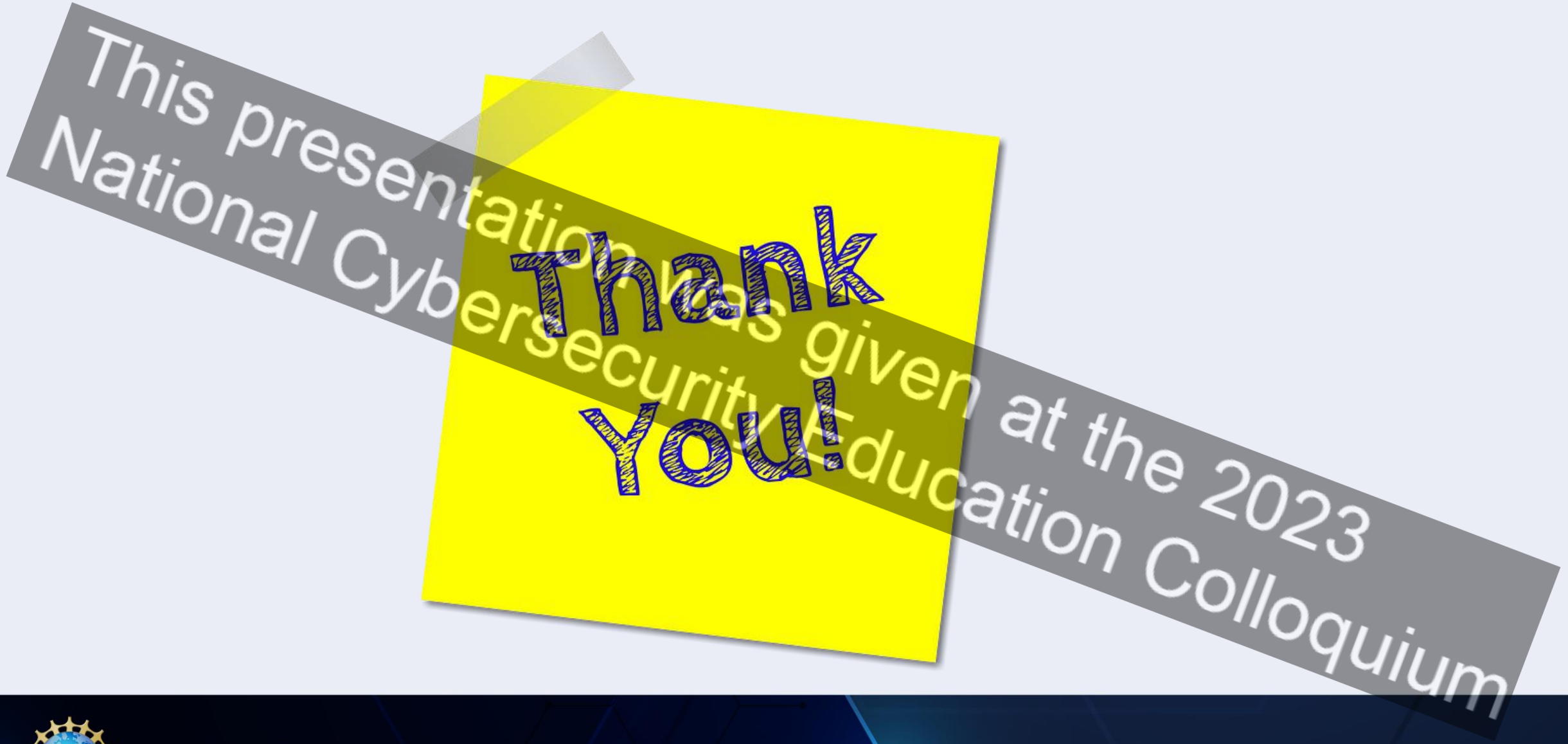
EDU | DIRECTORATE FOR STEM EDUCATION

Updates on Cybersecurity Education & Workforce Development Initiatives

NCEC 2023

Ambareen Siraj, NSF

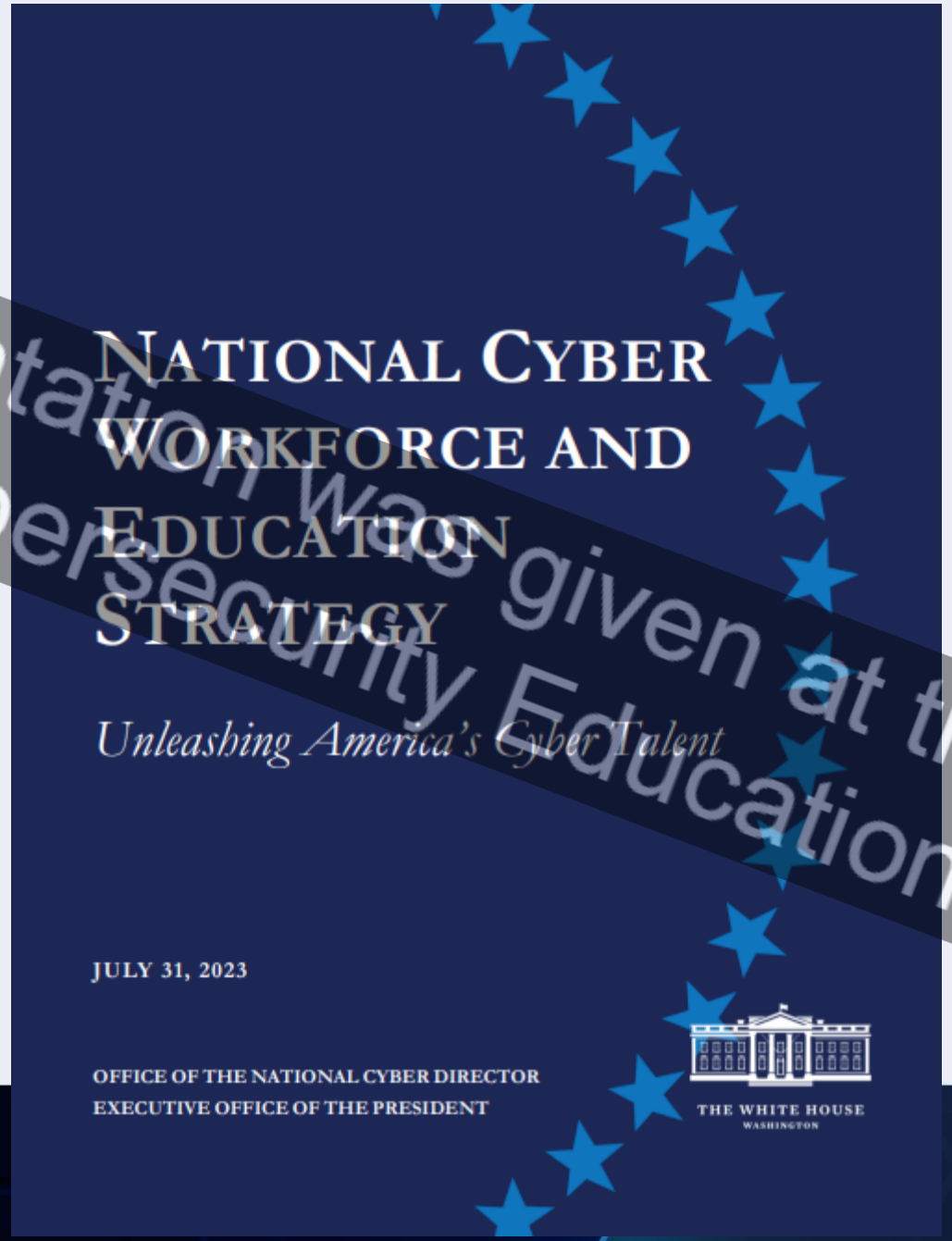

This presentation was given at the 2023
National Cybersecurity Education Colloquium
Thank
You!

Outline

- National Cyber Workforce and Education Strategy and YOU
- NSF SFS program overview
- NSF SaTC-EDU program overview
- Funding opportunities
- Special initiatives updates
- Program announcements
- Engagement opportunities

<Slide deck will be shared>

[Preparing Our Country for a Cyber Future | ONCD | The White House]



National Science Foundation
Directorate for STEM Education (EDU)

The Four Pillars

1. **Equip Every American with Foundational Cyber Skills**
2. **Transform Cyber Education**
3. **Expand and Enhance America's Cyber Workforce**
4. Strengthen the Federal Cyber Workforce(s)

Where you can make direct impact

Academia Engagement – Pillar 1 (Cyber Skills for All)

- Integrating foundational cyber skills in all educational frameworks, programs, and activities

- Fostering ecosystem approaches to enhance foundational cyber skill learning opportunities.

  - *STRATEGIC OBJECTIVE 1.1: MAKE **FOUNDATIONAL CYBER SKILL LEARNING OPPORTUNITIES AVAILABLE TO ALL***

Academia Engagement – Pillar 2 (Transform Education)

- Establishing/extending education and workforce development ecosystems through local/regional partnerships
- Facilitating innovative and broader engagement
- Integrating cybersecurity across disciplines
- Ensuring safe and secure cyber learning environments
  - *STRATEGIC OBJECTIVE 2.1: BUILD AND LEVERAGE ECOSYSTEMS TO **IMPROVE CYBER EDUCATION***

Academia Engagement – Pillar 2 (Transform Education)

- Evaluating effective learning practices for the development of **cyber education resources aligned with stages of cognitive development**
- Infusing **applied cyber content in interdisciplinary education** programs
- Making cyber curricula **available and accessible**
- Developing **concurrent and transferrable credit opportunities** for high school students
- Using innovative models for academic **credit with outside of class cyber learning experiences**.

- *STRATEGIC OBJECTIVE 2.2: **EXPAND** COMPETENCY-BASED **CYBER EDUCATION***

Academia Engagement – Pillar 2 (Transform Education)

- Growing advanced degree programs to strengthen research and development
- Increasing the cyber teaching capacity of K-12 systems and postsecondary institutions
- Expanding the cyber faculty pipeline
- Preparing interdisciplinary cyber educators

  - *STRATEGIC OBJECTIVE 2.3: INVEST IN **EDUCATORS** AND IMPROVE CYBER **EDUCATION SYSTEMS***

Academia Engagement – Pillar 2 (Transform Education)

- Development of learning opportunities and culturally connected cyber content attractive to broader audience.

- Reducing the financial burden on cyber learners with low cost or incentivized opportunities

    - *STRATEGIC OBJECTIVE 2.4: MAKE CYBER EDUCATION AND TRAINING MORE **AFFORDABLE AND ACCESSIBLE***

Academia Engagement – Pillar 3 (Workforce)

- Meaningful partnerships with community colleges
- Developing work-based learning opportunities
  - *STRATEGIC OBJECTIVE 3.2: PROMOTE SKILLS-BASED HIRING AND WORKFORCE DEVELOPMENT*

Academia Engagement – Pillar 3 (Workforce)

- Collaborating with organizations that serve or operate within underserved and underrepresented communities

- Supporting veterans' participation in cyber workforce

  - *STRATEGIC OBJECTIVE 3.3: LEVERAGE THE **DIVERSITY** OF AMERICA TO STRENGTHEN THE CYBER WORKFORCE*

Major Theme Across the Strategy

Implementing the Strategy

- Your role as Educator is critical to make this national mission successful.

NSF's History & Mission

An independent federal agency created by Congress in 1950 "*to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense...*"

- The only federal agency whose mission includes support for all fields of fundamental science and engineering.

EDU | DIRECTORATE FOR STEM EDUCATION

Division of Graduate Education (DGE)

Supports innovative, inclusive, high quality graduate education in the STEM (Science, Technology, Engineering, and Mathematics) fields.

National Science Foundation
Directorate for STEM Education (EDU)

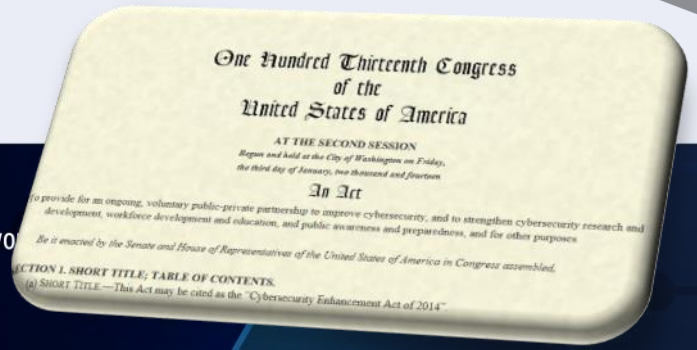
Preparing a diverse STEM workforce and a well-informed citizenry

Cybersecurity Education and Workforce Development Team at DGE

- Victor P. Piotrowski, Lead Program Director,
- Ambareen Siraj, Program Director
- ChunSheng Xin, Program Director
- Li Yang, Program Director

CyberCorps®: Scholarship for Service (SFS) Program

- **Federal scholarship grant program by National Science Foundation (NSF)**
  - recruit and train the next generation of cybersecurity professionals to serve in the cybersecurity mission for federal, state, local, and tribal governments.
  - Interagency partnership between NSF, the Office of Personnel Management (OPM), and the Department of Homeland Security (DHS).


One Hundred Thirteenth Congress
of the
United States of America

AT THE SECOND SESSION

An Act

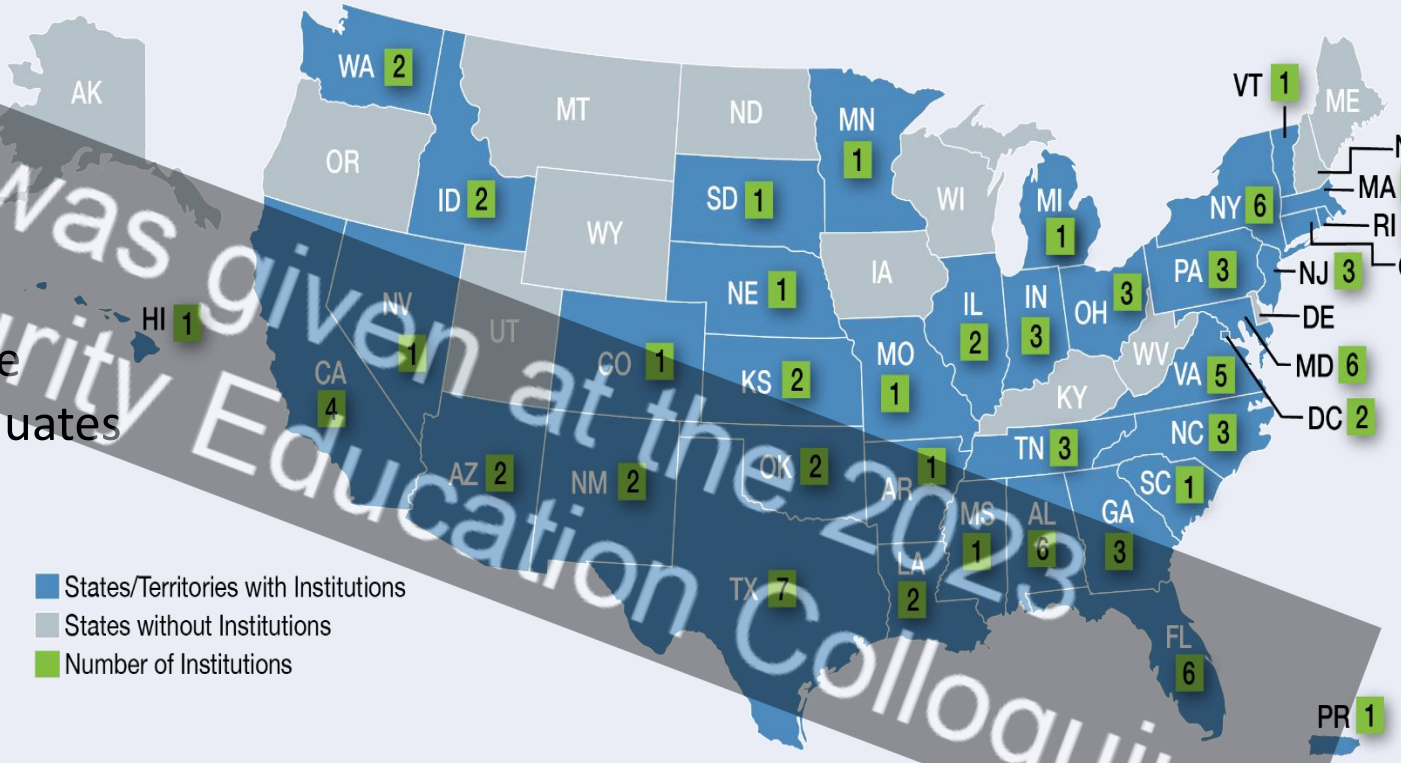
Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

(a) SHORT TITLE.—This Act may be cited as the "Cybersecurity Enhancement Act of 2014".

Cybersecurity Enhancement Act of 2014

SFS Program Impact

- 98 institutions with active scholarship awards, plus 8 community colleges in the Community College Cyber Pilot (C3P) and 28 community college Pathway partners
- 39 states + District of Columbia and Commonwealth of Puerto Rico
- Since 31 students in 2001, 5,110 students have been awarded scholarships with 350-400 graduates each year
- Placement rate 95% in 357 government organizations



CyberCorps® Scholarship for Service (SFS) – NSF 23-574 Solicitation Criterion

(Student Eligibility and Stipends)

- **Students must be US citizens or permanent residents.**

- Pays **tuition** annually.

- Academic-year stipends of **$27,000 per year for undergraduate students and $37,000 per year for graduate students**.

- A **professional allowance of $6,000 per academic year** for the SFS Job Fair and other related travel, conferences, research materials, books and supplies including a one-time purchase of a laptop, professional training, and certifications, etc.

SFS Grant Application

- CyberCorps(R) Scholarship for Service (SFS) (nsf23574) | NSF - National Science Foundation
  - July annually

- Questions? Contact SFS Team at sfs@nsf.gov

CyberCorps® Scholarship for Service (SFS) – NSF 23-574 Solicitation Criterion

(Institutional Eligibility)

A proposing institution must provide **clearly documented evidence of a strong existing academic program in cybersecurity.**

*In addition to information provided in the proposal narrative, such evidence can include **ABET accreditation in cybersecurity**; a designation by the National Security Agency and the Department of Homeland Security as a Center of Academic Excellence in Cyber Defense Education (**CAE-CDE**), in Cyber Operations (**CAE-CO**) or in Research (**CAE-R**); or **equivalent evidence** documenting a strong program in cybersecurity.*

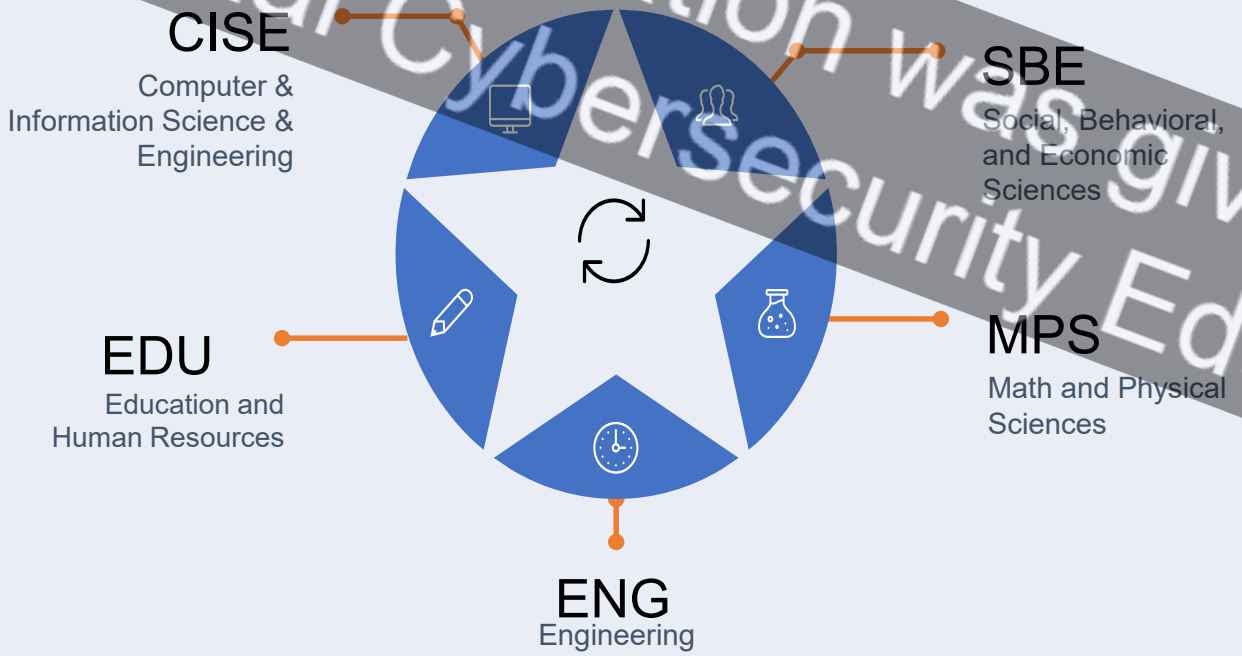
Additional Solicitation Specific Review Criterion

- The quality of **education and research in cybersecurity at the institution**, the extent to which they are **integrated**, and research opportunities for students.
- The quality of **experiential learning environment** to increase students' knowledge, skills, and competencies in cybersecurity.
- The quality and extent to which **students are engaged in extra-curricular activities** related to cybersecurity and privacy.
- The **evidence-based broadening participation strategies**.

SFS Workshop at NCEC

- Thursday, Sept 21st
  - **Becoming an NSF CyberCorps® Institution** (8:00 – 10:00 AM)
  - Room M202 (2nd floor)

Secure and Trustworthy Cyberspace (SaTC)



Mission & Vision

"To promote a secure, safe, and trustworthy future for cyberspace and cyber enabled society."

"To support rigorous research and advances on the challenges and opportunities for security, safety, and trust in global cyberspace and its many consequences for the nation and the world."

>1000 Active Awards Across Broad Topic Areas

- Authentication
- Biometrics
- Cryptography
  - Applied and Theory
- Cyber Physical Systems
- **Cybersecurity Education**
- Formal Methods
- Hardware Security Architectur
- Data Science
- Information Integrity
- Language-Based Security
- Mathematics and Statistics
- Networking & Intrusion Detection
  - Wired and Wireless
- Privacy
  - Applied and Theory
- Social, Behavioral and Economic Sciences
- Software
- Systems
- Transition to Practice (TTP)
- Usability and Human Interaction

M workforce and a

Types of SaTC Awards across Directorates

CORE (CISE)	Transition to Practice (TTP)	Education (EDU)
Focus: **Fundamental research** in one/more of CISE/SBE/MPS/ENG Funding levels: • **Small**: Up to 3 years, $600K • **Medium**: Up to 4 years, $1.2M No submission deadlines Open to universities & non-profits; PI may submit 2 proposals/FY Int'l collaboration programs with Israel, Ireland, Canada, Germany, India, Czechia **Medium** MUST include BPC plan at time of submission	Focus: **transitioning existing research** results to practice Funding levels: • **Small**: Up to 3 years, $600K • **Medium**: Up to 4 years, $1.2M No submission deadlines Open to universities & non-profits; PI may submit 1 proposal/FY **Medium** MUST include BPC plan at time of submission	**Focus: cybersecurity education** Funding levels: • Up to 3 years, $400K • If include both computer scientist and education specialist, up to $500K No submission deadlines Open to universities & non-profits; PI may submit 1 proposal/FY

Secure and Trustworthy Cyberspace Education Designation (SaTC-EDU)

- Improve
  - cybersecurity learning and learning environments for students in formal or informal settings
- Develop
  - activities to help K-16 teachers create or integrate cybersecurity into formal and informal learning settings
  - new assessment tools to measure student learning
- Investigate
  - approaches to make cybersecurity education and workforce development broadly diverse and inclusive
- Evaluate
  - the effectiveness of cybersecurity learning approaches, outreach, and retention activities

SaTC Projects of Special Interest

- **Technical**
  - Increased focus on emerging areas and future threats
  - Significantly expand Transition to Practice focus
  - Large-scale testbeds and datasets
- **Educational**
  - Education tied to all of the above
  - Education supplements for core research projects
- **Interdisciplinary**
  - Increased focus on holistic and inter-disciplinary research
  - Increased emphasis on privacy across technologies
  - Consider richer notions of trust beyond security and privacy
  - Broader integration of new technology, people, applications, contexts, and education
  - Significantly expand inter-disciplinary community building efforts
- **Increased industry/govt partnerships**

CHIPS and Science ACT of 2022

- AI and Cyber
- Quantum computing and cyber
- Aerospace and cyber
- Advanced manufacturing and cyber
- Emerging wireless technologies and cyber
- Engineering and Cyber

SaTC-EDU Grant Application

- Secure and Trustworthy Cyberspace (SaTC) (nsf22517) | NSF - National Science Foundation
  - Accepted ANYTIME

- Questions?
- Contact SFS Team at sfs@nsf.gov

NSF 23-149

Dear Colleague Letter: Inviting Proposals Related to Open-Source Software Security to the Secure and Trustworthy Cyberspace Program

September 12, 2023

Encourage the submission of novel and high impact proposals:

- **Software engineering frameworks/tools/methodologies**
- **Handling unsafe legacy code**
- **Dependency management**
- **Trust and safety**
- **Incentive and organizational structures for a secure OSS ecosystem**
- **Education and workforce development**

Special Projects Funding

- Per SFS Solicitation:
- *"program is also interested in ideas for forward-looking or unconventional activities that show real promise to have a broad national impact on cybersecurity education and workforce development but fall outside the SFS and SaTC-EDU program boundaries."*

- For example:

Application for **workshop/convening/conference** on emerging topics bringing diverse groups of folks together for a bigger purpose

- Up to 50K

SaTC Aspiring PI Workshop Series

- Next In-person event in Spring 2024 (date TBD April 2024)
  - 1.5 days
    - About 60 attendees in 2023
    - Support for most attendees
- Program
  - Mock Panels
  - One-on-one mentoring sessions
  - Meetings with SaTC PDs
  - Discussion of research ideas
  - Proposal writing skills

Contact: Anna Squicciarini
Email: asquicci@nsf.gov

Other Funding Opportunities at NSF

- ENGINES
- CyberTraining

DIVERSE INNOVATION ECOSYSTEMS

NSF Regional Innovation Engines (NSF Engines) program supports the **development of diverse, regional coalitions** to engage in use-inspired research, drive research results to the market and society, promote workforce development, and ultimately stimulate the economy and create new jobs.

NSF Engine Development Awards – (Type 1)
up to **$1 million** for up to **2** years to plan for an Engine.

NSF Engine projects are funded up to **$160 million**
for up to **10** years (Type 2)

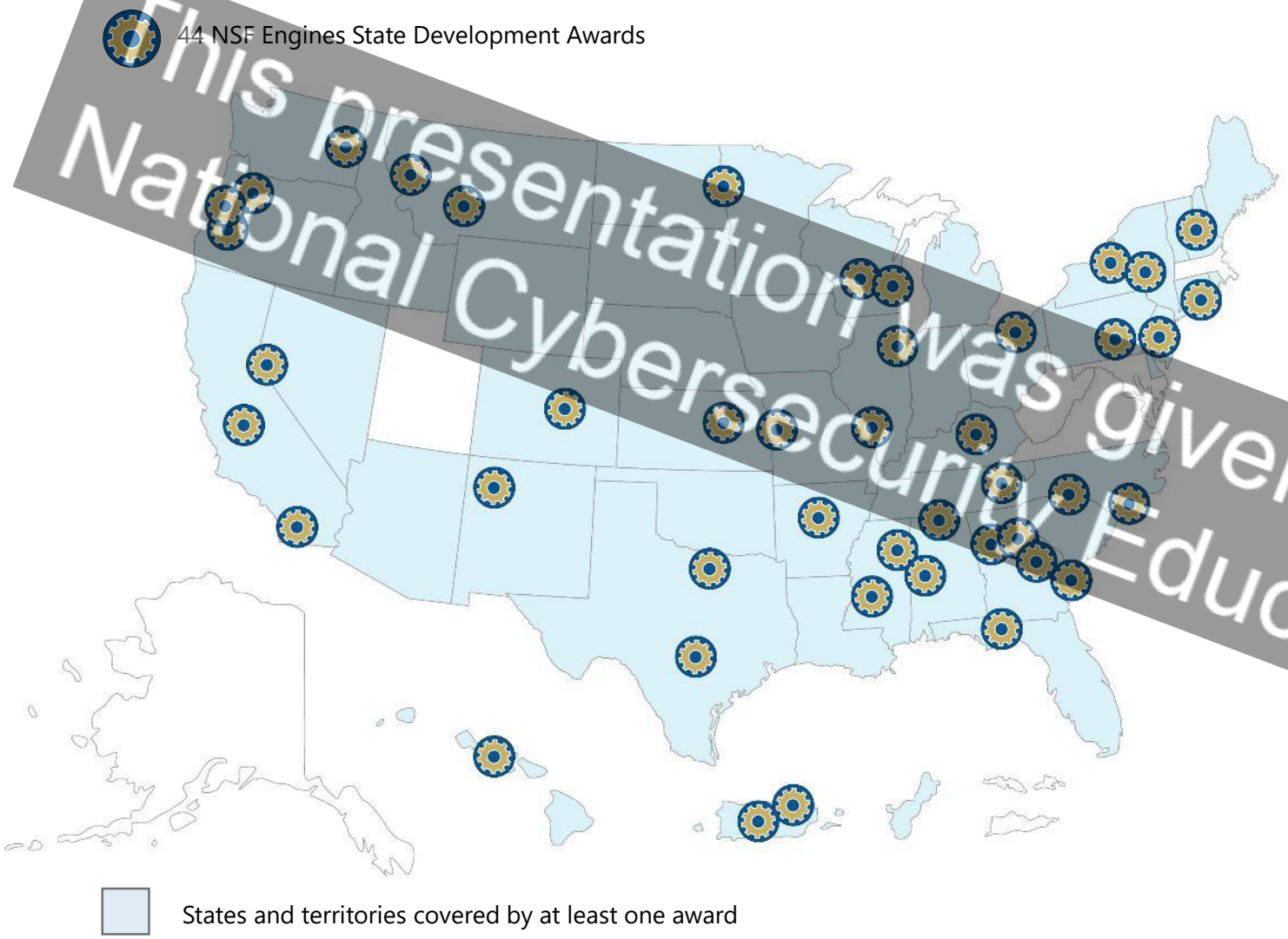
Opportunity available to:

- Academia
- Business & Industry
- Governments
- Nonprofits

NSF invests more than $43 million in NSF Regional Innovation Engines Development Awards (Type 1)

- 44 Type 1 awards to teams across 46 U.S. states and territories in May 2023
- The NSF Engines Development Awards help organizations create connections and develop their local innovation ecosystem **to prepare a strong proposal for becoming a future NSF Engine**
- Each awardee team receives up to $1 million for two years.

DIVERSE INNOVATION ECOSYSTEMS



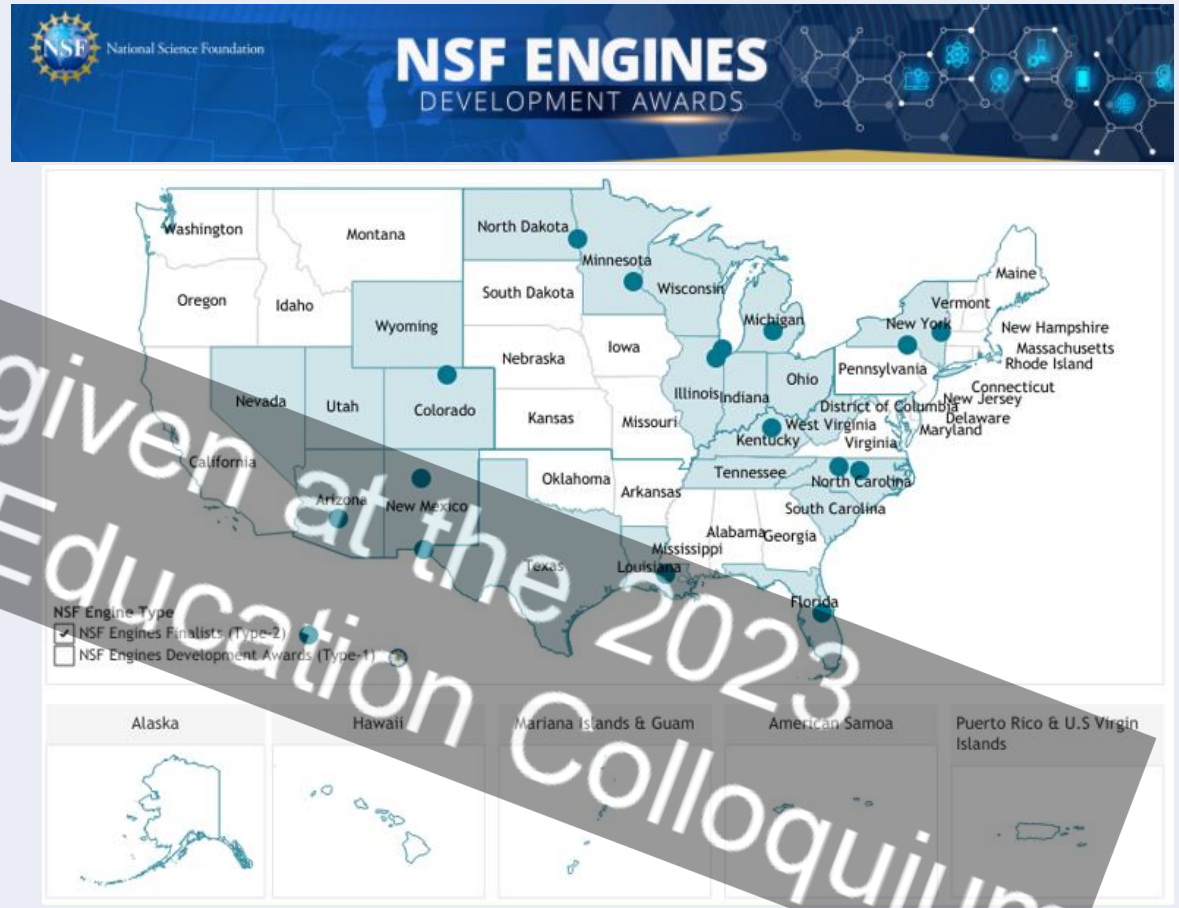
The first-ever NSF Engines Development Awards will help regional partners collaborate to advance key technologies, address societal challenges, and create economic opportunities. The awards to 44 unique teams span universities, nonprofits, business and other organizations across U.S. states and territories.

Topics

Each Award is aligned with one of the following topics.

NSF Engines program selects 16 finalists

- In August, 16 finalist teams selected span a range of key technology areas and societal and economic challenges highlighted in the "CHIPS and Science Act".
- Awards will be announced this winter, with each awardee initially receiving about $15 million for the first two years.
  - Each NSF Engine could receive up to $160 million over 10 years.
- **Pending funding, next round in 2024-25.**



View a map of the NSF Engines finalists.

Training-based Workforce Development for Advanced Cyberinfrastructure (CyberTraining)

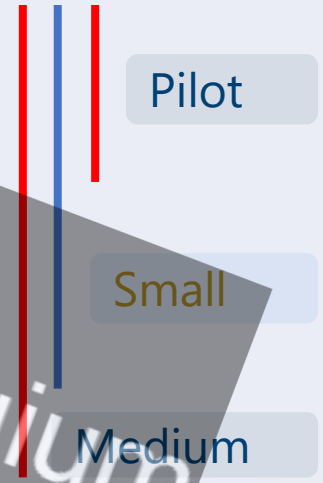
- Spans multiple NSF directorates including EDU/DGE
- Seeks to prepare, nurture, and grow the **national scientific *research* workforce** for ***creating, utilizing,* and *supporting* advanced cyberinfrastructure (CI)** to enable and potentially transform fundamental science and engineering research and contribute to the nation's overall economic competitiveness and security.
- **The specific goals of this solicitation are**
  - (i) to ensure ***broad adoption* of CI tools, methods, and resources** by the research community in order to catalyze major research advances; and
  - (ii) to **integrate** core literacy and **discipline-appropriate** advanced **skills in advanced CI** as well as computational and data-driven science and engineering into the nation's **educational *curriculum and instructional fabric,*** spanning both undergraduate and graduate courses to advance fundamental research.

Cyber Training Project Classes

- **Pilot:** Exploratory projects, $300K over 2 years
- **Small implementation:** $500K over 4 years
- **Medium implementation:** $1M over 4 years

At least one option in #2

1. Identify challenges in research workforce development
2. (a) Broaden use of CI resources (b) CI skills training – expected to coordinate with ACCESS (access-ci.org)
3. Scalability and sustainability of the training program
4. Recruitment and evaluation plans
5. Collective impact strategy
6. Fostering a suitable community



NSF CyberTraining Solicitation (NSF 23-520)

- https://new.nsf.gov/funding/opportunities/training-based-workforce-development-advanced

- **Proposals due January 18, 2024**

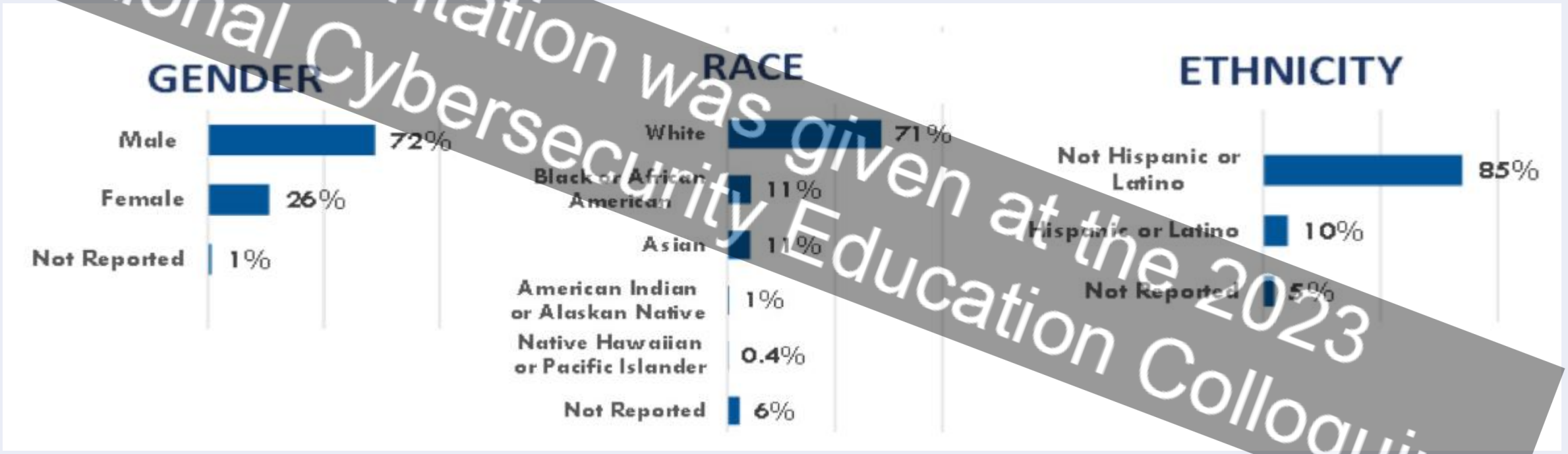
Contact: Chunsheng Xin
Email: cxin@nsf.gov

Newly Launched Special Initiatives Report

- In support of NSF's commitment to attract, retain, and graduate students from diverse backgrounds in cybersecurity workforce
- Three initiatives
  - Bridge to Cyber
  - Jumpstart to Cyber Programs
  - Special engagement program for aspiring PIs from and/or serving underrepresented communities

Motivation

- To increase diversity in SFS scholars



Bridge to Cyber Program

- Three year collaboration between SFS program and the Center for Inclusive Computing (CIC) at Northeastern University
- Focused on building bridge programs that connect students from non-computing backgrounds to the graduate degrees in cyber
- Two cohorts of up to 8 SFS institutions in 2023 and 2024
  - 1st cohort of 7 members underway
  - Next cohort call OPEN

- Questions? Contact Carla Brodley at c.brodley@northeastern.edu

Bridge to Cyber Program 1st Cohort

Name of School	Primary PI	Degree Bridge Connects To	Target student profile	Target student URG%	Total students served over life of funding	Mode of Bridge	Mode of Degree Program	Duration of Bridge
George Washington University	Arkady Yerukhimovich	Master's in Cybersecurity in Computer Science	domestic recent non-CS graduates + upskilling working professionals	50% women, 25% races/ethnicities historically underrepresented in tech.	25	online, asynch	on ground, synchronous	3 semesters; 12 months
New York University	Nasir Memon	MS in Cybersecurity; MS in Computer Science; equivelent MS degrees at 9 partner schools	non-STEM recent grads + working professionals + upskilling STEM grads	50% women, 25% races/ethnicities historically underrepresented in tech.	1100	online, combo sync/async	on ground, synchronous	7.5 months
Oakland University	Huirong Fu,	Master of Science in Cybersecurity	working adults with undergrad degree in something other than CS	50% women, 25% races/ethnicities historically underrepresented in tech.	25	on line, asynchronous + optional in person elements	on line, asynchronous + optional in person elements	up to 12 months
Old Dominion University	Brian Payne, Rafael Diaz	MS in Cybersecurity	Recent graduates and alumni of ODU	50% women, 25% races/ethnicities historically underrepresented in tech.	0	on ground, synchronous with asynch component	on ground, synchronous	projected at 2 semesters; ~9 months
Tuskegee University	Fan Wu,	MS in Information Systems and Computer Security	Third and fourth year UG students + alumni career changers	60% women, 40% races/ethnicities historically underrepresented in tech	10	on ground/synch (UG) + online/asynch (career changers) options	on ground, synchronous	2 semesters; 9 months
University of Alabama at Birmingham	Ragib Hasan	Masters in Cyber Security	Students with no CS background.	50% women, 30% races/ethnicities historically underrepresented in tech	24	on ground	on ground, synchronous	2 semesters; 9 months
University of Rhode Island	Victor Fay-Wolfe	Professional Science Master Degree in Cyber Security	Non-CS undergrads, emphasis on students from pops. historically marginalized in cyber + career changers + those w/economic need.	50% women, 25% races/ethnicities historically underrepresented in tech.	20	on line, asynchronous	on line, asynchronous	6 months

Contact: fu@oakland.edu

Oakland University (NSF Award# 2146280)

- Target group:
  - Working adults with undergraduate degree in something other than CS
- Mode of delivery: Online, asynchronous + optional in person elements
- Duration and Timeline of Bridge: Up to 12 months for each individual
- Bridge Courses and Activities:
  - **Computer Networking, Intro. to Programming, System Administration**
  - Guided self-paced and individualized study, Learning framework, Library of educational modules + OU labs, Problem-solving demonstrations online and in-person weekly at different levels providing a scaffolding approach for students.
- Projected# of participants:
  - 60

Contact: ragib@uab.edu

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

(NSF Award# 2234868)

- Target group:
  - Students with a Bachelor's degree but No Computer Science background
- Mode of delivery:
  - In-person
- Duration and Timeline of Bridge:
  - Two semester bridge with four courses, bridge graduates with a min of 3.0 GPA to be admitted directly into MS Cyber Security program
- Bridge Courses and Activities:
  - Four compact fast-paced courses on **Python, C++/Java, Discrete Mathematics, Algorithms and Data Structures**
  - Structured mentoring support and tutoring, Full tuition support for bridge courses
- Projected# of participants:
  - 20 students

Contact: arkady@gwu.edu

The George Washington University (NSF Award# 1753983)

- Target group:
  - non-STEM students seeking pathway into cyber security
- Mode of delivery:
  - online bridge, in-person MS-Cybersecurity
- Duration and Timeline of Bridge:
  - 1 year, 4 courses (4th course included in MS degree)
- Bridge Courses and Activities:
  - **Programming 1+2+3 and intro-to-security**
- Projected# of participants:
  - 5-10 in AY24, more in later years

Contact: Abhijit Chitnis aac664@nyu.edu

New York University Tandon (NSF Award#1922291)

- Target group:
  - Recent college graduates, as well as mid-career professionals with non-technical degrees/backgrounds.
- Mode of delivery:
  - Fully online, both synchronous and asynchronous learning
  - 3 starts per year
- Duration and Timeline of Bridge:
  - 21-week format (20 – 30 hours per week), or
  - 28-week format (30 – 40 hours per week)
- Bridge Courses and Activities:
  - 30+ topics including, **Data Structures and Algorithms in C++, Discrete Math, Operating Systems, Networks, Hardware Systems**
- Projected# of participants:
  - 800 students per year

Contact: Vic Fay-Wolfe vfaywolfe@uri.edu

University of Rhode Island (NSF Award# 2042416)

- Target group:
  - Undergraduates with degrees from a non-computing field who wish to enter a career in cybersecurity
- Mode of delivery:
  - Completely online
- Duration and Timeline of Bridge:
  - 6 months, June - December each year
- Bridge Courses and Activities:
  - Courses: **Intro to programming, Intro to Computer Systems, Intro To Cybersecurity**
  - Activities: Co-curricular academic support, career readiness, cohort community building/support
- Projected# of participants:
  - 10 bridge participants per year

Contact: Brian Payne (bpayne@odu.edu)

Old Dominion University (NSF Award# 2042882)

- Target group:
  - Cybersecurity Bridge for Enrollees New to Technology **(C-BENT)** is designed to attract graduate students from populations historically marginalized in technology
- Mode of delivery:
  - Asynchronous
- Duration and Timeline of Bridge:
  - One semester
- Bridge Courses and Activities:
  - MS assessment (Summer 2023 / Summer 2024) to align technical and non-technical coursework
  - Course development (using digital learning guidance) and piloting
  - Focus groups to identify barriers and outreach to targeted students
  - Integration of High-Impact Practices into students' courses and experiences
- Projected# of participants:
  - 50 students each year

Contact: Dr. Fan Wu (fwu@tuskegee.edu)

Tuskegee University (NSF Award# 2234911)

- Institutional objective:
  - To formalize the currently informal Cybersecurity bridge and focus its reach on undergraduate students pursuing college degrees in non-computer science areas.
- Target group:
  - Non-CS majors from populations that are historically marginalized in technology.
- Mode of delivery:
  - Onsite
- Duration and Timeline of Bridge:
  - One-year bridge program (Complete four bridge courses in senior year and start master program in the following fall)
- Bridge Courses and Activities:
  - Programming I
  - Discrete Mathematics
  - Introduction to Statistics
  - Introduction of Computer Information System
- Projected# of participants:
  - 15 students in pilot cohort

Bridge to Cyber Round 2 Open to SFS Institutions

- 2nd Cohort Application open until October 6
- https://tinyurl.com/ykqqmjph

- If selected, funding will be provided as supplemental award
- Funding can cover salaries, marketing and recruiting, student tuitions/incentives, etc.
- Questions? Contact Carla Brodley at c.brodley@northeastern.edu

Jumpstart into Cyber Program Overview

- **Program open for public student registration until Oct 1**
- https://www.sans.org/mlp/jumpstart-into-cyber/

  - 1000+ applications for 250 seats (Two cohorts of Approximately 125 each)
    - 91% of applicants from under-represented groups
  - Cohort 1 on Step 2 (completing their SANS course and GFACT certification)
  - Cohort 2 on Step 1 (registering and playing CyberStart for qualification)
    - Will transition to Step 2 in mid-October

JumpStart into Cyber Program

- One year collaboration between SFS, Sinclair Community College and SANS Institute
- Exclusive two-step cybersecurity journey specially designed to engage and empower underrepresented student groups, including women, Black, African American, Latino(a), Hispanic, and Indigenous students

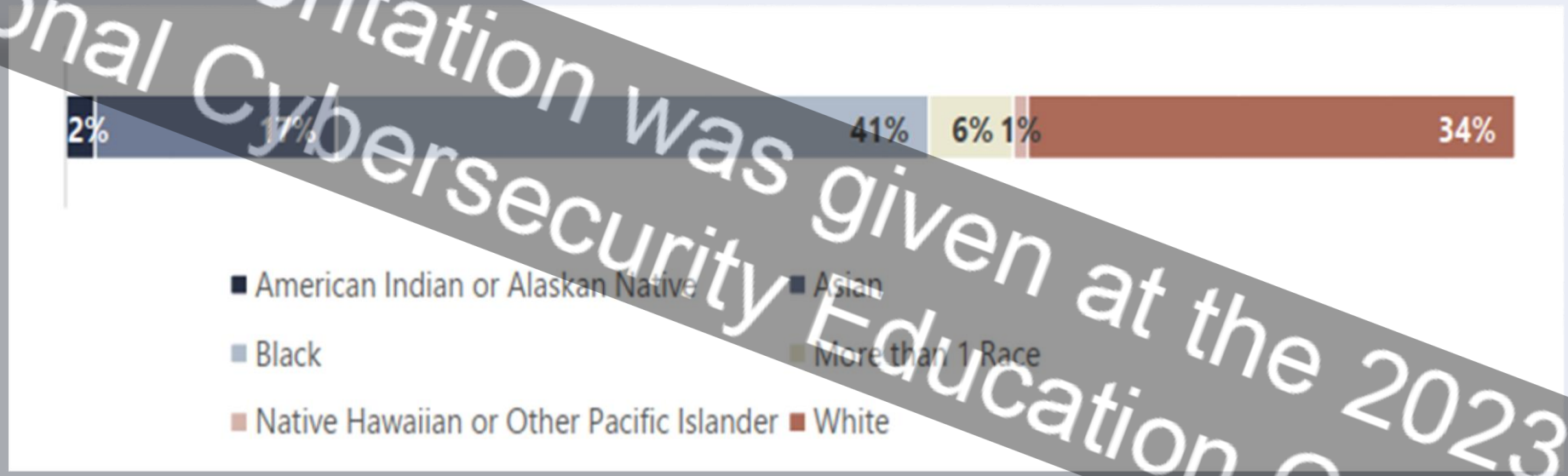
JumpStart into Cyber Program Update

- **1000+ applications for 250 seats** (so far)
- **91% of applicants from under-represented groups**
- **Cohort 1** on Step 2 (completing their SANS course and GFACT certification)
  - 89% GIAC success rate to date
  - 48 pending exam results
- **Cohort 2** on Step 1 (registering and playing CyberStart for qualification)
  - Will transition to Step 2 in mid-October
- **Program open for public student registration (Cohort 2) until Oct 1**

https://sinclairwfd.regfox.com/cyberstart

JumpStart into Cyber Cohort 1 Demographic Data

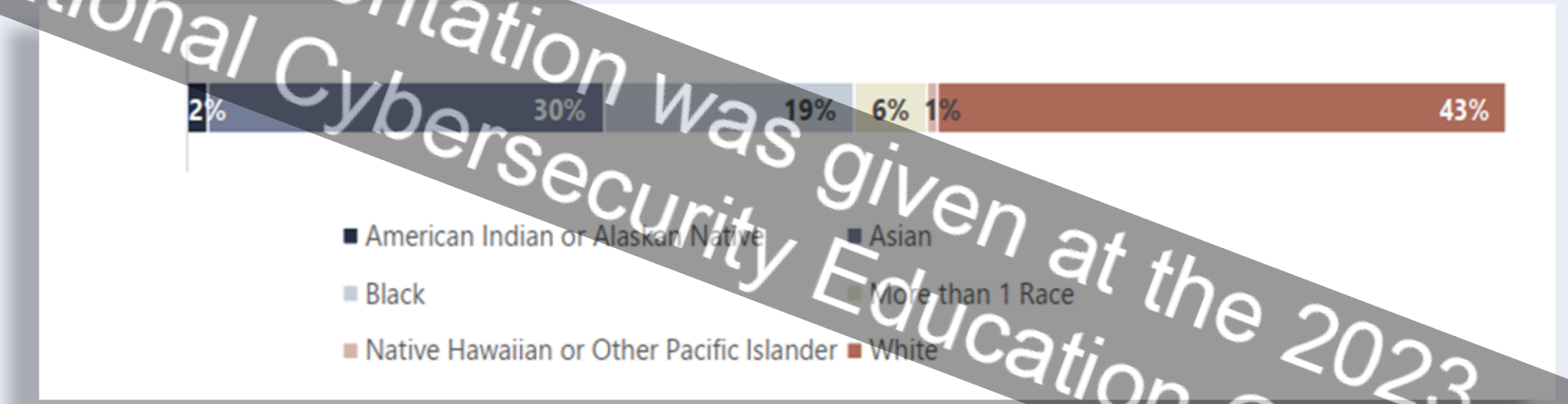
Step 1 - CyberStart



*Figures provided by The Rucks Group, LLC. The Rucks Group, LLC is a leading research and evaluation firm based in Dayton, Ohio with extensive experience providing evaluation and consultation services to federally funded projects.

JumpStart into Cyber Cohort 1 Demographic Data

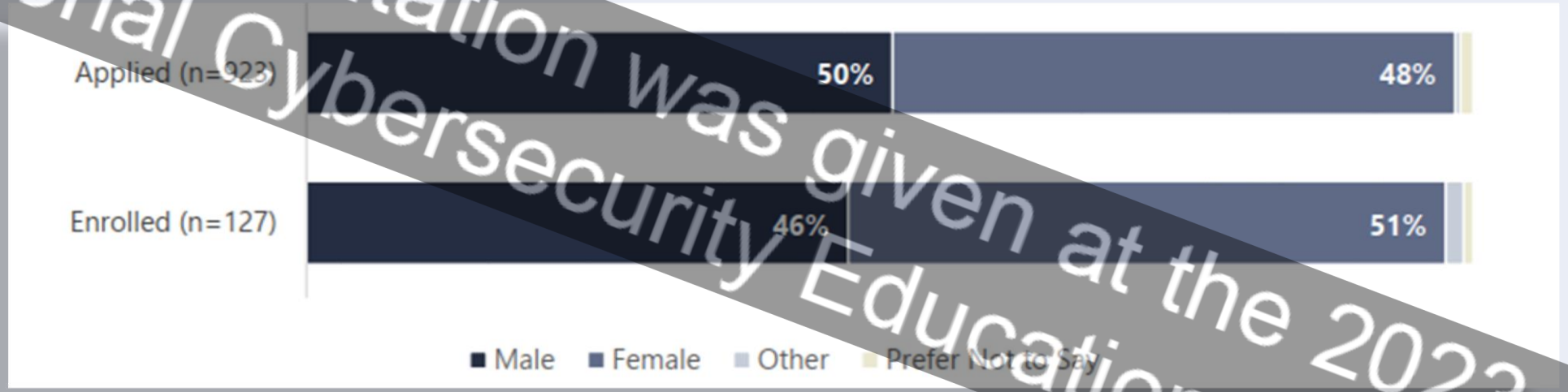
Step 2 - SANS SEC275: Foundations course and GFACT Certification



*Figures provided by The Rucks Group, LLC. The Rucks Group, LLC is a leading research and evaluation firm based in Dayton, Ohio with extensive experience providing evaluation and consultation services to federally funded projects.

JumpStart into Cyber Cohort 1 Demographic Data

Step 2 - SANS SEC275: Foundations course and GFACT Certification



*Figures provided by The Rucks Group, LLC. The Rucks Group, LLC is a leading research and evaluation firm based in Dayton, Ohio with extensive experience providing evaluation and consultation services to federally funded projects.

Engaging With Faculty from Underrepresented Communities

- To build pool of successful PIs from underrepresented communities who can impact cybersecurity education and workforce development in their institutions

- Special Engagement session for around 40+ faculty in September (Informed by two listening sessions held in May)
  - Funding programs overviews
  - Panel of PIs from target groups discussing overcoming challenges with best practices
  - **Peer support groups**

- **Connect and STAY CONNECTED (Forum hosted by Tuskegee University)**
  - https://discord.gg/AgMmu4a4

Finally!! CFR: 45 CFR 620

Contact: Li Yang (liyang@nsf.gov)

FEDERAL REGISTER

The Daily Journal of the United States Government

® Rule

NSF Federal Cyber Scholarship-for-Service Program (CyberCorps® SFS)

A Rule by the National Science Foundation on 08/01/2023

National Science Foundation
Directorate for STEM Education (EDU)

Preparing a diverse STEM workforce and a well-informed citizenry

AI SFS Initiative at NSF

Per CHIPS and Science Act of 2022

the NSF Director, in coordination with the Office of Personnel Management, shall **submit a report** on the **need and feasibility**, and if appropriate, plans to implement a program to recruit and train the next generation of **artificial intelligence professionals** to meet the needs of Federal, State, local, and Tribal governments.

Contact: Li Yang (liyang@nsf.gov)

AI SFS Initiative Tasks: Report in Summer 2024

Task (A) recent statistical data on the **size, composition, and educational requirements of the Federal AI workforce**, including an assessment of **current and future demand** for additional AI professionals across the Federal Government;

Task (B) an **assessment of the capacity of institutions of higher education** to produce graduates with degrees, certifications, and relevant skills related to artificial intelligence that meet the current and future needs of the Federal workforce; and

Task (C) an evaluation of the **need for and feasibility of establishing a scholarship-for-service** program to recruit and train the next generation of artificial intelligence professionals to meet the needs of Federal, State, local, and Tribal governments, including opportunities for leveraging existing processes and resources for administering the Federal Cyber Scholarship-for-Service Program established under section 302 of the Cybersecurity Enhancement Act of 2014 (15 U.S.C. 7442) in standing up such a program.

Contact: Li Yang (liyang@nsf.gov)

NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 23-099

Dear Colleague Letter: Request for Information on the Capacity of Institutions of Higher Education to Produce Graduates with Degrees, Certifications, and Relevant Skills Related to Artificial Intelligence

May 8, 2023

Received over 110 Reponses from the community about AI courses and programs in IHEs.

Please email liyang@nsf.gov if you have an existing or prospective AI programs in your institution

Apply to Serve as Panelist

- Want to be considered to serve on SFS and SaTC-EDU panels?

https://www.surveymonkey.com/r/CyberED

Stay Informed with SFS Team

- NSF SFS Mailing list server
  - Open to anyone/public
  - To announce updates and opportunities from our programs (SFS and SaTC-EDU)
    - No more than twice a month

  - SUBSCRIBE by:
  - Sending an email with
    - no subject line
    - a body of "SUBSCRIBE SFS Firstname Lastname“ (without quotes)
    - to LISTSERV@LISTSERV.NSF.GOV
  - and then
    - respond to the confirmation message by typing OK.

NSF SFS & SaTC-Edu Team Contacts

- Victor P. Piotrowski, Lead Program Director,
  - Telephone: (703) 292-5141
  - email: vpiotrow@nsf.gov
- Ambareen Siraj, Program Director
  - Telephone: (703) 292-8182
  - email: asiraj@nsf.gov
- ChunSheng Xin, Program Director
  - Telephone: (703) 292-7353
  - email: cxin@nsf.gov
- Li Yang, Program Director
  - Telephone: (703) 292-2677
  - email: liyang@nsf.gov


This presentation was given at the 2023
National Cybersecurity Education Colloquium

Applying for NSF Grants 1

- Assumptions
  - Have expertise in related field
  - Have university support and resources
  - Have bandwidth
  - Have tenacity

Applying for NSF Grants 2

- Have an idea? Great!!
- Now find out:
  - Did anyone else have this idea?
  - Why does your idea need to see the daylight?
  - Did NSF ever fund similar ideas?
  - What are these NSF funded programs doing?
  - Which programs in NSF will be interested in your idea?
- Reach out to NSF!

Applying for NSF Grants 3

- Ask NSF for an appointment
- Discuss your idea for feedback
- Gather team and resources
- Write your proposal and submit (adhering to compliance)
- Fingers crossed and wait
- Is yours among the 80%?
  - If so, ask NSF for an appointment to get feedback
- Use the review feedback to submit a stronger proposal