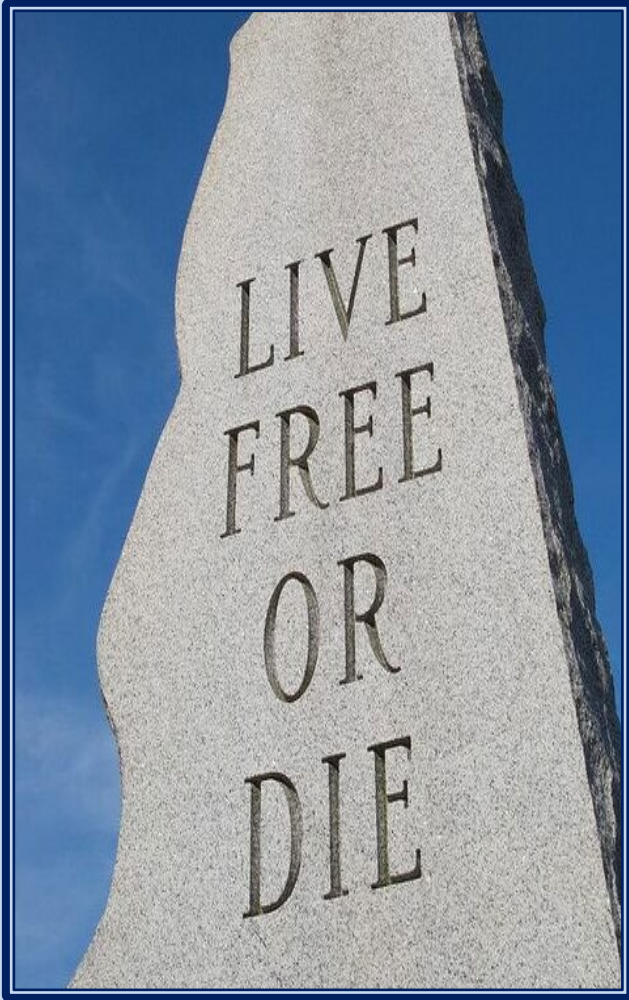


“Cybersecurity In a Box”



Securing and Defending New Hampshire Municipalities, K12s, and Critical Infrastructure

State: New Hampshire

Agency: Department of Information Technology

Category: Cybersecurity

Initiated: December 2022

Completed: December 2024

Ken Weeks

Chief Information Security Officer

kenneth.l.weeksiii@doit.nh.gov

(603) 931-9234

Executive Summary

New Hampshire has 10 Counties, 13 Cities, 221 Towns, 25 Unincorporated places, 108 K12 Public School Administrative Units (SAU), 223 Public Libraries and approximately 700 community public water systems (Drinking water and Wastewater) across the State. 26% of the Municipal entities and 1% of the Water Systems are on a .GOV domain. Based on assessments done by the NH CISA Cyber Advisor, Mr. Rick Rossi over the last 15 months, and reviewed by NH State Leaders, cybersecurity for the Water Sector in NH is essentially non-existent.

Granite Staters depend on each of these organizations and the Critical Infrastructure (CIKR) they operate to ***maintain and sustain our very way of life***. Each of these New Hampshire Public Sector organizations is potentially under attack by malicious cyber actors from anywhere in the world, 24 hours a day, 7 days a week, 365 days a year!

In 2022, several like-minded people sat down, broke bread, enjoyed a cigar and glass of bourbon (or two) and decided, “We’ve all seen the data on NH Cyber Attacks. We need a vehicle to optimize ROI for grant dollars, so they are spent on real outcomes and not profit and taxes – those [expletive deleted] coming after us don’t get to win.”

From this gathering, ***The Overwatch Foundation*** was born. Overwatch, founded in 2022 is a 501(c)(3) not-for-profit foundation that delivers grant-based services in cybersecurity, critical systems modernization, network and physical defense, training, and workforce development to state and local government organizations in New Hampshire and across the Nation.

In 2024, New Hampshire established three “Cybersecurity in a Box” programs for delivery by The Overwatch Foundation:

- .GOV in a Box
- Drinking Water Cybersecurity in a Box
- Wastewater Cybersecurity in a Box

The “Cybersecurity in a Box” framework is unique because the first principle is equity of outcome,

so services are customized based on the organization’s function, the employee roles and responsibilities, and the organization’s existing cybersecurity readiness. It is universal because it applies to every NH Local Public Sector Government Organization and Publicly owned Drinking Water and Wastewater Systems.

By delivering essential cybersecurity services “In a Box” New Hampshire ensures equity of outcome in cyber resiliency and makes it more difficult for Malicious Cyber Actors to achieve their objectives against State and Local entities in New Hampshire.

Since these programs started:

- 152 Local Government Organizations and K12s have requested .GOV in a Box service and the rate of completed migrations is trending upwards.
- 5 of the most important Drinking Water systems in NH have completed the project.
- The second largest wastewater facility, owned and operated by the New Hampshire Department of Environmental Services is in process.

What’s Next? Growth for Cybersecurity in a Box programs for 2025 include:

- Managed Endpoint Detection and Response in a Box to the 108 NH K12 SAUs (\$3.6M)
- Accelerated Drinking Water and Wastewater Cybersecurity in a Box (\$1.2M) across New Hampshire systems.

By securing and defending Local Governments and New Hampshire critical infrastructure, we are literally increasing the amount of time between a major cyber incident and the first loss of life attributable to that cyber incident. Live Free or Die!

PART I: THE IDEA

The Problem: *New Hampshire needed a “turnkey service” to migrate municipal organizations and K12s to .GOV domains and improve the cybersecurity and resilience of our public Drinking Water and Wastewater systems (and other CIKR)!*

New Hampshire has 10 Counties, 13 Cities, 221 Towns, 25 Unincorporated places, 108 K12 Public School Administrative Units (SAU), and 223 Public Libraries. **Only 23% of the NH Municipalities and K12s are on a .GOV domain** – those that are not on a .GOV domain are significantly more prone to email impersonation. Email impersonation is a significant enabler for successful Phishing attacks against Public Sector organizations. A recipient of one of these emails is more likely to click on a malicious link or open a malicious attachment because the sender’s email address appears to be an address they expect to see. The user’s organization’s own “.org” or “.com” domains make the bad guys’ job easier!

In March of 2024, Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies said, “The nation’s water systems face cyber threats from criminals and countries alike. We must lock our digital doors to meet the threat...and [provide] services to help companies operating critical infrastructure act quickly.” Across the State, there are 700 community public water systems and 108 Wastewater systems. **Based on hundreds of cybersecurity assessments of these systems, cybersecurity for the Water Sector in NH can only be described as “non-existent.”**

Why is “Cybersecurity in a Box” Unique?

There is not another program like this anywhere in the United States. The State of New Hampshire & Overwatch Foundation partnership delivers grant-funded cybersecurity services to municipalities, K12s, and CIKR operators. NH doesn’t “throw grant dollars at locals and hope the problem gets fixed.” The NH “Cybersecurity in a Box” implements the solution(s) at no cost to the recipient. Turnkey solutions that eliminate all the typical “reasons to say no” to migrating a municipal domain to .GOV or implementing cybersecurity into Drinking Water and Wastewater Systems are simply not delivered by any other program we know of in the United States or its Territories.

Weaknesses of .ORG and .COM Domains

Email impersonation is one of the most successful methods cyber criminals use to complete major financial frauds in NH. And lookalike email addresses are used with alarming frequency.

These lookalike addresses are called “Squat Domains”. They are usually registered with only one letter off. So ticketmaster.com could be forged as ticketmister.com.

There are also simple techniques that trick the eye like using an r and an n to look like an m.

rn = m

Why Does it Matter?

“Cybersecurity is not the sole responsibility of one single water system, one single state, or the federal government. Instead, cybersecurity is a collective responsibility...it’s critical that we work together with our state partners to help set a course toward cyber-resilience that will deliver essential protections across the country.”

-Janet McCabe, EPA Deputy Administrator

Why is “Cybersecurity in a Box” Universal?

Although the partners, political environment, and degree of Home Rule vary greatly, any other NASCIO member can duplicate this framework and create the ability to deliver turnkey cybersecurity solutions to municipalities, K12s, and CIKR systems. NH “Cybersecurity in a Box” implements solutions to a #1 NASCIO CIO Priority – Cybersecurity and the NASCIO emphasis on eligible entities transitioning to .GOV domains. The NH “Cybersecurity in a Box” Program ensures equity of outcome through the consistent application of solutions regardless of the level of readiness an organization receiving services starts at. All “Cybersecurity in a Box” services are provided at no cost.

PART II: NH IMPLEMENTATION OF “CYBERSECURITY IN A BOX”

The roadmap: This is New Hampshire. We are the people who plaster the State Motto, “Live Free or Die” on EVERYTHING. What that meant was Overwatch and the State Agencies would be confronted by many real (and imagined) reasons local governments would resist migrating their domains to .GOV. (Did you know that if you are on a .GOV domain connected to a 5G tower that everything you do can be monitored and tracked by the NSA? Did you know that if you log into a .GOV domain through that same 5G connection on your cell phone that you could be automatically vaccinated for hoof-in-mouth disease [not even a human disease] from space?) Although these are slight exaggerations, there were legit concerns anyone has when moving to a new domain – especially when you hear “I’m from the Government and I’m here to help.” With this very real constraint, the group knew we needed to deliver turnkey solutions that accounted for as many reasons we could think of for eligible entities to say “No!” So, the Chairman of the Board of The Overwatch Foundation and the NH State CISO white-boarded all the reasons they could think of to “just say no” and then we solutioned them and put them “In the Box” for each program. You need new business cards? There are some in the Box. Those same guys used a similar process to develop the tech stack for the water sector programs, but those sessions included massive partnering with the NH CISA Cyber Advisor and the NH Department of Environmental Services. (We never did solve that “vaccinated from space” thing...yet.)

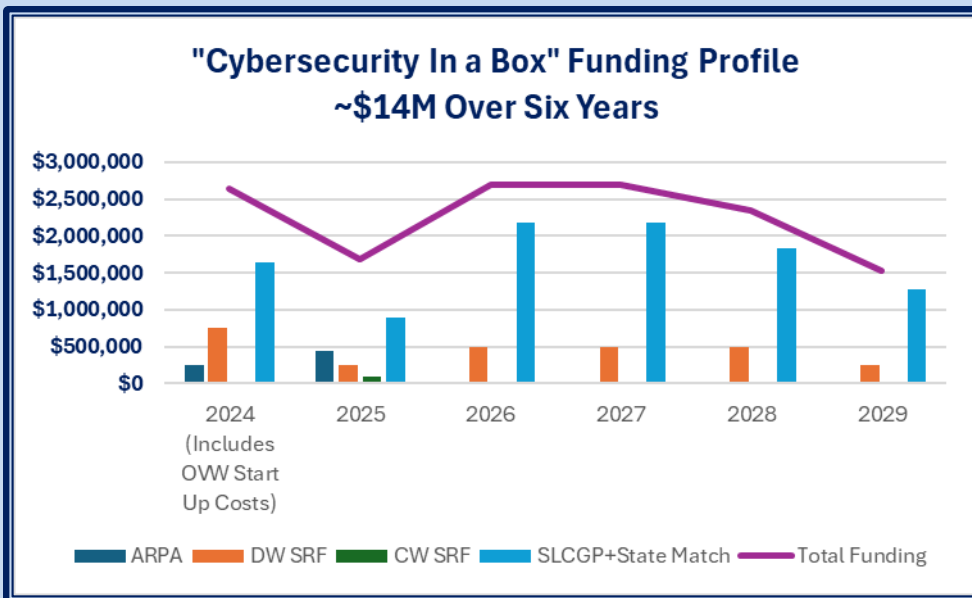
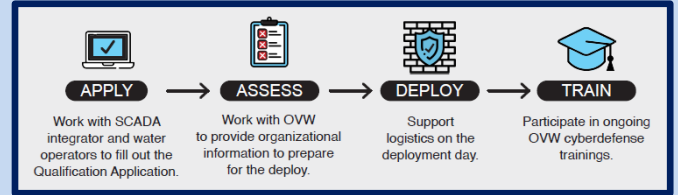
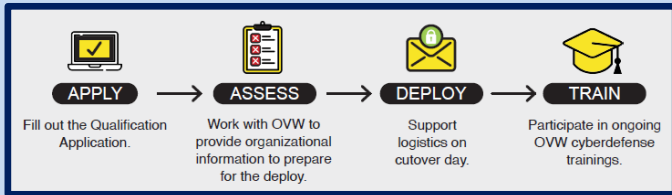
Who was involved? In 2022, several like-minded people sat down, broke bread, enjoyed a cigar and glass of bourbon (or two) and decided, “We’ve all seen the data on NH Cyber Attacks. We know what the solutions look like. We need a vehicle to optimize ROI for grant dollars, so they are spent on our defined outcomes and not profit and taxes – those [expletive deleted] coming to attack our CIKR don’t get to win.” From this gathering, **The Overwatch Foundation** was born. Overwatch, founded in 2022 is a 501(c)(3) not-for-profit foundation that delivers grant-based services in cybersecurity, critical systems modernization, network and physical defense, training, and workforce development to state and local government organizations in New Hampshire and across the Nation. **Partnerships and relationships were even more important than funding to make NH “Cybersecurity in a Box” programs real instead of just a good idea. Everyone in this partnership already had trust relationships. We simply built on those relationships to deliver “Cybersecurity in a Box!”**

Who Was Involved – The Public-Private Partnership

- **The OG “Group of Three”**
 - Chairman of the Board of The Overwatch Foundation/The Senior Partner of the Atom Group Security and Privacy Practice
 - Lead Cybersecurity Risk Manager for the New Hampshire Public Risk Management Exchange (Primex³)
 - NH State Chief Information Security Officer (CISO).
- **The Overwatch Foundation, a NH Not-for-Profit with the mission to protect 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.**
- **The New Hampshire Department of Information Technology (CIO) and the Chief Information Security Officer (CISO).**
- **Primex³ is a NH Not-For-Profit Public Entity Risk Pool that covers cities, towns, school districts, counties, village districts, and other governmental entities. Primex³ is codified in New Hampshire Revised Statute as Amended (RSA) Title I, The State and Its Government, Chapter 5-B, Pooled Risk Management Programs.**
- **The New Hampshire Department of Safety, Homeland Security and Emergency Management is the SAA for NH.**
- **The New Hampshire Department of Environmental Services / Water Division and Office of the Commissioner**
- **The NH CISA Cybersecurity Advisor**
- **The NH Municipal Association (NHMA)**

In 2024, the NH DoIT, NH DES, and The Overwatch Foundation coordinated with the NH CISA Cybersecurity Advisor and established three “Cybersecurity in a Box” programs for delivery by OVERWATCH:

- 1) .GOV in a Box
- 2) Drinking Water Cybersecurity in a Box
- 3) Wastewater Cybersecurity in a Box.

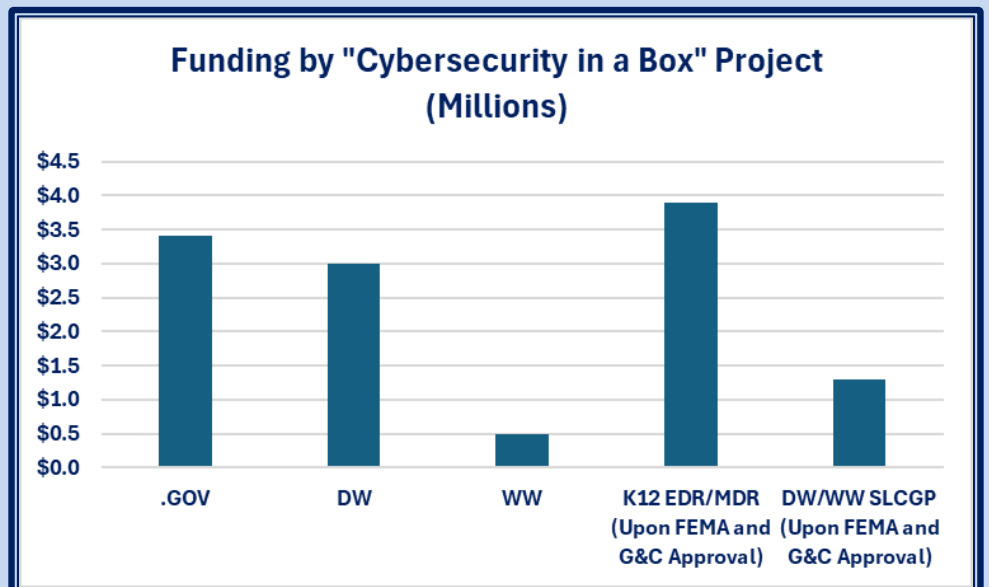


How did we do it? The program is entirely funded by the NH Department of Information Technology and the NH Department of Environmental Services with American Rescue Plan Act (ARPA), State Revolving Funds (SRF) and the State and Local Cybersecurity Grant Program (SLCGP).

Depending on the overall health of the Drinking Water and Clean Water State Revolving Fund(s) additional funding may be applied in the out years to sustain those “In a Box” programs.

The first two years of the program focus on “. Gov in a Box” and “Water and Wastewater Cybersecurity in a Box.” For the first 6 months, Overwatch, in partnership with NH DoIT and NH DES organized and conducted five pilot projects representative of the range of sizes and complexity of the total population of eligible entities for each “In a Box” program.

Lessons learned from the pilot programs informed best practices for execution. The main lessons applied to relationship building and technical execution. Based on the success of these pilot programs, the New Hampshire SLCGP Planning Committee approved and funded a fourth “Cybersecurity in a Box” program for Year 3 of the SLCGP – CROWDSTRIKE Falcon Complete for High Value Targets at all 108 NH K12 School Administrative Units (SAU).



Based on the success of these pilot programs, the New Hampshire SLCGP Planning Committee approved and funded a fourth “Cybersecurity in a Box” program for Year 3 of the SLCGP – CROWDSTRIKE Falcon Complete for High Value Targets at all 108 NH K12 School Administrative Units (SAU).

PART III: Impact of the NH “Cybersecurity in a Box” Program

What Did We Make Better with .GOV in a BOX? As you can see at the right, towns or K12s that receive “.GOV in a Box” services were required to do a significant amount of planning and “discovery.” They received a detailed assessment of their current IT/Security environment, created change management and communications plans, cleaned up unused accounts, and received major security and technical training as part of the process. In every case, when Overwatch left, “.GOV in a Box” directly improved the security of their email and web environments and significantly **mitigated the threat of email impersonation** that cyber criminals could use for major financial frauds against them.

<p>.Gov in a Box Provides:</p> <ul style="list-style-type: none"> • Email and Website Domain Migration • Web Platform Hosting (e.g. Google Workspace, M365) • Printed Materials (such as new business cards) • Cybersecurity Training 	<p>What we need from the recipient:</p> <ul style="list-style-type: none"> • Gain necessary approval to work with OVW and execute necessary contracts within 2 weeks of program acceptance • Lead internal communication during preparation, cutover, and OVW requests of your staff and IT leaders • Lead process of settling on new .GOV domain name with your organization • Provide list of email users and their roles in the organization, noting anyone that might be using a personal email and should be on your email (91-A) • Create plan for rolling out changes to your community members • Provide estimates for marketing materials impacted by domain change for OVW review • Review assessment results with your technology and organization leadership to make final decisions on solution acceptance • Collaborate on creation of onsite cutover training plans • Participate in any recommended cybersecurity and incident response training throughout the three-year support period
--	---

<p>Water System Cybersecurity in a Box Provides:</p> <ul style="list-style-type: none"> • 3 Years of Support • Community-owned software and hardware • Secure SCADA systems • Remote Access Tablets • Cybersecurity Training 	<p>What we need from the recipient:</p> <ul style="list-style-type: none"> • Gain necessary approval for your community to work with OVW and execute necessary contracts within 2 weeks of program acceptance • Review assessment results with your technology and organization leadership to make final decisions on solution acceptance • Collaborate on creation of onsite training plans • Participate in any recommended cybersecurity and incident response training throughout the 3-year support period • Be prepared to bring technical support onboard to manage new technology (e.g. firewall, new email accounts, tablets) at the end of the 3-year support window
---	--

What Did We Make Better with “Water Cybersecurity in a BOX?” The program provided detailed assessments to community water systems and wastewater facilities. From the assessments, we created a cybersecurity risk management program for the systems/facilities, and installed mitigations to prevent a cyberattack from impacting system operations. **Participating community water systems are more resilient against attacks that may affect their ability to provide clean and safe drinking water to customers, process wastewater, and erode customer confidence.**

How Do We Know We Succeeded? Since the “Cybersecurity in a Box” Programs started:

- The Overwatch Foundation is up and running, staffed with administrators, project managers and engineers to deliver both current and future “Cybersecurity in a Box” services in New Hampshire and soon to the New England region if requested and funded by neighboring States.
- Per NASCIO, nearly twenty years after making .gov available to state and local governments, less than 10 percent of local governments are registered on the domain. In New Hampshire, 152 Local Government Organizations and K12s have requested .GOV in a Box service and the rate of completed migrations is trending upwards. Upon completion, more than 62% of NH municipalities and K12’s will be on a .GOV Domain.
- Five of the most important Drinking Water systems in NH have completed the project, including the system that provides cooling water to the Seabrook Nuclear Power Plant in New Hampshire. We’ve still got a ton of work to do in the Drinking Water sector!
- The second largest wastewater facility, which serves 12 communities along the Winnepesaukee River Basin,

and is owned and operated by the New Hampshire Department of Environmental Services, has executed the “Wastewater Cybersecurity in a Box” process.

National Praise for NH “Cybersecurity in a Box”. On March 28, 2024, Ms. Anne Neuberger, Deputy National Security Advisor sent a letter to State Governors requesting states develop water and wastewater system cybersecurity action plans. On June 27, 2024, Mr. Robert Scott, Commissioner of NH Department of Environmental services responded to this letter with not only New Hampshire’s plan as requested, but attestation that New Hampshire was already implementing the plan via The Overwatch Foundation’s delivery of both the “Drinking Water Cybersecurity in a Box” and “Wastewater Cybersecurity in a Box” programs. In a subsequent July 10, 2024, meeting, Ms. Neuberger specifically pointed out “...the New Hampshire ‘In a Box’ programs are the example other States should follow.” The program was also commended by Administrator Michael S. Regan, US Environmental Protection Agency, Director Jen Easterly, Cybersecurity and Infrastructure Security Agency (Under the Department of Homeland Security) and U.S. Senators Jeanne Shaheen and Maggie Hassan of New Hampshire and U.S. Representatives Annie Kuster and Chris Pappas of New Hampshire either by correspondence or in person.

Local Praise for NH “Cybersecurity in a Box.”

“Since I’ve been at Primex³, there has never been this level of federal and state dollars applied, or even this much ‘care about’ from the State for the Cybersecurity and Cyber Resiliency of our membership. What DoIT and DES have done with ‘In a Box’ programs through The Overwatch Foundation has significantly improved cyber hygiene of, and reduced the cyber risk to, the Primex³ membership and reduces our [Primex³] costs to re-insure the Risk Pool.”

- Cori Casey, Cyber Risk Manager, NH Primex³

“Our technology project with the New Hampshire Department of Information Technology was a positive experience with an outcome that clearly benefits our school district safety and security. As we worked with the NHDOIT and the Overwatch Foundation, our Technology Director was able to transition our school district to a .gov [domain], which protects our staff, students, and overall school community. The process was well executed, and we consistently felt that we were a team, problem solving and moving forward together for the outcome we all expected.”

- Dr. Sydney Leggett, Superintendent, SAU 100.

What Now? Growth for Cybersecurity in a Box programs include:

- We feel existing funding is sufficient to complete all requested .GOV migrations over the period of performance of the SLCGP funds.
- Coming in 2025 and beyond: Managed Endpoint Detection and Response in a Box to the 108 NH K12 SAUs (\$3.6M)
- Coming in 2025 and beyond: Continuation of Drinking Water and Wastewater Cybersecurity in a Box (\$1.2M) across New Hampshire systems.

“When I got this CISO job a couple years ago, my Boss, the NH CIO, Denis Goulet said, ‘Ken, talk to Jason Sgro from Atom Group. See if he is somebody you can work with. Then figure out what you two can do to improve the Cybersecurity of Local Governments and the Schools. Talk to Cori at Primex³ as well. We really need to do better there, even if the State won’t pay for it.’ Well, Jason and I ate some Barbeque, had a few drinks and some cigars over a couple months and we came up with this silly “in a Box” idea. (I’ll neither confirm nor deny we laughed about a certain Saturday Night Live sketch.) We spoke with Cori about being additive vice redundant with Primex³. Securing CIKR is about protecting our way of life. Now we have OVERWATCH, so stand by for more boxes.” - Ken Weeks, NH State CISO