Rural Tech Project

Builder: Louisa County Public Schools

RURAL TECH PROJECT

Table of contents

Builder overview

This builder is organized into six sections, arranged in chronological order: program introduction, foundational considerations, program design and planning, community engagement, program evaluation, and sustainability. Each section describes opportunities and decisions, processes, and outcomes made by one Rural Tech Project finalist team — and offers considerations for developing a similar program in your own community.

About the Rural Tech Project

The Rural Tech Project was a $600,000 challenge to advance technology education, support rural educators, and prepare students for the careers of today and tomorrow. The challenge, which launched in June 2020, invited high schools and local educational agencies to propose technology education programs that use competency-based distance learning.

Five finalist teams each won $100,000 and received on-the-ground support to implement their programs over the 2021-2022 and 2022-2023 school years.

- **iLEAD Academy (Carrollton, Kentucky)**. The Virtual Computer Science Career Academy offers students across five high schools the opportunity to take virtual, dual-credit courses leading to the completion of computer science degrees.
- **Louisa County Public Schools (Mineral, Virginia)**. The Louisa County Cybersecurity Program prepares students to meet a critical need in the workforce through sequential, high-quality course work, work-based learning, and leading industry certifications.
- **Premont Independent School District (Premont, Texas)**. In collaboration with the Rural Schools Innovation Zone, the Leaders in Future Technology Startup Incubator helps students learn about technology and use it to solve real-world problems in their community.
- **Ravenna Public Schools (Ravenna, Michigan)**. The Start the Buzz Let's Grow MainStreet project empowers students to develop competencies and build portfolio experiences in technology, science, and business — with the goal of stimulating economic growth within the Ravenna agricultural community.
- **Woodlake High School (Woodlake, California)**. The Woodlake Aviation Pathway prepares students for regional aviation careers or postsecondary degrees, utilizing drone operations, geometry, and aerodynamic principles.

1. Program introduction: Louisa

Learn more about Louisa County High School's program, its history and context, and its team.

Description

The Louisa County High School Cybersecurity Program prepares students for cybersecurity careers or postsecondary degrees through courses, community events, and work-based learning opportunities. First piloted during the Rural Tech Project, this two-year pathway allows students in all grades to learn cybersecurity skills through project-based learning and individualized instruction. Courses include Cybersecurity Operations, Cybersecurity Fundamentals, and Cybersecurity Operations Advanced.

Through the pathway, students have the opportunity to obtain industry credentials, such as TestOut IT Fundamentals Pro, TestOut Security Pro, and CompTIA Security+. Louisa's program is ideal for students interested in pursuing careers in cybersecurity, but is open to all students who are interested in building STEM skills through applied learning opportunities.

Outcomes

During its first two years, the program demonstrated success through sustained and diverse student engagement, academic achievement, development of career-readiness skills, and attainment of industry credentials.

- **Student engagement.** Students demonstrated deep engagement with the content through courses and extracurricular activities, motivated by project-based learning opportunities. Students also participated in regional and national extracurricular cybersecurity programs.
- **Academic achievement.** Student academic success was demonstrated through the completion and passage of courses. Almost all students enrolled in Cybersecurity Operations and Cybersecurity Fundamentals over the initial implementation phase passed the courses.
- **Career-readiness skills.** Through applied learning activities, students developed collaboration and communication skills. Students demonstrated their knowledge and skills during community nights where they taught visitors how to improve the security of their devices. Students also led sessions at the local elementary school to teach students about cybersecurity. Students gained work-based experiences through industry guest speakers and tours of local employers. In addition, three students in the program worked in the district's IT department, where they translated what they learned in the classroom to a workplace setting.

- **Industry credentials.** Over half the students passed their TestOut certification exams. Students who pass the TestOut Security Pro exam have the opportunity to register for the relevant CompTIA certification exam at the end of each school year. These credentials prove skills to future employers, increasing hireability and workforce readiness. The credentials also provide a sense of accomplishment for both students and educators.

Team

The schools and core team members involved are listed below.

- Schools involved: Louisa County High School, Reynolds Community College
- Team Lead: Justin Griggs (Assistant Superintendent, Louisa County Public Schools)
- Community Engagement Manager: Brian DeMuth (General Partner, Riphaen Investments)
- Classroom educator: Crystal Torbush (Cybersecurity Fundamentals, Cyber Operations, and Cybersecurity Operations Advanced)

As you reflect on Louisa's program, consider:

- What outcomes are you hoping to achieve for your students and broader school community?
- Who within your community might support program design and delivery?

2. Foundational considerations

Before your own planning begins, consider the following foundational elements that were in place when the team at Louisa first developed the Cybersecurity Program.

Summary

Louisa County High School was well-suited to creating a cybersecurity CTE pathway because of its existing CTE pathways, the presence of supportive school personnel, and a strong industry network in the surrounding region.

The success of Louisa's other CTE pathways had created built-in support from the district. In addition, the classroom educator already knew about the cybersecurity industry and was eager to build cybersecurity skills.

Louisa is located in Mineral, Virginia (between Charlottesville, Fredericksburg, and Richmond) and is a few hours away from Washington, D.C. Louisa's relative proximity to these cities, where cybersecurity skills are in high demand, made this pathway a strong fit for the school.

Opportunity

The Cybersecurity Program created more opportunities for career and postsecondary exposure for students at Louisa. It also motivated students to build advanced computing skills and addressed college affordability.

At the time of piloting, the cybersecurity industry was growing rapidly and facing a significant talent gap. Louisa's Cybersecurity Program was designed to prepare students to join this growing workforce.

The program's design also addressed a continued need to make college more affordable for students, as courses may one day count towards college credit. Many careers in cybersecurity also offer high-paying salaries directly out of high school. In some instances, companies also cover continuing education costs for employees who take cybersecurity classes while employed.

Community support

The presence of existing champions for cybersecurity education in the local community contributed to the program's success in its first two years. The Community Engagement Manager (CEM) connected easily with regional industry leaders. The district and school stakeholders were also enthusiastic about adding a pathway focused on building skills that prepare students for careers that are in high demand. With this strong base of support, interest in cybersecurity quickly spread to students.

Budget

A high-level overview of Louisa's budget can be found in Appendix A. The bulk of the costs were for computers and monitors to create the physical cybersecurity lab. The funds also covered the classroom educator's cybersecurity training. In addition to what is noted in Appendix A, the CEM role was a substantial development cost.

Louisa funded its program primarily from the prize purse awarded through the Rural Tech Project.

As you explore designing your own program, consider:

- What does your school have in common with Louisa's community? What is different about your school?
- What student, community, and/or workforce needs would this program meet?
- What support already exists within your community?
- What funding sources are available?

3. Program details

As you begin thinking about implementation, learn from how Louisa structured its program design and how it achieved its desired outcomes.

Summary

Students in the Cybersecurity Program gain the knowledge, skills, and certifications to pursue a cybersecurity career after graduation or continue on with cybersecurity training in a higher education institution. The pathway's flexibility allows students to complete the program in two or four years. Students can earn several certifications in IT fundamentals, networking, and security.

Primary objectives

The pathway helps students increase academic achievement, build career-readiness skills, and obtain industry credentials and/or college credits. All of these outcomes grow student career confidence and exposure, ensuring they can thrive in their local community and beyond.

More specifically, students within the pathway prepare for high-wage careers in the surrounding region. They also are able to complete a cybersecurity program at a two- or four-year college more quickly than they would otherwise.

Program activities

The program includes coursework and out-of-school opportunities, such as regional student challenges and internships.

Courses

Upon enrollment in the pathway, students learn the basics in Cybersecurity Fundamentals. Once complete, they are eligible to enroll in Cybersecurity Operations, followed by Cybersecurity Operations Advanced. Each course is one semester long, so students have the option to complete the pathway in two years, or spread the coursework out over four years.

The courses are self-paced and competency-based, and they use project-based learning. Some courses also include interdisciplinary projects. This makes the course appealing to students at a wide variety of levels, which in turn creates a culture of teaching and learning between students. Students with more knowledge may also become teaching assistants.

At the end of each course, all students are eligible to take TestOut certification exams to demonstrate mastery. Students who earn an 85% or higher on their TestOut exams also have the opportunity to take comparable CompTIA licensure tests. Students may take the following certifications:

- **Fundamentals:** TestOut IT Fundamentals Pro, CompTIA IT Fundamentals+
- **Networking:** TestOut Network Pro, CompTIA Network+
- **Security:** TestOut Security Pro, CompTIA Security+

The list of modules for each course can be found in the Appendix B.

Work-based learning

The Cybersecurity Program also includes work-based learning opportunities and site visits. In the first two years of the program, eight students from Louisa's cybersecurity classes toured Dominion Energy, a power and energy company headquartered in Richmond, Virginia. While there, students participated in mock interviews. In the future, the company plans to offer internships to students.

In the second year of the initial implementation phase, the Community Engagement Manager (CEM) secured priority for internships at X Corp Solutions and the Cyber Bytes Foundation. The CEM also reviewed cover letters and resumes, and coordinated the interviews for the students.

Community engagement

Students participate in regional cybersecurity-related events. In the initial implementation phase of the program, students participated in programs such as CyberPatriot and a statewide "Capture the Flag"-style cybersecurity competition.

Students also contribute to school events and community activities. For example, students may showcase their skills in credential hacking, website cloning, and programming at school-wide events and celebrations. Students in the pathway also teach cybersecurity concepts to elementary school students, contributing to a stronger educational ecosystem overall. Cybersecurity students also collaborate with students across the school, finding intersections between cybersecurity and other disciplines such as art, health sciences, automotive, economics, and sports marketing.

The Louisa team also organizes opportunities for industry professionals to connect directly with students and share insights about cybersecurity careers.

Competencies

Competencies developed were predominantly tracked through the industry credentials, math scores, and qualitative data. These competencies include:

- **Academic skills**, such as math and reading comprehension.
- **Technical skills**, such as cybersecurity ethics, risk management, computer networking, and data analysis.
- **Career-readiness skills**, such as communication, collaboration, reliability, and adaptability.

Staffing

Leaders from across the high school and in the wider Louisa community helped to design

and pilot this program. Formal roles and responsibilities included:

Role	Responsibilities	Expertise
Cybersecurity educator	Design and teach hybrid courses.	Cybersecurity education, secondary education, project-based learning, and student engagement.
CEM	Used regional industry contacts to set up potential internships for students, connect community members to relevant school staff.	Community outreach and engagement.
Director of CTE, Workforce Development	Build work-based learning experience opportunities for students.	Community outreach and engagement, work-based learning.
Director of Middle School Education and Virtual/Professional Learning	Conduct data collection and ongoing program assessment.	Program evaluation and reporting.

Time commitment

Before considering capacity to build a program, a team must determine if students, classroom educators, administrators, and local community leaders have time available. This includes time to collaborate and iterate with each other and with other community stakeholders.

Program design and implementation. As part of the Rural Tech Project challenge, Louisa's Cybersecurity Program development spanned three years between proposal and refinement.

Propose	Plan	Run	Refine
June - Oct. 2020	Jan. - July 2021	July 2021 - June 2022	July 2022 - June 2023

In the proposal phase, Louisa's team lead created the vision for the program; generated buy-in from district leaders, administrators, educators, and students; and recruited the right talent. The classroom educator then developed and tested new curriculum. The team worked together to refine or adjust strategy, providing real-time assessment and student counseling. The CEM also found, built, and maintained relationships with community members.

Below is a table that provides insights into the amount of time Louisa stakeholders dedicated to the design and execution of the program over the three years.

Stakeholder	Activities	Time required
Director of CTE Workforce Development	Community outreach and engagement	40-45 hours per semester
Director of Middle School Education and Professional/Virtual Learning K-12	Student support with Department Head of Guidance and Cybersecurity educator	10-20 hours per semester
	Reporting	40-60 hours per semester
Cybersecurity educator	Curriculum-building	60-80 hours one time
	Iterating and reporting on curriculum	2-4 hours per week
Administrators including Director of CTE, STEAM and Innovation; Director of Facilities, Director of Technology; Director of CTE Workforce Development; Building Level Principal; and Department Head of Counseling	Program design and planning	80-90 hours one time, and 3-5 hours per semester

Ongoing program execution. Below is a table that describes the amount of time needed to administer and participate in Louisa's pathway after the initial implementation phase.

Stakeholder	Activities	Time required
Students	Year one: Cybersecurity Fundamentals course	1-2 additional hours of class time and coursework per week in comparison to parallel course; 5-6 hours total per week
	Year two: Cybersecurity Operations and Cybersecurity Operations Advanced	2-6 hours of class time and coursework per week
	Ad hoc events such as regional "capture the flag" and other community service	6-10 hours for preparation and attendance per event

Stakeholder	Activities	Time required
	events (not all students)	
Classroom educator	Onboarding including cybersecurity education and program design	50-60 hours throughout the first year
	Courses	5-6 additional hours of class time and coursework per week in comparison to parallel course; 6-8 hours total per week
	Cross-team communication and collaboration	3 hours per week
	Planning and reporting	1-2 hours per week
Administrators	Cross-team communication and collaboration	1-2 hours per week
	Planning and reporting	1-2 hours per week
School community collaborators	Cross-team communication and collaboration	4-5 hours per month

Resources

In addition to the staff time required for this program, the team uses the following equipment for the cybersecurity lab.

- Computers and monitors
- Television screens equipped for screen sharing
- Dedicated intranet

As you move your program from concept to implementation, consider:

- What program activities will you need to create or adapt to meet the needs of your school community?
- What competencies are you hoping students will develop?
- Within the school community, who will work on this program? How much time could participants (including students, educators, and administrators) spend?
- If current staff cannot fill all the needed roles, who and how will you recruit?
- What additional resources will you need?

4. Community engagement

Learn from Louisa's community engagement strategy, including the specific individuals and entities involved, and why and how they were engaged.

Summary

Community engagement is vital for CTE pathway development. At Louisa, the team leveraged student excitement over the first two years to build and maintain momentum in the school and local community.

Engaging the school community

The first cohort of students, especially those who continued into the second year, were energized by the pathway and supporting activities. Their enthusiasm spread to other students through word-of-mouth and in more formal settings.

Student participation in school-wide events elevates the program's visibility overall, deepening engagement with other students, teachers, and parents. Students in the pathway present to incoming students at ninth-grade transition day, to establish early awareness of the pathway. The pathway is also highly visible within the school because of the designated cybersecurity lab. In addition, students who are not eligible or available for courses benefit from the program through school-wide events that showcase Cybersecurity Program students and their skills.

Engaging external partners

In their approach to engaging external partners, Louisa has focused primarily on informing the wider community about the importance of cybersecurity education. Through student-led community events, cybersecurity education has reached many different types of stakeholders, including parents, neighbors, and local small business owners. Cybersecurity has been elevated as an important topic for all, rather than just for big businesses like banks.

Louisa also holds relationships with local industry partners to introduce students to different cybersecurity careers and help them obtain internships. In the initial implementation phase of the program, three students interned in the district's IT department.

As you design your community engagement strategy, consider:

- How are you already connected with each stakeholder group? Who are your existing champions?
- Who would a dream industry or postsecondary partner be, and what would their partnership bring to the program?
- Who from your existing school community can help forge connections?
- What is your outreach strategy, and what are your expectations?

5. Program evaluation

Learn more about Louisa's approach to evaluating program outcomes and the tools used to track results over time.

As part of the Rural Tech Project, Louisa created a logic model (template for reference in Appendix C) to align on the goals, activities, and outcomes they would like to track. When the pathway was in its second year, the Rural Tech Project provided a tool to facilitate iterative program improvements over a 90-day period: the Plan / Study / Do / Act framework (Appendix D).

Program milestones

Program milestones typically follow school calendars. Given this program's involvement in the Rural Tech Project challenge, Louisa High School's program milestones were also situated within the challenge phases. The program milestones listed below follow the challenge structure.

Run	Refine
July 2021 - June 2022	July 2022 - June 2023
• Cybersecurity Fundamentals curriculum designed. • Cybersecurity Fundamentals taught for the first time. • Student survey results and data from the Microsoft Technology Associates exam showed curricular misalignment. • TestOut and CompTIA were chosen as substitute certifications and curricula were tweaked slightly to align with assessments.	• Cybersecurity Operations and Cybersecurity Operations Advanced curricula designed. • Cybersecurity Operations and Cybersecurity Operations Advanced taught for the first time. • Students took TestOut and CompTIA certifications in IT, networking, and security.

Data collection

The team collected data on student engagement, student success, and career outcomes over the course of the two years. They used this data to continuously assess and improve their program.

Student engagement

Louisa collects demographic data on students in the program and adjusts its recruitment strategy to address underrepresented groups. The team also surveys students on a regular cadence to assess satisfaction and identify areas for improvement.

Student success

Student success is predominantly evaluated through the attainment of industry credentials, completion of courses, and qualitative data.

Career outcomes

Career outcomes data collection is focused on qualitative insights around employability skills. In addition, the team tracks the number of students in internships, graduation rates, and enrollment in postsecondary institutions. As the program continues and Louisa gathers more data, the team also plans to track employment rates.

Key improvements

Over the first two years, Louisa implemented key programmatic improvements based on qualitative and quantitative data collection and assessment.

- **Expanding industry partnerships.** In the second year, the team targeted additional local companies to build relationships with, including Dominion Energy. Outcomes included additional internship opportunities, field trips, guest speakers, and mentoring; for example, students received mentor feedback through mock interviews.
- **Increasing cross-collaboration and project-based learning opportunities.** Based on student feedback, the classroom educator increased opportunities for project-based learning, and sought opportunities to collaborate with students and educators in other disciplines.

As you determine your own program evaluation approach, consider:

- What are the major milestones you would like to accomplish in the first 30, 60, and 90 days? What would success look like in years one, two, and three of the program?
- What data would help you understand your program's performance?

- How would you collect that data within the systems that currently exist? What could you build or change to collect and analyze that data?
- What would a logic model for your program look like?

6. Sustainability

Learn more about Louisa's short-term and long-term visions for its program.

Summary

Moving forward, the team hopes to continue the program with full classes of students. They plan to expand remote cybersecurity classes to three other districts in the region. The team also expects to support neighboring districts in implementing their own cybersecurity pathways. Finally, the team intends to expand employer partnerships to create more internship opportunities.

Community engagement

The team hopes to deepen engagement with industry partners to offer more work-based learning opportunities to students. In particular, the team intends to expand internship opportunities at Dominion Energy, X Corp Solutions, and the Cyber Bytes Foundation.

The team has also begun working with Reynolds Community College to discuss an articulation agreement for college credits earned through the pathway. Through this partnership, the team also hopes to create opportunities for educators to participate in cybersecurity boot camps to deepen content knowledge.

Staffing

The cybersecurity educator will continue to teach courses in the pathway. The team has also built a relationship with Virginia Tech to support recruiting one additional educator as they expand to reach more students. Project Lead The Way, a nonprofit that partners with local colleges to deliver boot-camp-style CTE educator training, will provide additional education to onboard a new educator.

Funding

There were no significant additional material needs to sustain the program. The school plans to reallocate funds or seek additional funding for an additional cybersecurity teacher, and the education and training that teacher may require.

As you determine your own program's longevity, consider:

- What are your goals around sustaining and growing your program?
- What is the intended length of the program? Will your program continue indefinitely, or will it be designed to last for a certain number of years?
- For programs designed to exist indefinitely, how might the program adapt to evolving student, school, industry, and community needs over time?
- What would be needed to achieve the goals and vision described above? What staffing, funding, and community engagement would be required?

Appendix A: High-level budget

Budget item	Relevant notes	Approximate amount ($)
EXPENSES		
Computer hardware	One-time purchase	50,000
Computer software	One-time purchase	21,000
Computer lab room expenses	One-time purchase	8,000
Professional development for cybersecurity educator	One-time purchase	1,500
Total spent		**80,500**

Appendix B: Course modules

Cybersecurity Fundamentals	Cybersecurity Operations	Cybersecurity Operations Advanced
• Module 1: Intro to Cyber • Module 2: Cyber Ethics • Module 3: Internet of Things • Module 4: Computer Operating Systems, Linux and Command line Interface • Module 5: VM, Virtualization • Module 6: Cryptography • Module 7: Midterm Review • Module 8: Networks • Module 9: Cyber threats and vulnerabilities • Module 10: Digital Forensics • Module 11: Certification Prep • Module 10: Careers	• Module 1: Digital Forensics • Module 2: Introduction to Networking • Module 3: Networking Hardware & Devices • Module 4: Understanding Media Types • Module 5: Linux Operating System • Module 6: Network Topologies & WANs • Module 7: The OSI Model • Module 8: Understanding TCP/IP (IPv4, IPv6, TCP on the Command LIne) • Module 9: Certification Test Prep • Module 10: CyberStart America • Module 11: Software, Hardware & Network Security • Module 12: Countermeasures Against Cyberattacks • Module 13: Cyber Politics & Cyber Crime • Module 14: Developing Employability Skills & Career Exploration	• Module 1: Introduction to Security • Module 2: Threat Management & Cybersecurity Resources • Module 3: Threats & Attacks on Endpoints • Module 4: Endpoint & Application Development Security • Module 5: Mobile, Embedded, & Specialized Device Security • Module 6: Basic Cryptography • Module 7: Public Key Infrastructure & Cryptography Protocols • Module 8: Networking Threats, Assessments, and Defenses • Module 9: Network Security Appliances & Technologies • Module 10: Cloud and Virtualization Security • Module 11: Wireless Network Security • Module 12: Authentication • Module 13: Incident Preparation, Response, and Investigation • Module 14: Cybersecurity Resilience • Module 15: Risk Management & Data Privacy • Module 16: Developing Employability Skills & Certification

Appendix C: Logic model template

PROGRAM GOALS What are your latest program goals? Make updates as needed.	1. 2...

CURRENT CONDITIONS What are the starting resources available for your program? Consider **strengths**, **challenges**, or any neutral conditions you assume will be true and necessary for your program to launch.	EXTERNAL FACTORS What are the external factors — **risks** and **opportunities** — that may impact your work? Some factors you might consider to be unpredictable or beyond your control, but others may benefit your program or be manageable with forward planning.
1. 2...	1. 2...

RESOURCES	→	ACTIVITIES	OUTPUTS	→	OUTCOMES	
What resources do you need to achieve your goals?		What are students and staff doing as part of the program?	What staff or structural changes will result from each activity?		What short-term outcomes and measures do you anticipate as a result of each activity?	What long-term outcomes and measures do you anticipate as a result of each activity?
1. 2...		1. 2...	1. 2...		1. 2...	1. 2...

VALIDATION Why are these the right activities to help you reach your target outcomes and goals?	

GAPS What is missing that you will need to consider in order to achieve the desired outcomes?	

Appendix D: Plan / Study / Do / Act framework

Beginning of cycle	**PLAN**	What is the specific process change that you will test and why? What are you hoping to learn? What are your prediction(s)? What specific steps have you planned to enact this change? What data collection tool(s) will you use? When and for long will you test? Who is the project owner(s)? Who else will be involved, including who will be the tester(s)?
End of cycle	**STUDY**	How well were you able to answer each learning question? How do the results compare to your prediction(s)? What did you learn?
	DO	What happened, including what data and observations did you collect?
	ACT	What will you adapt, adopt, abandon, or repeat again — and why?