Industry Sector Grant

Applicant	Edward Vasko
Applicant ID	APP-000469
Company Name	Boise State University
Recipient Address	Boise State University 1910 University Dr Boise, Idaho 83725-1135
Email	edwardvasko@boisestate.edu
Funding Requested	$806,433.94
Status	Submitted
Funded	

Review Notes:
January 25th, 2022 Grant Review Committee Notes:
Boise State University – Industry Sector Grant
The Boise State University (BSU) program is working with multiple partners for the Cyberdome project including Micron, INL, Intuit, Thermo Fisher Scientific, and Choice Hotels International. Partners have committed to hire the students who complete training. BSU is actively recruiting subject matter expert educators for this program. The program will train +80 individuals over the next 3 years. The grant will fund student stipends and certification cost for students enrolled in the program.

The Cyberdome platform enables an appropriate combination of traditional training and real-world experience through the broadened online access, storage and services; training will be accessible to learners in all parts of Idaho, including rural Idaho where training and workers may not have been previously available.

The labor market data shows there will be a 36% growth in cybersecurity analysts over the past 12 months 979 Cybersecurity Analysts job openings posted in Idaho.

WDTF Request: $806,433.94

Discussion:

For whom is the program available?
• Participants will be recruited from around the state.
• Students from the previously awarded 2019 BSU Cyber Operation and Resilience (CORe) Industry Sector grant students would also be targeted for this opportunity.

It looks like some of the funds will pay for stipends for students, but it also includes associated fees. Do you know what that includes?
• Fees like workers compensation are required for an individual to perform work for an employer. Majority of funds would pay the student a stipend.

This project seems to align with our work-based learning goals, and the majority of funding is being used for a work-based learning experience for the student. The funds are also going towards funding the certification which is important component for students as the costs associated with certificates can be prohibitive.

Motion by Mr. Cox to recommend approval of the Boise State University - Industry Sector Grant in the full amount of $806,433.94 to the Executive Committee. Second by Mr. Barrera. Motion carried.

Company Information

Question: Business entity name

Institute for Pervasive Cybersecurity

Question: “Doing business as” entity name

Boise State University

Question: Federal Tax ID Number

82-0290701

Question: Street address

1910 University Dr

Question: PO Box (If applicable)

1910 University Dr

Question: City

Boise

Question: State

ID

Question: Zip code

83725-1135

Question: Business website

www.boisestate.edu/cybersecurity

Question: First name of person to be contacted about this application

Edward

Question: Last name

Vasko

Question: Job title

Director, Institute for Pervasive Cybersecurity

Question: Street address

1910 University Dr

Question: City

Boise

Question: State

ID

Question: Zip Code

83725-1135

Question: Email address

edwardvasko@boisestate.edu

Question: Contact phone

(208) 426-2480

Consortium

The applicant must be an employer or educational entity representing a consortium of at least three employer partners with a similar occupational training need. All members of the consortium will be required to complete a Memorandum of Understanding (MOU). A link to the grant MOU is provided below. Please upload all completed and signed MOU's by the consortium to this section of the application.

Employer Partner MOU

Question: Please describe how employer partners are involved in the project and how they will engage with trainees who receive training.

Local, regional, and national cybersecurity companies are committed to hiring students receiving training from the Institute's skillset development platforms (e.g. Cyberdome).

Examples of the companies / organizations involved include Idaho National Laboratory, Micron, Intuit, and Choice Hotels International.

Question: Do each of the industry partners pay at least $12 per hour

☑ Yes

☐ No

Question: Please upload completed MOU here.

Micron 2022_Benefits_Guide.pdf (1/15/2022 8:48 AM)
Intuit-FY 2022 Plan Snapshot-092821.pdf (1/15/2022 8:35 AM)
Thermo 2021-Benefits Highlights.pdf (1/15/2022 8:35 AM)
ThermoFisher MOU.pdf (1/15/2022 8:35 AM)
Micron ISG Consortium MOU.pdf (12/17/2021 9:33 AM)
INL MOU.pdf (12/15/2021 3:56 PM)
Ben-Sum_HSA-80_01.01.2022_Choice-Hotels-International--Inc._3335066.pdf (12/15/2021 11:39 AM)
Intuit MOU.pdf (12/15/2021 11:38 AM)
Choice MOU - 20211124.pdf (12/15/2021 11:38 AM)

Project Overview

Question: Please provide a brief overview/executive summary of the training need(s), current/projected skills gaps, and what you're trying to accomplish with this project. (You are limited to 2000 characters for this section so please be concise.)

Cybersecurity is at the forefront of concern for every public, private, non-profit and educational institution today. If our infrastructure cannot be secured, it can quickly become dangerous, resulting in the loss of critical data, critical physical services, or even lives. In the United States, the demand for professionals with cybersecurity expertise has outpaced supply. There are over 450,000 open cybersecurity positions throughout the United State with over 2,500 such positions in Idaho.

Securing rural community cyber / physical assets provides two benefits. First, it reduces the overall risk to the state and its citizens. Second, done correctly, such efforts create a cybersecurity ready workforce that makes Idaho a leader across the nation. Our goal is to secure rural government assets using fiscally responsible methods by engaging partners across the state, including the INL, the State of Idaho, Idaho's Universities and Colleges, and private industry. This effort simultaneously reduces critical cybersecurity risks for rural county, education, and municipal clientele while creating competency-based learning platforms for Idaho cybersecurity learners. This differentiates Idaho workers to employers inside, and outside of the state.

Building the "Cyberdome" - a holistic environment for competency-based learning in cybersecurity - is the goal of this workforce development effort. The Cyberdome couples a cybersecurity as a service model for rural communities across the state (e.g. counties, cities, education & health districts), using the force-multiplying effect of our learners, and a scalable operational model upon which new services and applications can be innovated over time - thereby cutting costs and time to implement.

The program is already in process of activating service for the City of Sun Valley, Midvale and Cambridge School Districts and Jefferson County. Requested funding will enable the activation of up to 84 learners over a 3-year period.

Question: How will the project change and/or enhance the current landscape of Idaho's talent pipeline/development efforts.

The Cyberdome initiative is meant to align with each Idaho public higher-education institution in order to provide "live fire" skillset development for learners. This will differentiate learners as they move into the workforce. In doing so, the Cyberdome has two core goals: a short-term goal of reducing risk for Cyberdome clientele, and a long-term goal of producing significantly more cyber-activated workers into the workplace than our current pace.

The platform leverages two critical assets to provide distributed collaboration and workforce development. First the Idaho Regional Optical Network (IRON) is used to connect the state higher-education institutions together. This high speed network enables on-campus learners to have real-time video and data sharing for enhanced collaboration and response to threats.

Second, the platform is leveraging Amazon Web Services (AWS) so learners can access the environment from anywhere they have appropriate Internet connectivity, including their homes. This enables learners to work in their communities while participating in the protection of critical rural assets.

The outreach and collaboration to the other institutions is done through the Idaho Cybersecurity Education Initiative (ICEI). The ICEI is a collaborative initiative where all Idaho public institutions come together and discuss sharing cyber curriculum and platforms supporting learners and research. Learners from southern and eastern Idaho are already engaged in the Cyberdome platform.

Further outreach is underway through collaboration with the Idaho Career Technical Education (CTE) and Idaho Learning Digital Academy (IDLA) to enable secondary student awareness of the career pathways available in cybersecurity, including the Cyberdome platform as a method of "service oriented" competency development.

By leveraging learners from all public institutions of higher-learning, we intend to accelerate the number of highly skilled, differentiated workers into industry.

Question: What specific skills training will be provided? Include any planned enhancements that will be made to current training.

A key goal of the Cyberdome is workforce development. This is accomplished by hiring, training and developing "learner workers" in the roles of Cybersecurity Analyst and Cybersecurity Engineer. To this end, the Institute leveraged the educational background and experience of a graduate assistant as well as the industry experience of the Cyberdome Manager to create a comprehensive training program built around available cybersecurity resources.

To ensure that the training program fully aligned with industry expectations, an analysis was conducted of the cybersecurity industry roles specified at the National Initiative of Cybersecurity Careers and Studies (NICCS). These roles are defined in the NICE framework developed by NIST. In particular, the roles of Cyber Defense Analyst and Cyber Defense Infrastructure Support Specialist were identified as being highly aligned with the goals of our broader public sector clientele and private sector partners. Further, these general, entry-level roles align across both public and private sector needs, which means that there is no need for specialized trainings to support a particular sector, thereby maximizing the benefit to our learners and those organizations hiring our learners. Since the roles defined in the NICE framework are competency based, the objective of making a competency based learning platform is strongly realized through this.

Once industry roles were identified, the knowledge, skills and abilities (KSAs) defined for each role were utilized to create an assessment tool for both pre and post evaluation of the participants. This assessment tool uses both self and peer evaluation methods to determine a baseline skill set as well as determine what progress a participant has made towards being a workforce ready graduate.

Leveraging previously mentioned statewide cybersecurity collaboration efforts (e.g., the ICEI) and this assessment tool, prospective learners from around Idaho can provide a list of courses taken at any public institution and the Cyberdome management team can produce a knowledge and skill gap assessment for each learner worker. Utilizing this output, proscriptive training support is enabled for learner workers before they engage in production monitoring activities. As our college and university partners further build and enhance their respective cybersecurity curriculum, the assessment tool will continue to be updated. Further, this tool is being examined for possible technology transference.

Following these initial assessments, baselines are produced from which further training is developed/enhanced to close the gap between actual and desired competencies. Training content is organized into a comprehensive course shell housed in Boise State's learning management system (Canvas). This allows the Institute to provide training remotely, track learner progress and selectively expose training modules based on determined knowledge and skills of a participant. As the learner workers are engaged throughout Idaho, but paid for through Boise State, they will have access to the Boise State instance of Canvas for specific learning development. Boise State is open to further collaboration on transference of training content and other avenues of learner worker enablement.

Current training content covers a variety of areas related to the determined roles:
1. General Cybersecurity concepts
2. Networking concepts and practical networking tools

3. Common attack types and attributes
4. Cybersecurity defense principles
5. Platform specific programs and tools
6. Communication skills

The Cyberdome is utilizing both open-source and commercial platforms and technologies. Training on the individual components of the platform is obtained from several sources (vendors, projects, online courses, etc). In addition to this, the Cyberdome staff mentor and guide individual workers using industry experience.

Besides training on role activation, the goal of this proposal is to enable learner workers to obtain technical certifications (from technology partners) and next-level industry certifications such a the CompTIA CyberSecurity Analyst+ (CySA+), amongst others. As part of the stipends

provided to learner workers, training time will be provided to work on learning objectives aligned with these industry certifications.

Question: How will the project accelerate the pathway to a career for individuals being trained.

The cybersecurity industry requires a workforce with a combination of technical and essential (formerly known as “soft”) knowledge, along with strong competency-based skills, in order to be successful. To obtain this ideal, most employers currently hire a fresh entry-level graduate, and then put them through a series of supportive, yet costly trainings in order to get them on par with the rest of their peers. This added cost (or “Activation Gap”) impacts the hiring organization not only in terms of hard dollars for training, but also in lost time to activate a fully-competent employee, ready to dive in and reduce risk to critical data and infrastructure. Further complicating this process is that the new employee – now enabled with a requisite and robust skill set – becomes highly desirable to other employers desperate to bring on competent workers to their respective organizations. This is one reason for the “revolving door” of recruitment and attrition that currently plagues the cybersecurity industry. This can be alleviated through the introduction of competency-based skills training whereby learners, before departing their institution, are enabled with the core knowledge via coursework AND the necessary core technical competencies garnered though in-depth real-time experiences.

Question: If training exists in the marketplace, describe why this project better meets employer and/or workforce needs.

Traditional training for entry-level cybersecurity professionals is currently activated through some combination of the following:
1. Curriculum at university or community college.
2. Self-learning via publicly available content (e.g. YouTube, Coursera)
3. Certification efforts (e.g. CompTIA, SANS)
4. On the job training via employer environments

The Cyberdome platform enables an appropriate combination of these four elements and the result is a more effective, more desirable worker for industry. Utilizing cybersecurity learners at our institutions of higher learning, combined with industry certifications in these varying curriculum, AND enabling early-stage competency development using a real-world operational environment produces a worker ready to move into industry without expected on the job training efforts.

The Cyberdome competency development program is a 6-month long effort that covers an initial baselining of knowledge (using the assessment tool as mentioned above), followed by a compact training program to enhance the knowledge and skills across the following six areas:
1. General Cybersecurity concepts
2. Networking concepts and practical networking tools
3. Common attack types and attributes
4. Cybersecurity defense principles
5. Platform specific programs and tools
6. Communication skills

This compacted effort will not exceed 20-hour / week of work on the learner worker part, and will be accomplished through training modules, and time within dedicated simulation environments so learners can build their skills before entering in a production environment where live fire situations occur. Before a learner is graduated from this compacted training, a skills and

knowledge assessment is conducted to ensure quality to our Cyberdome clientele. If a learner does not match the expected level of competency, then a performance plan is initiated that may result in the learner being removed from the platform with a development plan.

For those learners that graduate to the production Cyberdome platform, the remaining 5 months of "in seat" learning will be split into time and effort conducting the same real-world tasks other industry early-career cybersecurity professionals have to undertake. A short, non-comprehensive list of these tasks include: monitoring client networks, reviewing logs and daily reports, triaging events & alerts for severity, notifying clients of possible issues and alerts, and hunting for new possible threats. Other tasks the learner workers will have include: additional certification-oriented training, developing knowledge base articles for future Cyberdome learner workers, conducting talks on particular topics of relevance & interest across the cybersecurity landscape, and working in teams to improve processes within the Cyberdome portfolio. The overarching goal of this entire effort is to "push left" the competency development of learners so they may enter the workforce and activate in their roles faster and with less risk for our industry partners.

Before departing the Cyberdome platform, learner workers will also be exposed to potential employers, and will work with the Institute's board of advisors to conduct mock interviews. The Institute is also engaging with career service departments at each of our public higher education institutions to ensure alignment with their objectives.

During this 6-month effort, the learner workers will also be engaged in their respective degree field of study at their home institution. Over the planned 500+ hours of on the job training received from the Cyberdome platform, coupled with the degree program at their home institution, the learner worker is expected to graduate with a degree (A.S./A.A.S, B.S., B.A.S., etc), multiple entry-level and "next-step" industry certifications (A+/Net+/Sec+, CySA+, etc), and

the ability to clearly articulate to an employer the competencies that an early-stage career professional needs to secure employment.

Question: Who will receive training from this project (examples – general public or current employees) and how will they be recruited?

Initially, learners recruited from the public higher education institutions around the state, including the community colleges. One of the benefits of leveraging AWS as our core platform is to allow rural community learner engagement. A broadband enabled learner in a rural community can not only engage with online degree programs (e.g. Lewis-Clark, Boise State, and others have on-line cyber-industry degree programs), but they can also participate in the Cyberdome platform. This "double benefit" engages rural/remote students who may not have the means to depart their communities to build competency in a service oriented career pathway WHILE also protecting the very communities of which they are a part.

Outreach to rural students is occurring through a combination of on-line curriculum targeting rural students (such as those provided by Online Idaho, and the Boise State CyberOperations & Resilience (CORe) program) and outreach programs showing rural students the opportunities presented by a cybersecurity career. We also intend to engage our commercial partners in this latter effort. The national need is so large that even tacit outreach to possible national partners has resulted in high interest in Cyberdome learners, irrespective of their urban or rural location.

Finally, after the pilot year, we intend to enable pathways for existing employers to send their current staff through the Cyberdome program in order to receive enhanced operational training.

Question: Please describe any credentials that participants will obtain.

The intent is to pursue both commercial and state-level credentials for learners activated through the Cyberdome. For example, we intend to pursue specific CTE micro-credentials / badging to identify obtained skills learners receive. Further, if possible, we intend to pursue CompTIA CyberSecurity Analyst+ (CySA+) or EC-Council Certified Security Analyst (CSA) certifications for learner workers prior to their graduation from the Cyberdome. The Institute is a CompTIA Academy and is pursuing EC-Council certification and intends to provide the necessary on-the-job training and testing vouchers as part of this grant request.

Question: Who will provide the training? (Identify the entity that will provide training, the qualifications of the trainer(s), and location of training site.)

Each Cyberdome worker will be assessed for core competencies prior to full activation. This enables the Cyberdome manager(s) and lead(s) to provide learning modules specific to the learner in order to enhance their respective skills. The learning modules will be made up of available courses from on-line and in-person sources, as well as team collaborations and simulation platforms.

Question: Where will the training be provided?

As previously mentioned, training will occur through three steps and can be done on-site at each learner worker home institution, or remotely online, depending on their preference:
1. Post-assessment compacted training to fill gaps in knowledge and skills. This training will be accomplished through online training modules, and time within dedicated remote simulation environments so learners can build their skills before entering in a production environment. Simuation environments are accessible via Virtual Private Network (VPN) connection.

2. The production Cyberdome environment where learner workers will collaborate remotely or in-person to conduct the same real-world tasks other industry early-career cybersecurity professionals undertake in industry.
3. Other tasks and learner learning objectives conducted remotely or in-person include: additional certification-oriented training, developing knowledge base articles for future Cyberdome learner workers, conducting talks on particular topics of relevance & interest across the cybersecurity landscape, and working in teams to improve processes within the Cyberdome portfolio.

All weekly development efforts are built not to exceed 20-hour / week of work. Over the proposed 6-month period, this results in over 500 hours of paid competency development time. If a learner wishes to spend more time development knowledge or skills, they are welcome to do so, outside the provided stipend, and will have remote / on-site access to the Cyberdome training and facilities.

Question: Please provide a detailed description of why funding is needed for this project?

Funding is needed for this project to provide a stipend / pay the individual learner workers a wage commensurate with their pre-graduation knowledge and skill level development.

Funding is also needed for the on-going Cyberdome solutions and platforms being offered to clientele, thereby enabling learner workers to receive the primary goal of the Cyberdome - real world experience.

Question: Will tuition be charged? If yes, please explain.

We do not intend to charge tuition for this effort. The requested funds for this effort will be utilized for learner worker stipends over the 6-month competency development window. Over the course of this three-year grant request, the Cyberdome intends to enable a minimum of 84 total students (24 students / year).

Training Schedule

Provide a quarterly training break-out for year one and year two. For year three show the number of planned NEW participants entering training and number of individuals exiting training for each course of training, for each quarter. Any example is provided on the provided training schedule.

Training Schedule

Question: Please provide an anticipated project start date?

2/1/2022

Question: How many training sessions will be held during the 36 months of the grant?

There will be a rolling set of training sessions during the 6-month window for each student participates in the Cyberdome. These sessions differentiate between the two key roles the Cyberdome produces (Cybersecurity Defense Analyst and Cybersecurity Engineer) and engages workers with a base set of training, followed up with on-going on-the-job and deeper

subject training. Over the course of the 36-month grant window, we intend to have six (6) training windows.

Question: Please upload Training Schedule form here. A link to the form is provided at the top of this section.

Industry Sector Grant Training Schedule new.xlsx (11/10/2021 1:45 PM)

Sustainability

The industry consortium will need to show if and how the project will be sustained past the grant period.

Question: Please describe if and how the project will be sustained past the grant period?

We are actively pursuing sustainable funding from employer partners, federal funding, as well as state-appropriation funding for this program. Further, the Institute is actively conducting outreach to industry for sustainable funding sources.

Our anticipated sustainable funding model will come through the enhanced return on investment employers can make by funding a student stipend for each early-stage cybersecurity career professional. As previously mentioned, employers have an "Activation Gap" problem and are spending 6-9 months activating new employees on methods and techniques. Under the model that 3 months of that activation period is a result of teaching new employees what they will learn via the Cyberdome, then an employer can achieve "twice the training for half the cost." Here is a simply model to validate the opportunity:
"Fully-loaded" annual salary of Security Analyst: $60,000 base + 35% = $81,000
Monthly cost: $6,750
Three (3) months of salary to provide technical training: $20,250
Estimated technical training costs: $5,000
Total hard costs to "activate" a security analyst: $25,250

If an employer provides the Institute half of this expected costs ($12,625) as a gift, the employer potentially receives a tax-deduction AND an employee ready to activate in their environment faster than expected. The reduction in downtime and training costs that is passed on to the Institute enables the Institute to double the training time (6 months), enables a better qualified employee, and helps to reduce the risk to our rural and remote communities around the state.

Project Outcomes

Grant objectives must have measurable results on an individual participant level. Employees or job candidates should learn new skills that were not previously available and gain enhanced skills that allow them to achieve to a higher earning level.

Question: Number of participants/incumbent workers who will receive classroom training?

84.00

Question: Number of participants/incumbent workers who will complete classroom training?

84.00

Question: Number of participants/incumbent workers who will receive structured on-the-job training?

84.00

Question: Number of participants/incumbent workers who will complete structured on-the-job training?

84.00

Question: Number of individuals attaining some type of recognized credential, including degrees, occupational licenses, industry certifications and/or Idaho SkillStack Badges.

84.00

Question: Average wage for incumbent workers prior to training?

$31,200.00

Question: Average wage for incumbent workers after training?

$69,000.00

Question: Number of open enrollment individuals entering training-related employment within 30 days of training completion?

14.00

Budget

The application must provide a detailed budget identifying the direct personnel costs, fringe benefits, equipment cost, facility costs and other identified costs to deliver this training. For each line item on the budget, provide the budget amount, a detailed narrative describing how the line item amount was determined, the necessity of the item to develop/deliver training, and whether the cost is supported by grant funds or partner match (cash or in-kind).

Budget Sheet

Question: How else have you sought to fund this project?

IGEM-HERC (March, 2021), Dept of Labor with WDC & ITC (2020)

Question: Why do you think WDTF is a good source of funding for this project?

The Cyberdome is about enabling the creation of a differentiated cybersecurity workforce while also reducing risk to our critical data and infrastructure. Enabling this platform enables us to differentiate Idaho workers and potentially enables economic development by attracting employers to establish facilities in Idaho. Because this program activates competencies in high paying, high demand jobs around Idaho and the nation, WTDF funding seems a natural funding source for program activation.

Question: Please download the attached budget. Once completed, upload budget here. A link to the budget is provided above.

Copy of 10352 Sponsor Budget Template Updated elv3.xlsx (1/19/2022 4:11 PM)

Tracking and Reporting

WDTF grant funds must be expended within a 36-month period. Award of funds will require the lead applicant/grant recipient to provide “skill training plans” for each job classification, identification of vendor training, training descriptions, skill attainments and costs. If the consortium provides internal training, the training must be a structured on-the-job training with a specific outline of the training curriculum, skills gained, expected outcomes and details on the effectiveness of the training.

Question: Entity responsible for tracking and reporting.

Boise State University

Question: Contact Person First Name

Edward

Question: Contact Person Last Name

Vasko

Question: Job Title

Director, Institute for Pervasive Cybersecurity

Question: Contact Phone

(208) 426-2480

Question: Email Address

edwardvasko@boisestate.edu

Question: Street Address

1910 University Dr

Question: City

Boise

Question: State

ID

Question: Zip Code

83725-1135

Organizational and Fiscal Capacity

The grant recipient – either the lead applicant or the training provider identified above – must have the organizational and fiscal capacity to track funds and safeguard spending.

Question: Please provide a short summary outlining your organizational capacity to complete this project?

The Institute of Pervasive Cybersecurity has four (4) full-time staff, three (3) assigned graduate assistants, and also supports four (4) faculty members looking to conduct research and mentoring. Two staff members are fully engaged with mentoring and maintaining the Cyberdome platform. Further, there are three graduate assistants conducting support and research utilizing the Cyberdome platform. Among these staff members, student workers utilizing this grant will have an very favorable worker to mentor ratio of either 7:1 (using full-time staff) or 2.8:1 (using full-time staff and graduate assistants).

Question: Please describe the grant recipient's accounting structure, job titles, and qualifications of staff responsible for fiscal actions.

The Office of Sponsored Programs (OSP) oversees sponsored project activities at Boise State University. OSP's primary mission is to support the University's sponsored activities by providing exceptional expertise and collaborative service. With a long history of federal, foundation and contractual awards, Boise State has all the resources needed to manage grants, and rank as an R2: Doctoral University – High Research Activity, in the Carnegie Classification. The Carnegie Classification is conducted by an entity outside of Boise State entity and has been the leading framework for recognizing and describing institutional diversity in U.S. higher education for the past four and a half decades. The R2 category includes only institutions that award at least 20 research/scholarship doctoral degrees and had at least $5 million in total research expenditures (as reported through the National Science Foundation (NSF) Higher Education Research & Development Survey (HERD). Boise State is a public institution that complies with all State and Federal requirements.

Question: Please provide a statement from the entity's independent auditing firm regarding the entity's most recent fiscal audit to include a statement of any audit findings. The

application may be rejected if audit findings exist. Attach signed statement here.

Boise-State-University-Annual-Financial-Statement-FY20-w-single-audit.pdf (11/15/2021 4:49 PM)

Terms and Conditions

Terms and Conditions

Question: I certify I have read the terms and conditions governing the Workforce Development Training Fund grant and agree to comply if awarded a training grant. Click on the link above to view a copy of the terms and conditions.

- [x] Yes
- [ ] No