

Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development

April 19, 2024

Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development

NEW funding opportunity available for all non-Federal entities

Goal to create **multistakeholder partnerships** to develop a skilled and diverse workforce to meet industry needs within a **local or regional economy**

Premised on Department of Commerce Principles for Highly Effective Workforce Investments and Good Jobs Principles

Application deadline: May 24, 2024

www.nist.gov/nice



An FAQ is available online.
Informational webinar recording coming soon.

Spring 2024 New RAMPS Communities



NEWS

**NIST Awards \$3.6 Million for
Community-Based Cybersecurity
Workforce Development**

A collage of images related to cybersecurity and community development, including hands shaking, a person using a laptop, and a person using a smartphone, overlaid with a network diagram and a circular graphic containing the text '18 New RAMPS Communities'.

18 New
RAMPS
Communities

2016 Pilot Program

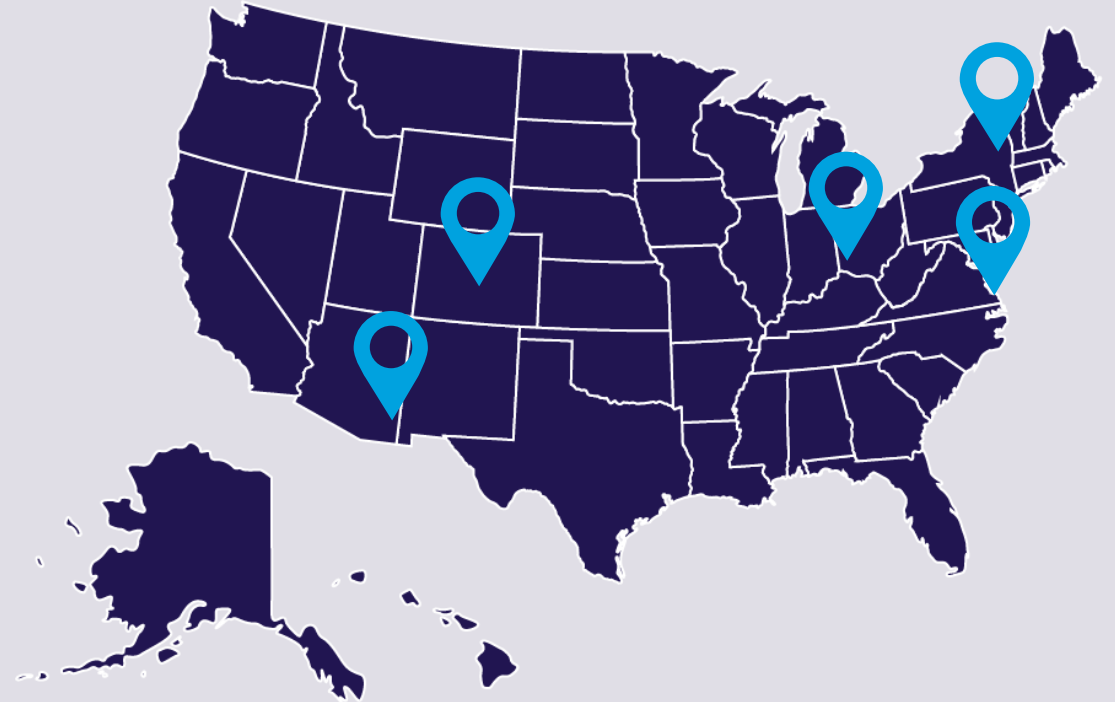
Southwest Region: Arizona Statewide Cyber Workforce Consortium

Western Region: Cyber Prep Program

Central Region: Cincinnati-Dayton Cyber Corridor (Cin-Day Cyber)

Mid-Atlantic Region: Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCyber)

Northeast Region: The Partnership to Advance Cybersecurity Education and Training (PACET)



A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce

NISTIR 8287

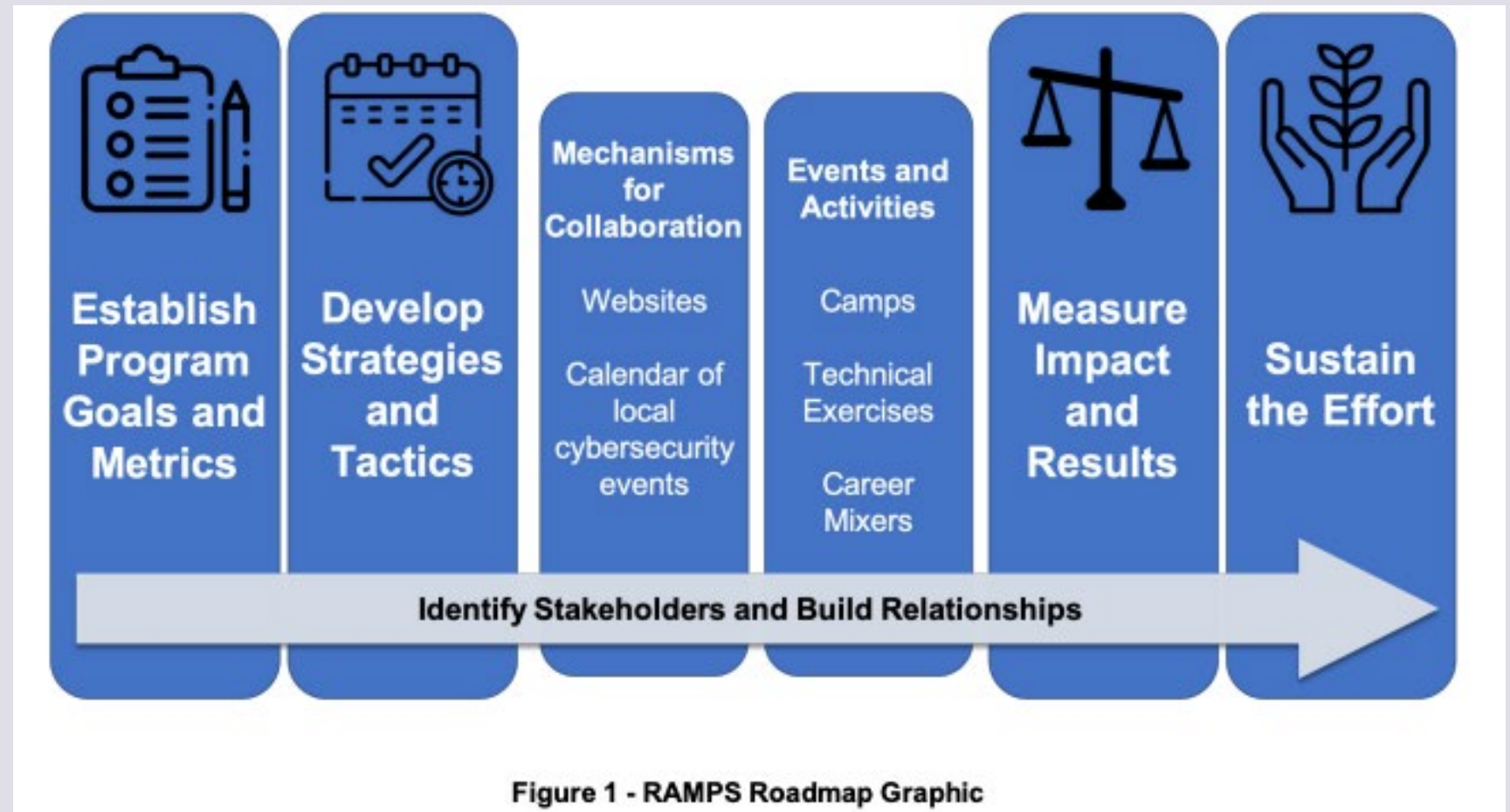


Figure 1 - RAMPS Roadmap Graphic

<https://doi.org/10.6028/NIST.IR.8287>

Applicants Project Must

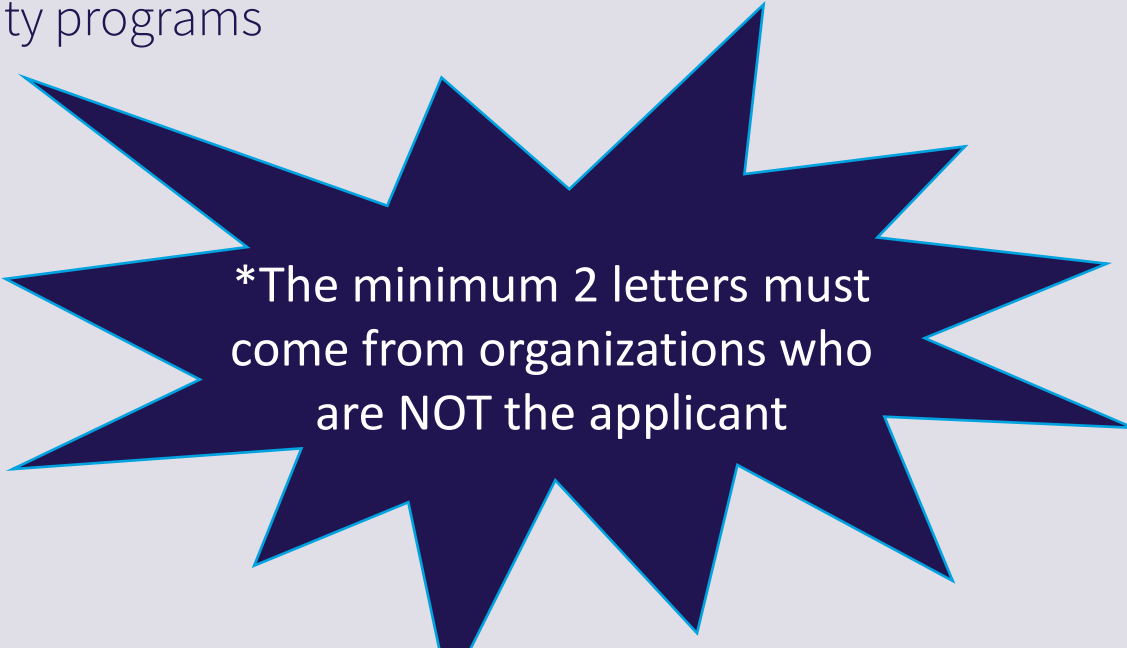
- Demonstrate how the activity aligns with the **Department of Commerce Strategic Plan**, meets the **Effective Workforce Investment Criteria**, and advances the **Good Jobs Principles**.
- **Prioritize Diversity, Equity, Inclusion, and Accessibility** as an essential requirement in strategies intended to diversify the cybersecurity workforce and reach underserved and underrepresented communities.
- Ensure that the partnership is **employer-led, community-focused, learner-centered, standards-based, and outcomes-driven**.
- Describe planned initiatives that align to the goals and objectives of **the NICE Strategic Plan** or help support the strategies of the NICE Implementation Plan.
- Advance uses of the **NICE Framework**, including through demonstration of how the stakeholders intend to use the NICE Framework.
- Identify the workforce **needs of the local economy and assess such workforce** in accordance with the NICE Framework, including ideas for how the multistakeholder organization would leverage the CyberSeek job heat map and career pathways.

Applicants Project Must (cont.)

- Identify opportunities available and recruit employers to **support paid internships, externships, apprenticeships, or cooperative education programs** in conjunction with education and training providers in the local community.
- Identify how it would collaborate with one or more **Center of Academic Excellence in Cybersecurity (CAE), Advanced Technological Education (ATE) programs, or Federal CyberCorps Scholarship for Service (SFS)** institutions located in the region.
- Define **metrics that will be used to measure the success** of their efforts. Metrics should include but not be limited to the number of CAE and ATE programs that participate in the program, outcomes of workforce demand and supply assessment, increases in diversity and inclusion, outcomes of recruitment activities, timeliness of milestones reached, etc.

Program Requirements

- Plan to establish a **multistakeholder** education and workforce **partnership** that includes, at minimum:
 - One institution of higher education or nonprofit training organization*
 - One local employer or owner or operator of critical infrastructure*
- Partnerships are encouraged to have participation from one or more:
 - Federal Cyber Scholarship for Service programs
 - National Centers of Academic Excellence in Cybersecurity programs
 - Advanced Technological Education programs
 - Elementary and secondary schools
 - Training and certification providers
 - Economic development organizations
 - Other community organizations



*The minimum 2 letters must come from organizations who are NOT the applicant

Questions?

Subject Area	Point of Contact
Programmatic and Technical Questions	Danielle Santos Phone: 202-308-3909 E-mail: Danielle.Santos@nist.gov with '2024-NIST-RAMPS-01' in subject line
Technical Assistance with Grants.gov Submissions	grants.gov Phone: 800-518-4726 E-mail: support@grants.gov
Grant Rules and Regulations	Nuria Martinez Phone: 301-975-6215 E-mail: nuria.martinez@nist.gov

Helpful Information

Deadline to Apply:
Friday, May 24, 2024, by 11:59
p.m. Eastern Time.

Link to opportunity on
Grants.gov:
[https://grants.gov/search-
results-detail/353143](https://grants.gov/search-results-detail/353143)

LEARN MORE

- 2016 RAMPS Pilot Programs and NIST Publication on Roadmaps to Successful RAMPS
 - Learn more at nist.gov/nice/ffo
- 2024 RAMPS Program:
 - Webinar recording
 - Grants.gov information
 - ASAP.gov information
 - nist.gov/news-events/events/applicants-webinar-2024-nice-ramps-funding-opportunity
- NICE Webinar: Community-Based Partnerships for Cybersecurity
 - View recording: nist.gov/nice/webinars