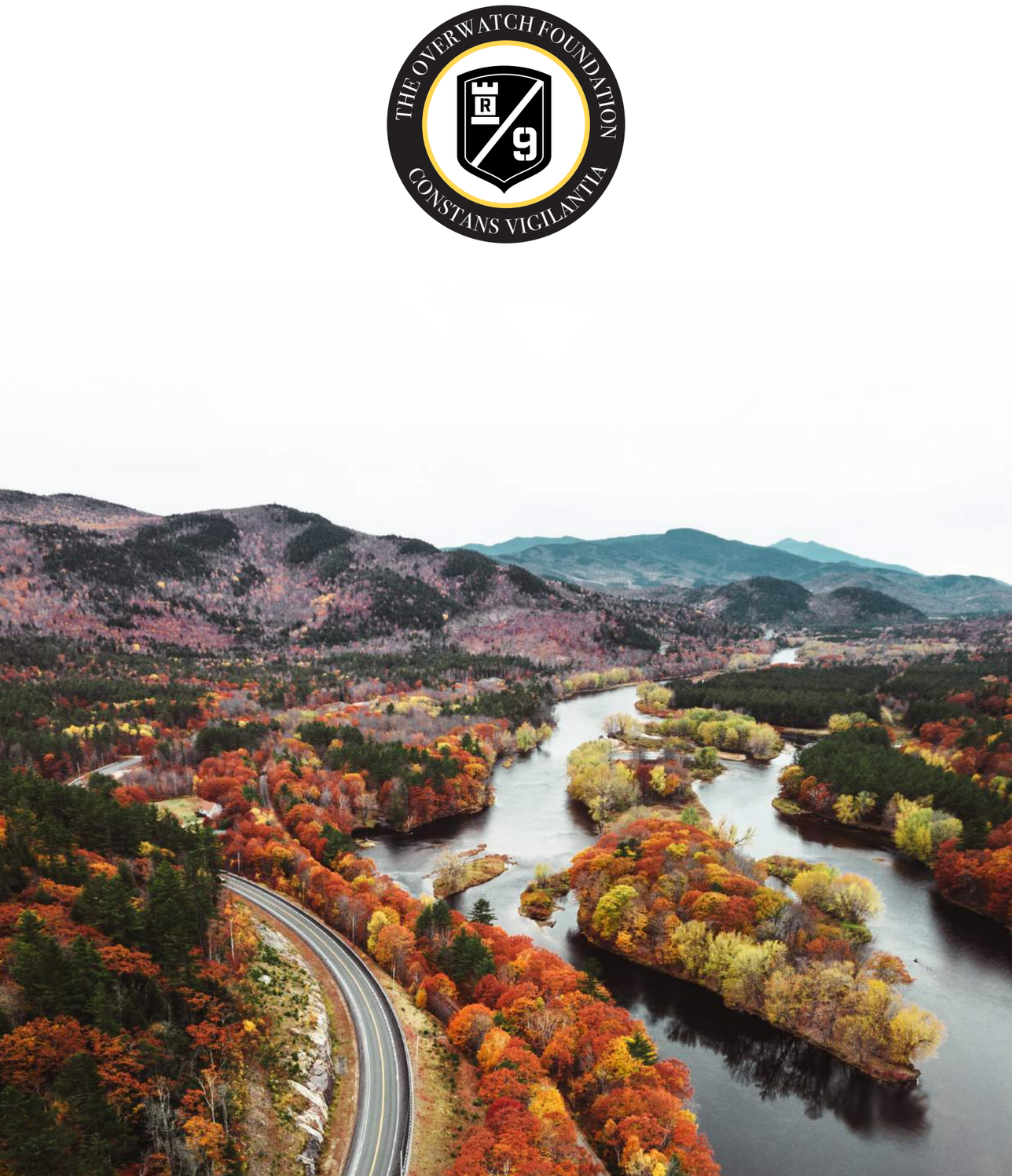
THE OVERWATCH FOUNDATION

CONSTANS VIGILANTIA

Cybersecurity Improvement Services for NH Local Entities Proposal / December 1, 2023



Introduction Letter

Request for Proposal Decision Committee, fellow New Hampshire residents, and believers in a safer New Hampshire:

It is our honor and pleasure to submit this proposal for grant-based funding in accordance with the Request for Proposal Guidelines you have set forth. As New Hampshire business owners, dedicated community members, and believers in the New Hampshire way of solving big problems in effective, streamlined, and financially responsible ways, we are privileged to submit this proposal to you and introduce our NH-based, 501(c)(3) not-for-profit foundation, The Overwatch Foundation. This proposal is the work of countless hours and individuals in New Hampshire–from advisors to our dedicated board–and our partnerships throughout the State. The thoughtfulness of these solutions and this response are credited to them, and stand as a wonderful testament to the strength of character and professionalism that flows through New Hampshire.

As you will learn in detail in this proposal, Overwatch was created–indeed, it was purpose-built–to serve the New Hampshire public sector in the most efficient, timely, and cost-effective way. We exist to provide New Hampshire with a not-for-profit vehicle to deploy capital for the collective security and the cyber safety of our great State. In New Hampshire, we are small but mighty. We are confident you will find this same spirit flows not only through every page of this document, but also through every person in our organization, every mission we undertake, and every solution we deliver.

In this proposal, you will be presented with information on how we will deploy your grant optimally, which is not just a function of us being a not-for-profit foundation. You will learn about our commitment to meet or beat negotiated government pricing on all software, hardware, and services used in this proposal, in addition to our promise never to mark up any of those items. You'll learn about our significant knowledge of State and municipal organizations, and the companies that already serve them. We value these existing relationships, and promise never to use your grant to sell any additional services to those entities, disrupting dozens of established New Hampshire small businesses and creating unfair competition instead of unified teamwork when solving the critical challenges of cybersecurity. Your grant isn't a sales enablement or business development tool, and it should not be used that way to the detriment of the grant outcomes, established relationships, and our valued New Hampshire small businesses.

In addition, we are proud to share in this proposal our deep commitment to supporting transitioning veterans, new students exiting our university system, and those transitioning careers into cybersecurity. By mission, we will target the staffing of our team to be at least 10% of each population. This strategy expands the technical workforce in New Hampshire in addition to creating new jobs for our State's existing technical talent.

Lastly, we are excited to have a chance to discuss our turnkey programs, which we call "in a box" solutions. These programs for .GOV email and domains, and community drinking water cybersecurity truly are turnkey. They come with all the licensing, support, and engineering required to deploy, maintain, and transition the ongoing support to the local entity responsible for it. We are here to solve challenges but also to implement self-sustaining, long-term strategies. We will be here still yet to help along the way after the 3-year horizon. Still, we believe it is critical to the success of this grant program that our NH organizations increase their ability to protect themselves so that we develop the workforce as well as deliver services. Today, many of the proposed grant recipients simply cannot perform these important upgrades on their own. They need us to do the work for them, not just tell them what work they need to do. The time for action is now and your grant recognizes that–but your grant cannot support them forever, nor should it. This proposal addresses that in a thoughtful way that achieves near-term results but sets us up for long-term success.

On behalf of the entire Overwatch Foundation, we look forward to your questions and consideration of this proposal.

Very Respectfully,

Jason J. Sgro
Chairman

Alyssa C. Rosenzweig,
Deputy Director

Table of Contents

PART 1

Welcome to The Overwatch

Our mission is to safeguard the Republic and the People of the United States of America by defending the foundational institutions and infrastructure they rely on.

The Overwatch Foundation ("OVW") is dedicated to protecting the Homeland, United States critical infrastructure, the New Hampshire competitive advantage, and the public trust by providing grant-funded cybersecurity auditing and engineering, infrastructure and software modernization, and workforce development.

OVW is founded on the belief that defending the United States Homeland and Critical Infrastructure is actually the process of defending our homes, our businesses, our vulnerable populations, and the institutional services we rely on. It is about power, clean water, emergency responses, healthcare, and private industry. It is about protecting our State's economic and cultural advantages at home and at large. This is our mission.

To accomplish this, we've built a foundational group of New Hampshire-based leaders who have set aside profit and prestige in the interest of making New Hampshire a safer place to raise a family, start a business, or just enjoy its beauty on a well-deserved vacation for generations to come.

The truth is that our State is under attack. It is under attack by those who seek to disrupt our way of life, sow distrust in our institutions, and prey upon our vulnerable populations. We are here with our partners, donors, and grantors—both local and federal—to meet the challenge of repelling that threat through our 10-year Phase 1 Mission, which evaluates and mitigates cyber threats through "in a box" turnkey programs, cybersecurity education, workforce enablement, and the modernization of critical components of our infrastructure and applications.

New Hampshire's Cyber Defense

A challenging landscape

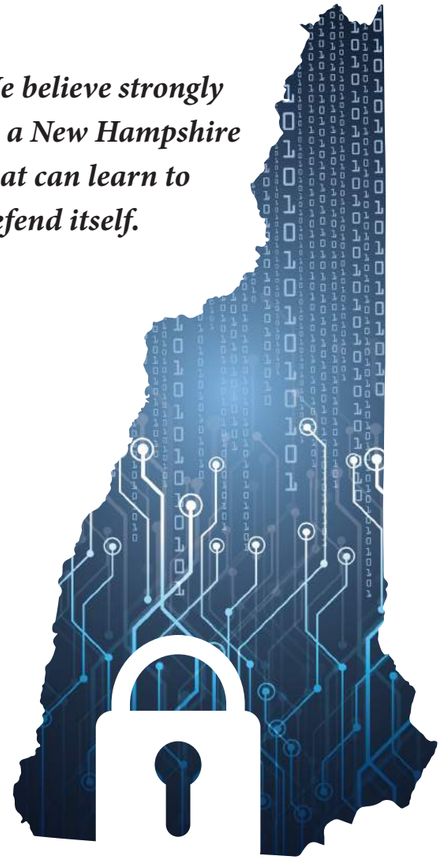
The Overwatch Foundation is built upon a deep understanding of the challenges facing New Hampshire local governments and municipal-serving organizations. We understand that the municipal landscape is one based upon local control. Over 575 entities in New Hampshire qualify for services under these grant proposals, and each one faces challenges unique to their geography, organization type, and the resources available to them. What is not unique is that each of these entities safeguards data entrusted to them by the residents of New Hampshire and each one of them provides an essential service. Further, whether it's to provide clean and available drinking water or emergency services, motor vehicle registrations, or essential town functions, these organizations share a common financial challenge. This proposal outlines a strategy that not only assists qualifying entities in planning to protect their email systems, web systems, and drinking water infrastructure but also provides turnkey solutions (including the engineering work required to actually get the job done).

However, this work cannot be approached and managed in a traditional way. We know this from years of direct experience. The high level of variation in these environments requires the type of deep knowledge working with municipal entities that the Overwatch leadership has spent the better part of a decade learning. We've been in the trenches of the cybersecurity battle in New Hampshire working alongside these organizations for years. Our deep appreciation for how they work and the challenges they face is a key differentiator in our ability to understand what strategies work and what strategies fail.

In order to properly plan a cyber defense program at a State level, we feel it is important to raise four baseline understandings. These are:

1 The people who manage our cities, towns, public works, and drinking water systems should not be provided with a solution that must be managed for them indefinitely. We believe it is critical that our initial service carry drinking water system upgrades, and .GOV email and web enhancements for a period of 3 years following the implementation at no additional cost to the municipality. We believe it is critical to provide all licensing required upfront. We believe strongly in a New Hampshire that can learn to defend itself. A key part of our proposal is a multiyear program to support, teach, and train these entities to maintain for themselves and continually develop the workforce required to do just that.

We believe strongly in a New Hampshire that can learn to defend itself.



2 Over 54% of the State of New Hampshire has a meaningful and established relationship with a New Hampshire-based small business IT provider that helps with day-to-day operations and technology projects. We believe a not-for-profit organization that is entirely grant focused and respects these relationships as a cornerstone of how New Hampshire manages technology today is a critical component to this strategy. Our leadership has learned by working with municipalities for the better part of a decade that these small businesses are critical to getting work done. Because The Overwatch Foundation poses no threat to the existing relationships, and because we have no designs to supplant them as managed service providers, our strategy will be able to work collaboratively with them–not only during the project but also in the ongoing support of these enhancements. While they will not be directly involved in the engineering efforts supported by this grant, they will be instrumental in ensuring smooth transitions. In short, these relationships are critical to the success of New Hampshire and The Overwatch Foundation respects that. We believe that if these grant-supported initiatives are allowed to be used as a business development tool for a for-profit organization or one that competes with managed service providers, the disruption caused will be a detriment not only to the outcomes of this program, but to New Hampshire itself.

3 Our ability to maximize return on investment is unmatched. We are a 501(c)(3) not-for-profit foundation created with the specific purpose of maximizing the transference of grant programs and dollars into New Hampshire's future. We have almost no overheads and our primary costs are attributed to engineering talent and compensation. This means every dollar entrusted to us can do its job for New Hampshire; it's not lost to profit margins, federal taxes, or markups on equipment, software licensing, marketing, or business development expenses. Our organization does not serve non-government customers. This means entities we serve in this program get our full attention.

4 Our relationships with The New Hampshire Public Risk Management Exchange, The New Hampshire Municipal Cyber Defense Program, and the experience of our leadership implementing state-sized cyber initiatives allows us to work together with those managing cyber risk in New Hampshire at all levels. No one organization can achieve the best outcomes of these two important grant programs on their own, and we wouldn't ever try to do that. The most important parts of executing these programs may be devising the correct vision or the outcome and strongly executing on that vision, but the true force multiplier will always be collaboration across the amazing agencies, teams, and organizations that serve New Hampshire. This is a "do it together" strategy. It is collaborative, cooperative, focused on New Hampshire. We built The Overwatch Foundation to set aside profit, prestige, and personal interest in the service of our home. We hope you enjoy the vision and implementation outlined in the following sections.

Key People and Partnerships

“Small but mighty” is the New Hampshire Way

No organization of any size can accomplish state-wide impact alone. Cybersecurity is a large and complicated battlefield, and success will require strong partnerships with key individuals and entities across the State. Over the last 5 years, the founders and board members of The Overwatch Foundation have worked to create these partnerships and understand the risks ahead, positioning us strongly to lead these initiatives. Below we present the key individuals affiliated with the Foundation. Not listed, but certainly part of our “at large” team across the State, are countless other dedicated individuals and organizations in NH that we have the distinct honor of working beside—and plan to continue to do so for decades to come.

Jason J. Sgro

Chairman

Leading New Hampshire’s largest dedicated municipal incident response efforts, Jason serves as Sr. Partner, Business Strategy, and Head of Cybersecurity & Human Privacy at The ATOM Group, headquartered in Portsmouth, NH. He is the current President of the FBI’s InfraGard Program in New Hampshire, and serves as the Director of ATOM’s New Hampshire Office for Cooperation in Cybersecurity which provides training and emergency response services in partnership with the NH Public Risk Management Exchange (Primex3). A lifelong native of New Hampshire, and alumni of the Union Leader’s 40 Under Forty, Jason is a strategist at heart, comprised of equal parts speaker, founder, evangelist, coach, and operator. He has secured and advised public and private entities throughout New Hampshire and is widely recognized for his contributions toward building a future we can trust.

Kevin M. O’Shea, Esq.

Director, Vice Chair, Rook

Attorney O’Shea is a lawyer and equity member at Sulloway & Hollis, PLLC. He concentrates his practice on commercial litigation, including contract disputes, and defense of manufacturers warranties. A significant portion of his practice focuses on the Internet and technology law, including privacy and domain registration disputes. In 2022, Kevin earned the Certified Information Privacy Professional/United States (CIPP/US) designation from the International Association of Privacy Professionals. In complex litigation cases, he is often called upon to spearhead discovery efforts in connection with electronically stored information (ESI) and the related spoliation motion practice

Kevin serves as the firm’s chair of both Sulloway’s Technology Committee and Ethics Committee. In 2018, Kevin was named to the Thomson Reuters’ Super Lawyer® list for Business Litigation and has been included on the list for the years 2021, 2022 and 2023.

Outside of work, Kevin has been an adjunct professor at the University of New Hampshire Franklin Pierce School of Law, a Commissioner on the New Hampshire Higher Education Commission, and a Panelist for the National Endowment for the Arts, National Heritage Fellowships. In 2023, he was awarded the Distinguished Eagle Scout Award to recognize Eagle Scouts who have achieved extraordinary national-level recognition, fame, or eminence within their profession and/or service to the nation and have a strong record of voluntary service to their community. Prior to entering law school, Kevin worked for more than 10 years as a musical agent and manager for Emmy® and Grammy® nominated artists.

Vincent M. Chambers

Director, Secretary, Rook / National Security Subcommittee (Chair)

Vince’s career has focused on service to the Country. Vince started his professional career as an active-duty Army Officer, serving nine years in both CONUS and OCONUS assignments. Vince attained the rank of Captain and served as a Platoon Leader, Company Commander, and in various Army staff positions. After his military service, Vince was appointed and continues to serve as a Special Agent with the Federal Bureau of Investigation. Vince has served for over 19 years as an FBI Special Agent leading complex investigations into violations of the Foreign Corrupt Practices Act, international narcotics trafficking, counter-terrorism, domestic terrorism, inner-city gang violence, white-collar crime, and computer intrusion crimes. Vince has a passion for upholding the Constitution of the United States and protecting the people of America.

Vince earned a Bachelor of Arts in International Relations from Norwich University, The Military College of Vermont (Magna Cum Laude) in 1994 and is scheduled to graduate in December 2023 with a Master of Science in Cybersecurity, Policy, and Governance from Boston College.

When Vince is not continuing his education in cybersecurity, he focuses his time on his family, jiu-jitsu, scuba diving, “Frankie” the Boykin Spaniel, triathlons, and traveling.

Alyssa C. Rosenzweig, MSc.

Director, Rook / Inaugural Deputy Director (Operating Executive)

Alyssa’s career is dedicated to how technology can transform lives and serve people—from the most basic technological advancements to artificial organs to cybersecurity. Alyssa began this pursuit with the study of both human behavior and computer science, and the possibilities that exist between them, earning dual Bachelor’s degrees in Psychology and in Applied Computer Science from the University of Pennsylvania. She further pursued this vocation at the University of Toronto at the intersection of both fields, earning a Master’s of Science, specializing in Human-Computer Interaction for chronic illness and health behavior change.

Once out of academia, her career has been a winding one, ranging from medical device human factors to software testing to IT application support to US Intellectual Property strategy; she’s turned over every stone towards developing and designing the best application of technology for human performance and optimization. These efforts led to her selection in the Union Leader’s 40 Under Forty and Leadership New Hampshire’s programs.

Alyssa continues to be involved in a variety of initiatives focused on how technology can improve lives. She is a Partner at the New Hampshire technology consulting firm, ATOM, running operations and the Experience practice. More recently, she has joined our nation’s cybersecurity defense initiatives as New Hampshire’s Healthcare Sector Chief for InfraGard, the FBI’s public-private partnership organization.

When she’s not serving in these capacities, you can find Alyssa with her community therapy dog, Lana, spreading joy to everyone they meet; supporting women with chronic health conditions through her company, GRIT + GRACE; getting her sweat on at her favorite gym, Seacoast Athletics; or cherishing New Hampshire’s seacoast and great outdoors.

Matthew Chepeleff

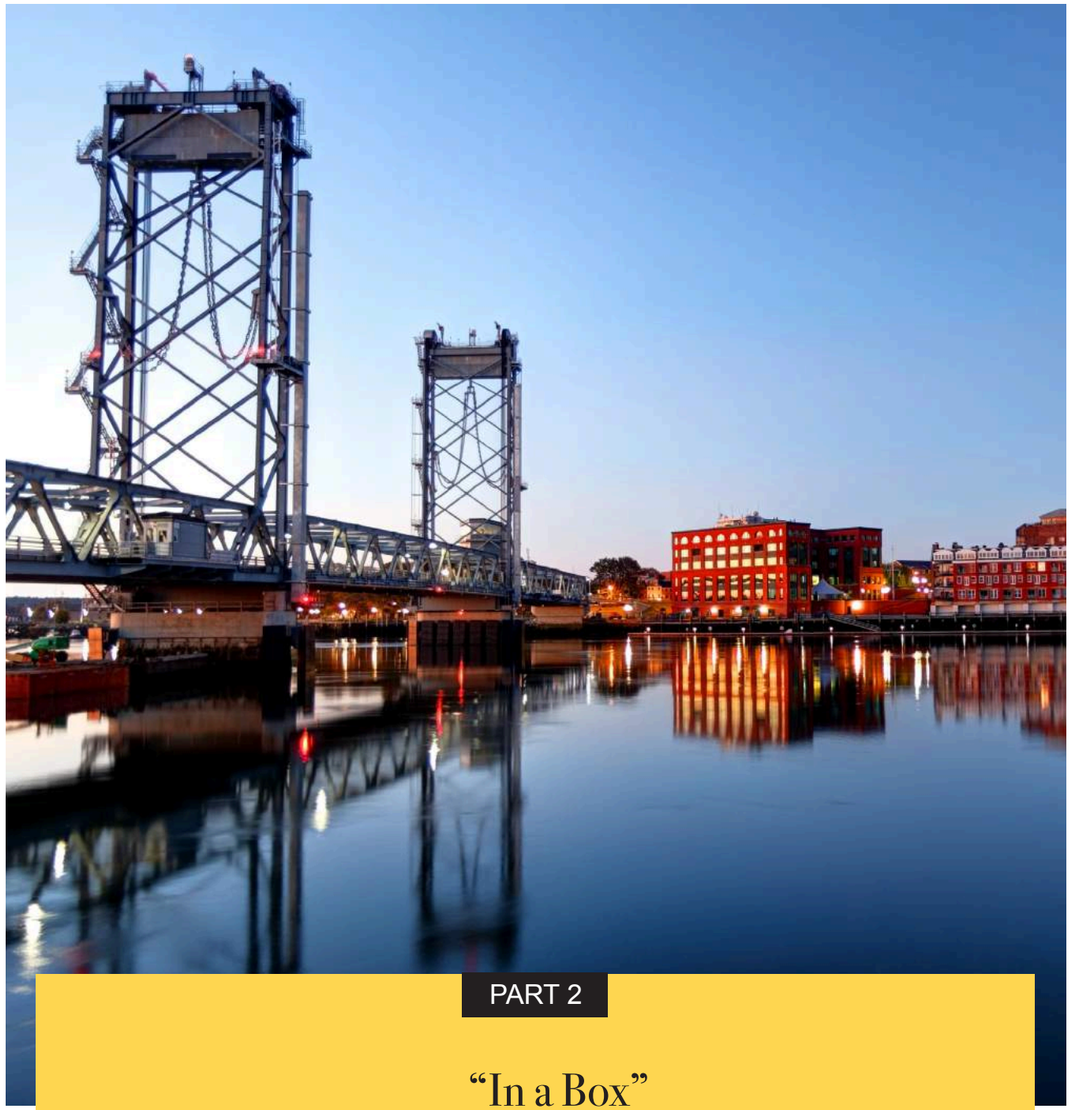
Director, Treasurer, Rook / National Security Subcommittee

Matt spent the first 20 years of his career in the space where technology and business overlap. To this day, he keeps one foot deep in technology — right in the code itself — and the other in the business world looking at organizations and their strategy, business model, and P&L. Matt's foray into the business world grew from entrepreneurial roots in SaaS startups.

Driven by curiosity and love for building things, Matt believes passionately that technology should always be used purposefully and pragmatically. Over the past 5 years Matt has focused on building and leading teams in addition to building products. His focus on performance and value in a product has transitioned into a focus on developing people and organizations.

Matt currently serves as partner and leads ATOM's software development practice, focusing on mobile, web, and enterprise software for SMBs. His primary goal is ensuring the software we ship either delivers or enables key business objectives. This results in successful projects, satisfied clients, and business growth. Matt's experience ranges from technical product development for 3-25 person teams to product integrations, acquisitions, business model development, and team growth/reorganization. This experience has been gained in small, bootstrapped startups; in rapid-growth, venture funded startups; and in private SMBs across a range of verticals.

In 2019, Matt joined the board as a founding director of the AFMS Foundation, a not-for-profit in Connecticut focusing on Advocating for Families with Multiple Sclerosis. Matt is an entrepreneur at heart and technologist in practice. He keeps focus on the intersection of technology and the organizations that use it — the ideal vantage point to deliver secure solutions and drive growth.



PART 2

"In a Box"

Developing Turnkey Solutions

The .GOV "In a Box" is a turnkey program designed to address one of New Hampshire's top cyber vulnerabilities: impersonation and insecure email systems. However, while email addresses may be the first thing that comes to mind, the .GOV program isn't just about email or safeguarding domain impersonation. It also safeguards against public disinformation campaigns, helps safeguard our election process, and easily recognizes official sources of information for the public through websites and applications. In the next section we describe the details of our approach.

.GOV “In a Box”

Turnkey anti-impersonation protection

When planning this approach, we break the .GOV “In a Box” program down into four components. It is critical that these are all “turnkey” initiatives, meaning that when Overwatch finishes the engagement and begins the 3-year period of support, we will ensure the entity is fully functional using the new technology with no additional investment in either money, time, or training.

The four components of this solution are: email domains, web hosting, printed materials, and training. You may be surprised that we included printed materials in what seems to be a technical project. That is because, as is true throughout New Hampshire, the reason for not doing a technical project may be as simple as “we’ve already invested money in business cards that have our old email on them.” We respect this mindset, but also recognize that it inappropriately favors small expenses over important cyber protections. Nevertheless, our approach is one founded in spending years working with municipal entities and responding to their feedback. As a result, we’ve incorporated that into our program to reduce friction and increase efficacy wherever possible.

Our approach begins with readiness. Not every qualifying entity is currently prepared for the steps and disruptions required to migrate to a .GOV domain email system and web hosting service. We will provide dedicated resources to evaluate readiness and work with entities to load the project and engineering pipeline for maximum efficiency. It is important that we approach this first step carefully. On one hand, our staff will consult with entities that have signaled they are interested in the .GOV program through one of our mechanisms for collecting the demand signal (explanatory web videos, web forms, email campaigns, and mail campaigns), and help them complete a formalized readiness assessment. In certain cases, entities may be requested to work with us to complete important prep work before we engage in formal planning, while other entities may be fully prepared and ready to go. What we know for sure is that starting email transitions with entities that are unprepared or ones that have not considered all of the readiness criteria will cause project delays, extended timelines, and wasted dollars. Our readiness auditing approach avoids this without causing delays to the start of services. Critically, we intend to have stakeholders in DoIT and DES collaborate with us in prioritizing assessments, as well as utilize previous assessments done by private companies, CISA, or other federal agencies to efficiently ensure the deepest impact.

> ***When Overwatch finishes the engagement and begins the 3-year support period, we will ensure the entity is fully functional with no additional investment needed in either money, time, or training.***

In the planning phase of the project we acknowledge that different entities will begin at different places. Some may have industry standard and well-supported email and web systems that house large amounts of data or complex applications, while others may have a single “myfairpoint.net” (or equivalent) email address that needs to be rehomed in modern location and technology as a .GOV domain. The variation of email and web hosting platforms that exist in New Hampshire cannot be understated or underestimated. Further, we will identify the applications, emails, technologies, mobile devices, and any other systems or printed materials that need to be addressed in the project. Understanding these variations and diverse needs are critical and integral to the design of our workflow. Notably, the .GOV “In a Box” turnkey solution does not require a set starting point. We will support a multitude of requirement configurations and pathways to move forward from any of the variations we identify. You’ll see a sample workflow diagram on the next pages that will give you a high-level idea of the steps we envision.

At the end of the readiness assessment, and evaluation of key project and success metrics to define the project plan, we will require a formal sign-off on the scope of services before we begin engineering so that we can align resources and manage a state-wide program. These sign-offs will also allow you to have full visibility into the workload, progress, and efficiency of the programs.

The engineering phase will encompass all parts of the transition. From registering the domains to migrating email, setting up new hosting tenants, helping users reconfigure mobile devices, and providing modern security solutions, Overwatch will take care of it all. When we say “turnkey,” we mean turnkey. Further, we also recognize that the opportunity exists to modernize email and web hosting for New Hampshire while implementing this program. For this reason, qualifying entities will have the choice to maintain internal hosting (as long as it is still on a manufacturer-supported version). Still, they will be encouraged to migrate email to Microsoft 365 or Google GSuite cloud platforms, with web hosting remaining at third-party providers or migrating to Microsoft Azure Cloud, Google Cloud, or Amazon Web Services. We believe that the standardization of these environments on modern platforms is critical to our state’s long-term security. Importantly, every entity will own and retain full control over its new environment. While we will use bulk pricing to drive costs down, Overwatch will not own any part of this infrastructure. We’re not here to sell licensing and services to these entities, we’re here to help them. We pledge to never mark up software or hardware, and consistently achieve New Hampshire government-negotiated pricing or better on all services.

> ***To efficiently ensure the deepest impact, we intend to have stakeholders in DoIT and DES collaborate with us in prioritizing assessments, as well as utilize previous assessments done by private companies, CISA, or other federal agencies.***

Following a successful transition, where all email is migrated, new accounts are set up, and users are correctly and fully migrated to new modern platforms with security auditing completed and using .GOV domains, we will begin an important 3-year journey toward training and migration of these services onto local support. It is our plan to provide support for these email and web hosting service environments for up to 3 years during this training. Support will include the creation of a helpdesk that will work on configuration changes, security updates, and second-level support for issues. We will freely share administrative control of the environment with the entity who owns the email and web systems, and their managed service provider or internal IT team. The day-to-day use and administration of small tasks, such as setting up a new email account or making a web page modification, will stay with the entity and their IT support staff, while larger issues, security changes, and level two support will reach the Overwatch Helpdesk.

Key Takeaways for .GOV “In a Box”

1. Overwatch will provide a truly turnkey service with a 3-year horizon that allows for training and transfer of management, always maintaining ownership, licensing, and administrative access with the entity we serve.
2. Overwatch will provide these services without competing unfairly or disrupting relationships with more than half the State’s qualifying entities that rely on managed service providers for day-to-day IT. This initiative is not a business development vehicle.
3. We have a multiphase plan to efficiently engage with entities that want to pursue a .GOV migration that gives you flexibility, the ability to prioritize with us, and transparency into the performance of the program.
4. Our ability to generate return on investment is unmatched. We will never make money on hardware, software licenses, or labor. We’re a not-for-profit. All costs go directly to engineering salaries and compensation, managing the grant, and the systems required to deliver the grant. We’re transitioning every dollar possible into benefit for New Hampshire, not benefit for ourselves.

For more information on our approach to the .GOV “In a Box” program, please review the diagram on the next page.

Key Deliverables

- 3 years of support
- Secure email
- Secure hosting
- Secure web applications
- Updated business cards and letterhead

.GOV Migration Workflow Diagram

1

ASSESS READINESS

- Assess readiness and scope of migration in cooperation with existing programs at Primex, CISA, and existing private sector assessments.

.....

- Perform assessment, if none exist.

2

FACILITATE KEY DECISIONS

- Assist in making key decisions (e.g., What is the new domain name?). This involves working with boards and elected officials.

.....

- Evaluate providers and readiness (including internet capability, and training and technology needs) for migration to ensure long-term outcomes.

.....

- Create migration project plan.

3

LEAD MIGRATION EFFORT

- Migrate email to Google or O365.

.....

- Migrate all existing data and accounts.

.....

- Assist end users in migrating desktops, phones, and other devices.

.....

- Update websites, performing redirects and changing content where needed.

4

CONFIGURE SUPPORT SYSTEMS

- Provide 3-year licenses for all technology and a helpdesk to call if issues arise with the service.

.....

- Perform security configurations, including updating and improving security baselines and known issues.

.....

- Configure backups and capabilities for right-to-know requests.

5

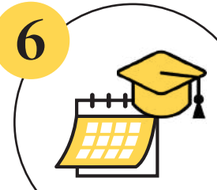
SUPPORT BUSINESS ACTIVITIES

- Provide financial support for updating business cards and letterhead.

.....

- Record data for demographic use and outcome measurement. This data may also be used for decision-making and risk evaluation later, if desired.

6



GUIDE TRANSITION

Transition system maintenance responsibility through continuous training on new technology over the course of 3 years of support services to enable an engaged and effective workforce.

Community Water Cybersecurity "In a Box"

Turnkey protection for critical infrastructure

Our Community Drinking Water "In a Box" program is based on three basic elements: cybersecurity best practices, hardware and software "in a box," and ongoing training and support. By combining elements of pre-fabricated solutions with the unique cybersecurity requirements of each drinking water system, we are able to devise a cost-effective and scalable solution for drinking water cybersecurity.

We understand that the Cybersecurity Infrastructure Security Agency (CISA) has already completed numerous drinking water assessments and we will aim to leverage this body of work in our first phase of establishing readiness to receive the "in a box" program. In cases where water systems are not already audited, we will perform the readiness assessment. The assessment will address three key areas of focus.

1. Cybersecurity auditing for IT and OT systems.
2. Physical security of the water system infrastructure (both facilities and pump stations).
3. The age and makeup of the SCADA equipment, including manufacturer supportability, best practices, and current SCADA control and data historian software.
4. Environmental protections, including firewall, computing systems, networking equipment, endpoint protection, and VPN remote connectivity needs. This assessment will allow us to pull the right prefabricated components from our hardware and software "in a box" plans, and customize them to the specific needs of the environment.

> ***Drinking water is a life-sustaining resource for New Hampshire. We must evaluate all aspects of proposed changes and collaborate with key parties to ensure our deployments are planned with the utmost regard for the safety and availability of our water systems.***

Another key part of readiness will include working with the SCADA provider that installed the environment. There are currently three major providers, and numerous smaller providers and manufacturers of SCADA systems that cover most of the community drinking water system in New Hampshire. During our readiness, we will engage with the SCADA provider to establish:

1. Is there a manual operation mode, redundancy, or fault tolerance in the environment such that the work being done during this program will not negatively impact the availability or safety of the drinking water? This assessment will be done with the SCADA provider and those responsible for the drinking water systems, and these criteria must be met before work can be accomplished.
2. What level of support is available from the manufacturer of the SCADA system (hardware, firmware, and control software). In certain cases, an environment may be too old to receive updates in a key category or the overall system may be better served through a significant SCADA upgrade. SCADA technologies cannot be handled in the way most traditional IT systems are approached. Our staff–which includes the role of Critical Infrastructure Cybersecurity Technicians who specialize in cybersecurity, and the key differences and challenges SCADA systems represent–are central to the engineering work required to upgrade our water facilities. We will work with local technology and community leaders to evaluate the best path forward based on the findings from the readiness assessment and emergency operations preparedness.

As all of the readiness evaluations and scope are finalized for a project, the delivery of the hardware and software for the upgrade will be customized and staged in parallel. These systems will include (as specified by the evaluation) a web application-controlled firewall from a major manufacturer that can be supported over the performance period of the grant, managed LAN network hardware, endpoint protection for SCADA controllers, 2-4 new SCADA controller hardware systems, and up to four remote access tablets enabled with VPN and 2FA for remote system maintenance (a key function needed to maintain this critical infrastructure service).

All software licensing and hardware support will be pre-purchased by Overwatch, allowing us to leverage government discounts and bulk ordering discounts for all items. As explained later in the proposal, to maximize the impact of the grant, we pledge to meet or beat all existing NH negotiated rates on similar software and hardware, and to never mark up any hardware or software.

The implementation of these items will occur over a dedicated, onsite installation and go-live window which may require staffing of the facilities during the installation period. We will cooperate with SCADA installers or OEM manufacturers to perform required software updates to SCADA controllers and device firmware. This cost will be paid as part of delivering this service to the receiving entity.

Post-installation, a cybersecurity analysis will be conducted in the environment and results will be provided to all key stakeholders. The recipient will be entitled to up to 3 years of support following the go-live of the new enhancements, which will provide Level Two support items like firewall troubleshooting, remote access issues, or hardware issues with the networking gear Overwatch deploys. Hardware will be 100% covered under manufacturer support. In addition to technical support, recipients will be entitled to unlimited training for SCADA engineers and community drinking water system workers regarding cybersecurity general practices, and specific training on how to use 2FA and the remote access tablets safely. This training will be updated on a yearly basis. The goal is to train the workforce in addition to solving the immediate cybersecurity concerns. Technology deployments that do not include significant training efforts often fail to meet their intended outcomes long term, so our program design better ensures the intended goal of safeguarding New Hampshire.

Of course, any entity wishing to exit the 3-year training and support period, change provider, train a managed service provider to take over support, or discontinue using the solution altogether is entirely free to do so at any time. Overwatch will issue a contract to govern terms and scope of support with each entity, but this contract will not include any cost or duration commitment to the entity. We're here to help, not lock anyone in!

Key Takeaways for Community Water Cybersecurity "In a Box"

1. Assessments will be additive, not duplicative. They will be focused on readiness and scope, but more importantly, on maintaining the safety and availability of the community drinking water systems during our program deployment. Safety is top priority.
2. Hardware and software will be purchased upfront at scale, with no markups, for the full 3-year period of support. This will reduce costs. The standardization of equipment will aid managed service providers and workforce members in supporting these systems long term.
3. This work will include close coordination with SCADA system OEMs and installers throughout New Hampshire. It will focus on software, hardware, network, firewall, remote access VPN, physical security, endpoint protection, and cybersecurity best practices in each environment. While we will standardize as much as possible, each system will be different in key ways.
4. Overwatch will support these installations for 3 years beyond the installation date but no entity will be locked into a contract or billed directly for these services.
5. Unlimited training will be provided to drinking water employees on the systems we implement, and on cybersecurity best practices both directly and in cooperation with the existing Municipal Cyber Defense Program Grant.

For more information on our approach to the Community Water Cybersecurity program, please review the diagram on the next page.

Key Deliverables

- 3 years of support
- Community-owned software and hardware
- Secure SCADA systems
- Remote access tablets

Community Water Cybersecurity Workflow Diagram

1

ASSESS READINESS

- Assess readiness in cooperation with existing programs at Primex, CISA, and existing private sector assessments.
- Perform assessment, if none exist.
- Identify SCADA equipment in scope (and third-party provider).
- Create initial project plan.

2

ENSURE EMERGENCY OPERATIONS

Define an Emergency Operations Plan for use during project, as a key part of readiness is making sure all emergency operations can be covered in the case of an issue with updates.

3

BUILD KEY TECHNOLOGY

- Build SCADA controllers and change them over.
- Build firewall and remote connectivity capability.
- Build remote connectivity iPads (eliminating personal phone use)

4

SECURE ENVIRONMENT

- Create an Internet Network Security Plan and implement baseline security updates.
- Implement endpoint protection on all applicable systems in the SCADA networks.
- Contract with SCADA installer to perform PLC and firmware updates, as required by assessment.

5

TEST SOLUTION

- Perform full testing and validation of the environment and all new hardware.
- Provide results of post-installation cybersecurity analysis.

6

GUIDE TRANSITION

Transition system maintenance responsibility through continuous training on new technology over the course of 3 years of support services to enable an engaged and effective workforce.

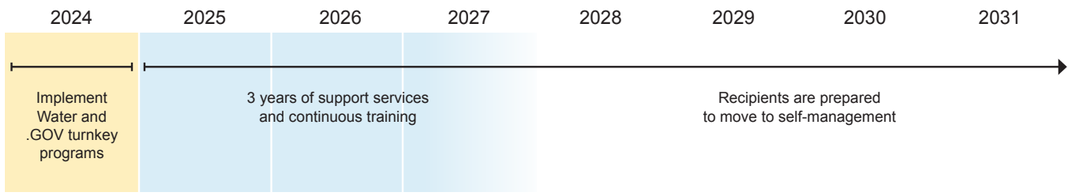
The 3-Year Horizon

Supporting long-term success

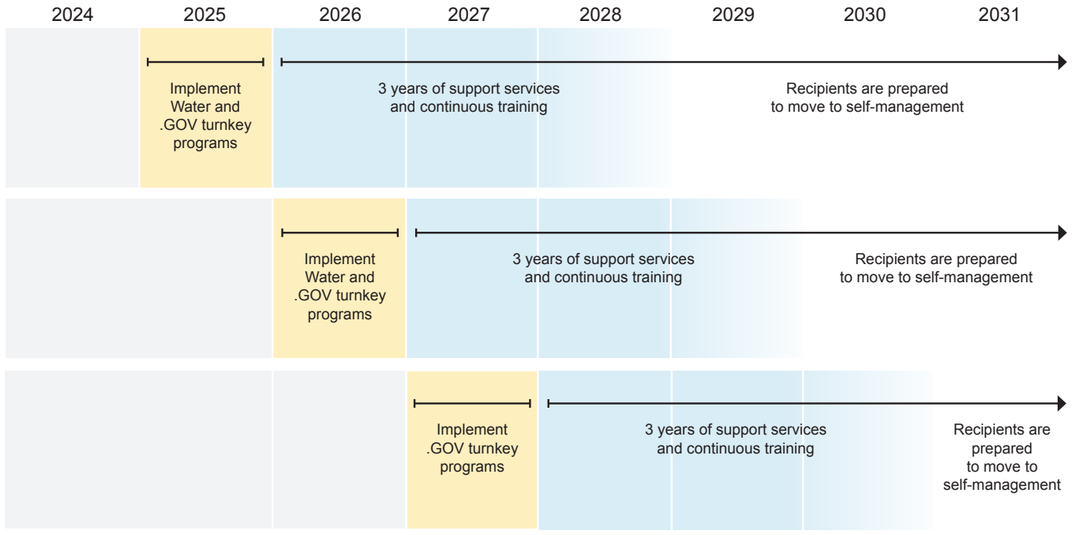
While the scope of the initial engineering work is planned to be one year, we want to ensure system adoption and autonomy for recipients. As a result, we envision including a 3-year horizon of support services as part of this proposal to allow recipients the opportunity to embrace these enhancements without the fear, resistance, or the financial burden of supporting them initially; these are all issues we've encountered through our significant work throughout the State, so we want to proactively be prepared to counter them. Further, if a recipient needs longer, we're open to discussing extending this to continue to support the State.

The diagram below illustrates at a high-level the key initiatives and statuses of the grant delivery for both the current scope and potential renewal year considerations, noting our reach could extend as far as 2031 with these investments.

Initial Grant Timeline



Renewal Year Timelines



PART 3

Program Methodology and Financial Considerations

There are countless things to consider when choosing to invest taxpayer dollars in any large-scale initiative. Alongside the implementation approach and methodology, investment breakdowns are certainly of critical importance. Both of these programs are some of the first of their kind and, as a result, we approach this first year with a pilot mindset.

From a methodology perspective, we will look at the costs to successfully execute the programs with entities that have both greater and less readiness (with collaboration from DoIT and DES) to help us build a stronger understanding of what it takes for progress toward both these initiatives.

From a cost perspective, what we propose on the following pages represent not fixed budget line items, but our preliminary, pre-pilot estimated breakdowns from years of providing services to local entities in New Hampshire. What we also know from this experience, though, is that every entity has its unique needs that need to be carefully considered. Our pilot mindset and program workflows allow for this adaptability because true impact and effectiveness is of utmost importance for our work, so the investment fluidity will follow suit.

Know that, no matter what, Overwatch approaches things from the not-for-profit foundation perspective with our "no mark up pledge" on labor, software, and hardware. We are not in the business of building recurring revenue streams by implementing solutions that will need forever maintenance and licensing through us. We also have a commitment to meet or beat negotiated government pricing wherever possible. We will always provide transparency into our spend and will welcome your feedback if anything seems awry. We plan to tune our budgets in subsequent years, if grant renewal is provided to Overwatch. We are in this to protect not only the people of New Hampshire, but also taxpayer dollars.

Approach and Methodology

Our approach and methodology are focused on quickly getting these programs up-and-running, and making timely adjustments to our implementation plans and workflow as we proceed into year one. Overall, we will take a pilot-first methodology for both programs beginning in year one that, if we are granted renewals, we can iterate on for follow-up grant years. This methodology is critical because every entity will be materially different. At this stage in the proposal, it is impossible to firmly grasp the variation, time, and exact costs of each implementation. From years of working with these entities, we know we will need to develop a way of addressing these unknowns and efficiently working through them.

Each organization, regardless of which program they sign up for, will be initially evaluated using "t-shirt sizing" of Small, Medium, or Large (S, M, L) based on the cybersecurity readiness of the organization, the number of employees in the environments, and the estimated duration of the work required to complete the workflows discussed earlier in the proposal. During the assessment phase, these assumptions will be formalized and a label will be given to each qualifying entity that has completed an assessment.

To focus our work initially, we will curate ten (10) entities for the first implementations. For the .GOV program, we will partner with DoIT to select three (3) priority recipients, two small and one medium; we will do the same with DES for the community water cybersecurity program. The Overwatch Foundation will additionally select two (2) small, one (1) medium, and one (1) large entity to serve. These ten will make up the "pilot group."

> ***Our approach and methodology are focused on quickly getting these programs up-and-running, and making timely adjustments to our implementation plans and workflow as we proceed into year one.***

The purpose of the pilot is to refine the cost, timeline, and any implementation workflow changes required in order to streamline the delivery of this proposal. We seek to begin making impact right away, so even with this pilot mindset, we will still have services beginning within 30 days of acceptance of this proposal and initial funding. We estimate the pilot program to take up to 90 days. However, this time will be an invaluable investment in the future of the programs. Following the pilot, all costs associated with these programs will be refined for the duration of the grant performance period.

Our pilot program will also allow us to identify the time and human resources required to execute the S, M, and L versions of both programs. This will drive our staffing plan. Engineering and project management talent at Overwatch will consist of individuals who are equivalent in salary (+/-10%) to similar roles paid by the State of New Hampshire. The staffing plan in these programs will be 100% dedicated to these grant programs and will not be used on any other customer or project.

After the pilot program is complete, we will establish a cadence for accepting and assessing new recipient organizations, and work with you to prioritize them appropriately in a monthly update meeting. We will publish ongoing hardware and software costs, and completed status on a quarterly basis (or at your request) and will provide you with feedback from the organizations about how the programs are delivered for consistent improvement cycles.

While described in detail in the previous sections, our overall approach is grounded in "readiness" assessments to ensure delays are not caused by starting work on unready organizations. We will leverage "in a box" turnkey solutions that will offer immediate technical and cybersecurity risk improvements complete with up to 3 years of ongoing support and training. This approach, which leverages bulk buying power, limits delivery costs from salary, and leverages the knowledge and experience of a group of cross-functional leaders who know these entities well, is the key to transitioning from a pilot-based approach to a full-scale, statewide, solution quickly.

Preliminary Program Cost Proposals

We ground these two program cost proposals on information gained from organizations in New Hampshire that have done similar projects, as well as our awareness of third-party government software and hardware pricing. Where possible, items will be purchased in bulk, and will include licensing and support for 3 years. These are preliminary estimates, though, that will be refined once the pilot is complete. Regardless, the cost per implementation will vary based on organization size (S, M, L), and overall readiness state and implementation requirements. However, for the sake of example, we illustrate below program cost proposals for an entity that was assessed to be a Medium.

Pre-Pilot .GOV Migration Cost Proposal

The initial estimated budget range for Small, Medium, and Large organizations is $7,500, $25,000, and $50,000, respectively–although it should be noted that extremely small organizations will cost considerably less. This cost will vary most substantially based on the choice to utilize Google services versus Microsoft services, and whether sufficiently secure email hosting is already available. The migration time for accounts and web applications can also be considerable. If a recipient is already satisfied with their current hosting service, as long as it can pass a standard cybersecurity evaluation, the cost of this program will drop significantly. (This will be explored thoroughly in the pilot year.) The below breakdown is for a Medium entity (~50 employees) that does not have cloud-based or secure local email and web hosting services.

Key Service/Activity	Estimated Budget
Readiness Assessment	$1,900
2FA Tokens	$1,500
Direct Costs to Third-Party MSP Support	$5,000
Email and Website Transition Services*	$5,000 - $10,000
• If Microsoft O365 (with 2FA) is selected	$7,500 annually
• If Google (with 2FA) is selected	$4,000 annually
Printing Services for Letterhead and Business Cards	$1,250
3 Years of Ongoing Support and Training Materials	$9,500

* *For cloud email services, Google is preferred based on cost, but Microsoft is acceptable.*

Pre-Pilot Community Water Cybersecurity Cost Proposal

The initial estimated budget range for Small, Medium, and Large organizations is $25,000, $50,000, and $75,000, respectively–although it should be noted that extremely small organizations will cost considerably less. It should also be noted that most of this cost goes directly to SCADA updates and equipment, and not to services. We illustrate the below estimates for a Medium entity that does not already have a complete assessment.

Key Service/Activity	Estimated Budget
Readiness Assessment	$1,900
Hardware (includes firewall, VPN, switching hardware, two (2) SCADA controllers, and up to four (4) tablets for remote connectivity)	$10,000 - $16,000
Software (includes endpoint protection, monitoring software, and firewall licensing)	$2,500 - $3,500
SCADA Security Replacements and Updates	$20,000
Direct Costs to Third-Party SCADA Installers	$5,000
3 Years of Ongoing Support and Training Materials	$7,500

Return on Investment

As fellow residents of New Hampshire, it's important to us to see our tax dollars spent wisely. While simple in explanation, the significance of these three concepts below is not to be underestimated, so we dedicate a full page to our core commitments to responsibly spending taxpayer funds. A not-for-profit organization is the smartest, most effective way to deploy taxpayer dollars and gain the greatest return on investment.

Maximizing New Hampshire dollars with not-for-profit foundation approach.

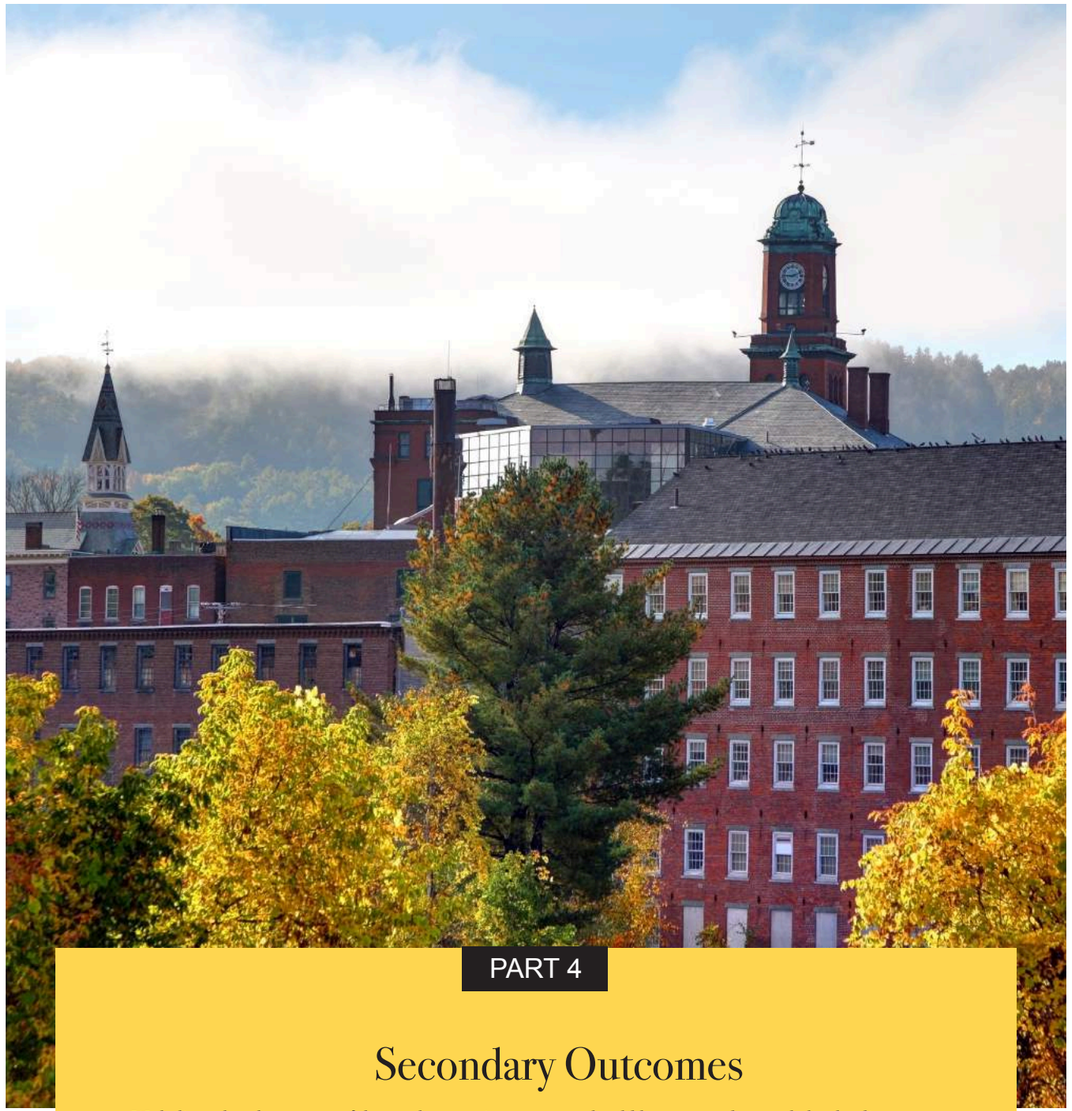
Our not-for-profit approach allows The Overwatch Foundation to deliver maximum value to New Hampshire by making sure the most dollars go to safeguarding our State through these programs. We feel that our ability to steer dollars into efficacy is unmatched. This is because we have no profit margins, we have no investors, we have no highly compensated executive team, our office overheads are minimal, and we plan to pay no federal taxes as a 501(c)(3). In addition, our status as a not-for-profit in New Hampshire gives a level of financial transparency that we believe is important.

Our "no mark up pledge" on labor, software, and hardware.

The Overwatch Foundation pledges to you that we will never mark up our services, which includes pricing transparency and no markups on software or hardware. Since software, hardware, and direct labor are the largest expenses in this proposal, we want you to know that we are 100% focused on building strong outcomes, not making money on hardware orders or software licensing deals.

Minimizing costs through pre-negotiated pricing.

The pricing offered on hardware and software will meet or beat pre-negotiated prices for the same equipment as previously used by the State of New Hampshire. As The Overwatch Foundation will not be including any margin on top of these purchases, what we pay is what you pay, and what you pay is at least as good as you'd have paid if you negotiated the deal yourself.



PART 4

Secondary Outcomes

We believe that the success of these cybersecurity programs should be measured not only by the direct benefits to communications systems and community drinking water enhanced by our proposal, but also by the secondary outcomes that keep our State headed in the right direction. We're confident that our approach delivers strong cybersecurity protections while maximizing the dollars invested but also supports local businesses and builds a cybersecurity workforce in New Hampshire. Protecting our drinking water systems and our email is about more than expert technology implementation. It is about doing our part to create a New Hampshire that can embrace, support, and sustain the tools, collaboration, and knowledge required to make these programs a true success.

Supporting Local Small Business

Enhancing existing commerce and relationships

Local small businesses run New Hampshire and give it a rich, economic vibrancy. Through nearly a decade of leading cybersecurity emergency response and key training initiatives throughout the State, we've learned how much we can accomplish together–and also how little we accomplish when key relationships are not preserved. Overwatch seeks to honor these relationships and, in fact, strengthen them through technical collaboration and training.

More than 55% of New Hampshire public entities use a managed service provider (MSP) for either a primary or secondary day-to-day IT services. More than half of all local government entities in New Hampshire rely on small business managed service providers (MSP) and SCADA installers for IT support and cybersecurity help. These relationships exist as part of a key fabric of professionals who own or work for technology businesses in the State. These relationships between MSP and local government entities are key to the smooth operation and delivery of this proposal. Overwatch will be able to cooperate with local small businesses to manage a smooth and effective delivery of these programs.

These businesses are deeply connected to the municipalities they serve. The Overwatch Foundation understands and respects the long-standing service these small businesses perform for the residents of New Hampshire and local government entities on a daily basis. Our leadership has spent the better part of a decade leading cybersecurity emergency response throughout the State, working with hundreds of local government entities, emergency services providers, and critical infrastructure. We've learned how much we can accomplish together and also how little we accomplish when key relationships are not preserved.

These businesses could be disrupted if a traditional organization is awarded this grant and permitted to establish relationships on top of these MSPs. This creates friction, not teamwork. Since The Overwatch Foundation is not a managed service provider or a SCADA installer and we do not seek to supplant an existing MSP or to leverage this proposal in order to gain market share in New Hampshire unfairly, the existing relationships will not be disrupted. This opens the opportunity for teamwork, learning, and collaboration, especially as we transition the current state into a future state through the methodology outlined in this proposal. We believe that a cybersecurity program that weakens key, small business managed service providers creates more risk than it solves.

Training and Workforce Development

The key to success

On the whole, eligible entities for the two "in a box" cybersecurity programs in this proposal are currently vulnerable and in a weakened state of cybersecurity readiness. This is primarily due to budgetary restrictions and cybersecurity workforce gaps. In recognition of this, our proposal aims to support all implemented solutions for up to 3 years. This graceful sunsetting of services creates an opportunity for gradual training, learning, and workforce development to occur while also giving receiving entities time to financially plan for the new, ongoing operating costs in year four and beyond. We'd like to emphasize the following points in our 3-year plan that we believe are critical.

1 We will provide unlimited training on all of the hardware, software, and security best practices for recipient's workforce members or managed service providers that plan to support these solutions long term. We know that every entity will have unique challenges in the learning process, and we plan to support each and every one of them as much as it takes to truly build the workforce required to make these solutions a success.

2 The Overwatch Foundation will perform the training in-house and in partnership with the existing Municipal Cyber Defense Training Program. We will leverage the training mechanisms already available in the State, not try to subcontract this work and incur added software training or professional development expenses. Training programs will be in collaboration with you, The Overwatch Foundation, the MCDP Grant Program Managers, and in cooperation with the New Hampshire Public Risk Management Exchange's extensive risk management training program efforts. Our goal is to be additive, not duplicative. Together, we will train the workforce in New Hampshire–and training on these solutions is absolutely critical to the success of both these programs and New Hampshire.

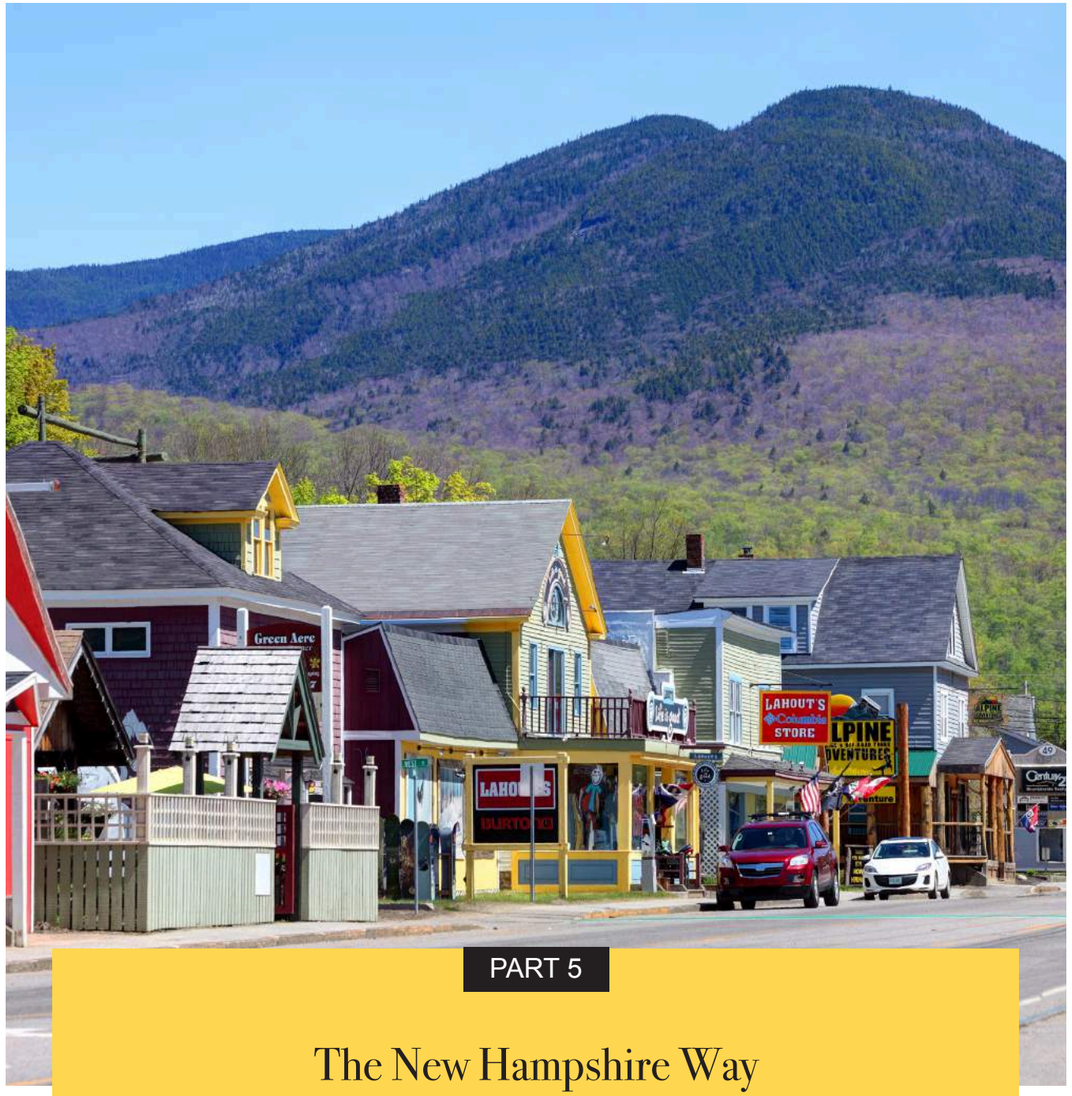
3 No receiving entity will be "locked in" or required to receive support services from The Overwatch Foundation. We are not in the business of building recurring revenue streams by implementing solutions that will need forever maintenance and licensing through us. If an entity wants to take advantage of the full 3 years while preparing for year four, we will happily support them or respect their decision to proceed independently.

4 Beyond supporting local entity workforce development, Overwatch, by mission, will target staffing our team to be at least 10% each of transitioning veterans, new students exiting our university system or local bootcamps, and those transitioning careers into cybersecurity. A stronger cybersecurity workforce–regardless of what capacity the person serves–is a stronger NH.

Overall, we believe in a collaborative approach to training that produces a strong cybersecurity workforce in New Hampshire, strengthening more than the outcomes of the grant while also doing so in a way that does not add any additional cost or delay to grant performance.

Overwatch's Target Organization Makeup

Our commitment to transitioning veterans and university system talent



PART 5

The New Hampshire Way

We're proud of New Hampshire's history of doing big things with small teams.

Dedicated New Hampshire Teams Protecting Critical Infrastructure

Serving New Hampshire requires understanding New Hampshire. What works in other places doesn't always work here. We're different here in "The 603." We're not perfect. Our communities have their differences. We have a robust political history. Our State has a deep belief in the policy of local control. In most ways, we have tremendous advantages, beautiful landscapes, and some of the best communities on earth in which to live. But our legacy of local control, siloed efforts, and tight fiscal budgets has contributed to us falling behind in technology investment in the realm of cybersecurity.

In order to address that shortfall, we must understand what works in New Hampshire. The Overwatch Foundation was founded and is managed by New Hampshire business leaders who believe in the power of small teams. New Hampshire has a long history of accomplishing great things with small teams and protecting critical infrastructure is no different. When more effort is required, small teams become a team of teams, allowing us to control costs, target our efforts, and make deep impacts without being overly burdensome or wasteful. Further, at Overwatch we plan to have dedicated teams for each grant program (not partial resources dividing their time simultaneously with other initiatives) to maximize the impact of the program outcomes in the performance period. This small, dedicated team approach is the New Hampshire Way, it is the approach that we founded our organization on and one we will continue to endorse for all future endeavors.

> ***From our perspective, The New Hampshire Way is to lead the way.***

We also believe in our "small but mighty" heritage as a differentiating factor from not only our neighbors in the region, but also across the country. Overwatch has a 10-year Phase 1 Mission to create pilot programs to protect the State of New Hampshire, critical infrastructure, and vulnerable populations within our area of operations that we believe will set the standard for other states to follow to build a stronger, safer country. Our two-fold approach to both improved technology implementations and supporting training programs for workforce development will prepare New Hampshire to lead the way for the country and to meet the challenges of the future our nation faces in protecting our communities. From our perspective, the New Hampshire Way is to lead the way.

Thank You for Investing in Cybersecurity

On behalf of all of us at The Overwatch Foundation, as citizens of our State, Americans, and believers in a bright, competitive New Hampshire, we are delighted that you have led New Hampshire to invest in these essential programs. Improving cybersecurity readiness, protection, and workforce are a crucial concern for all of us. In fact, we founded Overwatch as a vehicle to meet this specific challenge. Your funding from this program will accelerate our effort toward safeguarding our drinking water system and our communications systems in a coordinated and efficient manner.

We understand that these programs are some of the first of their kind, providing new opportunities for impact and breadth of reach. As individuals, it has been an honor to work with you all in various capacities toward the goal of protecting New Hampshire. We're excited to forge our collective strengths together and continue the charge with you.

If you have any questions about this proposal, want to request additional information about specific elements of the workflow, or if you'd like to propose any changes to our proposal, we're all ears. We have thoughtfully designed workflows and programs that we believe are efficient, flexible, and modular. Because all of the recipients of this work will be somewhat unique, we must be ready to adapt to the conditions in the field. That flexibility also allows us to quickly receive feedback from you and modify our plans both before we begin and once these programs are up and running. We plan to work with you to adapt our programs consistently and especially after the first 90 days.

Thank you for your time, support, and consideration of this proposal. But also, thank you for supporting cybersecurity in New Hampshire. We'd love to do this vital work for all of us in the State, but we know New Hampshire could never do it without you. Thank you.

Very Respectfully,

Jason J. Sgro
Chairman

Alyssa C. Rosenzweig,
Deputy Director


THE OVERWATCH FOUNDATION
CONSTANS VIGILANTIA