Cyber and Artificial Intelligence (AI) Pilot Clinic Grant Initiative

Request for Proposals

Maryland Department of Labor

Key Information Sheet Summary

Purpose: To build Cyber and AI clinics that provide real-world training for Marylanders while strengthening the cybersecurity of critical community institutions.

Issue Date: October 3, 2025

CGP Issuing Office: Maryland Department of Labor

Submission To: Mary Keller at mary.keller@maryland.gov

Pre-Proposal Virtual Conference: October 15, 2025 at 11:00 am

Proposals Due: December 10, 2025

Application Size: Application narratives may not exceed 10 pages with a minimum of 11-point font, 1-inch margins, and 1.15 line spacing

Selection Announcement: January 2026

Funding Available: $1,000,000

Funding Ceiling: $500,000

Period of Performance: February 1, 2026 - January 31, 2029

Eligible Applicants: Institutions of Higher Education, non-profit organizations, local workforce development boards, Registered Apprenticeship Sponsors, and other organizations at MD Labor's discretion

MD Labor Contact: Seeyew Mo, Maryland Department of Labor

Seeyew.mo@maryland.gov

Key Definitions:

- **Learner:** an individual seeking a career in cybersecurity that has the appropriate classroom training to work in the clinic and provide on-site support to client organizations
- **Client:** organizations that will receive cybersecurity services offered by clinics and delivered by learners. Clients can expect to receive cyber awareness training, cybersecurity assessments, recommendations for necessary remediations, and free or reduced-cost cyber tools and additional services that increase their cyber resiliency.

- **Hiring Partner:** Employers who agree to consider hiring learners who complete an experiential learning opportunity in a cyber clinic. Hiring partners may also agree to provide internship opportunities for learners that complete the cyber clinic work experience.

Section 1 - Project Objectives & General Information

Goals of the Project

Cybersecurity threats are escalating, becoming more advanced, and affecting every sector – from small businesses to schools to hospitals, water utilities, power companies, and local governments. Yet the industry does not have enough professionals to adequately defend against active threats, with thousands of cybersecurity jobs remaining unfilled annually in Maryland.

Artificial Intelligence (AI) is also reshaping the cyber landscape. Emerging tools are beginning to autonomously identify software vulnerabilities, in some cases before they are publicly known, and initiate preemptive mitigation. AI is emerging as a force multiplier that can tip the balance toward under-resourced defenders. As these capabilities grow and become more sophisticated, they are reshaping the role of cyber professionals. It is clear that threat hunting, penetration testing, analysis, and cyber engineering roles will look drastically different in the years ahead.

Maryland faces a dual challenge: an acute shortage of cyber talent today, and a rapidly changing skillset required for the workforce of tomorrow.

To close the workforce gap and prepare for AI-driven change, investment into new models that combine employer demand with real-world experience and forward-looking skills is critical. The Maryland Cybersecurity Talent Strategy report identifies cyber clinics as a strategy that offers learners real-world cybersecurity experience while providing cybersecurity services to a variety of organization types. Learners will strengthen the technical and professional skills they learn in the classroom by delivering cybersecurity services to organizations that otherwise lack access.

Cyber and AI are inseparable in the next era of cybersecurity. By seeking proposals for initiatives as Cyber and AI-focused clinics, programs will help learners not only for today's cyber workforce but also for the AI-enabled roles of the future. In the clinic, learners will gain hands-on experience in completing cybersecurity tasks (with AI tools as appropriate), including but not limited to automating security operation center and compliance functions, running assessments and generating policies, and accelerating threat detection and penetration testing. This model bridges a critical gap: it gives learners

applied learning at scale while providing communities with a trusted local resource to strengthen their cyber resilience.

The goals of this initiative are to:

- Prepare Maryland's current and future cyber workforce by equipping learners with hands-on experience in cybersecurity and AI, building both technical expertise and professional skills needed for evolving roles.
- Strengthen community resilience by using AI tools as a force multiplier by providing organizations – including small businesses, schools, hospitals, nonprofits, local governments, and critical infrastructure – with cyber risk or Cybersecurity Maturity Model Certification (CMMC)-aligned readiness assessment, development of policies and procedures, hands-on mitigation support (patching, Multi-Factor Authentication (MFA) implementation, network segmentation,and incident response services. Learners will apply AI tools responsibly to scale defenses (including assessing cyber and AI risks), automate routine tasks, and extend protection to organizations that otherwise lack in-house resources.
- Position Maryland as a national leader in next-generation cyber workforce development by piloting a scalable clinic model that integrates applied learning with real-world organizational impact.

General Information

I. Summary Statement

The Maryland Department of Labor (MD Labor) is releasing this Cyber and AI Clinic Competitive Grant Proposal (CGP) which aims to ensure employers have the highly-skilled cyber workforce they need by offering hands-on training and real-world experience to current and prospective cyber professionals through Cyber and AI clinics. MD Labor's Cyber Maryland Program and the Division of Workforce Development and Adult Learning will jointly administer this grant on behalf of the State of Maryland.

Successful applicants will demonstrate the ability to develop, launch (and/or expand), and implement cyber clinics as a demand-driven strategy that reflects employers' needs, ensuring training is practical, immersive, and future-focused. Applicants will be responsible for securing clients in critical infrastructure sectors as defined in the 2025 Maryland Laws Ch. 218 (S.B.867) like water, elementary and secondary schools, healthcare, energy, small businesses, emergency services, and nonprofit organizations. In addition, applicants will be responsible for recruitment, screening, case management, wrap-around services, career coaching, job placement, and advancement strategies for all learners that work in

the clinic. A successful proposal will build a consortium to support the goals above, including employers, non-profit organizations, and other stakeholders, and demonstrate the ability to have training lead directly to career growth including internship opportunities, full-time employment, credential attainment, and/or advancement within the cyber industry. Applicants that are not two or four-year institutions of higher education are strongly encouraged to partner with one, and those with multiple institutions of higher education in the consortium will receive preference. Applicants are also strongly encouraged to partner with Local Workforce Development Boards to support further employer connections and job development post-clinic experience.

II. Eligible Applicants

Organizations that are eligible to apply for this opportunity are:

1. Institutions of Higher Education;
2. Non-profit Organizations;
3. Local Workforce Development Boards;
4. Registered Apprenticeship Sponsors;
5. Other organizations at MD Labor's discretion.

Organizations do not need to be based in Maryland, but should have a significant presence in the State. Applicants must have established partnerships with employers in Maryland and be familiar with state level workforce and education systems.

As the main goal of this project is to strengthen the talent pipeline and better prepare current and prospective cyber professionals for future roles, applicants must partner with clinic "clients." For the purposes of this competitive grant proposal, applicants are required to secure the following types of commitments from partners:

1. **Client** - Applicants are required to secure clients to utilize the clinic. While employers in any industry can participate as a client, applicants should prioritize securing clients in critical infrastructure sectors as defined in the 2025 Maryland Laws Ch. 218 (S.B.867) as well as State agencies and local governments. Clients can expect to receive cyber awareness training, cybersecurity assessments, recommendations for necessary remediations, and free or reduced-cost cyber tools and additional services that increase their cyber resiliency. To be eligible to receive funding, applicants must include a letter of commitment from at least one employer who will serve as a client. Applicants with letters of commitment from multiple employers to act as clients will receive preference.
2. **Hiring Partner**- Learners that work in the cyber clinic are honing skillsets in preparation for careers in cyber. It is critical that the applicant develop strong relationships with employers who agree to consider learners that have experience

in the clinic for hire. In order to be considered for funding, applicants must include a letter of commitment from at least one employer who will consider learners with cyber clinic experience for hire. Employers may also commit to providing internship opportunities for learners. Applicants with letters of commitment from multiple employers who commit to act as hiring partners will receive preference.

At a minimum, the consortium must include at least one partner that will serve as a client at the cyber clinic and one employer that commits to serve as a hiring partner. Employers are encouraged to commit to serve as both a client and hiring partner and commitments may span beyond these two roles (e.g. curricula review, mentorship).
State Agencies such as the Maryland Department of Information Technology or the Maryland Department of Labor may serve as both a "Client" or "Hiring Partner" employer.

In order to avoid any conflicts of interest or the appearance of a conflict of interest, any organization that had staff participate in the creation of this Competitive Grant Proposal or any policies and procedures relevant hereto are not eligible to apply for a grant, be awarded a grant, or receive funding as a subcontractor or subgrantee.

III. Funding

Funds for this initiative have been allocated in the FY 2026 state budget and this initiative is being administered pursuant to the Maryland Code Annotated, Labor and Employment Art., §11-701 et. seq and Section 4 of 2025 Maryland Laws Ch. 218 (S.B. 867). This solicitation is being issued after consultation with the Cyber Maryland Board. This grant is based on reimbursable funding. Funds are reimbursed after the Grantee provides a proper fiscal invoice for completed work. Funding for these projects will be available for three years beginning on February 1, 2026. MD Labor will consider applications that are geographically diverse across the State of Maryland and that develop regional consortiums.

IV. Contact Information

Prior to the award of a grant, all questions, correspondences, etc. of this CGP are to be sent to seeyew.mo@maryland.gov.

MD Labor may change the Program Manager at any time by written notice to prospective Applicants.

V. Revisions to the CGP

If it becomes necessary to revise this CGP before the due date for proposals, amendments will be provided to all prospective Applicants who were sent this CGP or otherwise are known by the Program Manager to have obtained this CGP. Amendments

made after the due date for proposals will be sent only to those Applicants who submitted a timely proposal and remain under consideration for award as of the issue date of the amendment.

If the applicant receives notice of an amendment to the CGP before the applicant submits their completed proposal, then that applicant shall also include as part of their application a formal acknowledgment of receipt for said amendment. Acknowledgement of the receipt of amendments to the CGP issued after the proposal due date shall be in the manner specified in the amendment notice. Failure to acknowledge receipt of amendments does not relieve the Applicant from complying with all terms of any such amendment.

VI. Pre-Proposal Conference

MD Labor will host a Pre-Proposal Conference in preparation for application to this CGP opportunity to review the application process, answer applicants' questions, and provide general technical assistance. The Pre-Proposal Conference will take place on October 15, 2025 at 11:00 a.m. (Eastern Time).

VII. Proposals Due Date

An electronic copy of the proposal must be sent to Seeyew Mo (seeyew.mo@maryland.gov). Proposals must be submitted no later than 11:59 PM (Eastern Time) on December 10, 2025 in order to be considered.

Requests for extension of the closing date or time shall not be granted. Proposals received by the Program Manager after the due date, 11:59 PM (Eastern Time) on December 10, 2025, shall not be considered.

VIII. Amendments, Cancellations, and Discussions

The State reserves the right to amend or cancel this CGP at any time; to accept or reject any and all proposals, in whole or in part, received in response to this CGP; to waive or permit cure of minor irregularities; and to conduct discussions with all qualified or potentially qualified Applicants in any manner necessary to serve the best interests of the State of Maryland. The State also reserves the right, in its sole discretion, to award a grant based upon the written proposals received without prior discussions or negotiations with the applicant.

IX. Oral Presentation

Applicants may be required to make oral presentations to MD Labor representatives in an effort to clarify information contained in their proposals. Significant representations

made by an Applicant during the oral presentation must be put into writing within five business days of the presentation. All such written representations will become part of the Applicant's proposal and are binding if the Grant is awarded and should be submitted to the Program Manager. The Program Manager shall notify Applicants of the time and place of any oral presentations.

X. Applicant Responsibilities

The selected Applicants shall be responsible for rendering services as required by this CGP. Any subcontractors or sub-grantees shall be identified and a complete description of their role relative to the proposal shall be included in the Applicant's proposal. The selected applicants are responsible for ensuring that any subcontractor or sub-grantee is aware of the terms and conditions of the grant and has fully agreed to comply with the terms and conditions. The Applicant will be responsible to the Grantee for any breaches of the terms and conditions by its subcontractors or sub-grantees.

XI. Grant

By submitting a proposal in response to this CGP, an Applicant, if selected for award, shall be deemed to have accepted the terms of the CGP.

XII. Compliance with Laws / Arrearages

By submitting a proposal in response to this CGP, the Applicant agrees that if selected for award, it will comply with all Federal, State and local laws applicable to its activities and obligations under the grant. In addition, the Applicant agrees to ensure that all subgrantees involved in the consortium possess and maintain any and all necessary licenses and approvals, certifications, and are in compliance with all applicable State and federal laws and regulations. Such approvals, licensing, certifications, and compliance include, but are not limited to, the laws, regulations, and policies of:

i) Maryland Unemployment Insurance

ii) The Comptroller of Maryland

iii) Maryland Higher Education Commission

By submitting a response to this CGP, each Applicant represents that it is not in arrears in the payment of any obligations due and owing the State of Maryland, including the payment of taxes and employee benefits, and that it shall not become so in arrears during the term of the grant if selected for grant award.

Section 2 - Scope of Work

I. Introduction

MD Labor is seeking applications from organizations that will design, launch, and implement Cyber and AI clinics as an alternative method to providing high-quality training, strengthen Maryland's workforce pipeline, and fill critical vacancies. A cyber clinic provides cybersecurity services to a variety of organization types while giving learners real-world cybersecurity experience. Clinics serve both as a skills-based learning environment for learners and as a vital local resource for improving the cybersecurity resilience of communities.[1]

This CGP also recognizes the rapid evolution of the field, particularly the impact of AI. AI tools are increasingly capable of autonomously detecting vulnerabilities, automating compliance tasks, and accelerating incident response. As these capabilities expand, they are reshaping both the threat landscape and the skills required of cyber professionals. Applicants must therefore demonstrate how their proposed Cyber and AI Clinic will incorporate or advance responsible AI-enabled practices as a force multiplier.

The aim of this CGP is aligned with Governor Moore's strategic vision for Maryland, as outlined in the Moore-Miller Administration 2024 State Plan[2]:

- Creating an Equitable, Robust, and Competitive Economy by developing key sectors including IT/cybersecurity;
- Setting Maryland's learners up for Success; and
- Connecting Marylanders to Jobs by helping workers move to in-demand occupations and supporting Marylanders in connecting to quality jobs.

This CGP will award funding to applicants who demonstrate the ability to design, launch, and implement Cyber and AI clinics as an innovative strategy to deliver practical, AI-enabled, future-focused training for cybersecurity roles. The Cyber and AI clinics will equip current and prospective cyber professionals with the skills needed for today's critical roles and tomorrow's AI-driven challenges, while simultaneously providing under-resourced organizations with cybersecurity services that strengthen their resilience today. Applicants will be expected to train at least 200 current or prospective cyber professionals during the period of performance and equip them with skills that will enhance career mobility. Learners must have the appropriate skill level to provide, at a minimum, the following services to clients using most-up-to-date AI tools for:

A. cyber awareness and training;

[1] https://cybersecurityclinics.org/about/

[2] https://governor.maryland.gov/priorities/Documents/2024%20State%20Plan.pdf

B. cybersecurity assessments;
C. recommendations for necessary remediations; and
D. additional cyber tasks as appropriate, including but not limited to cyber engineering, auditing, monitoring, threat hunting, etc.

The grantees selected for funding must commit to actively participate in the Cyber Maryland program and broader ecosystem by collaborating with any other grantees funded under the CGP to share lessons learned, successful models, and best practices.

II. General Provisions and Other Requirements

1. Within the proposal, applicants must:

- **Clinic Model**
  - Present a Cyber and AI Clinic model that delivers immersive, hands-on training aligned with employer demand. Possible models include, but are not limited to, the following:
    - **Population Specific Clinics** - Designed to serve a defined group of learners, such as emerging professionals, veterans, or career transitioners (e.g., individuals seeking to move into cyber-focused occupations or those impacted by federal reductions-in-force). For example, a clinic might reskill former attorneys or federal IT staff (e.g., GS-2210 help desk or system administrators) into roles such as CMMC program managers, cyber analysts, or penetration testers.
    - **Industry Specific Clinics** - Designed to meet the needs of a particular sector, such as operational technology (OT) security for energy or water, IT security for K-12 schools, or integrated OT/IT security for hospitals. For example, a clinic might focus on reskilling existing staff in these sectors into specialized cybersecurity analyst roles, or prepare early-career professionals whose interests bridge cybersecurity and the target industry.
  - Clinics should clearly demonstrate how the chosen model supports Maryland's workforce needs and prepares learners for evolving cyber roles.
- **Learner Recruitment and Readiness**
  - Present a plan on how learners will be recruited and selected for training
  - Cyber Clinics must ensure learners obtain the following skills **prior to** joining the cyber clinic:
    - **Foundational Cyber and AI Skills**:

            - Digital and AI literacy such as using common software and online tools safely, critical thinking and problem solving using technologies tool, navigating cloud platforms, and understanding how digital systems and AI tools work, and practicing basic cybersecurity habits like creating strong passwords and recognizing phishing attempts;
            - Digital resilience such as adapting to new technologies, quickly learning new tools, keeping skills current as technology evolves, incorporating AI tools into everyday tasks, and maintaining safe online behaviors when encountering new software or platforms;
            - Computational literacy such as learning basic coding and scripting including orchestrating and configuring AI systems, understanding how systems and networks operate, applying simple problem-solving to technology challenges, and using AI tools to analyze or automate tasks, and performing basic cybersecurity tasks like monitoring system activity or identifying potential vulnerabilities, and assessing risks.
    - Include a plan that encourages participation from underrepresented groups in cyber, including women, individuals of color, and persons with differing abilities, as well as those from Engaging Neighborhoods, Organizations, Unions, Governments, and Households (ENOUGH) Act communities. The 27 ENOUGH communities can be found here.
- **Clinic Experience**
    - Provide a clear plan that equips learners with both specialized cybersecurity skills and essential professional skills:
        - **Specialized Cybersecurity Skills** that are tailored to the clinic's focus area, the client sectors being served, and the workforce roles being targeted. For example, they may include configuring and defending networks through firewalls, segmentation, and zero-trust architectures; conducting vulnerability assessments, penetration tests, and red-teaming exercises, including the use of AI-enabled tools to identify weaknesses before adversaries do; securing cloud platforms, endpoints, and IoT devices while automating compliance and monitoring; applying governance, risk, and compliance frameworks such as NIST and CMMC while leveraging AI to accelerate policy drafting and reporting; responding to incidents through investigation, log analysis, and forensics with AI-assisted containment tools; and assessing and mitigating AI-specific risks such as adversarial manipulation, data poisoning, and ethical

misuse of models. Not every clinic will require the same specialized skill set. Instead, skills should be modular and aligned to real-world demand, with clinics encouraged to prioritize depth in the areas most relevant to their focus, client sectors, and targeted workforce roles.

        - **Essential skills** such as using technology to analyze data and communicate insights, thinking critically and solving problems creatively, staying curious and adaptable as tools evolve, translating technical concepts for non-technical audiences, taking initiative on projects, making decisions with business context in mind, and approaching work with a mission-driven mindset.
    - Demonstrate how the clinic design incorporates experiential learning, with learners applying skills on real projects under the guidance of qualified professionals (e.g., faculty, instructors, field experts). Proposals are encouraged to leverage AI-enabled support systems to personalize learner pathways, help participants identify skill gaps, acquire in-demand skills, and connect efficiently to job opportunities.
- **Clients and Industry Engagement**
    - Demonstrate active employer involvement, secure client participation (with preference for multiple commitments), and outline how client engagement will keep curricula and services aligned with industry needs.
- **Job Placement and Career Pathway**
    - Include a strategy for learner placement into internships, apprenticeships, or employment, with at least one employer hiring partner providing a letter of commitment.
- **AI Integration**
    - Show how AI tools will be incorporated into the clinic to enhance both learner training and client cybersecurity services, with consideration for adapting emerging AI models or tools where appropriate.
- **Sustainability**
    - Include a plan for maintaining the clinic beyond the grant period. The plan should identify long-term funding mechanisms (e.g., fee-for-service models, employer consortium contributions, pooled industry support) and demonstrate how the clinic will stay responsive to emerging AI-driven workforce needs over the next decade.
- **Organizational Capacity and Timeline**
    - Present a 36-month implementation timeline, demonstrate organizational capacity (staff qualifications, consortium members, infrastructure), identify learner supports, and provide evidence of past performance where

applicable. Applicants are strongly encouraged to develop a timeline that provides for clinics to be operational by September 30, 2026.

2. Applicants must provide expected outcomes over a 36-month period of performance. At a minimum, outcomes must include:

- Participant-level demographic data, including but not limited to date of birth, race, sex, county of residence, highest level of education, veteran status
- Number of learners participating in cyber clinic activities
- Number of learners who demonstrate measurable improvement in cybersecurity and AI related skills as a result of participation in the clinic
- Number of learners who secure internships in cybersecurity or related technology fields following participation in the clinic
- Number of learners who secure full-time, unsubsidized employment in cybersecurity or related technology fields following participation in the clinic
- Number and type of clients served
- Number of clients who report improved cyber resilience as a result of partnering with the clinic

Applicants may include other deliverables or metrics that will be tracked.

3. Applicants must include letters of commitment from each consortium member. At a minimum, the consortium **must** include at least one employer that will serve as a client at the cyber clinic and one employer that commits to serve as a hiring partner. A single employer can commit to serving as both a client and hiring partner. Employers are also encouraged to provide internship opportunities for learners.

Applicants are strongly encouraged to partner with groups with national security missions including, but not limited to, the Maryland Defense Force (MDDF), Maryland National Guard, and Cyber Resilient Corps Project Franklin. In addition, applicants are encouraged to partner with other stakeholders, including other institutions of higher education, training providers, local workforce development boards, non-profits, and industry associations that can support the goals of the project.

4. Allowable Uses of Funds include:

- Sub-grantee payments
- Salaries for individuals that support clinic operations
- Grantee administrative costs, subject to any limitations as determined by the MD Labor
- Training-related expenses, including:

    - Cyber infrastructure and capital costs
    - Instructor and faculty costs
    - Curriculum design and development
    - Equipment (software and hardware)
    - Training materials and supplies
- Certification costs
- Supportive services for learners including but not limited to:
    - Learner stipends
    - Tutoring, mentorship, or related coaching
    - Career counseling and job search support
    - Job placement or interview prep
    - Licensing, exam, or credential prep support
    - Access to technology to fully engage in clinic programming
- Other costs, as determined by the applicant, that are necessary for clinic operations as approved by the Department.

Applicants are strongly encouraged to provide leveraged resources to support the implementation of the clinic. This may include classroom space, equipment, and staff time.

5. Reporting Requirements

Awardees must submit quarterly financial and narrative program progress reports to MD Labor. Templates for these reports will be provided by MD Labor. Reports will be due on the 15th of the month following the reporting period. MD Labor will conduct regular programmatic and fiscal monitoring to ensure that activities of its service providers are on target to meet grant goals.

Section 3 - Proposal Format

I. Proposals

One electronic copy of the proposal must be received by Mary Keller (mary.keller@maryland.gov) no later than 11:59 PM (Eastern Time) on December 10, 2025 in order to be considered.

II. Submission

The proposal must include the Competitive Grant Proposal (CGP) Narrative (Attachment A). All sections of the CGP Narrative form must be completed with as much detail as possible.

The Applicant must submit a detailed line item budget using the forms provided as Attachment B for their project's period of performance. Attachment B includes a budget narrative and information on leveraged resources the applicant will offer in support of the project. The budget must reflect the cost per participant.

The Applicant must include Letters of Commitment from all members of the consortium as Appendix C. To be considered, applicants **must** include a letter of commitment from at least one partner who will serve as a client and at least one employer who will serve as a hiring partner. Applicants with multiple letters of commitment from clients and hiring partners will receive preference.

Attachment A - Competitive Grant Proposal

1. **Clinic Model (15 points)**
    a. Describe the proposed Cyber and AI Clinic model, including the specific implementation design (population specific, industry specific, or other). Include the rationale for the implementation design.
    b. Describe the types of roles learners will be prepared to perform.
2. **Learner Recruitment and Readiness (10 points)**
    a. Describe how learners will be recruited and selected for training, including any organizations that will support recruitment.
    b. Describe how learners will be assessed for foundational cyber and AI skills (digital and AI literacy, digital resilience, and computational literacy) during the screening process.
    c. Will the applicant or members of its consortium provide any training or coursework pre-clinic experience to ensure learners have the appropriate skills to work in the clinic? If yes, please describe.
    d. Describe strategies to recruit and support underrepresented populations in cyber, including those without formal education and certification, women, people of color, people with differing abilities, and individuals from ENOUGH Communities.
3. **Clinic Experience (15 points)**
    a. Describe how the clinic will ensure learners in the clinic will learn specialized cyber security skills.
    b. Describe the skills embedded in the curriculum. How do these skills build on learners' existing foundational skills?
    c. Detail the amount of time learners will be engaged in classroom training vs. in the clinic providing services. (e.g. 50% time in classroom training, 50% time in clinic).
    d. How will essential skills training be incorporated into the clinic experience?
    e. On average, how long will learners work in the clinic?
    f. What supports (stipends, tutoring, coaching, wrap-around services) will be provided to ensure retention and success?
4. **Clients and Industry Engagement (15 points)**
    a. Explain how employers and industry partners have been involved in designing the clinic model and curriculum.
    b. Is the clinic focused on providing services to clients in a specific industry or sector? If yes, please list.

c. List at least one secured client and describe their commitments (e.g., participation as clinic clients, internships, hiring, mentoring). Applicants with letters of commitment from multiple employers to act as clients will receive preference.
d. Describe the strategy for securing additional clients and the specific cybersecurity or AI services these clients will receive.
e. Explain how client engagement will be maintained to ensure that clinic services and curriculum remain aligned with industry needs.

5. **Job Placement and Career Pathways (15 points)**
    a. Describe the overall strategy for connecting learners to internships, apprenticeships, and/or full-time employment after clinic participation.
    b. Identify the staff member(s) or service responsible for job development and placement, including their role and level of effort.
    c. List at least one hiring employer that has committed to consider or hire clinic participants, and attach letters of commitment where available. Applicants with letters of commitment from multiple employers who commit to act as hiring partners will receive preference.
    d. Explain how employers will remain engaged as hiring partners to support learner placement and career advancement.
6. **AI Integration (2.5 points)**
    a. Describe how AI tools will be incorporated into the clinic to support both learner training and client services (e.g., SOC automation, compliance, threat detection). If applicable, include plans to adapt emerging AI models or tools, such as those from DARPA's AIxCC competition, to address client cybersecurity needs.
7. **Sustainability (2.5 points)**
    a. Describe how the clinic will remain sustainable in the absence of state funding.
8. **Organizational Capacity and Timeline (10 points)**
    a. List the individuals that will provide support to the clinic. Describe their role and the percentage of time they will spend dedicated to the functions in detail.
    b. If there are other organizations that will support the implementation of the clinic (consortium members), please list and describe their role and how it will contribute to the success of the project.
    c. Describe any existing infrastructure, partnerships, or resources that will support the successful launch and implementation of the clinic.
    d. Describe past performance on a project of similar scope (if applicable).

e. Provide a detailed timeline for planning and implementation over a 36-month period of performance. Applicants are strongly encouraged to develop a plan that has the clinic operational by September 30, 2026.

9. **Outcomes and Metrics (10 points)**
    a. Grantees will be required to track demographic and outcome data for learners. How will these data points and outcomes be tracked?
    b. Complete the chart below to include anticipated outcomes.

Number of learners participating in cyber clinic activities	
Number of learners who demonstrate measurable improvement in cybersecurity and AI related skills as a result of participation in the clinic	
Number of learners who secure internships in cybersecurity or related technology fields following participation in the clinic	
Number of learners who secure full-time, unsubsidized employment in cybersecurity or related technology fields following participation in the clinic	
Number of clients served	
Number of clients who report improved cyber resilience as a result of partnering with the clinic	

10. **Budget (5 points)**
    a. Describe how the funding will be used.
    b. Will the applicant provide leveraged resources to support the implementation of the clinic. If yes, please list and include the estimated amount of resources.

Attachment B - Please complete Attachment B - Budget using a template provided by MD Labor

Attachment C - Please submit all Letters of Commitment as Attachment C.