills but without opportunities to engage in simulated work environments.
- Because many skills are taught in isolation of other skills (Linux, Windows, networking devices, coding, etc) those skills may be lost and forgotten by the time of graduation.

Reasons for this disconnect pt.2

- We start too late.
- Lack of hands-on experience opportunities
- Students lack knowledge of available work roles, and therefore lack self-efficacy in designing careers which they will enjoy and where they will excel.

Talking about competency

- Transforms knowledge and skills into workplace capabilities.
- Develops "breach-ready" workforce.
- Potential win-win-win situation (win for the educator, win for the employer and, most importantly, win for the student)
- BUT, important that we are all speaking the same language



This presentation was given at the 2023 National Cybersecurity Education Colloquium

"COMPETENCY IS
THE ABILITY FOR THE STUDENT
TO COMPLETE A TASK OR TASKS
WITHIN THE CONTEXT OF A WORK ROLE."

Step 1:

Begin with the work role

DoD Cyber Workforce Framew

public.cyber.mil/wid/dcwf/

News Writing Recipes Cybersecurity

Login with CAC

DoD CYBER EXCHANGE PUBLIC

Topics Training PKI/PKE SRGs/STIGs Resources Help

DoD Cyber Workforce Framework

The DoD Cyber Workforce Framework establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator.The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).

Workforce Elements

Workforce Elements | Elements Map | Search Work Roles | Search KSATs

Click the arrow to expand/collapse the Workforce Elements. Then select the Workforce Element to see the associated Work Roles.

IT Cyberspace

IT (Cyberspace)

Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

Workforce Framework for Cybersecurity (NICE Framework)

Categories/Specialty Areas | Work Roles | Tasks | Knowledges | Skills | Abilities

The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

To explore the NICE Framework, click on the Categories below or use the links above to search within the NICE Framework components or by keyword. To learn more, review the Using the NICE Framework PDF.

DISCUSSION

- Choose a work role that interests you.
- Identify educational activities suited to prepare you for these tasks?
- Think of curricular (e.g. classroom-based), co-curricular (e.g. exercises, tools) and extra-curricular (e.g. competitions, internships) that might prepare you for these tasks.

Step 2:

Build a competency statement (ABCDE)

The Essential Elements of Competency

Competency is most effectively described using 5 key elements:

A - actor (who exhibits the competency);

B - behavior (what task the actor is expected to complete);

C - context (how the behavior is enacted);

D - degree (how much time, accuracy and degree of completion);

E - employability (what professional skills are necessary for this task to be enacted in a way that would be appropriate for the workplace).

A - actor (who exhibits the competency);

B - behavior (what task the actor is expected to complete);

C - context (how the behavior is enacted);

D - degree (how much time, accuracy and degree of completion);

E - employability (what professional skills are necessary for this task to be enacted in a way that would be appropriate for the workplace).

Cybersecurity students taking an IS136 Disaster Recovery Business Continuity level community college course who have completed Introduction to Information Systems, Information to Operating Systems and Networking Security Fundamentals will act as vulnerability assessment analysts (VAM) with access to the risk assessments of Dr. Know's medical office network and the CSET 10.3 tool to perform technical and non-technical risk and vulnerability assessments of the local computing environment (T0549). They will identify 5 key risks within 4 hours and produce a risk assessment and recommendations report which clearly communicates the found risks for a non-technical user.

A - Actor

- Identify level of participant (e.g. high schooler, freshman, junior etc.)
- State any previous courses and/or knowledge they should have acquired before attempting this competency
- Summarize assumed level of knowledge
- Infers anticipated level of proficiency

B - Behavior

- Corresponds with work role and task listed in existing frameworks (e.g. NICE framework or DoD DCWF)
- Identifies work role and specific task (s)
- Note: identifying the task and work role builds a direct connection between the educational activity and the workplace.

C - Context

- This is the context in which the task is performed.
- Describe the scenario in which the competency is demonstrated.
- What resources and technology are provided, what constraints are enforced.

D - Degree

- Identifies how much time might be assumed for competent engagement with task, how much accuracy is required and how much of the task needs to be completed
- Shifts focus from academic (potential 100% by each individual) to 'would this be good enough for an employer?'

E - Employability

- A person can be technically able but remain unemployable unless they also have the professional skills required by a specific workplace.
- Professional skills tend to include teamwork, critical thinking, communication, integrity, and ethical judgement and reasoning (https://www.montreat.edu/student-life/montreat-360/).
- These cannot be tacitly assumed, but need to be identified and stated.

Step 3:

Inputs and Outputs

This presentation was given at the 2023 National Cybersecurity Education Colloquium

CPNC

Next steps

- Workshops on Thursday 21st and Friday 22nd September (NCEC)
- Two day workshop on Thursday 12th and Friday 13th October
- E-Handbook available - https://www.caecommunity.org/national-center/careers-preparation-national-center
- Contact zfowler@norwich.edu

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Break

3:15 - 3:30pm

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Education Pathways National Centers Workshop

This presentation was given at the 2023 National Cybersecurity Education Colloquium

This presentation was given at the 2023 National Cybersecurity Education Colloquium