LEGISLATIVE TRACKING FORM

Filing for Council Meeting Date: 08/05/25 ☑ **Resolution** ☐ **Ordinance**

Contact/Prepared By: Pearl Amanfu **Date Prepared:** 06/24/25

Title (Caption): The Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS Program) Application

Submitted to Planning Commission? ☑ **N/A** ☐ **Yes-Date:** _____ **Proposal No:** _____

Proposing Department: Information Technology Services **Requested By:** Information Technology Services

Affected Department(s): Mayor's Office, ITS, MAC **Affected Council District(s):** All

Legislative Category (check one):

☐ Bonds	☐ Contract Approval	☐ Intergovernmental Agreement
☐ Budget - Pay Plan	☐ Donation	☐ Lease
☐ Budget - 4%	☐ Easement Abandonment	☐ Maps
☐ Capital Improvements	☐ Easement Accept/Acquisition	☐ Master List A&E
☐ Capital Outlay Notes	☐ Grant	☐ Settlement of Claims/Lawsuits
☐ Code Amendment	☑ Grant Application	☐ Street/Highway Improvements
☐ Condemnation	☐ Improvement Acc.	☐ Other: _____

FINANCE **Amount +/-: $** 195482.64 **Match: $** _____

Funding Source:

Capital Improvement Budget	Judgments and Losses
Capital Outlay Notes	Local Government Investment Project
Departmental/Agency Budget	Revenue Bonds
Funds to Metro	Self-Insured Liability
General Obligation Bonds	Solid Waste Reserve
Grant	Unappropriated Fund Balance
Increased Revenue Sources	4% Fund
	Other: _____

Approved by OMB: Aaron Prott kH Date to Finance Director's Office: _____

Approved by Finance/Accounts: _____ **APPROVED BY**

Approved by Div Grants Coordination: Juanita Paulsen **FINANCE DIRECTOR'S OFFICE:** _____

ADMINISTRATION

Council District Member Sponsors: _____

Council Committee Chair Sponsors: _____

Approved by Administration: _____ **Date:** _____

DEPARTMENT OF LAW Date to Dept. of Law: _____ Approved by Department of Law: _____

Settlement Resolution/Memorandum Approved by: _____

Date to Council: _____ For Council Meeting: _____ ☐ E-mailed Clerk

☐ All Dept. Signatures ☐ Copies ☐ Backing ☐ Legislative Summary ☐ Settlement Memo ☐ Clerk Letter ☐ Ready to File

Department of Law – White Copy *Administration – Yellow Copy* *Finance Department - Pink Copy*

GRANT APPLICATION SUMMARY SHEET

Grant Name:	NIST NICE Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) 25-27
Department:	INFORMATION TECHNOLOGY SERVICES
Grantor:	U.S. DEPARTMENT OF COMMERCE
Pass-Through Grantor (If applicable):	
Total Applied For:	$195,482.64
Metro Cash Match:	$0.00
Department Contact:	Pearl Amanfu 4296459
Status:	NEW

Program Description:
The Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS) seeks to build multistakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. Effective multistakeholder workforce partnerships will organize multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.

Plan for continuation of services upon grant expiration:
NCWA aims to bridge this talent gap by developing a comprehensive and sustainable cybersecurity workforce pipeline by leveraging the strengths of strategic partners to provide training, pre-apprenticeships, apprenticeships, and job placement services, aligning with the NICE Workforce Framework for Cybersecurity.

APPROVED AS TO AVAILABILITY OF FUNDS:

Jennifer Reed/mgw
Director of Finance
Date 6/27/2025 | 12:30 PM CDT

APPROVED AS TO FORM AND LEGALITY:

Micki Fike
Metropolitan Attorney
Date 6/27/2025 | 3:47 PM CDT

APPROVED AS TO RISK AND INSURANCE:

Balogun Cobb
Director of Risk Management Services
Date 6/27/2025 | 1:55 PM CDT

Freddie O'Connell
Metropolitan Mayor
Date 6/30/2025 | 5:23 AM PDT

(This application is contingent upon approval of the application by the Metropolitan Council.)

6062

Grants Tracking Form

Part One

Pre-Application ○ **Application** ◉ **Award Acceptance** ○ **Contract Amendment** ○

Department	Dept. No.	Contact	Phone	Fax
INF. SYSTEMS	014	Pearl Amanfu	4296459	

Grant Name:	NIST NICE Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) 25-27		
Grantor:	U.S. DEPARTMENT OF COMMERCE	**Other:**	
Grant Period From:	10/01/25	(applications only) **Anticipated Application Date:**	07/01/25
Grant Period To:	09/30/27	(applications only) **Application Deadline:**	07/01/25
Funding Type:	FED DIRECT	**Multi-Department Grant** ☐ → **If yes, list below.**	Metro Action Commission Metro General Services
Pass-Thru:		**Outside Consultant Project:** ☐	
Award Type:	COMPETITIVE	**Total Award:**	$195,482.64
Status:	NEW	**Metro Cash Match:**	$0.00
Metro Category:	New Initiative	**Metro In-Kind Match:**	$98,458.55
CFDA #	11.620	**Is Council approval required?** ☑	
Project Description:		**Applic. Submitted Electronically?** ☑	

The Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS Program) seeks to build multistakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. Effective multistakeholder workforce partnerships will organize multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.

Plan for continuation of service after expiration of grant/Budgetary Impact:

NCWA aims to bridge this talent gap by developing a comprehensive and sustainable cybersecurity workforce pipeline by leveraging the strengths of strategic partners to provide training, pre-apprenticeships, apprenticeships, and job placement services, aligning with the NICE Workforce Framework for Cybersecurity. Our program objectives are aligned to help deliver entry-level to mid-level cybersecurity training pathways to 1) expand hands-on learning

How is Match Determined?

Fixed Amount of $		**or**	30.3%	**% of Grant**	**Other:** ☑

Explanation for "Other" means of determining match:

This is calculated as a portion of the Digital Inclusion Officer (Program Director, Digital Learning and Access) salary at 59.37%.

For this Metro FY, how much of the required local Metro cash match:

Is already in department budget?	$98,458.55		**Fund**	51137	**Business Unit** 14561010
Is not budgeted?			**Proposed Source of Match:**		
(Indicate Match Amount & Source for Remaining Grant Years in Budget Below)					

Other:

Number of FTEs the grant will fund:	0.00	**Actual number of positions added:**	0.00	
Departmental Indirect Cost Rate	4.90%	**Indirect Cost of Grant to Metro:**	$9,578.65	
***Indirect Costs allowed?** ◉ Yes ○ No **% Allow.**	2.00%	**Ind. Cost Requested from Grantor:**	$6,565.55	**in budget**
				1954.8264

Draw down allowable? ☐

Metro or Community-based Partners:

CFMT, Comcast, Global Action Platform, Nashville Chamber of Commerce, Tech Goes Home, Urban League of Middle Tennesse

Part Two

Grant Budget

Budget Year	Metro Fiscal Year	Federal Grantor	State Grantor	Other Grantor	Local Match Cash	Match Source (Fund, BU)	Local Match In-Kind	Total Grant Each Year	Indirect Cost to Metro	Ind. Cost Neg. from Grantor
Yr 1	FY26	$97,741.32				10401023	$49,229.28	$146,970.60	$4,789.32	$3,282.78
Yr 2	FY27	$97,741.32				10401023	$49,229.28	$146,970.60	$4,789.32	$3,282.78
Yr 3	FY__									
Yr 4	FY__									
Yr 5	FY__									
Total		$195,482.64					$98,458.55	$293,941.19	$9,578.65	$6,565.55

Date Awarded:		**Tot. Awarded:**		**Contract#:**	
(or) **Date Denied:**		**Reason:**			
(or) **Date Withdrawn:**		**Reason:**			

Contact: trinity.weathersby@nashville.gov
vaughn.wilson@nashville.gov

Rev. 5/13/13
6062

GC Rec'd
06/26/25

GC Approved
06/26/25

VW

RESOLUTION NO. _____

A resolution approving an application for a Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS) grant from the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), to the Metropolitan Government, acting by and through the Information Technology Services Department, to build cybersecurity education and workforce development partnerships between employers, educational institutions, and community organizations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.

WHEREAS, the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) is accepting applications for a Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS) grant with an award of $195,482.64 with an in-kind match of $98,458.55; and,

WHEREAS, the Metropolitan Government is eligible to participate in this grant program; and,

WHEREAS, it is to the benefit of the citizens of The Metropolitan Government of Nashville and Davidson County that the grant application be approved and submitted.

NOW, THEREFORE BE IT RESOLVED BY THE COUNCIL OF THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY:

Section 1. That the application for a Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS) grant, with an award of $195,482.64, a copy of which is attached hereto and incorporated herein, is hereby approved, and the Information Technology Services Department, is authorized to submit said application to the U.S. Department of Commerce, National Institute of Standards and Technology (NIST).

Section 2. That this resolution shall take effect from and after its adoption, the welfare of The Metropolitan Government of Nashville and Davidson County requiring it.

APPROVED AS TO AVAILABILITY OF FUNDS:

Jenneen Reed/mgw
Jenneen Reed, Director
Department of Finance

INTRODUCED BY:

_____

_____

_____
Member(s) of Council

APPROVED AS TO FORM AND LEGALITY:

Nicki Eke
Assistant Metropolitan Attorney

U.S. Department of Commerce,
National Institute of Standards and Technology (NIST),
Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS)
Cybersecurity Education and Workforce Development, 2025-NIST-RAMPS-01

Funding Opportunity Description:	The NIST National Initiative for Cybersecurity Education (NICE) program is seeking applications from eligible applicants for activities to establish community-based partnerships to develop cybersecurity career pathways that address local workforce needs. Effective multistakeholder workforce partnerships will organize multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.
Announcement Type:	Initial
Funding Instrument:	Cooperative Agreement
Assistance Listing (CFDA Number):	11.620: Science, Technology, Business and/or Education Outreach
Award Project Period:	Project performance period of up to two (2) years
Goals & Objectives:	The Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS Program) seeks to build multistakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. Effective multistakeholder workforce partnerships will organize multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.
Eligible Applicants:	Eligibility for the RAMPS Program listed in this NOFO is open to all non-Federal entities. Eligible applicants include accredited institutions of higher education; non-profit organizations; for-profit organizations incorporated in the United States; State, local,

	Territorial, and Indian Tribal governments. Please note that individuals and unincorporated sole proprietors are not considered "non-Federal entities" and are not eligible to apply under this NOFO. Additionally, foreign public entities and foreign organizations are not eligible to apply under this NOFO. Although Federal entities are not eligible to receive funding under this NOFO, they may participate as unfunded collaborators. Applicants must demonstrate, through commitment letters from project partners, that at least one of each of the following types of organizations is committed to being part of the proposed multistakeholder workforce partnership: ○ at least one institution of higher education or nonprofit training organization (that is not the applicant), and ○ at least one local employer or owner or operator of critical infrastructure (that is not the applicant). Participation from academic institutions in the Federal CyberCorps Scholarship for Service Program, the National Centers of Academic Excellence in Cybersecurity Program, or Advanced Technological Education programs, as well as elementary and secondary schools, training and certification providers, State and local governments, economic development organizations, or other community organizations is encouraged.
Funding Amount:	In Fiscal Year 2025 (FY25), NIST anticipates funding up to sixteen (16) awards for up to $200,000 per award. The authorized period of performance for awards issued pursuant to this NOFO is no more than two (2) years.
Cost Share/Matching Requirements:	Non-federal cost share is required. See section III.4. Specifically, non-federal cost share, including in-kind contributions, in an amount equal to not less than 50 percent of the Federal funds provided, is required for awards issued pursuant to this NOFO.
Estimated Number and Type of Award(s):	Up to sixteen (16) cooperative agreements with an initial period of performance of no more than two (2) years.

Submission Dates and Times:	Full Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, July 1, 2025. Applications received after this deadline will not be reviewed or considered. NIST expects to complete its review, selection of successful applicants, and award processing by September 2025. NIST expects the earliest start date for awards under this NOFO to be October 2025.
How to Apply:	Applications must be submitted using Grants.gov. Paper applications will not be accepted.
Review and Selection Process:	Group competition with defined evaluation criteria. See Section V. of this NOFO for additional information on the review and selection process for this NOFO.
Agency Contacts:	**Programmatic and Technical Questions:** Susana Barraza Information Technology Laboratory 240-457-2638 Susana.Barraza@nist.gov **Grant Rules and Regulations:** Nuria Martinez Financial Assistance and Agreements Office nofo@nist.gov
Additional Information:	NIST's NICE Program Office will host a webinar information session for applicants that are interested in learning about this funding opportunity. This webinar will provide general information regarding 2025-NIST-RAMPS-01 and offer general guidance on preparing proposals. Please reference https://www.nist.gov/nice for the most up to date information, including scheduling details about the webinar. Proprietary technical questions about specific proposal ideas will not be permitted, and NIST will not critique or provide feedback on any proposal ideas during the webinar or at any time before the deadline for all applications. However, questions about the funding opportunity, eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application will be addressed at the webinar and by e-mail to nice@nist.gov. There is no cost to attend the webinar, but participants must register in advance. Participation in the webinar is not required and will not be considered in the review and selection process.

Table of Contents

FULL ANNOUNCEMENT TEXT

I. Program Description

The statutory authority for the NIST NICE Program and for the Regional Alliances and Multistakeholder Partnerships to Stimulate Cybersecurity Education and Workforce Development Program (RAMPS Program) is 15 U.S.C. § 272(b)(4) and 15 U.S.C. § 7443.

The RAMPS Program seeks to build multistakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. Effective multistakeholder workforce partnerships will organize multiple employers with skill shortages in specific occupations to focus on developing the skilled workforce to meet industry needs within the local or regional economy.

a) Background Information

In our connected society almost every organization in the United States uses the Internet for commerce, communication, or service provision. Cybersecurity has therefore, emerged as one of our nation's top priorities for both national and economic security. Increasing our security of cyberspace requires a skilled workforce to design secure products and services and to protect businesses, non-profit organizations, academic institutions, and governments at all levels in order to minimize enterprise risks.

NICE, led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce (DoC) is a partnership between Federal agencies, industry, educational institutions, and other organizations to coordinate a national cybersecurity awareness and education program. The mission of NICE is to energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful

programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity practitioners helping to keep our Nation secure.

NICE was initially established to meet the cybersecurity training, education, and awareness priorities expressed in Section II. of the 2009 Cyberspace Policy Review, Building Capacity for a Digital Nation. It expanded upon the 2008 Comprehensive National Cybersecurity Initiative (CNCI) number 8: Expand Cyber Education, which acknowledged that in order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically- skilled and cyber-savvy workforce and an effective pipeline of future employees."

To guide NICE's efforts, a strategic plan has been established and is updated every five years. The current NICE Strategic Plan (available at https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan) covers 2021-2025 and has the following goals:

- Goal #1: Promote the Discovery of Cybersecurity Careers and Multiple Pathways;
- Goal #2: Transform Learning to Build and Sustain a Diverse and Skilled Workforce;
- Goal #3: Modernize the Talent Management Process to Address Cybersecurity Skills Gaps;
- Goal #4: Expand Use of the Workforce Framework for Cybersecurity (NICE Framework); and
- Goal #5: Drive Research on Effective Practices for Cybersecurity Workforce Development.

Jennieen Reed/nyw

Additionally, NICE seeks to build upon and support existing Federal strategies that provide key elements of effective workforce practices, including but not limited to recruitment, hiring, and retention. Alignment with these strategies enable a unified ecosystem for cybersecurity workforce development.

Further, the NICE Program Office publishes guidance, reports, use cases, and white papers related to cybersecurity education, training, and workforce development. NICE's signature publication is the Workforce Framework for Cybersecurity (NICE Framework) (available at http://nist.gov/nice/framework/). The NICE Framework defines the cybersecurity workforce and provides a common taxonomy and lexicon by which to classify and categorize workers. The NICE Framework lists Work Roles and Competency Areas of cybersecurity work and provides a description of each. The NICE Framework also identifies common Task, Knowledge, Skill (TKS) statements, also known as building blocks. The NICE Framework is used within the federal government and is available for use

by the private, public, and academic sectors for describing cybersecurity work and aligning related education, training, and professional development content.

In 2016, NIST conducted a one-year pilot of the NICE RAMPS program with five organizations dispersed across the country. NIST Interagency Report (NISTIR) 8287: A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce was published to provide a summary of the five programs and outline a roadmap for building similar programs based on the best practices found and lessons learned.

In 2023 and 2024, NIST awarded 33 cooperative agreements based upon new authorization in the FY21 National Defense Authorization Act and appropriated for FY23 and FY24.

b) Program Requirements

Each application for funding pursuant to this NOFO must include a plan to establish a multistakeholder education and workforce partnership that includes, at a minimum, one institution of higher education or nonprofit training organization (that is not the applicant), and one local employer or owner or operator of critical infrastructure (that is not the applicant).

Participation from one or more of the following types of organizations is also encouraged: academic institutions in the Federal CyberCorps Scholarship for Service Program, the National Centers of Academic Excellence in Cybersecurity Program, or Advanced Technological Education programs; elementary and secondary schools; training and certification providers; economic development organizations; and other community organizations.

The applicant's **proposed project must:**

1. Ensure that the partnership is employer-led, community-focused, learner-centered, standards-based, and outcomes-driven.
2. 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.
3. Advance uses of the NICE Framework, including through demonstration of how the stakeholders intend to use the NICE Framework.
4. 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 (see https://cyberseek.org)[1].
    a. CyberSeek is a free online tool that provides data on the

[1] CyberSeek is supported by NIST through NICE, under financial assistance award # 60NANB22D100.

supply and demand of cybersecurity talent.

   b. CyberSeek's interactive map shows a snapshot of open jobs across the United States. Additionally, the career pathway provides insight on the progression of a cybersecurity career.

5. 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. Inclusion of programs that seek to include veterans, Indian Tribes, and underrepresented groups, including women, minorities, persons from rural and underserved areas, and persons with disabilities is encouraged. Identify how it would collaborate with one or more Federal CyberCorps Scholarship for Service (SFS) (https://sfs.opm.gov/), National Centers of Academic Excellence in Cybersecurity (CAE) (http://www.caecommunity.org), or Advanced Technological Education (ATE) program (http://www.nsf.gov/ate) institutions located in the region.
   a. The SFS Program, coordinated by the National Science Foundation, includes over 100 institutions of higher education aimed at improving the national capacity for the education of cybersecurity professionals.
   b. Additionally, the CAE program, coordinated by the National Security Agency and the Cybersecurity and Infrastructure Security Agency, and the ATE program, coordinated by the National Science Foundation, each have designated regional centers for advancing cybersecurity education.
   c. It is critical that RAMPS coordinate with the applicable regional centers and institutions to decrease duplication of efforts and to build on existing successful approaches.
6. Define metrics that will be used to measure the success of their efforts. Metrics should include but not be limited to the number of SFS, CAE, and ATE programs that participate in the program, outcomes of workforce demand and supply assessment, outcomes of recruitment activities, timeliness of milestones reached, etc.

A successful project will create the local conditions (e.g., infrastructure for education providers, employers, and others to develop the cybersecurity education capabilities) to create an ecosystem equipped to fill a critical skill gap for the economy.

NIST requires the award recipients to attend **two** quarterly meetings following the submission of their performance technical reports. The two quarterly meetings will be held virtually using NIST-approved meeting platforms. More information regarding meeting times and dates will be provided by the NIST-NICE Program Office once awards are issued.

In accordance with 15 U.S.C. § 7443(f)(5), all recipients (regardless of organizational type) of a NICE award issued pursuant to this NOFO are subject to the audit requirements under 2 C.F.R. part 200, Subpart F.

II. Federal Award Information

1. **Funding Instrument.** The funding instrument that will be used is a cooperative agreement. Where cooperative agreements are used, the nature of NIST's "substantial involvement" will generally include collaboration with the recipient organization in developing and implementing the approved scope of work, consistent with the definition of cooperative agreement in 2 CFR § 200.1.

2. **Multi-Year Funding Policy.** When a proposal for a multi-year award is approved, funding will usually be provided for only the first year of the program. If a project is selected for funding, NIST has no obligation to provide any additional funding in connection with that award. Continuation of an award to increase funding or extend the period of performance is at the sole discretion of NIST. Continued funding will be contingent upon satisfactory performance, continued relevance to the mission and priorities of NIST'S Information Technology Laboratory, and the availability of funds.

3. **Funding Availability.** In FY25, NIST anticipates funding up to sixteen (16) awards for up to $200,000 in federal funding per award and with a project performance period of no more than two (2) years.

4. **Indirect (F&A) Costs.** NIST will reimburse applicants for proposed indirect (F&A) costs in accordance with 2 CFR § 200.414. Applicants proposing indirect (F&A) costs must follow the application requirements set forth in Section IV of this NOFO.

III. Eligibility Information

1. **Eligible Applicants**
   Eligibility for the program listed in this NOFO is open to all non-Federal entities. Eligible applicants include accredited institutions of higher education; non-profit organizations; for-profit organizations incorporated in the United States; state, local, territorial, and Indian tribal governments. Please note that individuals and unincorporated sole proprietors are not considered "non-Federal entities" and are not eligible to apply under this NOFO. Additionally, foreign public entities and foreign organizations are not eligible to apply under this NOFO. Although Federal entities are not eligible to receive funding under this NOFO, they may participate as unfunded collaborators.

Applicants must also demonstrate, through commitment letters from project partners, that at least one of each of the following types of organizations is committed to being part of the proposed multistakeholder workforce partnership:

- at least one institution of higher education or nonprofit training organization, and
- at least one local employer or owner or operator of critical infrastructure.

The minimum two required commitment letters must come from entities that are not the applicant.

Participation from academic institutions in the Federal CyberCorps Scholarship for Service Program, the National Centers of Academic Excellence in Cybersecurity Program, or Advanced Technological Education Program, as well as elementary and secondary schools, training and certification providers, State and local governments, economic development organizations, or other community organizations is encouraged.

2. **Cost Sharing or Matching Funds**

Non-federal cost share is required. Specifically, non-federal cost share contributions, including in-kind contributions, in an amount not less than 50 percent of the Federal funds provided, is required for awards under the award issued pursuant to this NOFO. Non-federal cost sharing is that portion of the project costs not borne by the Federal Government. The applicant's share of expenses may include cash, services, and third-party in-kind contributions, as described at 2 CFR §200.306. The source and detailed rationale of the cost share, including cash, full- and part-time personnel, and in-kind donations, must be documented in the Budget Narrative and Justification submitted with the application and will be considered as part of the review under the evaluation criterion found in Section V of this NOFO. As with the Federal share, any proposed costs included as non-Federal cost sharing must be an allowable/eligible cost under this program and under the Federal cost principles set forth in 2 CFR part 200, Subpart E.

Non-federal cost sharing incorporated into the budget of an approved financial assistance award is subject to audit in the same general manner as Federal award funds. See 2 CFR part 200, Subpart F.

IV. Application and Submission Information

1. Address to Request Application Package

The application package is available at Grants.gov under Funding Opportunity Number 2025-NIST-RAMPS-01.

2. **Content and Form of Application Submission.** Set forth below are the required content and form of applications submitted pursuant to this NOFO.

   a. **Required Forms and Documents. The Application must contain the** following:

      (1) SF-424, Application for Federal Assistance. The SF-424 must be signed by an authorized representative of the applicant organization.

      For SF-424, Item 8.d. Zip/Postal Code field, should reflect the Zip code + 4 (#####-####) format.

      For SF-424, Item 12, should list the NOFO number 2025-NIST-RAMPS-01.

      SF-424, Item 18, should list the total budget information for the duration of the project.

      The list of certifications and assurances referenced in Item 21 of the SF-424 is contained in the Federal Financial Assistance Certifications and Representations (Certs and Reps) as part of the SAM.gov entity registration.

      (2) SF-424A, Budget Information for Non-Construction Programs. The budget should reflect anticipated Federal and non-Federal expenses for the entire project, considering all potential cost increases, including cost of living adjustments.

         a) The applicant should reflect each year of the project, up to the first four (4) years, on the SF-424A form that appears as part of the mandatory forms in the Grants.gov application package.

         b) In Section A, the Grant Program Function or Activity on Line 1 under Column (a) should be entered as Science, Technology, Business, and/or Education Outreach, CFDA 11.620, or an abbreviation thereof. The Catalog of Federal Domestic Assistance Number on Line 1 under Column (b) should be entered as “11.620”. The total federal budget amount for the term of the award should be listed in Section A, Line 1, Column (e). The total non-federal budget amount for the term of the award should be listed in Section A, Line 1, Column (f).

c) Section B, Column (1) of the SF-424A should reflect the costs for each object class category, to include indirect charges, for the first year of the award. These costs should reflect the total Federal share plus non-Federal cost share for each category. Section B, Column (2) of the SF-424A should reflect the costs for each object class category, to include indirect charges, for the second year of the award. These costs should reflect the total Federal share plus non-Federal cost share for each category.

d) Section C must account for all non-Federal resources / match for the entire project. For Column (b) enter resources provided by the applicant. If not applicable, leave blank. For Column (c), enter resources provided by one or more states. If not applicable, leave blank. For Column (d) enter resources provided by other sources (e.g., in-kind contribution, program income). If not applicable, leave blank.

e) Section D requires a breakdown of the first year's Federal share and non-Federal share of the budget by quarter.

f) Section E requires the budget estimate of Federal funds needed for each year of the project. The budget estimate for the first year of the award should be entered in Section E, Line 16, Column (b). The budget estimate for the second year of the award should be entered in Section E, Line 16, Column (c). The budget estimate for the third year of the award should be entered in Section E, Line 16, Column (d). And the budget estimate for the fourth year of the **award should be entered in Section E, Line 16, Column (e).**

(3) CD-511, Certification Regarding Lobbying. Enter "2025-NIST-RAMPS-01" in the Award Number field. Enter the title of the application, or an abbreviation of that title, in the Project Name field.

(4) SF-LLL, Disclosure of Lobbying Activities (if applicable**).**

(5) Project Narrative. The Project Narrative is a word-processed document of no more than fifteen (15) pages (double-spaced between lines), which is responsive to the program description and the evaluation criteria.

The page limit includes *Cover Page; Table of Contents (if included); Project Narrative with all required information, including figures, graphs, tables, images, and pictures).*

The projective narrative should contain the following information:

a) **Executive Summary.** An executive summary of the proposed project, consistent with the objectives, requirements, and priorities of this program (*see* Section I. of this NOFO). his section must include a listing of the stakeholders planning to participate in the multistakeholder workforce partnership, the organizational structure for that partnership, and an outline of the planned cybersecurity education and workforce development related activities of that partnership. The executive summary should also include information indicating how each evaluation criterion (see Section V.1. of this NOFO) and its sub-factors are addressed. A table can be helpful in providing this information. The executive summary should not exceed two (2) pages.

b) **Project Approach and Project Execution Plan.** A detailed discussion of the applicant's approach in planning for and in executing the proposed project consistent with the objectives, requirements, and priorities of this program (see Section I. of this NOFO). A description of how employers in the community will be recruited to support internships, externships, apprenticeships, or cooperative education programs in conjunction with providers of education and training. A description of how the proposed project would include veterans, Indian Tribes, and underrepresented groups, including women, minorities, persons from rural and underserved areas, and persons with disabilities. This section should also include details on the approach to collaborate with academic institutions in the SFS, CAE, and ATE programs, as well as elementary and secondary schools, training and certification providers, State and local governments, economic development organizations, or other community organizations. Evidence that the applicant already has a strong multistakeholder workforce partnership with demonstrated outcomes is helpful. If the applicant is building on an existing partnership, provide a detailed explanation of the current scope of that partnership, information about outcomes, and supporting evidence of proven effectiveness. The summary should also include a description of how the workforce partnership would identify the workforce needs of the local economy. This section should also provide a description of the proposed project plan and execution strategy sufficient to permit evaluation of the proposal, in accordance with details included in the proposal Evaluation Criteria (see Section V.1.a. of this NOFO).

c) **Project Impacts and Evaluation.** A detailed discussion of the: (i) anticipated impacts of the proposed project; (ii) methodology for identifying and evaluating project outcomes; and (iii) dissemination

of project learnings consistent with the objectives, requirements, and priorities of this program. This section should provide a definition of the metrics to be used in determining the success of the efforts of the regional alliance or partnership under the agreement. Explanation of what organizational data related to workforce demand and available supply of skilled workers will be collected, how such data will be collected or analyzed about cybersecurity workforce needs, and the available supply of a skilled cybersecurity workforce from the State and/or local area. This State and/or local cybersecurity workforce assessment will identify gaps and support development of CyberSeek. This section should address the Project Impact, in accordance with details included in the proposal Evaluation Criteria (see section V.1.b. of this NOFO).

d) Qualifications. description of the qualifications of the key personnel, the time commitments of the key personnel, and how the project staff qualifications will enable them to complete the project work. This section should address the Staff and Institution Capability to Perform the Work, in accordance with details included in the proposal Evaluation Criteria (see Section V.1.c. of this NOFO).

e) Dissemination Plan. A description of the applicant's approach to broadly disseminate the results of the project to the public. The plan should include an approach to publish results in appropriate literature, and through presentations at public meetings or events. This section should address the Dissemination of Results, in accordance with details included in the proposal Evaluation Criteria (see section V.1.b. of this NOFO).

(6) Resume(s) of Key Personnel. Resumes for all key personnel assigned to the project must be provided. Resumes are limited to two (2) pages per individual.

(7) Budget Narrative and Justification. There is no set format for the Budget Narrative and Justification; however, further explanation must be provided for the specific cost categories and line items that you identified in the SF-424A form as well as any other information you deem necessary for NIST's consideration.

The written justification should include the necessity and the basis for the cost, as described below. Proposed funding levels must be consistent with the project scope, and only allowable costs should be included in the budget. Information on cost allowability is available in the

Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200, which apply to awards in this program.

When cost share is included in the budget, the written justification must also identify the Federal and non-Federal portion of each cost, to include indirect costs, as applicable. (see Cost Sharing section of this NOFO for match requirements).

The Budget Narrative does not count against the fifteen (15) page limit of the Project Narrative.

This section will be evaluated in accordance with the Budget Narrative evaluation criteria. It will also be reviewed to determine if all costs are reasonable, allocable, and allowable under 2 C.F.R. Part 200 Subpart E, Cost Principles.

Information needed for each budget category is as follows:

a) **Personnel**- At a minimum, the budget justification for all personnel should include the following: job title, commitment of effort on the proposed project in terms of average number of hours per week or percentage of time, salary rate, total personnel charges for each identified position on the proposed project, description of the role of the individual on the proposed project and the work to be performed. The cost of the time required to prepare presentations to report on the progress of the project to the NICE Conference & Expo should also be included in this category.

b) **Fringe Benefits**- Fringe benefits for each position should be identified separately from salaries and wages and based on rates determined by organizational policy. The items included in the fringe benefit rate (e.g., health insurance, parking, etc.) should not be charged under another cost category.

c) **Travel**- NIST will require that award recipients report on their projects at the NICE Conference & Expo (see https://niceconference.org/) at the start and conclusion of their projects (i.e., in June 2026 and June 2027) and participate in half-day, pre-conference workshops adjacent to the NICE Conference for sharing information. Therefore, applicants must include travel costs for the NICE Conference & Expo. For all travel costs, the budget justification for travel should include the following: destination; names or number of people traveling; dates and/or duration; mode of transportation, lodging and subsistence rates;

and description of how the travel is directly related to the proposed project. For travel that is yet to be determined, please provide best estimates based on prior experience. If a destination is not known, an approximate amount may be used with the assumptions given for the location of the meeting.

d) **Equipment**- Equipment is defined as an item of property that has an acquisition cost of $5,000 or more (unless the organization has established lower levels) and an expected service life of more than one year. The budget justification should list each piece of equipment, the cost, and a description of how it will be used and why it is necessary to the successful completion of the proposed project. Please note that any general use equipment (computers, etc.) charged directly to the award should be allocated to the award according to expected usage on the project.

e) **Supplies**- Supplies are defined as all tangible personal property other than that described as equipment. Provide a list of each supply, and the breakdown of the total costs by quantity or unit of cost. Include the necessity of the cost for the completion of the proposed project.

f) **Contractual (i.e., Contracts or Subawards)**- Each contract or subaward should be treated as a separate item. Identify the cost and describe the services to be provided and the necessity of the subaward or contract to the successful performance of the proposed project. Contracts are for obtaining goods and services for the Non-Federal Entity's own use and creates a procurement relationship with the contractor. A subaward is for the purpose of carrying out a portion of a Federal award and creates a Federal assistance relationship with the subrecipient.

g) **Construction**- Not an allowable activity or cost under this NOFO.

h) **Other Direct Costs**- For costs that do not easily fit into the other cost categories, please list the cost, and the breakdown of the total costs by quantity or unit of cost. Include the necessity of the cost for the completion of the proposed project. Only allowable costs can be charged to the award.

i) **Indirect Costs**- Commonly referred to as Facilities & Administrative Costs, Indirect Costs are defined as costs incurred by the applicant organization that cannot otherwise be directly assigned or attributed to a specific project. The justification should include a cost calculation that reflects the applicable indirect cost

rate. For more details, *see* Section IV.2.a.(8) of this NOFO.

(8) Indirect Cost Rate Agreement. If indirect costs are included in the proposed budget, provide a copy of the approved negotiated agreement if this rate was negotiated with a cognizant Federal audit agency. If the rate was not established by a cognizant Federal audit agency, provide a statement to this effect. If the successful applicant includes indirect costs in the budget and has not established an indirect cost rate with a cognizant Federal audit agency, the applicant will be required to obtain such a rate in accordance with Section B.06 of the Department of Commerce Financial Assistance General Terms and Conditions, dated October 1, 2024.

Alternatively, in accordance with 2 C.F.R. § 200.414(f), applicants that do not have a current negotiated (including provisional) indirect cost rate except for those non-Federal entities described in appendix VII, paragraph D.1.b. of 2 CFR 200 may elect to charge a de minimis rate of 10 percent of modified total direct costs (MTDC). Applicants proposing a 10 percent de minimis rate pursuant to 2 C.F.R. § 200.414(f) should note this election as part of the budget portion of the application.

(9) Letters of Commitment. Letters of Commitment must be submitted by all funded and unfunded entities that will have an active role in executing the activities outlined in the Project Narrative. Letters of Commitment must address the level of participation, qualifications of the personnel who will be actively involved, and how successful completion of this project would positively impact their profession or community. Letters of Commitment must also specify any voluntary committed cost-share, including the specific services and/or products to be used in the project. Letters of Commitment must be signed by an individual with authority to legally bind the organization to its commitment. Letters of Commitment do not count against the page limit of the Project Narrative.

Applications must include commitment letters from at least one of each of the following types of organizations as specified below. Failure to include these Letters of Commitment will result in applications not being reviewed.

- At least one institution of higher education or nonprofit training organization, and
- At least one local employer or owner or operator of critical infrastructure.

While letters of commitment from the applicant may strengthen a proposal, the minimum two required letters must come from entities that are not the applicant.

Inclusion of letters of commitment from additional organizations of the above types as well as training and certification providers, economic development organizations and other community organizations may further strengthen the application. Applicants with strong existing regional partnerships should indicate this in the letters.

(10) Current and Pending Support Form. Any application that includes investigators, researchers, and key personnel must identify all sources of current and potential funding, including this proposal. Any current project support (e.g., Federal, state, local, public, or private foundations, etc.) must be listed on this form. The proposed project and all other projects or activities requiring a portion of time of the Principal Investigator (PI), co-PI, and key personnel must be included, even if no salary support is received. The total award amount for the entire award period covered, including indirect costs, must be shown as well as the number of person-months per year to be devoted to the project, regardless of the source of support. Similar information must be provided for all proposals already submitted or that are being submitted concurrently to other potential funders.

Applicants must complete the Current and Pending (Other) Support Common Form, using multiple forms as necessary to account for all activity for each individual identified in the PI, co-PI, and key personnel roles. A separate form should be used for each identified individual.

Applicants must download the Current and Pending (Other) Support Common Form from the NIST website at: Current and Pending Support | NIST and reference the guidance provided as it contains information to assist with accurately completing the form.

b. Attachment of Required Documents

Items IV.2.a.(1) through IV.2.a.(4) above are part of the standard application package in Grants.gov and can be completed through the download application process.

Items IV.2.a.(5) through IV.2.a.(10) should be attached to field 15 of the SF-424 form by clicking on “Add Attachments”.

Following these directions will create zip files which permit transmittal of the documents electronically via Grants.gov.

Applicants should carefully follow specific Grants.gov instructions at Grants.gov to ensure the attachments will be accepted by the Grants.gov

system. A receipt from Grants.gov indicates only that an application was transferred to a system. It does not provide details concerning whether all attachments (or how many attachments) transferred successfully. Applicants will receive a series of e-mail messages over a period of up to two business days before learning whether a Federal agency's electronic system has received its application.

Applicants are strongly advised to use Grants.gov's "Download Submitted Forms and Applications" option to check that their application's required attachments were contained in their submission.

After submitting the application, check the status of your application here: CHECK APPLICATION STATUS. If any, or all, of the required attachments are absent from the submission, follow the attachment directions found above, resubmit the application, and check again for the presence of the required attachments.

If the directions found on the Grants.gov Online Help page are not effective, please contact the Grants.gov Help Desk immediately. If calling from within the United States or from a U.S. territory, please call 800-518-4726. If calling from a place outside the United States or a U.S. territory, please call 606-545-5035. E-mails should be addressed to support@grants.gov. Assistance from the Grants.gov Help Desk will be available around the clock every day, with the exception of Federal holidays. Help Desk service will resume at 7:00 a.m. Eastern Time the day after Federal holidays.

Applicants can track their submission in the Grants.gov system by following the procedures at the Grants.gov Track My Application page. It can take up to two business days for an application to fully move through the Grants.gov system to NIST.

NIST uses the Tracking Numbers assigned by Grants.gov and does not issue Agency Tracking Numbers.

c. Application Format

(1) Paper, Email, and Facsimile (fax) Submissions. Will not be accepted.

(2) Figures, Graphs, Images, and Pictures. Should be of a size that is easily readable or viewable and may be displayed in landscape orientation. Any figures, graphs, images, or pictures will count toward the page limits for the Project Narrative.

(3) Font. Easy to read font (10-point minimum). Smaller type may be used in figures and tables but must be clearly legible.

(4) Page Limit. The Project Narrative is limited to fifteen (15) pages double-spaced, noting the limit of two (2) pages for the Executive Summary. Resumes are not included in the page count of the Project Narrative. However, if resumes are included, resumes must be a maximum of two (2) pages each.

(5) Page Limit Exclusions:
SF-424, Application for Federal Assistance;
SF-424A, Budget Information for Non-Construction Programs;
CD-511, Certification Regarding Lobbying;
SF-LLL, Disclosure of Lobbying Activities (if applicable);
Resumes;
Budget Narrative and Justification;
Indirect Cost Rate Agreement;
Letters of Commitment;
Current and Pending Support Form.

(6) Page Layout. The Proposal must be in portrait orientation.

(7) Page size. 21.6 centimeters by 27.9 centimeters (8 ½ inches by 11 inches).

(8) Page numbering. Number pages sequentially.

(9) Application language. All documents must be in English, including but not limited to the initial application, any additional documents submitted in response to a NIST request, all reports, and any correspondence with NIST.

(10) Typed document. All applications, including forms, must be typed; handwritten forms will not be accepted.

d. **Application Replacement Pages.** Applicants may not submit replacement pages and/or missing documents once an application has been submitted. Any revisions must be made by submission of a new application that must be received by NIST by the submission deadline.

e. **Pre-Applications.** Pre-applications will not be accepted under this NOFO.

3. **Unique Entity Identifier and System for Award Management (SAM).** Pursuant to 2 C.F.R. part 25, applicants and recipients are required to: (i) be registered in SAM before submitting its application; (ii) provide a valid unique

entity identifier in its application; and (iii) continue to maintain an active SAM registration with current information at all times during which it has an active Federal award or an application or plan under consideration by a Federal awarding agency, unless otherwise excepted from these requirements pursuant to 2 C.F.R. § 25.110. NIST will not make a Federal award to an applicant until the applicant has complied with all applicable unique entity identifier and SAM requirements and, if an applicant has not fully complied with the requirements by the time that NIST is ready to make a Federal award pursuant to this NOFO, NIST may determine that the applicant is not qualified to receive a Federal award and use that determination as a basis for making a Federal award to another applicant.

4. **Submission Dates and Times**
   Dates: Full Applications must be received at Grants.gov no later than 11:59 p.m. Eastern Time, July 1, 2025. Applications received after this deadline will not be reviewed or considered.

   Applicants should be aware, and factor in their application submission planning, that the Grants.gov system closes periodically for routine maintenance. Applicants should visit Grants.gov for information on any scheduled closures. Applications cannot be submitted when Grants.gov is closed.

   NIST expects to complete its review, selection of successful applicants, and award processing by September 2025. NIST expects the earliest start date for awards under this NOFO to be October 2025.

   When developing the submission timeline, please keep in mind that: (1) all applicants are required to have current registrations in the electronic System for Award Management (SAM.gov) and Grants.gov; (2) the free annual registration process in the SAM.gov generally takes between three and five business days but can take more than three weeks; and applicants will receive e-mail notifications over a period of up to two business days as the application moves through intermediate systems before the applicant learns via a validation or rejection notification whether NIST has received the application. (See Grants.gov for full information on application and notification through Grants.gov.) Please note that a Federal assistance award cannot be issued if the designated recipient's registration in the System for Award Management (SAM.gov) is not current at the time of the award.

5. **Intergovernmental Review**
   Applications submitted by State and local governments are subject to Executive Order (E.O.) 12372, "Intergovernmental Review of Federal Programs," pursuant to which each State designates an entity to coordinate, and review proposed federal financial assistance and direct federal

development. All other applicants should consult the Intergovernmental Review State Single Point of Contact (SPOC) to determine whether the application is subject to State review pursuant to E.O. 12372. The current SPOC List may be found here.

6. **Funding Restrictions**
   Construction is not an allowable activity or an allowable cost under this program. In addition, a recipient or a subrecipient may not charge profits, fees, or other increments above cost to an award issued pursuant to this NOFO. Applications for product development and/or commercialization are not considered responsive to this NOFO.

7. **Other Submission Requirements**

   a. **Applications must be submitted at Grants.gov. Paper applications will not be accepted.** Applicants should carefully follow specific Grants.gov instructions to ensure that all attachments will be accepted by the Grants.gov system. A receipt from Grants.gov indicating an application is received does not provide information about whether attachments have been received. For further information or questions regarding applying electronically for the 2025-NIST-RAMPS-01 announcement, contact the Grants.gov Help Desk at 800-518-4726

   b. **Amendments.** Any amendments to this NOFO will be announced through Grants.gov. Applicants may sign up on Grants.gov to receive amendments by e-mail or may request copies by e-mail from nice@nist.gov.

V. Application Review Information

1. Evaluation Criteria

The evaluation criteria that will be used in evaluating applications and their assigned weights are as follows:

a. **Project Approach.** The rationality, innovation, and creativity of the project approach, including planning and executing the proposed project objectives, requirements, and priorities of this program (see Section I.2. of this NOFO). The perceived existing strength or potential strength of the proposed regional, multistakeholder partnerships and the extent to which the project(s) align to and support NICE, NIST, DoC, and other strategies as outlined in Section I.1. of this NOFO. **(35 points)**

b. **Project Impact and Dissemination of Results.** The potential effectiveness of the proposed activity, and the likelihood and potential impact of the applicant's approach to strengthen and enhance the mission of the RAMPS Program. The applicant's proposed approach to publish results in appropriate literature, and through presentations to the public. **(35 points)**

c. **Staff and Institution Capability to Perform the Work.** The quality of the facilities and experience of the staff in achieving the objective of the proposed activity. The extent of the key personnel's experience and education relevant to the project(s) proposed. **(15 points)**

d. **Match of Budget to Proposed Work.** Assessment of the suitability and focus of the applicant's budget against the proposed activities to ascertain whether the budget projections are reasonable and appropriate for the scale of effort to be undertaken by the applicant. **(15 points)**

2. Selection Factors

The Selection Factors for this competition are as follows:

(1) Priority consideration shall be given to a regional alliance or partnership that includes one or more institution of higher education that is designated as a National Center of Academic Excellence in Cybersecurity, Advanced Technological Education program, or which received an award under the Federal CyberCorps Scholarship for Service program located in the State or region of the regional alliance or partnership;
(2) The availability of funding;
(3) Whether the project duplicates other projects funded by NIST or other Federal agencies;
(4) Regional diversity;
(5) Diversity of the proposed project topics relative to the overall portfolio of activities funded under this NOFO;
(6) Diversity of the proposed project topics relative to the overall portfolio of NICE projects; and
(7) The institutional diversity of project participants, which may include the extent of active project participation of small- and medium-sized manufacturing enterprises, and career and technical education schools, community colleges, and universities.

3. Review and Selection Process

Proposals, reports, documents, and other information related to applications submitted to NIST and/or relating to financial assistance awards issued by

NIST will be reviewed and considered by Federal employees, or non-Federal personnel who have entered into conflict of interest and confidentiality agreements covering such information, when applicable.

a. **Initial Administrative Review of Applications.**
Applications received by the deadline will be reviewed to determine eligibility, completeness, and responsiveness to this NOFO and to the scope of the stated program objectives. Applications determined to be ineligible, incomplete, and/or nonresponsive may be eliminated from further review. However, NIST, in its sole discretion, may continue the review process for an application that is missing non-substantive information, the absence of which may easily be rectified during the review process.

b. **Full Review of Eligible, Complete, and Responsive Applications.**
Applications that are determined to be eligible, complete, and responsive will proceed for full reviews in accordance with the review and selection process below:

(1) Merit Review. At least three (3) independent, objective reviewers, who may be Federal employees or non-Federal personnel, with appropriate professional and technical expertise relating to the topics covered in this NOFO, will evaluate, and score each eligible, complete, and responsive application based on the evaluation criteria. While every application will have at least three (3) reviewers, applications may have more than three (3) reviewers if specialized expertise is needed to evaluate an application. During the review process, the reviewers may discuss the applications with each other, but scores will be determined on an individual basis, not a consensus. Based on the numerical average of the reviewers' scores, a rank order will be prepared and provided to the Evaluation Panel for further consideration.

(2) Evaluation Panel. Following the merit review, an evaluation panel consisting of NIST staff and/or other Federal employees with the appropriate technical expertise will conduct a panel review of the ranked applications. The evaluation panel may contact applicants via e-mail to clarify contents of an application. The evaluation panel will provide a final adjectival rating and written evaluation of the applications to the Selecting Official for further deliberation, considering:

• All application materials;
• Results of the merit reviewers' evaluations, including scores and written assessments;

• Any relevant publicly available information; and
• Any clarifying information obtained from the applicants.

The adjectival ratings are:

Outstanding
Very Good
Average
Deficient

For decision-making purposes, applications receiving the same adjectival rating will be considered to have an equivalent ranking, although their review scores may not necessarily be the same.

(3) Selection. The Selecting Official, the Director of NICE or designee, will make final award recommendations to the NIST Grants Officer. The Selecting Official shall generally select and recommend the most meritorious application[s] for an award based upon the final adjectival rating prepared by the Evaluation Panel. The Selecting Official retains the discretion to select and recommend an application out of rank order based on one or more of the Selection Factors.

NIST reserves the right to negotiate the budget costs with any applicant selected to receive an award, which may include requesting that the applicant removes certain costs. Additionally, NIST may request that successful applicants modify objectives or work plans and provide supplemental information required by the agency prior to award. NIST also reserves the right to reject an application where information is uncovered that raises a reasonable doubt as to the responsibility of the applicant. NIST may select some, all, or none of the applications, or part(s) of any application. The final approval of selected applications and issuance of awards will be by the NIST Grants Officer. The award decisions of the NIST Grants Officer are final.

c. Federal Awarding Agency Review of Risk Posed by Applicants. After applications are proposed for funding by the Selecting Official, the NIST Financial Assistance Agreements Management Office (FAAMO) performs pre-award risk assessments in accordance with 2 C.F.R. § 200.206, which may include a review of the financial stability of an applicant, the quality of the applicant's management systems, the history of performance, and/or the applicant's ability to effectively implement statutory, regulatory, or other requirements imposed on non-Federal entities.

In addition, prior to making an award where the total Federal share is expected to exceed the simplified acquisition threshold (currently $250,000), NIST FAAMO will review and consider the publicly available information about that applicant in the Responsibility/Qualification records about that applicant in SAM.gov (formerly the Federal Awardee Performance and Integrity Information System (FAPIIS)). An applicant may, at its discretion, review, and comment on information about itself previously entered into SAM.gov by a Federal awarding agency. As part of its review of risk posed by applicants, NIST FAAMO will consider any comments made by the applicant in SAM.gov in making its determination about the applicant's integrity, business ethics, and record of performance under Federal awards. Upon completion of the pre-award risk assessment, the Grants Officer will make a responsibility determination concerning whether the applicant is qualified to receive the subject award and, if so, whether appropriate specific award conditions that correspond to the degree of risk posed by the applicant should be applied to an award.

4. Anticipated Announcement and Award Date

Review of applications, selection of successful applicants, and award processing is expected to be completed by September 2025. The earliest start date for awards under this NOFO is expected to be October 2025.

5. Additional Information

a. Medical Services Related to Safety/Hazards. NIST shall perform health hazard evaluations associated with the recipient's employees contractors, and associates' work at a NIST-owned or operated site that involves the potential exposure to a health hazard, to make the determination of the need for medical surveillance. Award recipients are responsible for providing the medical services and tests required for any applicable medical surveillance program.

b. Notification to Unsuccessful Applicants. Unsuccessful applicants will be notified by e-mail and will have the opportunity to receive a debriefing after the opportunity is officially closed. Applicants must request within 10 business days of the email notification to receive a debrief from the program office. The program office will then work with the unsuccessful applicant in arranging a date and time of the debrief.

c. Retention of Unsuccessful Applications. Unsuccessful applications will be retained in accordance with the General Record Schedule 1.2/021.

VI. Federal Award Administration Information

1. **Federal Award Notices.** Successful applicants will receive an award package from the NIST Grants Officer.

2. **Administrative and National Policy Requirements**

   a. **Uniform Administrative Requirements, Cost Principles and Audit Requirements.** Through 2 C.F.R. § 1327.101, the Department of Commerce adopted Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 C.F.R. Part 200, which apply to awards in this program.

   b. **Department of Commerce Financial Assistance General Terms and Conditions.** The Department of Commerce will apply to each award in this program, the Financial Assistance General Terms and Conditions in effect on the date of award. The current version, dated October 1, 2024, is accessible at Department of Commerce Financial Assistance General Terms and Conditions. Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules, and Regulations, if you need more information.

   c. **Pre-Award Notification Requirements.** The Department of Commerce will apply the Pre-Award Notification Requirements for Grants and Cooperative Agreements dated December 30, 2014 (79 FR 78390). Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Grant Rules, and Regulations, for more information.

   d. **Funding Availability and Limitation of Liability.** Funding for the program listed in this NOFO is contingent upon the availability of appropriations. NIST or the Department of Commerce will not be responsible for application preparation costs, including but not limited to if this program fails to receive funding or is cancelled because of agency priorities. Publication of this NOFO does not oblige NIST or the Department of Commerce to award any specific project or to obligate any available funds.

      NIST issues this NOFO subject to the appropriations made available under the current continuing resolution funding the Department of Commerce: The Full-Year Continuing Appropriations and Extensions Act, 2025, Public Law 119-4 (March 15, 2025). NIST anticipates making awards for the program listed in this NOFO, provided that funding is continued beyond September 30, 2025, the expiration of the current continuing resolution.

e. Collaborations with NIST Employees.
All applications should include a description of any work proposed to be performed by an entity other than the applicant, and the cost of such work should ordinarily be included in the budget. If an applicant proposes collaboration with NIST, the statement of work should include a statement of this intention, a description of the collaboration, and prominently identify the NIST employee(s) involved, if known. Any collaboration by a NIST employee must be approved by appropriate NIST management and is at the sole discretion of NIST. Prior to beginning the merit review process, NIST will verify the approval of the proposed collaboration. Any unapproved collaboration will be stricken from the application prior to the merit review. Any collaboration with an identified NIST employee that is approved by appropriate NIST management will not make an application more or less favorable in the competitive process. NIST's costs should not be included in the application.

f. Use of Federal Government-Owned Intellectual Property. If the applicant anticipates using any Federal Government-owned intellectual property, in the custody of NIST or another Federal agency, to carry out the work proposed, the applicant should clearly identify such intellectual property in the proposal. This information will be used to ensure that no Federal employee involved in the development of the intellectual property will participate in the review process for that competition. In addition, if the applicant intends to use the Federal Government-owned intellectual property, the applicant must comply with all statutes and regulations governing the licensing of Federal government patents and inventions, described in 35 U.S.C. §§ 200-212, 37 C.F.R. Part 401, 2 C.F.R. §200.315, and in Section C.03 of the Department of Commerce Financial Assistance General Terms and Conditions, dated October 1. 2024. Questions about these requirements may be directed to the Chief Counsel for NIST, (301) 975-2803, nistcounsel@nist.gov.

Any use of Federal Government-owned intellectual property by a recipient of an award under this announcement is at the sole discretion of the Federal Government and will need to be negotiated on a case-by-case basis by the recipient and the Federal agency having custody of the intellectual property if a project is deemed meritorious. The applicant should indicate within the statement of work whether it already has a license to use such intellectual property or whether it intends to seek a license from the applicable Federal agency.

If any inventions made in whole or in part by a NIST employee arise in the course of an award made pursuant to this NOFO, the United States Government may retain its ownership rights in any such invention. Licensing or other disposition of the Federal Government's rights in such

inventions will be determined solely by the Federal Government, through NIST as custodian of such inventions, and include the possibility of the Federal Government putting the intellectual property into the public domain.

3. **Reporting**

   a. **Reporting Requirements.** The following reporting requirements described in Sections A.01, Reporting Requirements, of the Department of Commerce Financial Assistance General Terms and Conditions dated October 1, 2024, apply to awards in this program:

      (1) Financial Reports. Each award recipient will be required to submit an SF-425, Federal Financial Report on a semi-annual basis for the periods ending March 31 and September 30 of each year. Reports will be due within 30 days after the end of the reporting period. A final financial report is due within 120 days after the end of the project period.

      (2) Performance (Technical) Reports. Each award recipient will be required to submit a technical progress report on a semi-annual basis for the periods ending March 31 and September 30 of each year. Reports will be due within 30 days after the end of the reporting period. Technical progress reports shall contain information as prescribed in 2 C.F.R. § 200.329 and Department of Commerce Financial Assistance General Terms and Conditions dated October 1, 2024, Section A.01. A final technical progress report is due within 120 days after the end of the project period. In addition to the information prescribed in 2 C.F.R. § 200.329, the final performance report shall include:

      - An assessment of efforts made by the regional alliance or partnership to carry out the project.
      - The metrics used by the regional alliance or partnership to measure the success of the efforts of the regional alliance or partnership under the cooperative agreement.

      Additionally, NIST required award recipients to attend **two** quarterly meetings following the submission of their performance technical reports. More information regarding meeting time and dates will be provided by the NIST-NICE Program Office.

      (3) Patent and Property Reports. From time to time, and in accordance with the Uniform Administrative Requirements and other terms and conditions governing the award, the recipient may need to submit property and patent reports.

(4) Recipient Integrity and Performance Matters. In accordance with section 872 of Public Law 110-417 (as amended; see 41 U.S.C. 2313), if the total value of a recipient's currently active grants, cooperative agreements, and procurement contracts from all Federal awarding agencies exceeds $10,000,000 for any period of time during the period of performance of an award made under this NOFO, then the recipient shall be subject to the requirements specified in Appendix XII to 2 C.F.R. Part 200, for maintaining the currency of information reported to SAM that is made available in SAM.gov about certain civil, criminal, or administrative proceedings involving the recipient.

b. Audit Requirements. In accordance with 15 U.S.C. § 7443(f)(5), all recipients (regardless of organizational type) of a RAMPS award issued pursuant to this NOFO are subject to the audit requirements under 2 C.F.R. part 200, Subpart F. Applicants are reminded that NIST, the Department of Commerce Office of Inspector General, or another authorized Federal agency may conduct an audit of an award at any time.

c. Federal Funding Accountability and Transparency Act of 2006. In accordance with 2 C.F.R. Part 170, all recipients of a Federal award made on or after October 1, 2010, are required to comply with reporting requirements under the Federal Funding Accountability and Transparency Act of 2006 (Public Law No. 109-282). In general, all recipients are responsible for reporting sub-awards of $30,000 or more. In addition, recipients that meet certain criteria are responsible for reporting executive compensation. Applicants must ensure they have the necessary processes and systems in place to comply with the reporting requirements should they receive funding. Also see the Federal Register notice published September 14, 2010, at 75 FR 55663.

VII. Federal Awarding Agency Contacts

Questions should be directed to the following:

Subject Area	Point of Contact
Programmatic and Technical Questions	Susana Barraza Phone: 240-457-2638 E-mail: Susana.Barraza@nist.gov with '2025-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 E-mail: nuria.martinez@nist.gov

Subject Area	Point of Contact
	Email: nofo@nist.gov with '2025-NIST-RAMPS-01' in subject line E-mail: nofo@nist.gov

VIII. Other Information

1. **Personal and Business Information**
   The applicant acknowledges and understands that information and data contained in applications for financial assistance, as well as information and data contained in financial, performance and other reports submitted by applicants, may be used by the Department of Commerce in conducting reviews and evaluations of its financial assistance programs. For this purpose, applicant information and data may be accessed, reviewed, and evaluated by Department of Commerce employees, other Federal employees, and also by Federal agents and contractors, and/or by non-Federal personnel, all of whom enter into appropriate conflict of interest and confidentiality agreements covering the use of such information. As may be provided in the terms and conditions of a specific financial assistance award, applicants are expected to support program reviews and evaluations by submitting required financial and performance information and data in an accurate and timely manner, and by cooperating with Department of Commerce and external program evaluators. In accordance with 2 C.F.R. § 200.303(e), applicants are reminded that they must take reasonable measures to safeguard protected personally identifiable information and other confidential or sensitive personal or business information created or obtained in connection with a Department of Commerce financial assistance award.

   In addition, Department of Commerce regulations implementing the Freedom of Information Act (FOIA), 5 U.S.C. Sec. 552, are found at 15 C.F.R. Part 4, Public Information. These regulations set forth rules for the Department regarding making requested materials, information, and records publicly available under the FOIA. Applications submitted in response to this Federal Funding Opportunity may be subject to requests for release under the Act. If an application contains information or data that the applicant deems to be confidential commercial information that should be exempt from disclosure under FOIA, that information should be identified, bracketed, and marked as Privileged, Confidential, Commercial or Financial Information. In accordance with 15 CFR § 4.9, the Department of Commerce will protect from disclosure confidential business information contained in financial assistance applications and other documentation provided by applicants to the extent permitted by law.

2. **Public Website, Frequently Asked Questions (FAQs):**

NIST' NICE Program Office has a public website (https://www.nist.gov/nice) that provides a "Frequently Asked Questions" page and other information pertaining to this Funding Opportunity.

NIST has a public website, http://www.nist.gov/nice, that provides information pertaining to this Funding Opportunity[2]. Any amendments to this NOFO will be announced through Grants.gov.

3. Applicants must submit all questions pertaining to this funding opportunity in writing to nice@nist.gov with 2025-NIST-RAMPS-01 in the subject line.

4. **Webinar Information Session:**

NIST's NICE Program Office will host a webinar information session for applicants that are interested in learning about this funding opportunity. This webinar will provide general information regarding 2025-NIST-RAMPS-01 and offer general guidance on preparing proposals. Please reference https://www.nist.gov/nice for the most up to date information, including scheduling details about the webinar. Proprietary technical questions about specific proposal ideas will not be permitted, and NIST will not critique or provide feedback on any proposal ideas during the webinar or at any time before the deadline for all applications. However, questions about the funding opportunity, eligibility requirements, evaluation and award criteria, selection process, and the general characteristics of a competitive application will be addressed at the webinar and by e-mail to nice@nist.gov. There is no cost to attend the webinar, but participants must register in advance. Participation in the webinar is not required and will not be considered in the review and selection process.

[2] Refer to Section VII. of this NOFO, Federal Awarding Agency Contacts, Programmatic and Technical Questions if more information is needed.

Nashville Cybersecurity Workforce Accelerator: A Regional Partnership

to Build a Resilient and Inclusive Cyber Talent Pipeline

Lead Applicant: Metropolitan Government of Nashville and Davidson County

Primary Training Partner: LocalTek

Grant Program: NIST NICE RAMPS (2025-NIST-NICE-01)

I. Executive Summary

Led by the Metropolitan Government of Nashville & Davidson County (Metro) and powered by LocalTek's proven cybersecurity training platform, the Nashville Cybersecurity Workforce Accelerator (NCWA) will expand and diversify the region's cybersecurity talent pipeline by coordinating a multi-sector alignment of education, training, and employment pathways with local workforce demands. This initiative responds to workforce shortages in cybersecurity roles across government and private sectors to increase the number of qualified job candidates from historically underrepresented groups, including residents of low-income neighborhoods, veterans, and adult learners. Other partners include Comcast (corporate partner, infrastructure operator), Nashville State Community College (articulation of credits, academic advising), Blacks in Technology – Nashville Chapter (participant recruitment and outreach), and Vanderbilt University, our university partner and an institution that is designated as a national center of academic excellence in cybersecurity. Other partners are listed and described in later sections of this proposal.

Nashville has experienced unprecedented growth in its tech sector and the demand for skilled cybersecurity professionals has surged. NCWA aims to bridge this talent gap by developing a comprehensive and sustainable cybersecurity workforce pipeline by leveraging the strengths of strategic partners to provide training, pre-apprenticeships, apprenticeships, and job placement services, aligning with the NICE Workforce Framework for Cybersecurity. Our program objectives are aligned to help deliver entry-level to mid-level cybersecurity training pathways to 1) expand hands-on learning opportunities, 2) support employer partners with skills-based hiring tools and candidate matchmaking, and 3) track and report workforce outcomes, including credentials earned, job placements, and wage progression. LocalTek will also support recruitment and performance management processes related to natural progressions through pre-apprenticeship and apprenticeship paths.

A. Target participants

Target participants include 1) veterans, adult learners, and recent graduates from Metro Nashville Public Schools, and 2) jobseekers from communities underrepresented in tech and IT employment. 3) Metro and other public or private sector employees seeking cybersecurity upskilling,

B. Training

Led by LocalTek, the training component will include 1) 12–week cybersecurity bootcamps aligned with NICE roles, 2) embedded career readiness modules, 3) industry-recognized certifications (CompTIA Security+, Network+, etc.), and 4) employer-led capstone projects and mentoring that transform the learning process from purely classroom-based learning to hands-on, business-ready application. In addition to embedded career readiness modules, the training program will incorporate panel-based readiness assessment and support. This is comprised of representatives from academia, community-service organizations, and hiring organizations working together within a participant support structure. This process is intended for application with multiple employers, beginning with Comcast, one of Metro's core partners in the area of digital learning. Once piloted, this process will provide the missing link between educational institutions, employers, and other key stakeholders.

C. Outreach

Our proposed outreach model will promote exploration of cybersecurity careers by leveraging opportunities to engage the community through nonprofit and other community-serving organizations through live, interactive information and feedback sessions. At regional and national levels, we will utilize conference participation and submissions to outlets with distributed publications to disseminate our program discoveries.

D. Anticipated Outputs (2-Year Period)

- 100+ participants enrolled across two cohorts
- 85% completion rate of training programs
- 65% apprenticeship placement rate within six months of program completion
- 15+ employer partners engaged
- 100% of program participants from populations underrepresented in tech

II. Project Narrative

A. Nashville's Tech Growth and Cybersecurity Demand

Nashville's tech industry has witnessed remarkable expansion:

- **Tech Job Growth**: Between 2017 and 2022, Nashville's tech workforce grew by 36%, adding over 9,000 jobs, the highest percentage increase among U.S. markets during that period.
- **Economic Impact**: The tech sector contributes approximately $7.5 billion annually to the local economy.
- **Cybersecurity Demand**: The city's cybersecurity sector is booming, with a projected 32% increase in job openings by 2024. Key employers like Amazon and Oracle are actively seeking professionals skilled in network security, cloud security, and risk management.

Despite this growth, there's a significant talent shortage:

- **Supply vs. Demand**: The supply of cybersecurity workers in Nashville is insufficient to meet employer demand, with a supply/demand ratio below the national average.
- **Educational Gap**: From 2017 to 2021, Nashville created 9,950 tech jobs but produced only 5,270 tech graduates, highlighting a substantial skills gap of more than 4,600 workers.

B. Program Objectives

The Nashville Cybersecurity Workforce Accelerator seeks to:

1. **Develop Cybersecurity Training Programs**: Create and deliver training aligned with the NICE Workforce Framework, focusing on roles such as Cyber Defense Analyst and Security Operations Center Technician.
2. **Facilitate Job Placement Support**: Implement work-based learning opportunities, including internships and apprenticeships, to bridge the gap between education and employment.
3. **Engage Employers in Workforce Development**: Collaborate with local employers, especially in critical infrastructure sectors, to identify skill gaps and tailor training programs accordingly.

4. **Build Multistakeholder Partnerships**: Establish alliances that include educational institutions, nonprofit training organizations, and local employers or critical infrastructure operators.

C. Program Model

LocalTek, a seasoned training provider, will lead the delivery of a 12–week cybersecurity bootcamp, offering:

- **Certifications**: Training for industry-recognized certifications such as CompTIA Security+, Network+, and Linux+.
- **Career Readiness**: Modules on resume writing, interview preparation, and professional networking.
- **Hands-On Experience**: Simulated lab environments and real-world projects.
- **Pre-apprenticeship and Apprenticeship Opportunities**:
  - **Metro ITS**: As the city's internal technology services department, Metro ITS will host pre-apprenticeships, providing participants with experience in securing public infrastructure.
  - **Comcast**: As a major telecommunications provider, Comcast will offer apprenticeships focusing on network operations and cybersecurity.
  - Program data taken from the first round of pre-apprenticeships and apprenticeships will be used to inform future rounds, wherein we will recruit additional employers

D. Training Plan

Pre-work

I. Identify job titles eligible with federal government

II. Identify organization’s available positions

III. Identify organization’s financial resources

IV. Match selected job titles with job titles in the DOL database

V. Identify benchmarks and pay scales

Step 1: Recruitment & Outreach (Weeks 1-4)

Led by: LocalTek, with support from employer’s HR, local community-based organizations:

- Chamber of Commerce for employer roundtables
- **W**orkforce development organizations and organizations that offer job assistance to residents
- The state workforce board
- Community colleges
- Metro Nashville Public school to help reach prospective and recent graduates
- **O**ther nonprofit partners with relevant reach
- **Focus on reaching:**
    - Young adults (18–26)
    - Career changers
    - Veterans
    - Historically excluded groups in tech
- **Methods:**
    - Info sessions at libraries, community centers, and TechTies locations
    - Social media and job board announcements
    - Referrals from community partners

Step 2: Screening & Selection (Weeks 4–5)

- **Eligibility:** GED/high school diploma minimum, interest in IT, and willingness to commit
- **Assessment Tools:**
    - Digital skills baseline (typing, email, basic computer use)
    - Aptitude & motivation interviews
    - Optional tech screening for advanced placement

Step 3: Training Delivery (Weeks 6–18)

- **Training Partner:** LocalTek
- **Duration:** 12 weeks
- **Format:** Hybrid (in-person + virtual), with optional employer guest lectures

Curriculum includes:

- IT Fundamentals (CompTIA ITF+)
- Cybersecurity Basics (CompTIA Security+ prep)
- Intro to Networking (CompTIA Network+ fundamentals)
- **Career & Soft Skills:**
    - Resume and LinkedIn coaching
    - Interview practice
    - Prospective employer work culture & professionalism
- **Capstone Project:** Simulated scenario or security assessment case

Step 4: Wraparound Support

- **Nashville Digital Navigators assist in the process with:**
    - Laptop/device loans
    - Affordable broadband access
    - Tech troubleshooting
- **Support services:**
    - Transportation coordination
    - Childcare referrals
    - Program-based case management

Step 5: Work-Based Learning (Weeks 18–20)

- Job shadowing with employer's teams (e.g. cybersecurity, network ops, service desk)
- Mentorship from employer's staff
- Feedback loop: participants reflect on interests, strengths, and fit

Step 6: Transition to Apprenticeship (Week 21)

- **Selection Process:**
    - Participants apply for apprenticeship

- Priority consideration for pre-apprenticeship graduates
- Rolling or cohort basis

Step 7: Onboarding into Apprenticeship

- Apprentices are hired
- On-the-job training guided by LocalTek curriculum and employer-designated supervisors
- Eligible to earn industry certifications (e.g., Security+, Network+, or Azure Fundamentals)
- Structured advancement into full-time roles

E. Performance Metrics

- Recruitment numbers
- Completion rate (%)
- Certification attainment
- Employer commitments
- Pre-apprenticeship engagement/attrition
- Demographic equity of participants

F. Target Populations

The program will prioritize:

- **Underrepresented Communities**: Including residents of low-income neighborhoods, veterans, and adult learners.
- **Public Sector Employees**: Metro and public sector employees seeking cybersecurity upskilling.
- **Recent Graduates**: Alumni from Metro Nashville Public Schools and local community colleges.

G. Strategic Partnerships

Key partners include:

- **Metro Government**: Lead applicant, program coordinator
- **LocalTek**: Primary training provider
- **Comcast**: Infrastructure partner offering apprenticeships
- **Nashville State Community College**: Academic partner for credit articulation

- **Greater Nashville Technology Council**: Employer engagement and participant placement support
- **Global Action Platform:** Regional partner to support recruitment for regional collaboration efforts
- **Blacks in Technology-Nashville Chapter**: Participant recruitment and community engagement
- **The Urban league of Middle Tennessee**: Participant recruitment and support.

Key Personnel

Resumes are attached with this submission.

- Pearl Amanfu – Program Director, Digital Learning and Access: Responsible for aligning internal and community partnerships around the Nashville Cybersecurity Accelerator.
- Evan Davis – Grant Writer: Responsible for ensuring strategic alignment between the goals of Mayor Freddie O'Connell's office and the Nashville Cybersecurity Accelerator
- Holly Rachel – Training Lead: Responsible for curriculum design and training coordination and oversight
- Sally Stryker – Project Manager: Responsible for coordinating scope and logistics for the Nashville Cybersecurity Accelerator

H. Outreach and Dissemination of Information

Cross-sector Collaboration

Metro Nashville and Davidson County benefits from a strong appreciation for cross-sector collaboration, particularly around education. This initiative connects goals of collaboration across multiple areas of support to ensure that secondary education, post-secondary education, credentialing, workforce development, nonprofit community support, and employer engagement efforts align to create clear and direct paths for learners and job seekers.

Cross-sector information exchange and collaborative planning are foundational to successful execution of long-term, sustainable initiatives. Strategies and programs that Metro Nashville has designed over the past decade such as Mayor O'Connell's Choose How You Move, Livable Nashville, and

Connected Nashville have brought together residents, nonprofits, government agencies, and private corporations for conversations around shared goals. Those communications channels are alive and well. Metro has successfully utilized public listening sessions, advisory committees, and collaboration with other community-serving organizations to develop community-focused solutions.

We aim to use these active channels to engage the community and disseminate program information in a continuous communication loop that facilitates continuous program refinement and action research. Our approach to employ action research ensures the generation of reflective knowledge versus data collection from a neutral, detached perspective. Our program will employ pre-session, post-session, and periodic surveys for trainees, employer surveys and interviews, and nonprofit and program partner focus groups. Our aim is to build a loop process that enables interactive and reflective growth approaches and collect data that can be valuable not only for our own processes but for local and regional collaborative efforts.

Academic Publications

- Submit findings to peer-reviewed journals relevant to the field (e.g., *Journal of Applied Research*, *Science & Technology Review*).
    - Online Journal for Workforce Education and Development – *Covers workforce education, career training, and technical education*.
    - Journal of Workforce Education & Research – *A new peer-reviewed journal (Volume 1 published in March 2025) that publishes research on workforce education, talent development, and workplace learning.*
    - Career Development International – *Explores career strategies, workforce trends, and organizational career policies. We can publish in categories of Career Interventions, Government Policy and Practices, HR Planning and Recruitment, and Work and Occupational Contexts*

Industry & Professional Publications

- Publish articles in trade magazines and professional association newsletters (e.g., *Industry Insight*, *Engineering Today*).

Digital & Media Outreach

- Develop a project website featuring reports, visual summaries, and downloadable resources.
- Create a social media campaign (LinkedIn, X, YouTube) with infographics, key takeaways, and short video explainers.
- Issue press releases to news outlets and professional media organizations to raise awareness.
- Consider publishing an Op-Ed in The Tennessean similar to pieces that we have published on other topics in the past.

Conferences, Events & Public Engagement

- Present findings at national and international conferences, symposiums, and workshops.
    - ApprenticeshipTN Conference – A statewide event discussing workforce development strategies, including tech apprenticeships and public-private partnerships. *These are typically held in November, so we would aim for November 2026.*
- Host webinars and panel discussions with key experts and stakeholders to facilitate dialogue.
- Organize community outreach events, town halls, or lectures tailored to non-expert audiences.

Collaboration & Stakeholder Engagement

- Partner with universities, nonprofits, and government agencies to integrate results into ongoing research or educational programs. *We have reached out to Vanderbilt Peabody Learning Design and Technology.*
- Provide policy briefs summarizing key findings for government decision-makers.
- Share insights with corporate partners for industry innovation and application.

Evaluation & Impact Measurement

To assess the effectiveness of the Dissemination Plan:

- Track citations and references in academic literature.

- Monitor engagement metrics from online platforms and social media.
- Collect feedback from stakeholders via surveys or discussion forums.

I. Project Impacts and Evaluation

Anticipated Impacts of the Proposed Project

This initiative will significantly expand Nashville's cybersecurity talent pipeline by creating a locally anchored, inclusive, and scalable workforce development model. By integrating Metro Government (including Metro ITS as both an employer and infrastructure owner/operator), LocalTek as the training provider, and a network of regional partners (Comcast, Community Foundation of Middle Tennessee, Metro Action Commission, Tech Goes Home, and the Nashville Public Library), the project aims to:

- Increase the number of entry-level and mid-level cybersecurity professionals prepared to meet current and emerging workforce demands in both public and private sectors.
- Expand access to cybersecurity careers for historically underrepresented communities, with a focus on residents served by Metro's digital access and skills programs through nonprofit partner-centered outreach.
- Strengthen employers' capacities to hire and retain skilled cybersecurity workers through paid apprenticeships and on-the-job training.
- Develop a sustainable, data-informed training and employment ecosystem that aligns with Tennessee's and the Southeast region's cybersecurity infrastructure needs.

Workforce Data Collection and Analysis

The project will collect and synthesize data from the following sources:

- CyberSeek and CompTIA for labor market insights and occupation mapping
- JobsEQ and Tennessee Department of Labor for real-time job posting analytics and supply-demand matching
- Metro HR and partner employer data on job openings, hiring rates, skills gaps, and turnover
- Participant surveys and follow-ups to track program outcomes, satisfaction, and barriers.

This data will be used to conduct a local cybersecurity workforce gap analysis that maps current demand to training and hiring capacity. Findings will be shared with the U.S. Department of Labor to inform national cybersecurity workforce strategies and support CyberSeek's enhancement.

Methodology for Identifying and Evaluating Project Outcomes

Evaluation will be conducted in partnership with Metro Government's data insights team and LocalTek's training analytics systems, which will track both short-term outputs and long-term outcomes. Key metrics include:

- **Participant-level outcomes:**
    - Strong enrollment, completion, and certification rates in cybersecurity training pathways
        - Strong program retention and completion, showing that curriculum, support services, and training environments are effective and accessible
    - High apprenticeship placement and success, leading to higher job placement rates
    - Effective employer engagement
        - Strong industry buy-in and access to expanded placement opportunities for participants
        - Potential for scalable job pipelines in high-demand sectors
    - Enrollment, completion, and certification rates in cybersecurity training pathways
    - Demographic data to assess parity of opportunity in program reach and impact
        - Demonstration of compliance with employers' goals in diversifying the workforce
    - Early momentum toward systemic change
        - Creating pathways to economic mobility for individuals who are often excluded from the tech workforce

        - Closing talent gaps in local industries by upskilling residents already in the region

- **System-level outcomes:**
    - Meaningful workforce outcomes
        - Successful connections between training and real job opportunities
        - Effective leveraging of partnerships
        - Increase in local employers' cybersecurity hiring from local talent pools
    - Expanded numbers of apprenticeship, pre-apprenticeship or internship programs
    - Employer satisfaction for placed pre-apprenticeships and program engagement
        - Enhanced alignment between training curricula and employer-identified skill needs

J. Dissemination of Project Learning

Nashville's approach to cybersecurity workforce development will be shared through:

- Quarterly convenings hosted by Metro ITS and the Mayor's Office to update stakeholders and local employers
- Contributions to **CyberSeek** and other national repositories with real-time, localized supply-demand data on cybersecurity talent
- Open publication of anonymized outcome data, curriculum models, and employer engagement strategies via a public dashboard hosted on the city's open data portal
- Briefings at regional cybersecurity and workforce summits, such as those hosted by Tennessee's Department of Labor & Workforce Development and state higher ed institutions

***

PEARL **AMANFU**

https://www.linkedin.com/in/pearlamanfu/

Human and Organizational Development practitioner specializing in Leadership and Organizational Effectiveness, 15 years of researching, designing, funding, developing, and executing inter-organization and community programming. Expert listener, skilled at designing people-focused initiatives that center the human experience. Project Management professional with demonstrated success in both projectized and matrix organizations. Key strengths stakeholder engagement, training, and applying systems thinking to help transform organizations, their programs, and the services they deliver to their customers and the community.

EXPERIENCE

AUGUST 2022 TO PRESENT

PROGRAM DIRECTOR, DIGITAL LEARNING AND ACCESS, METROPOLITAN GOVERNMENT OF NASHVILLE & DAVIDSON COUNTY

Develop and direct Metro's digital opportunity programs to give all residents the ability to access the benefits of technology. Use department, city, state, and federal data along with community-engaged research to ensure that all of the technology services that Metro Government provides are designed with resident needs at the forefront.

Key accomplishments since August 2022:

- **Strategic Management:** Developed the digital opportunity strategy for Metro Information Technology Services and developed Metro's first digital opportunity strategic roadmap.
- **Fundraising:** Raised a $2,235,000 for digital opportunity programs through successful grant proposals.
- **Community-centered, Data-driven Program Planning:** Developed Metro's first Community Asset Inventory, collecting and analyzing data to develop an Asset Based Community Development approach to support collaboration with local nonprofits.
- **Program Development:** Employed a systems approach to develop the first-ever digital opportunity division for the Metropolitan Government of Nashville and Davidson county, supporting workforce development and technology training efforts for the Metropolitan Government of Nashville and Davidson County.
- Developed the first countywide digital opportunity program for Davidson County.
- **Leadership and Collaboration:** Selected to participate on the advisory board for the State of Tennessee's digital opportunity plan development.
- **Supervisory Experience:** Leading a team of four contractors to execute program recruitment, program management, community engagement, and grant management while also serving as the program lead for *TechTies: Connected Services for the Community*, coordinating the work of four internal contractors, three external vendor organizations, two grant staff in a partner department, and 22 Digital Navigators.
- **Leadership Excellence:** Nominated for 2022 Advocate of the Year (finalist) by Nashville Technology Council. Nominated for Community Leader of the Year by Nashville Technology Council.

OCTOBER 2016 TO AUGUST 2022

EXECUTIVE PROJECT MANAGER, METROPOLITAN GOVERNMENT OF NASHVILLE & DAVIDSON COUNTY - INFORMATION TECHNOLOGY SERVICES

Worked with the Chief Information Officer to build Metro's digital opportunity division from the ground up. Developed initiatives and led projects to support Metro Government goals and business activities.

Key accomplishments:

- **Product Launch:** Served as one of two project managers for the implementation of Metro's first enterprise tool for resident alerting during emergencies, working with our customers (Nashville Fire Department, Metro Nashville Police Department, and Office of Emergency Management) to ensure the final delivered product met customer expectations as well as end-user privacy, safety, and usability needs.
- **Performance Management:** Worked with the then-Chief Data Officer to co-develop a comprehensive business metrics program for the Information Technology Services department.
- **Business Development, Research, Collaboration, and Community Engagement:** Successfully raised funds for and led the execution of the first comprehensive digital opportunity study in Davidson County. This mixed method study included a quantitative community survey and qualitative nonprofit interviews and was conducted in partnership with Vanderbilt Peabody College.
- **Program Development:** Aided in the synthesis and publication of Metro's first smart city plan, *Connected Nashville*, a multi-year initiative aimed at developing projects and programs to use technology for public benefit.
- **Supervisory Experience:** Oversaw the work of one staff member, training this team member to become the application administrator for Metro's enterprise emergency alert and notification system.
- **Leadership Excellence:** Nominated for 2021 Initiative of the Year (finalist) by Nashville Technology Council.

2009 TO 2016

SENIOR PROJECT MANAGER, PRECISION DYNAMICS INTERNATIONAL (PDI)

Served as lead project manager and primary customer contact for large-scale training and business initiatives for Nissan North America. Key contributor to transformational customer service programs for Nissan and Infiniti. Product owner for every major product launch between 2009 and 2016 to support Infiniti USA's customer service training program including a nationally implemented tool to transform dealership service quality.

Key accomplishments:

- **Program Development and Program Management:** Co-designed, launched, and managed a new nationwide customer service training program for Infiniti USA, Nissan's luxury brand.
- **Process Improvement:** Led the development of a new quality control process and program for Nissan USA. Provided project management for the program implementation.
- **Product Ownership and Operations Management:** Directed the design and development of a custom tool and mobile app for Nissan quality control inspections. Oversaw the first year of operations prior to final hand-off to ensure a high-quality user experience and to serve as the connecting point between dealership inspectors, internal stakeholders, nationwide dealer management, Nissan North America's corporate leadership, and PDI's support team.
- **Project Management:** Led the project management process to support the instructional design, product development for the training tool, and nationwide launch of a sales and service training program for the brand launch of the Nissan LEAF electric vehicle.

- **PMO Leadership, Project Management, and Event Management:** Led the development of PDI's PMO, developing project management processes, training incoming project managers, and overseeing project assignments, successes, and risk management. Served as lead project and event manager for 41 vehicle launch training and consumer events.
- **Supervisory Experience:** Managed a team of 5 regionally assigned quality control inspectors. Managed contract and event staff for 41 vehicle launch events with 16 ongoing contractors, two instructional designers, five Infiniti trainer staff, and a rotating group of 26 event staff (vehicle specialists, vehicle coordinators, and event coordinators).
- **Executive Coaching:** Provided presentation coaching for executives at three national sales conferences.

2008 TO 2009

PROJECT MANAGER, TENNESSEE CONFERENCE ON SOCIAL WELFARE

Supported the organization in developing grant proposals, mapping short- and long-term goals and leading the execution of grant-funded initiatives. Developed programs to support people in caring occupations.

Key accomplishments

- **Grants Management and Program Development:** Supported TCSW in developing a proposal and becoming a grant recipient from Baptist Healing Trust and helped successfully launch a new training program for caregivers to help address compassion fatigue and build support within the social and community service network.
- **Event Management:** Successfully executed two citywide conferences for local social workers and caregivers.

CERTIFICATIONS.

PROJECT MANAGEMENT PROFESSIONAL (PMP)
CREDENTIAL ID 2701940

EDUCATION

VANDERBILT UNIVERSITY
MASTER'S IN COMMUNITY DEVELOPMENT AND ACTION (M.Ed.)

Department of Human and Organizational Development, Vanderbilt Peabody College | This program combines theory, community engaged research, and practice to equip learners to become change agents in their organizations and communities.

VANDERBILT UNIVERSITY
BACHELOR OF SCIENCE – HUMAN AND ORGANIZATIONAL DEVELOPMENT

Department of Human and Organizational Development, Vanderbilt Peabody College | Concentration in Leadership and Organizational Effectiveness

SKILLS

Knowledge of all major project management applications • Grant writing • Experienced public presenter • Excellent oral and written communication skills • Copywriting and editing • Systems thinking and systems mapping • Corporate presentation coaching • Solving human-centered problems within growing organizations.

Personnel

Item Description	Unit Cost	Number of Units	Unit	Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
EAC Human Resources Analyst 2 - Project documentation and program tracking	$34.00	104	hour	$3,536.00	$2,357.33	$1,178.67	104 working weeks, 1 hour per week	
Grant manager	$32.00	104	hour	$3,328.00	$2,218.67	$1,109.33	104 working weeks, 1 hour per week	
Program supervisor	$69.00	624	hour	$43,056.00	$28,704.00	$14,352.00	104 working weeks, 6 hours per week	
EAC Finance Manager	$68.00	52	hour	$3,536.00	$2,357.33	$1,178.67	104 working weeks, .5 hours per week	
Project Manager	$79.00	720	hour	$56,880.00	$37,920.00	$18,960.00	18 working weeks, 4 hours per week	
Total Personnel				**$110,336.00**	**$73,557.33**	**$36,778.67**		

Fringe Benefits

Item Description	Unit Cost	Number of Units	Unit	Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
EAC Human Resources Analyst 2 - Project documentation and program tracking	1.00	1.00	flat	$1,290.64	$860.43	$430.21	36.5% used by OMB during budget process	
Grant manager	1.00	1.00	flat	$1,214.72	$809.81	$404.91		
Program supervisor	1.00	1.00	flat	$15,715.44	$10,476.96	$5,238.48		
EAC Finance Manager	1.00	1.00	flat	$1,290.64	$860.43	$430.21		
Project Manager	1.00	1.00	flat	$20,761.20	$13,840.80	$6,920.40		
Total Fringe Benefits				**$40,272.64**	**$26,848.43**	**$13,424.21**		

Travel

Item Description	Unit Cost	Number of Units	Unit	Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
Airfare (BNA to DEN)	$450.00	2	each	$900.00	$600.00	$300.00	Costs range from to $245 to $617 as of June 5, 2025	
Lodging	$215.00	2	night	$430.00	$286.67	$143.33	2025 CONUS rate for Denver	
Meals	$92.00	6	day	$552.00	$368.00	$184.00	2025 CONUS rate for Denver	
Conference fees	$340.00	2	each	$680.00	$453.33	$226.67	Government early bird rate, 2025	
Total Travel				**$2,562.00**	**$1,708.00**	**$854.00**		

Equipment

Item Description	Unit Cost	Number of Units		Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
Laptops and peripherals for trainers (Metro rate)	$1,441.00	5	trainers	$7,205.00	$4,803.33	$2,401.67	Laptop, a HUB monitor, a bag and wired keyboard/mouse combo	
Total Equipment				**$7,205.00**	**$4,803.33**	**$2,401.67**		

Supplies

Item Description	Unit Cost	Number of Units	Unit	Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
Printed materials for participants	$10.00	150	trainee	$1,500.00	$1,000.00	$500.00		
Learning Management System License	$12,500.00	1	flat	$12,500.00	$8,333.33	$4,166.67		
JobsEQ subscription - 4 licenses	$17,000.00	1	flat	$17,000.00	$11,333.33	$5,666.67	CPI rate dictates renewal increase; it will fall between $16,428.50 and $17,226. Service Region + 75 Mile Radius Around + State	
Total Supplies				**$31,000.00**	**$20,666.67**	**$10,333.33**		

Contractual

Item Description	Unit Cost	Number of Units		Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
LocalTek Technology Education: Curriculum Development	$150.00	80	hours per 4 courses (# courses x hours	$12,000.00	$8,000.00	$4,000.00		
LocalTek Technology Education: Program Planning	$125.00	320	hours per 4 courses (# courses x hours	$40,000.00	$26,666.67	$13,333.33		
LocalTek Technology Education: Community assessment and engagement for training programs	$100.00	40	hours per 4 courses (# courses x hours hrs per course)	$4,000.00	$2,666.67	$1,333.33		
LocalTek Technology Education: Training	$600.00	20	hours per 4 courses (# courses x hours	$12,000.00	$8,000.00	$4,000.00		
LocalTek: Outreach	$75.00	160	hours	$12,000.00	$8,000.00	$4,000.00		
Total Contractual				**$80,000.00**	**$53,333.33**	**$26,666.67**		

Other Direct Costs

Item Description	Unit Cost	Number of Units		Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
Not applicable					$0.00	$0.00		
Total Other Direct Costs				**$0.00**	**$0.00**	**$0.00**		

Indirect Costs

Item Description	Unit Cost	Number of Units		Total Unit Cost	Grant Amount Requested	Match Amount	NOTES	REPLIES
Indirect cost of 4.9% applied below the line	1	1	flat	$14,012.12	$14,565.55	$8,000.00	$6,565.55	

Total Project Contingency				**$14,012.12**	**$14,565.55**	**$8,000.00**		
Grant total fund and required match				**$285,387.76**	**$195,482.64**	**$98,458.55**		

Proof of the project's financing including the ability of the applicant's to fund the total project costs, prior to reimbursement, is required in the Document Upload and Submission tab.

Metro Government of Nashville-Davidson will cover with in-kind match:	$98,458.55	
Funds from grantor	$195,482.64	50%
Total Project	$293,941.19	
In-kind match		
As a percentage of Program Director, Digital Learning and Access S.	64.62%	

RAMPS Budget Narrative

Personnel

With a total budget of $110,336, the Personnel categories includes $73,557.33 federal contribution and $36,778.67 local match. Personnel is the largest budget category, demonstrating the time and staff necessary to build and launch the new cybersecurity training program. Personnel include a human resource analyst (104 working weeks, 1 hour per week), a grant manager (104 working weeks, 1 hour per week), a program supervisor (104 working weeks, 6 hours per week), a finance manager (104 working weeks, .5 hours per week), and a project manager (18 working weeks, 4 hours per week). Led by the project manager, these individuals will support administration of this grant.

Fringe Benefits

The total budget for Fringe benefits is $40,272.64. This budget includes $26,848.43 federal contribution and $13,424.21 local match. Fringe benefits include amounts of 36.5% of the above personnel costs, applied at 36.5% of each calculated personnel line item. This percentage is determined by the Office of Management and Budget.

Travel

In alignment with the travel required in the NOFO, travel costs include costs to and from Denver for two personnel: Airfare, lodging, meals for three days, and conference fees. This budget category totals $2,562, including $1,708 federal support and $854 local match. Airfare ($450) is the current average of travel to Denver from Nashville International Airport as of June 5, 2025. Airfare rates are from $245 to $617 round-trip. Lodging ($215/night, individual rooms for two people) and meals ($92/day for a total of three days) are at 2025 CONUS rates. Conference fees ($340 per person for two people) are based on the early-bird pricing for the NICE Conference and Expo, advertised online at https://niceconference.org.

Equipment

$4,803.33 federal support and $2,401.67 bring the Equipment total budget to $7,205. Equipment includes laptops and peripherals for five program trainers, priced at the Metro-negotiated rate for Dell All-in-one laptop units.

Supplies

Supplies totaling $31,000 include $20,666.67 federal contribution and $10,333.33 local match. Printed materials for 150 participants at $10 each totaling $1,500 are designed by the training partner, LocalTek, and include one quick reference guide and two handouts. The Learning Management System ($12,500) references LocalTek.org, where all courses are housed, with separate licenses for each student and instructor, along with all quizzes and assignments. This category also includes four subscription licenses to JobsEQ, our selected source for local workforce information. The cost of $17,000 is based on a pre-negotiated Metro rate for previously purchased licenses for our service region + a 75 Mile Radius Around + State. This subscription will be used by the program director, Grants lead, project manager, and the Chief Information Officer for the Metropolitan Government of Nashville and Davidson County/Director of Information Technology Services, who will provide program oversight for any pre-apprenticeship and apprenticeship activities conducted through Metro.

Contractual

This budget category, which totals $80,000, is devoted to LocalTek, Metro's key training partner in this project. All contractual expenses will support LocalTek's proven cybersecurity training program. As this is a new collaboration, the largest line item, $40,000, is devoted to program planning. Outreach, Training, and Curriculum development all total $12,000 for the project with $8,000 requested from federal funds and $4,000 matched locally. Finally, community assessment and engagement is the smallest Contractual line item totaling, $4,000 - $2,666.67 federal and $1,333.33 local match.

Other Direct Costs

In alignment with the IDC allowance in the NOFO, we are requesting ITS's standard IDC of 4.9%, which equals $14,565.55. However, we will match this within our in-kind allotment, making our true IDC (in budget actuals) $6,565.55.

Indirect Costs

In alignment with the Indirect Costs allowance in the NOFO, Indirect Costs are calculated at the Metro Information Technology Services percentage of 4.9% for a total of $14,565.55. However, we are matching this within our in-kind allotment, making our true IDC (in budget actuals) $6,565.55.

Overview budget narrative

This project's total budget is $285,387.76, of which 67% ($195,482.64) is requested federal support and 33% (98,458.55) is locally matched. Personnel expenses are the largest budget category, totaling $110,336 and supporting five different administrators. Contractual expenses are the second largest budget category. $80,000 will support activities led Metro's key training partner, LocalTek. Aligning with Personnel expenses making up the highest budget category, Fringe Benefits are the third largest budget category, totaling $40,272.64. These expenses were calculated at a standard rate of 36.5% of Personnel costs. Metro's cybersecurity training program will require $31,000 for supplies, including critical licenses for a learning management system and JobsEQ, a labor market research software. Trainers will be key players in the success of this cybersecurity training program, and so the equipment category will support the purchase of 5 laptops to aid their work. The equipment totals $7,205. Finally, per the NOFO requirement, two staff members will travel to Denver to present this project. Thus, the travel budget totals $2,562, including $1,708 federal support and $854 local match. Each line item and budget category will work toward the success of this cybersecurity training, bridging a cybersecurity talent gap by developing a comprehensive and sustainable cybersecurity workforce pipeline.

APPLICATION FOR RAMPS

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

John Griffey

Director
Department of ITS

6/25/2025

Date

Nashville State Community College

June 25, 2025

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
100 Bureau Dr
Gaithersburg, MD 20899

To Whom It May Concern,

On behalf of Nashville State Community College, I am writing to 1) express our support for the Nashville Cybersecurity Workforce Accelerator (NCWA) program proposed for funding through the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development grant initiative and 2) state our interest in exploring possibilities to work with this multistakeholder collaborative. We recognize the vital importance of equipping our community with the necessary technical skills and workforce capabilities to thrive in our region's rapidly growing cybersecurity landscape.

With seven campuses in Middle Tennessee, Nashville State Community College offers programs and support designed to enable students to easily move from education to the workforce in the minimum amount of time through a flexible, accessible process. Our mission aligns closely with the goals of this grant program, and we are eager to explore ways to collaborate with the Metropolitan Government of Nashville and Davidson County to make a meaningful impact in the lives of residents.

Specifically, Nashville State Community College can potentially offer the following support:

1. **Employer Partnerships:** Exploring approaches for actively collaborating with employers to identify workforce needs to understand how our programs can meet those needs.
2. **Educational Partnership:** NSCC offers accessible and affordable education and training programs that align with local industry needs and will work closely with partners to align around shared education and workforce goals.

Nashville State Community College is enthusiastic about the potential of this program to drive significant, positive change in our community. We are fully committed to ongoing discussion about how to lend our resources, expertise, and time to support the Metropolitan Government of Nashville and Davidson County and other grant partners in successfully implementing the Nashville Cybersecurity Workforce Accelerator (NCWA) program.

Thank you for the opportunity to collaborate on this critical initiative. We look forward to our continued partnership and to the success of this program in empowering our community through training and workforce readiness support.

Sincerely,

Shanna L. Jackson SCR

Shanna L. Jackson
President
Nashville State Community College

Nashville Technology Council
500 Interstate Blvd., S.
Suite 200
Nashville, TN 37210

June 18, 2025

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
100 Bureau Dr
Gaithersburg, MD 20899

To Whom It May Concern,

On behalf of Greater Nashville Technology Council (GNTC), I am writing to formally express our commitment to support the Nashville Cybersecurity Workforce Accelerator (NCWA) program proposed for funding through the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development grant initiative. We recognize the vital importance of equipping our community with the necessary technical skills and workforce capabilities to thrive in our region's rapidly growing cybersecurity landscape.

We believe in our community's ability to produce and retain the nation's best talent. We empower growth by supporting the gifted individuals that comprise our workforce today and provide inspiration and education for the workforce of tomorrow. We are eager to collaborate with the Metropolitan Government of Nashville and Davidson County to make a meaningful impact in the lives of residents.

Specifically, GNTC commits to the following support:

1. **Employer Engagement:** GNTC will use our broad reach within the technological business community in Nashville to bring opportunities to the participants in the program, delivering results through internal and external collaboration.
2. **Employment Opportunities:** GNTC will leverage our knowledge of the community and partnerships with businesses and prospective trainees and hires to expand access to a diverse pool of potential participants in internship, pre-apprenticeship, and apprenticeship opportunities through member communications.

We look forward to our continued partnership and to the success of this program in empowering our community through training and workforce readiness support.

Sincerely,

Emily Bounds

Emily Bounds
Community Relations Manager

BLACKS IN TECHNOLOGY
NASHVILLE

June 17, 2025

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
100 Bureau Dr
Gaithersburg, MD 20899

To Whom It May Concern,

On behalf of Blacks in Technology-Nashville Chapter, I am writing to formally express our commitment to support the Nashville Cybersecurity Workforce Accelerator (NCWA) program proposed for funding through the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development grant initiative. We recognize the vital importance of equipping our community with the necessary technical skills and workforce capabilities to thrive in our region's rapidly growing cybersecurity landscape.

Blacks in Technology-Nashville Chapter exists to create a community of advocacy and allyship that ensures everyone in Nashville's Black technology community can find career advice, share their experiences and be a part of a rapidly growing community that opens doors for all. Our mission aligns closely with the goals of this grant program, and we are eager to collaborate with the Metropolitan Government of Nashville and Davidson County to make a meaningful impact in the lives of residents.

Specifically, Blacks in Technology-Nashville Chapter commits to the following support:

1. **Participant Recruitment:** We have a strong regional network and will support tis program by helping to share the opportunity with our program participants and partners.
2. **Thought Partnership and Feedback:** We will lend our expertise and understanding of the unique challenges our members and other Black technology professionals face in advancing their careers to support the development of the NCWA program.

Blacks in Technology-Nashville Chapter is enthusiastic about the potential of this program to drive significant, positive change in our community. We are fully committed to investing our resources, expertise, and time to support the Metropolitan Government of Nashville and Davidson County and other grant partners in successfully implementing the Nashville Cybersecurity Workforce Accelerator (NCWA) program.

Thank you for the opportunity to collaborate on this critical initiative. We look forward to our continued partnership and to the success of this program in empowering our community through training and workforce readiness support.

Sincerely,

Holly Rachel

President

Blacks In Technology - Nashville

LOCALTEK

June 17, 2025

U.S. Department of Commerce, National Institute of Standards and Technology (NIST)
100 Bureau Dr
Gaithersburg, MD 20899

To Whom It May Concern,

On behalf of LocalTek, I am writing to formally express our commitment to support the Nashville Cybersecurity Workforce Accelerator (NCWA) program proposed for funding through the Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development grant initiative. We recognize the vital importance of equipping our community with the necessary technical skills and workforce capabilities to thrive in our region's rapidly growing cybersecurity landscape.

LocalTek is a flexible workforce development program that combines on-the-job training with classroom instruction from industry leaders and 1-on-1 mentorship to accelerate learning and career access. Our mission aligns closely with the goals of this grant program, and we are eager to collaborate with the Metropolitan Government of Nashville and Davidson County to make a meaningful impact in the lives of residents.

Specifically, LocalTek commits to the following support:

1. **Curriculum Development and Delivery:** We will leverage our expertise to co-develop and deliver specialized training modules in cybersecurity, with a strong emphasis on practical, hands-on learning through digital tools and technologies.
2. **Participant Support:** LocalTek will also commit to providing mentorship and career guidance to program participants, helping them transition from education and training into meaningful employment opportunities.
3. **Monitoring and Evaluation:** We will work closely with the Metropolitan Government of Nashville and Davidson County to monitor and evaluate the progress of the program, ensuring that objectives are met and that we continuously improve our strategies and outcomes.

LocalTek is enthusiastic about the potential of this program to drive significant, positive change in our community. We are fully committed to investing our resources, expertise, and time to support the Metropolitan Government of Nashville and Davidson County and other grant partners in successfully implementing the Nashville Cybersecurity Workforce Accelerator (NCWA) program.

Thank you for the opportunity to collaborate on this critical initiative. We look forward to our continued partnership and to the success of this program in empowering our community through training and workforce readiness support.

Sincerely,

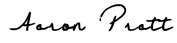
Holly Rachel
Vice President
LocalTek

Certificate Of Completion

Envelope Id: 200FF467-371B-4A9B-9D50-17291DCEB3ED
Status: Completed
Subject: Complete with Docusign: ITS NIST NICE RAMPS 25-27 Ready.pdf
Source Envelope:
Document Pages: 65
Signatures: 3
Envelope Originator:
Certificate Pages: 15
Initials: 1
Juanita Paulson
AutoNav: Enabled
730 2nd Ave. South 1st Floor
EnvelopeId Stamping: Enabled
Nashville, TN 37219
Time Zone: (UTC-06:00) Central Time (US & Canada)
Juanita.Paulsen@nashville.gov
IP Address: 170.190.198.185

Record Tracking

Status: Original
7/16/2025 8:02:56 AM
Holder: Juanita Paulson
Juanita.Paulsen@nashville.gov
Location: DocuSign
Security Appliance Status: Connected
Pool: StateLocal
Storage Appliance Status: Connected
Pool: Metropolitan Government of Nashville and Davidson County
Location: Docusign

Signer Events	Signature	Timestamp
Kenneth Hartlage kenneth.hartlage@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.190	Sent: 7/16/2025 8:07:50 AM Resent: 7/17/2025 1:57:08 PM Viewed: 7/17/2025 2:00:00 PM Signed: 7/17/2025 2:01:29 PM
Electronic Record and Signature Disclosure: Accepted: 7/17/2025 2:00:00 PM ID: eb70c1c7-d35a-49c2-8b1f-85a0391558fe		
Aaron Pratt Aaron.Pratt@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 7/17/2025 2:01:37 PM Viewed: 7/18/2025 8:13:47 AM Signed: 7/18/2025 8:14:18 AM
Electronic Record and Signature Disclosure: Accepted: 7/18/2025 8:13:47 AM ID: c052bf0d-e846-4ba1-92c0-29770c97b58b		
Jenneen Reed/mjw MaryJo.Wiggins@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 151.124.106.79 Signed using mobile	Sent: 7/18/2025 8:14:26 AM Viewed: 7/21/2025 2:23:23 PM Signed: 7/21/2025 2:24:44 PM
Electronic Record and Signature Disclosure: Accepted: 7/21/2025 2:24:42 PM ID: 74c61191-bdd4-4761-b3df-ba53b7811549		
Nicki Eke nicki.eke@nashville.gov Security Level: Email, Account Authentication (None)	 Signature Adoption: Pre-selected Style Using IP Address: 170.190.198.185	Sent: 7/21/2025 2:24:52 PM Viewed: 7/21/2025 4:29:08 PM Signed: 7/21/2025 4:32:07 PM
Electronic Record and Signature Disclosure:		

Signer Events	Signature	Timestamp
Accepted: 7/21/2025 4:29:08 PM ID: fdd365c1-b436-40f2-aece-7f3e77f8e222		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp
Karina Valdez karina.valdez@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 8/12/2022 8:07:55 AM ID: ec3de7a9-934b-431e-a2e7-878bc56f8182	COPIED	Sent: 7/21/2025 4:32:18 PM
Sally Palmer sally.palmer@nashville.gov Security Level: Email, Account Authentication (None) **Electronic Record and Signature Disclosure:** Accepted: 7/21/2025 10:47:05 AM ID: 94fa50fd-5008-4058-baf7-a6000983d172	COPIED	Sent: 7/21/2025 4:32:19 PM Viewed: 7/22/2025 7:47:30 AM

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/16/2025 8:07:50 AM
Envelope Updated	Security Checked	7/17/2025 1:57:07 PM
Envelope Updated	Security Checked	7/17/2025 1:57:07 PM
Certified Delivered	Security Checked	7/21/2025 4:29:08 PM
Signing Complete	Security Checked	7/21/2025 4:32:07 PM
Completed	Security Checked	7/21/2025 4:32:19 PM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

1. ACCEPTANCE OF TERMS AND CONDITIONS These Terms and Conditions govern your ("Subscriber" or "you") use of DocuSign's on-demand electronic signature service (the "Subscription Service"), as accessed either directly through DocuSign.com, DocuSign.net, or through a DocuSign affiliateâ€™s web page offering a Service Plan (collectively, the "Site"). By depositing any document into the System (as defined below), you accept these Terms and Conditions (including your corresponding Service Plan, the DocuSign.com Terms of Use, and all policies and guidelines referenced and hereby incorporated into these Terms and Conditions) and any modifications that may be made to the Terms and Conditions from time to time. If you do not agree to these Terms and Conditions, you should not use the Subscription Service or visit or browse the Site. These Terms and Conditions constitute a binding legal agreement between you and DocuSign, Inc. ("DocuSign," "we," "us," and "our"). Please read them carefully and print a copy for your future reference. 2. MODIFICATION OF TERMS AND CONDITIONS We reserve the right to modify these Terms and Conditions at any time and in any manner at our sole discretion by: (a) posting a revision on the Site; or (b) sending information regarding the amendment to the email address you provide to us. YOU ARE RESPONSIBLE FOR REGULARLY REVIEWING THE SITE TO OBTAIN TIMELY NOTICE OF ANY AMENDMENTS. YOU SHALL BE DEEMED TO HAVE ACCEPTED SUCH AMENDMENTS BY CONTINUING TO USE THE SUBSCRIPTION SERVICE FOR MORE THAN 20 DAYS AFTER SUCH AMENDMENTS HAVE BEEN POSTED OR INFORMATION REGARDING SUCH AMENDMENTS HAS BEEN SENT TO YOU. You agree that we shall not be liable to you or to any third party for any modification of the Terms and Conditions. 3. DEFINITIONS â€œAccountâ€? means a unique account established by Subscriber to enable its Authorized Users to access and use the Subscription Service. â€œAuthorized Userâ€? means any employee or agent of Subscriber, identified by a unique email address and user name, who is registered under the Account, provided that no two persons may register, access or use the Subscription Service as the same Authorized User. â€œeContractâ€? refers to a contract, notice, disclosure, or other record or document deposited into the System by Subscriber for processing using the Subscription Service. â€œEnvelopeâ€? means an electronic record containing one or more eContracts consisting of a single page or a group of pages of data uploaded to the System. â€œSeatâ€? means an active Authorized User listed in the membership of an Account at any one time. No two individuals may log onto or use the Subscription Service as the same Authorized User, but Subscriber may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time is equal to or less than the number of Seats purchased. â€œService Planâ€? means the right to access and use the Subscription Service for a specified period in exchange for a periodic fee, subject to the Service Plan restrictions and requirements that are used to describe the selected Service Plan on the Site. Restrictions and requirements may include any or all of the following: (a) number of Seats and/or Envelopes that a Subscriber may use in a month or year for a fee; (b) fee for sent Envelopes in excess of the number of Envelopes allocated to Subscriber under the Service Plan; (c) per-seat or per-user restrictions; (d) the license to use DocuSign software products such as DocuSign Connect Express in connection with the Subscription Service; and (e) per use fees. â€œSpecificationsâ€? means the technical specifications set forth in the â€œSubscription Service Specificationsâ€? available at http://docusign.com/company/specifications. â€œSubscription Serviceâ€? means DocuSignâ€™s on-demand electronic signature service, as updated from time

to time, which provides on-line display, certified delivery, acknowledgement, electronic signature, and storage services for eContracts via the Internet. â€œSystemâ€? refers to the software systems and programs, communication and network facilities, and hardware and equipment used by DocuSign or its agents to provide the Subscription Service. â€œTermâ€? means the period of effectiveness of these Terms and Conditions, as specified in Section 12 below. â€œTransaction Dataâ€? means the metadata associated with an Envelope (such as transaction history, image hash value, method and time of Envelope deletion, sender and recipient names, email addresses and signature IDs) and maintained by DocuSign in order to establish the digital audit trail required by the Subscription Service. 4. SUBSCRIPTION SERVICE During the term of the Service Plan and subject to these Terms and Conditions, Subscriber will have the right to obtain an Account and register its Authorized Users, who may access and use the Subscription Service, and DocuSign will provide the Subscription Service in material conformance with the Specifications. You must be 18 years of age or older to register for an Account and use the Subscription Service. Subscriber's right to use the Subscription Service is limited to its Authorized Users, and Subscriber agrees not to resell or otherwise provide or assist with the provision of the Subscription Service to any third party. In addition, DocuSignâ€™s provision of the Subscription Service is conditioned on Subscriber's acknowledgement and agreement to the following: (a) The Subscription Service facilitates the execution of eContracts between the parties to those eContracts. Nothing in these Terms and Conditions may be construed to make DocuSign a party to any eContract processed through the Subscription Service, and DocuSign makes no representation or warranty regarding the transactions sought to be effected by any eContract; (b) Between DocuSign and Subscriber, Subscriber has exclusive control over and responsibility for the content, quality, and format of any eContract. All eContracts stored by DocuSign are maintained in an encrypted form, and DocuSign has no control of or access to their contents; (c) If Subscriber elects to use one or more of the optional features designed to verify the identity of the intended recipient of an eContract that DocuSign makes available to its subscribers (â€œAuthentication Measuresâ€?), DocuSign will apply only those Authentication Measures selected by the Subscriber, but makes no representations or warranties about the appropriateness of any Authentication Measure. Further, DocuSign assumes no liability for: (A) the inability or failure by the intended recipient or other party to satisfy the Authentication Measure; or (B) the circumvention by any person (other than DocuSign) of any Authentication Measure; (d) Certain types of agreements and documents may be excepted from electronic signature laws (e.g. wills and agreements pertaining to family law), or may be subject to specific regulations promulgated by various government agencies regarding electronic signatures and electronic records. DocuSign is not responsible or liable to determine whether any particular eContract is subject to an exception to applicable electronic signature laws, or whether it is subject to any particular agency promulgations, or whether it can be legally formed by electronic signatures; (e) DocuSign is not responsible for determining how long any d to be retained or stored under any applicable laws, regulations, or legal or administrative agency processes. Further, DocuSign is not responsible for or liable to produce any of Subscriberâ€™s eContracts or other documents to any third parties; (f) Certain consumer protection or similar laws or regulations may impose special requirements with respect to electronic transactions involving one or more â€œconsumers,â€? such as (among others) requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. DocuSign does not and is not responsible to: (A) determine whether any

particular transaction involves a â€œconsumer;â€? (B) furnish or obtain any such consents or determine if any such consents have been withdrawn; (C) provide any information or disclosures in connection with any attempt to obtain any such consents; (D) provide legal review of, or update or correct any information or disclosures currently or previously given; (E) provide any such copies or access, except as expressly provided in the Specifications for all transactions, consumer or otherwise; or (F) otherwise to comply with any such special requirements; and (g) Subscriber undertakes to determine whether any â€œconsumerâ€? is involved in any eContract presented by Subscriber or its Authorized Users for processing, and, if so, to comply with all requirements imposed by law on such eContracts or their formation. (h) If the domain of the primary email address associated with the Account is owned by an organization and was assigned to Subscriber as an employee, contractor or member of such organization, and that organization wishes to establish a commercial relationship with DocuSign and add the Account to such relationship, then, if Subscriber does not change the email address associated with the Account, the Account may become subject to the commercial relationship between DocuSign and such organization and controlled by such organization. 5. RESPONSIBILITY FOR CONTENT OF COMMUNICATIONS As between Subscriber and DocuSign, Subscriber is solely responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, and written or audible communications submitted by any Authorized User or otherwise processed through its Account, the Subscription Service, or under any Service Plan. Accordingly: (a) Subscriber will not use or permit the use of the Subscription Service to send unsolicited mass mailings outside its organization. The term â€œunsolicited mass mailingsâ€? includes all statutory or common definitions or understanding of those terms in the applicable jurisdiction, such as those set forth for â€œCommercial Electronic Mail Messagesâ€? under the U.S. CAN-SPAM Act, as an example only; and (b) Subscriber will not use or permit the use of the Subscription Service: (i) to communicate any message or material that is defamatory, harassing, libelous, threatening, or obscene; (ii) in a way that violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability (other than contractual liability of the parties under eContracts processed through the Subscription Service); (iii) in any manner that is likely to damage, disable, overburden, or impair the System or the Subscription Service or interfere with the use or enjoyment of the Subscription Service by others; or (iv) in any way that constitutes or encourages conduct that could constitute a criminal offense. DocuSign does not monitor the content processed through the Subscription Service, but in accordance with DMCA (Digital Millennium Copyright Act) safe harbors, it may suspend any use of the Subscription Service, or remove or disable any content that DocuSign reasonably and in good faith believes violates this Agreement or applicable laws or regulations. DocuSign will use commercially reasonable efforts to notify Subscriber prior to any such suspension or disablement, unless DocuSign reasonably believes that: (A) it is prohibited from doing so under applicable law or under legal process, such as court or government administrative agency processes, orders, mandates, and the like; or (B) it is necessary to delay notice in order to prevent imminent harm to the System, Subscription Service, or a third party. Under circumstances where notice is delayed, DocuSign will provide the notice if and when the related restrictions in the previous sentence no longer apply. 6. PRICING AND PER USE PURCHASES The prices, features, and options of the Subscription Service available for an Account depend on the Service Plan selected by Subscriber. Subscriber may also purchase optional services on a periodic or per-use basis. DocuSign may add or change the prices, features or options available with a

Service Plan without notice. Subscriber's usage under a Service Plan is measured based on the actual number of Seats as described in the Service Plan on the Site. Once a per-Seat Service Plan is established, the right of the named Authorized User to access and use the Subscription Service is not transferable; any additional or differently named Authorized Users must purchase per-Seat Service Plans to send Envelopes. Extra seats, users and/or per use fees will be charged as set forth in Subscriber's Service Plan if allowed by such Service Plan. If a Services Plan defines a monthly Envelope Allowance (i.e. # Envelopes per month allowed to be sent), all Envelopes sent in excess of the Envelope Allowance will incur a per-Envelope charge. Any unused Envelope Allowances will expire and not carry over from one billing period to another under a Service Plan. Subscriberâ€™s Account will be deemed to have consumed an Envelope at the time the Envelope is sent by Subscriber, regardless of whether Envelopes were received by recipients, or whether recipients have performed any actions upon any eContract in the Envelope. Powerforms are considered Envelopes within an Envelope Allowance Service Plan, and will be deemed consumed at the time they are â€œclickedâ€? by any end user regardless of whether or not any actions are subsequently performed upon such Envelope. For Service Plans that specify the Envelope Allowance is â€œUnlimited,â€? Subscriber is allowed to send a reasonable number of Envelopes from the number of Seats purchased. If DocuSign suspects that the number of Envelopes sent from a particular Seat or a group of Seats is abusive and/or unduly burdensome, DocuSign will promptly notify Subscriber, discuss the use-case scenario with Subscriber and any continued monitoring, additional discussions and/or information required to make a final determination on the course of action based on such information. In the event Subscriber exceeds, in DocuSignâ€™s sole discretion, reasonable use restrictions under a Service Plan, DocuSign reserves the right to transfer Subscriber into a higher-tier Service Plan without notice. If you misrepresent your eligibility for any Service Plan, you agree to pay us the additional amount you would have been charged under the most favorable pricing structure for which you are eligible. DocuSign may discontinue a Service Plan at any time, and with prior notice to you, may migrate your Account to a similar Service Plan that may carry a different fee. You agree to allow us to charge your credit card for the fees associated with a substitute Service Plan, even if those fees are higher than those you agreed to when you registered your Account. Optional asures, are measured at the time of use, and such charges are specific to the number of units of the service(s) used during the billing period. Optional services subject to periodic charges, such as additional secure storage, are charged on the same periodic basis as the Service Plan fees for the Subscription Service. 7. SUBSCRIBER SUPPORT DocuSign will provide Subscriber support to Subscriber as specified in the Service Plan selected by Subscriber, and that is further detailed on DocuSignâ€™s website. 8. STORAGE DocuSign will store eContracts per the terms of the Service Plan selected by Subscriber. For Service Plans that specify the Envelope storage amount is â€œUnlimited,â€? DocuSign will store an amount of Envelopes that is not abusive and/or unduly burdensome, in DocuSignâ€™s sole discretion. Subscriber may retrieve and store copies of eContracts for storage outside of the System at any time during the Term of the Service Plan when Subscriber is in good financial standing under these Terms and Conditions, and may delete or purge eContracts from the System at its own discretion. DocuSign may, at its sole discretion, delete an uncompleted eContract from the System immediately and without notice upon earlier of: (i) expiration of the Envelope (where Subscriber has established an expiration for such Envelope, not to exceed 365 days); or (ii) expiration of the Term. DocuSign assumes no liability or responsibility for a party's failure or inability to electronically sign any eContract within such a period of time. DocuSign may retain Transaction Data for as long as it has a

business purpose to do so. 9. BUSINESS AGREEMENT BENEFITS You may receive or be eligible for certain pricing structures, discounts, features, promotions, and other benefits (collectively, "Benefits") through a business or government Subscriber's agreement with us (a "Business Agreement"). Any and all such Benefits are provided to you solely as a result of the corresponding Business Agreement and such Benefits may be modified or terminated without notice. If you use the Subscription Service where a business or government entity pays your charges or is otherwise liable for the charges, you authorize us to share your account information with that entity and/or its authorized agents. If you are enrolled in a Service Plan or receive certain Benefits tied to a Business Agreement with us, but you are liable for your own charges, then you authorize us to share enough account information with that entity and its authorized agents to verify your continuing eligibility for those Benefits and the Service Plan. 10. FEES AND PAYMENT TERMS The Service Plan rates, charges, and other conditions for use are set forth in the Site. Subscriber will pay DocuSign the applicable charges for the Services Plan as set forth on the Site. If you add more Authorized Users than the number of Seats you purchased, we will add those Authorized Users to your Account and impose additional charges for such additional Seats on an ongoing basis. Charges for pre-paid Service Plans will be billed to Subscriber in advance. Charges for per use purchases and standard Service Plan charges will be billed in arrears. When you register for an Account, you will be required to provide DocuSign with accurate, complete, and current credit card information for a valid credit card that you are authorized to use. You must promptly notify us of any change in your invoicing address or changes related to the credit card used for payment. By completing your registration for the Services Plan, you authorize DocuSign or its agent to bill your credit card the applicable Service Plan charges, any and all applicable taxes, and any other charges you may incur in connection with your use of the Subscription Service, all of which will be charged to your credit card. Each time you use the Subscription Service, or allow or cause the Subscription Service to be used, you reaffirm that we are authorized to charge your credit card. You may terminate your Account and revoke your credit card authorization as set forth in the Term and Termination section of these Terms and Conditions. We will provide you with one invoice in a format we choose, which may change from time to time, for all Subscription Service associated with each Account and any charges of a third party on whose behalf we bill. Payment of all charges is due and will be charged to your credit card upon your receipt of an invoice. Billing cycle end dates may change from time to time. When a billing cycle covers less than or more than a full month, we may make reasonable adjustments and/or prorations. If your Account is a qualified business account and is approved by us in writing for corporate billing, charges will be accumulated, identified by Account identification number, and invoiced on a monthly basis. You agree that we may (at our option) accumulate charges incurred during your monthly billing cycle and submit them as one or more aggregate charges during or at the end of each cycle, and that we may delay obtaining authorization from your credit card issuer until submission of the accumulated charge(s). This means that accumulated charges may appear on the statement you receive from your credit card issuer. If DocuSign does not receive payment from your credit card provider, you agree to pay all amounts due upon demand. DocuSign reserves the right to correct any errors or mistakes that it makes even if it has already requested or received payment. Your credit card issuer's agreement governs your use of your credit card in connection with the Subscription Service, and you must refer to such agreement (not these Terms and Conditions) with respect to your rights and liabilities as a cardholder. You are solely responsible for any and all fees charged to your credit card by the issuer, bank, or financial institution including, but not limited to, membership,

overdraft, insufficient funds, and over the credit limit fees. You agree to notify us about any billing problems or discrepancies within 20 days after they first appear on your invoice. If you do not bring them to our attention within 20 days, you agree that you waive your right to dispute such problems or discrepancies. We may modify the price, content, or nature of the Subscription Service and/or your Service Plan at any time. If we modify any of the foregoing terms, you may cancel your use of the Subscription Service. We may provide notice of any such changes by e-mail, notice to you upon log-in, or by publishing them on the Site. Your payment obligations survive any termination of your use of the Subscription Service before the end of the billing cycle. Any amount not paid when due will be subject to finance charges equal to 1.5% of the unpaid balance per month or the highest rate permitted by applicable usury law, whichever is less, determined and compounded daily from the date due until the date paid. Subscriber will reimburse any costs or expenses (including, but not limited to, reasonable attorneysâ€™ fees) incurred by DocuSign to collect any amount that is not paid when due. DocuSign may accept any check or payment in any amount without prejudice to DocuSignâ€™s right to recover the balance of the amount due or to pursue any other right or remedy. Amounts due to DocuSign under these Terms and Conditions may not be withheld or offset by Subscriber for any reason against amounts due or asserted to be due to Subscriber from DocuSign. Unless otherwise noted and Conditions are denominated in United States dollars, and Subscriber will pay all such amounts in United States dollars. Other than federal and state net income taxes imposed on DocuSign by the United States, Subscriber will bear all taxes, duties, VAT and other governmental charges (collectively, â€œtaxesâ€?) resulting from these Terms and Conditions or transactions conducted in relation to these Terms and Conditions. Subscriber will pay any additional taxes as are necessary to ensure that the net amounts received and retained by DocuSign after all such taxes are paid are equal to the amounts that DocuSign would have been entitled to in accordance with these Terms and Conditions as if the taxes did not exist. 11. DEPOSITS, SERVICE LIMITS, CREDIT REPORTS, AND RETURN OF BALANCES You authorize us to ask consumer reporting agencies or trade references to furnish us with employment and credit information, and you consent to our rechecking and reporting personal and/or business payment and credit history if, in our sole discretion, we so choose. If you believe that we have reported inaccurate information about your account to a consumer reporting agency, you may send a written notice describing the specific inaccuracy to the address provided in the Notices section below. For you to use the Subscription Service, we may require a deposit or set a service limit. The deposit will be held as a partial guarantee of payment. It cannot be used by you to pay your invoice or delayed payment. Unless otherwise required by law, deposits may be mixed with other funds and will not earn interest. We reserve the right to increase your deposit if we deem appropriate. You may request that we reevaluate your deposit on an annual basis, which may result in a partial or total refund of the deposit to you or credit to your account. If you default or these Terms and Conditions are terminated, we may, without notice to you, apply any deposit towards payment of any amounts you owe to us. After approximately 90 days following termination of these Terms and Conditions, any remaining deposit or other credit balance in excess of amounts owed will be returned without interest, unless otherwise required by law, to you at your last known address. You agree that any amounts under $15 will not be refunded to cover our costs of closing your account. If the deposit balance is undeliverable and returned to us, we will hold it for you for one year from the date of return and, during that period, we may charge a service fee against the deposit balance. You hereby grant us a security interest in any deposit we require to secure the performance of your obligations under these Terms and

Conditions. 12. TERM AND TERMINATION The term of these Terms and Conditions for each Account begins on the date you register for an Account and continues for the term specified by the Service Plan you purchase (the â€œTermâ€?). You may terminate your Account at any time upon 10 days advance written notice to DocuSign following the Notice procedures set forth in these Terms and Conditions. Unless you terminate your Account or you set your Account to not auto renew, your Service Plan will automatically renew at the end of its Term (each a â€œRenewal Termâ€?), and you authorize us (without notice) to collect the then-applicable fee and any taxes for the renewed Service Plan, using any credit card we have on record for you. Service Plan fees and features may change over time. Your Service Plan for a Renewal Term will be the one we choose as being closest to your Service Plan from the prior Term. For any termination (including when you switch your Account), you will be responsible for payment of all fees and charges through the end of the billing cycle in which termination occurs. If you terminate your annual Service Plan Account within the first 30 days of the Term, you may submit written request to DocuSign following the Notice procedures set forth in these Terms and Conditions, for a full refund of the prepaid fees paid by you to DocuSign. You will be limited to one refund. You agree that termination of an annual Service Plan after the first 30 days will not entitle you to any refund of prepaid fees. You will be in default of these Terms and Conditions if you: (a) fail to pay any amount owed to us or an affiliate of ours or any amount appearing on your invoice; (b) have amounts still owing to us or an affiliate of ours from a prior account; (c) breach any provision of these Terms and Conditions; (d) violate any policy applicable to the Subscription Service; (e) are subject to any proceeding under the Bankruptcy Code or similar laws; or (f) if, in our sole discretion, we believe that your continued use of the Subscription Service presents a threat to the security of other users of the Subscription Service. If you are in default, we may, without notice to you, suspend your Account and use of the Subscription Service, withhold refunds and terminate your Account, in addition to all other remedies available to us. We may require reactivation charges to reactivate your Account after termination or suspension. The following provisions will survive the termination of these Terms and Conditions and your Account: Sections 3, 9-11, and 15-23. 13. SUBSCRIBER WARRANTIES You hereby represent and warrant to DocuSign that: (a) you have all requisite rights and authority to use the Subscription Service under these Terms and Conditions and to grant all applicable rights herein; (b) the performance of your obligations under these Terms and Conditions will not violate, conflict with, or result in a default under any other agreement, including confidentiality agreements between you and third parties; (c) you will use the Subscription Service for lawful purposes only and subject to these Terms and Conditions; (d) you are responsible for all use of the Subscription Service in your Account; (e) you are solely responsible for maintaining the confidentiality of your Account names and password(s); (f) you agree to immediately notify us of any unauthorized use of your Account of which you become aware; (g) you agree that DocuSign will not be liable for any losses incurred as a result of a third party's use of your Account, regardless of whether such use is with or without your knowledge and consent; (h) you will not use the Subscription Service in any manner that could damage, disable, overburden or impair the System, or interfere with another's use of the Subscription Service by others; (i) any information submitted to DocuSign by you is true, accurate, and correct; and (j) you will not attempt to gain unauthorized access to the System or the Subscription Service, other accounts, computer systems, or networks under the control or responsibility of DocuSign through hacking, cracking, password mining, or any other unauthorized means. 14. DOCUSIGN WARRANTIES DocuSign represents and warrants that: (a) the Subscription Service as delivered to Subscriber

and used in accordance with the Specifications will not infringe on any United States patent, copyright or trade secret; (b) the Subscription Service will be performed in accordance with the Specifications in their then-current form at the time of the provision of such Subscription Service; (c) any DocuSign Products that are software shall be free of harmful or illicit code, trapdoors, viruses, or other harmful features; (d) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract not involving any consumer will be sufficient under the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Â§Â§ 7001 et seq. (the â€œESIGN Actâ€?) to ESIGN Act; (e) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract involving a consumer will be sufficient under the ESIGN Act to support the validity of such formation, to the extent provided in the ESIGN Act, so long as and provided that Subscriber complies with all special requirements for consumer eContracts, including and subject to those referenced in Section 4.(f) and (g) above; and (f) DocuSign has implemented information security policies and safeguards to preserve the security, integrity, and confidentiality of eContracts and to protect against unauthorized access and anticipated threats or hazards thereto, that meet the objectives of the Interagency Guidelines Establishing Standards for Safeguarding Subscriber Information as set forth in Section 501 (b) of the Gramm-Leach-Bliley Act. 15. DISCLAIMER OF WARRANTIES EXCEPT FOR THE REPRESENTATIONS AND WARRANTIES EXPRESSLY PROVIDED IN SECTION 14 OF THESE TERMS AND CONDITIONS, THE SUBSCRIPTION SERVICE AND THE SITE ARE PROVIDED â€œAS IS,â€? AND DOCUSIGN: (a) MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER; (b) EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, AND TITLE; AND (c) DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE OR SITE ARE OR WILL BE ERROR-FREE, WILL MEET SUBSCRIBERâ€™S REQUIREMENTS, OR BE TIMELY OR SECURE. SUBSCRIBER WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE RESULTING FROM THE USE OF THE SUBSCRIPTION SERVICE OR SITE. SUBSCRIBER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY. USE OF THE SUBSCRIPTION SERVICE AND SITE ARE AT YOUR SOLE RISK. Because some states and jurisdictions do not allow limitations on implied warranties, the above limitation may not apply to you. In that event, such warranties are limited to the minimum warranty period allowed by the applicable law. 16. SUBSCRIBER INDEMNIFICATION OBLIGATIONS You will defend, indemnify, and hold us, our affiliates, officers, directors, employees, suppliers, consultants, and agents harmless from any and all third party claims, liability, damages, and costs (including, but not limited to, attorneys' fees) arising from or related to: (a) your use of the Subscription Service; (b) your violation of these Terms and Conditions; (c) your infringement, or infringement by any other user of your Account, of any intellectual property or other right of any person or entity; or (d) the nature and content of all materials, works, data, statements, and other visual, graphical, written, or audible communications of any nature submitted by any Authorized User of your Account or otherwise processed through your Account. 17. LIMITATIONS OF LIABILITY NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THESE TERMS AND CONDITIONS, DOCUSIGN WILL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO SUBSCRIBER

FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTIONS CONTEMPLATED UNDER THESE TERMS AND CONDITIONS, INCLUDING BUT NOT LIMITED TO LOST PROFITS OR LOSS OF BUSINESS, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING. UNDER NO CIRCUMSTANCES WILL DOCUSIGN'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THESE TERMS AND CONDITIONS OR SUBSCRIBERâ€™S USE OF THE SUBSCRIPTION SERVICE (INCLUDING BUT NOT LIMITED TO WARRANTY CLAIMS), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID BY SUBSCRIBER TO DOCUSIGN UNDER THESE TERMS AND CONDITIONS DURING THE 3 MONTHS PRECEDING THE DATE OF THE ACTION OR CLAIM. EACH PROVISION OF THESE TERMS AND CONDITIONS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES REPRESENTS AN AGREED ALLOCATION OF THE RISKS OF THESE TERMS AND CONDITIONS BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY DOCUSIGN TO SUBSCRIBER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THESE TERMS AND CONDITIONS, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE WARRANTIES IN THESE TERMS AND CONDITIONS HAVE FAILED OF THEIR ESSENTIAL PURPOSE. Because some states and jurisdictions do not allow limitation of liability in certain instances, portions of the above limitation may not apply to you. 18. CONFIDENTIALITY â€œConfidential Informationâ€? means any trade secrets or other information of DocuSign, whether of a technical, business, or other nature (including, without limitation, DocuSign software and related information), that is disclosed to or made available to Subscriber. Confidential Information does not include any information that: (a) was known to Subscriber prior to receiving it from DocuSign; (b) is independently developed by Subscriber without use of or reference to any Confidential Information; (c) is acquired by Subscriber from another source without restriction as to use or disclosure; or (d) is or becomes part of the public domain through no fault or action of Subscriber. During and after the Term of these Terms and Conditions, Subscriber will: (i) use the Confidential Information solely for the purpose for which it is provided; (ii) not disclose such Confidential Information to a third party; and (iii) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature. If Subscriber is required by law to disclose the Confidential Information or the terms of these Terms and Conditions, Subscriber must give prompt written notice of such requirement before such disclosure and assist the DocuSign in obtaining an order protecting the Confidential Information from public disclosure. Subscriber acknowledges that, as between the parties, all Confidential Information it receives from DocuSign, including all copies thereof in Subscriber's possession or control, in any media, is proprietary to and exclusively owned by DocuSign. Nothing in these Terms and Conditions grants Subscriber any right, title, or interest in or to any of the Confidential Information. Subscriber's incorporation of the Confidential Information into any of its own materials shall not render Confidential Information non-confidential. Subscriber acknowledges that any actual or threatened violation of this confidentiality provision may cause

irreparable, non-monetary injury to the disclosing party, the extent of which may be difficult to ascertain, and therefore agrees that DocuSign shall be entitled to seek injunctive relief in addition to all remedies available to DocuSign at law and/or in equity. Absent written consent of DocuSign, the burden of proving that the Confidential Information is not, or is no longer, confidential or a trade secret shall be on Subscriber. 19. PRIVACY Personal information provided or collected through or in connection with this Site shall only by used in accordance with DocuSignâ€™s Privacy Policy and these Terms and Conditions are subject to the Privacy Policy on DocuSign's website which sets forth the terms and conditions governing DocuSign's collection and use of personal information from Authorized Users that is gathered through the Site. 20. ACCESS LIMITS Your use of the Site is at all times governed by our website Terms of is the owner of various intellectual property and technology rights associated with the Subscription Service, its document management, digital signature, and notary system, including patent, copyright, trade secret, and trademark and service mark rights. Except for the rights expressly granted in these Terms and Conditions, DocuSign does not transfer to Subscriber of any Authorized User any of DocuSignâ€™s technology or other intellectual property or technology rights. All right, title, and interest in and to DocuSignâ€™s technology and intellectual property will remain solely with the DocuSign. Subscriber agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or other trade secrets from the Subscription Service or DocuSignâ€™s technology. DocuSign agrees that data and information provided by Subscriber under these Terms and Conditions shall remain, as between Subscriber and DocuSign, owned by Subscriber. DocuSign hereby grants to users and licensees of its products and services a limited, revocable, nonexclusive and nontransferable right to use DocuSignâ€™s regular trade names, trademarks, titles and logos (â€œLicensed Marksâ€?) solely for purposes of identifying DocuSignâ€™s products and services. Details of this trademark license are available at: http://www.docusign.com/IP. 22. FEEDBACK By submitting feedback to DocuSign: (a) Subscriber automatically grants to DocuSign a perpetual, irrevocable, transferable, royalty-free license to use Subscriber's feedback for any and all purposes without any compensation to Subscriber; and (b) Subscriber agrees that it will not publish, submit, or display feedback submitted by Subscriber or its Authorized Users to or on any other web site or in any other publicly accessible forum without DocuSign's prior written consent. 23. GENERAL Subscriber acknowledges that the Subscription Service and any related products, information, documentation, software, technology, technical data, and any derivatives thereof, that DocuSign makes available to its Subscribers (collectively â€œExcluded Dataâ€?), is subject to export control laws and regulations of the United States and other jurisdictions (collectively â€œExport Lawsâ€?). Subscriber represents and warrants that: (i) it is not located in, under the control of, or a national or resident of an embargoed country or prohibited end user under Export Laws; and (ii) it will not access, download, use, export or re-export, directly or indirectly, the Excluded Data to any location, entity, government or person prohibited by export laws, without first complying with all Export Laws that may be imposed by the U.S. Government and any country or organization of nations within whose jurisdiction it operates or does business. Subscriber is solely responsible for complying with Export Laws for all Excluded Data and any of its content transmitted through the Subscription Service. Subscriber shall advise DocuSign in the event the Excluded Data requires DocuSign to obtain additional licenses, permits and/or approvals from any government in the jurisdiction where Subscriber intends to use the Subscription Service. Upon being advised of such a requirement, DocuSign may at its sole discretion: (a) terminate

Subscriber's Account; (b) obtain such licenses, permits, and/or approvals as may be required; or (c) modify these Terms and Conditions such that additional licenses, permits, and/or approvals are no longer required to be obtained by DocuSign. The Subscription Service will be accessed and delivered via the internet. Subscriber is responsible for obtaining the necessary equipment and internet connection in order to access and use the Subscription Service. In order to fully utilize the Subscription Service, Subscriber will need to maintain certain minimum hardware and software requirements. These requirements are set forth in the Specifications. DocuSign will be and act as an independent contractor (and not as the agent or representative of Subscriber) in the performance of these Terms and Conditions. These Terms and Conditions will not be interpreted or construed as: (a) creating or evidencing any association, joint venture, partnership, or franchise between the parties; (b) imposing any partnership or franchise obligation or liability on either party; (c) prohibiting or restricting either partyâ€™s performance of any services for any third party; or (d) establishing or as a foundation for any rights or remedies for any third party, whether as a third party beneficiary or otherwise. Subscriber must not represent to anyone that Subscriber is an agent of DocuSign or is otherwise authorized to bind or commit DocuSign in any way without DocuSignâ€™s prior authorization. Subscriber may not assign its rights, duties, or obligations under these Terms and Conditions without DocuSignâ€™s prior written consent. If consent is given, these Terms and Conditions will bind Subscriberâ€™s successors and assigns. Any attempt by Subscriber to transfer its rights, duties, or obligations under these Terms and Conditions except as expressly provided in these Terms and Conditions is void. DocuSign may freely assign its rights, duties, and obligations under these Terms and Conditions. DocuSign may utilize a subcontractor or other third party to perform its duties under these Terms and Conditions so long as: (a) DocuSign shall not be relieved of any responsibilities or obligations under these Terms and Conditions that are performed by the subcontractor or third party; and (b) DocuSign shall remain Subscriberâ€™s sole point of contact and sole contracting party. We may provide, or third parties may provide, links to other Web sites or resources that are beyond our control. We make no representations as to the quality, suitability, functionality, or legality of any sites to which links may be provided, and you hereby waive any claim you might have against us with respect to such sites. DOCUSIGN IS NOT RESPONSIBLE FOR THE CONTENT ON THE INTERNET OR WEB PAGES THAT ARE CONTAINED OUTSIDE THE SITE. Your correspondence or business dealings with, or participation in promotions of, advertisers or partners found on or through the Site, including payment and delivery of related goods or services, and any other terms, conditions, warranties, or representations associated with such dealings, are solely between you and such advertiser or partner. You agree that we are not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings or as the result of the presence of such advertisers or partners on the Site. Any notice required or permitted to be given in accordance with these Terms and Conditions will be effective if it is in writing and sent using the certified delivery function of the Subscription Service, by email, certified or registered mail, or insured courier, return receipt requested, to the appropriate party at the address set forth in Subscriber's registration information for Subscriber or on the Site for DocuSign. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notices are deemed given upon receipt if delivered using the Subscription Service or email, two business days following the date of mailing, or one business day following delivery to a courier. Written notification to terminate an Account shall be sent by email to support@docusign.com from the Subscriberâ€™s email address set forth in Subscriber's registration information for Subscriber, or by calling

1.866.219.4318. Neither party will be liable for, or be considered to be in breach of or default ns on account of, any delay or failure to perform as required by these Terms and Conditions as a result of any cause or condition beyond such partyâ€™s reasonable control, so long as such party uses all commercially reasonable efforts to avoid or remove such causes of non-performance or delay. These Terms and Conditions are governed in all respects by the laws of the State of Washington as such laws are applied to agreements entered into and to be performed entirely within Washington between Washington residents. Any controversy or claim arising out of or relating to these Terms and Conditions, the Hosted Service, or the Site will be settled by binding arbitration in accordance with the commercial arbitration rules of the American Arbitration Association. Any such controversy or claim shall be arbitrated on an individual basis, and shall not be consolidated in any arbitration with any claim or controversy of any other party. The arbitration will be conducted in King County, Washington, and judgment on the arbitration award may be entered into any court having jurisdiction thereof. The award of the arbitrator shall be final and binding upon the parties without appeal or review except as permitted by Washington law. Notwithstanding the foregoing, either party may seek any interim or preliminary injunctive relief from any court of competent jurisdiction, as necessary to protect the party's rights or property pending the completion of arbitration. By using the Site or the Subscription Service, you consent and submit to the exclusive jurisdiction and venue of the state and federal courts located in King County, Washington. Any legal action by Subscriber arising under these Terms and Conditions must be initiated within two years after the cause of action arises. The waiver by either party of any breach of any provision of these Terms and Conditions does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with these Terms and Conditions will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of these Terms and Conditions. If any part of these Terms and Conditions is found to be illegal, unenforceable, or invalid, the remaining portions of these Terms and Conditions will remain in full force and effect. If any material limitation or restriction on the grant of any license to Subscriber under these Terms and Conditions is found to be illegal, unenforceable, or invalid, the license will immediately terminate. Except as set forth in Section 2 of these Terms and Conditions, these Terms and Conditions may not be amended except in writing signed by both you and us. In the event that we make such a change that has a material adverse impact on your rights or use of the Service, you may terminate these Terms and Conditions by giving us notice within 20 days of the date we notify you, and you will not be charged any cancellation fee. These Terms and Conditions are the final and complete expression of the agreement between these parties regarding the Subscription Service. These Terms and Conditions supersede, and the terms of these Terms and Conditions govern, all previous oral and written communications regarding these matters. v140527 How it works eSignature Digital Transaction Management Legality Security Global Take a Demo Free Trial Resource Center By Industry Financial Services Healthcare High Tech Higher Education Insurance Real Estate Life Sciences Government By Department Sales Human Resources Finance IT/Operations Legal Marketing Facilities Support Product Management Procurement Partners & Developers Partner Programs Find a Partner Solution Showcase Partner Portal Dev Center Support & Training DocuSign Support Community DocuSign University Company About DocuSign Leadership Team Financial Investors Board of Directors Security & Trust Blog Events Press Room Careers Contact Subscriptions Follow Us Facebook Twitter LinkedIn Glassdoor Google + YouTube Validate TRUSTe privacy certification Â© DocuSign Inc., 2003 - 2014 221 Main St., Suite 1000, San

Francisco, CA 94105 Sales: +1.877.720.2040 | Support: +1.866.219.4318 North America Terms of Use Privacy Policy Intellectual Property Trending Topics: Digital Signature Free What Is Electronic Signature Pdf App For Signing Documents Sign Documents On Android What Is Digital Signature Processing DocuSign FREE TRIAL BUY NOW Validate TRUSTe privacy certification .