National Governors Association
Meet The Threat First Regional Summit
Media Clips

Terry McAulife Presses Cybersecurity at NGA

CivSource
By Bailey McCann
October 5, 2016

October is cybersecurity awareness month and newly appointed chair of the National Governor's Association, Virginia Governor Terry McAuliffe, used today's NGA regional summit to launch his new cybersecurity program Meet The Threat. Speaking to governors and representatives from 26 states at the summit currently underway in Boston, McAuliffe released a new program aimed at getting state government to take cybersecurity seriously.

As CivSource reported last month, new findings released at the National Association of State Chief Information Officers (NASCIO) Annual Conference show that more governors are aware of the importance of cybersecurity as an issue, but few are putting significant budget and resources behind it. According to the report, states are spending approximately 1-2 percent of their annual IT budget on cybersecurity. That's compared to the federal government, which has increased its spend by 35 percent this year alone.

Those findings are not good enough for Governor McAuliffe. In his comments before the NGA today, he pressed state leaders to understand cybersecurity as a threat to overall security in their states and also as an opportunity to create new jobs and foster economic development. "Cybersecurity jobs are the jobs of the twenty-first century," the governor said in an interview with CivSource. "In Virginia alone, thousands of these positions are unfilled. So we are focused on training people, working with our universities and employers, because we need people with these skills. These are jobs we can provide right now today."

Since McAuliffe took office, Cybersecurity has been a key focus area for his administration. After many Virginia residents had their personal information compromised in a recent cyber attack, McAuliffe says he wanted to find new ways to ensure it wouldn't happen again. "Governments have massive amounts of sensitive data, we have a responsibility to protect that data," he contends. "In Virginia especially, we have a significant defense industry and a number of other high-value targets. There were 36 million cyber attacks attempted on targets in Virginia in 2014 alone and there are more every year. We can't afford to ignore this issue."

Over his tenure, McAuliffe has been successful at getting both budget allocations and bond issues for cybersecurity projects through a conservative legislature that balks at the idea of government spending. The Commonwealth now has cybersecurity training and research programs in most of its major colleges and universities. Virginia is also supporting cybersecurity startups through the MACH-37 accelerator program at Virginia's Center for Innovative Technology. Additionally, in 2015, the governor created the nation's first state-level Information Sharing and Analysis Organization (ISAO). ISAOs are intended to complement existing structures and systems that are used to share critical cybersecurity threat information across levels of government and industry

sectors. The ISAO works with public and private entities to monitor cyber threats and vulnerabilities.

McAuliffe is using what he's done in Virginia, along with best practices from other forward thinking states, as foundational documents for the Meet The Threat initiative. The NGA has created a website and forthcoming podcast series that provides access to checklists, executive order language, legislative ideas, and other support for state governments to create a cybersecurity plan. "Nothing riles up governors like finding out what other states are doing," McAuliffe adds wryly. "I've said, we'll give you the legislation we put forward – I'll show my executive orders. I want to have the conversations about how to create centers of excellence for cybersecurity. In Virginia, we can be spending money and time building up protections, but if other states aren't doing the same thing, attackers can just use those unprotected systems as an open door."

As part of his Meet The Threat program, McAuliffe will be holding a series of regional summits like the one this week in Boston, to meet with NGA members and private sector stakeholders about how to improve cybersecurity nationwide. "This isn't just another initiative," he says. "We have created real deliverables. At the end of the year, I want governors to have gone through the checklist and be able to say they have a real plan for cybersecurity. It's not only important as a protective measure but, technology and cybersecurity are the jobs of the future. Creating those jobs should be important to governors everywhere."

https://civsourceonline.com/2016/10/05/governor-terry-mcauliffe-presses-cybersecurity-at-nga/?utm_campaign=shareaholic&utm_medium=twitter&utm_source=socialnetwork

Virginia Gov. Terry McAuliffe On Cybersecurity
WBUR Radio Boston
October 5, 2016

Virginia Gov. Terry McAuliffe, chairman of the National Governors Association, has created a new cybersecurity initiative called "Meet the Threat: States Confront the Cyber Challenge." It's aimed at helping states find solutions to cyber threats so that they can prevent and thwart attacks. The issue is particularly important in Massachusetts, which is a hub for cybersecurity companies.

http://www.wbur.org/radioboston/2016/10/05/terry-mcauliffe-cybersecurity

Virginia Governor Terry McAuliffe recruits 26 states for regional cybersecurity initiative

StateScoop
By Colin Wood
October 6, 2016

States will soon gain access to a growing repository of cybersecurity resources.

National Governor's Association Chair and Virginia Gov. Terry McAuliffe launched the first in a series of regional summits Wednesday comprising his "Meet the Threat" initiative — a bid to develop new strategies and compile information that will help states protect their networks and critical infrastructure against mounting digital threats.

Leaders from 26 states gathered in Boston to participate in the three-day event, share ideas during roundtables and listen to the keynote address issued by McAuliffe, who relayed his desire to lead the nation in cybersecurity.

"The federal government is going to spend billions of dollars on cybersecurity," McAuliffe said. "Now, I can speak for all the governors in America. You want every bit of that money you can get to your respective state and I want to see everyone get their fair share. […] They won't put a penny into a state if they don't see us making a priority out of cybersecurity. They just can't."

Partners joining McAuliffe, and other state leaders, were Deloitte, Accenture, Motorola Solutions Foundation, Splunk, ForeScout Technologies, Anthem and the National Association of State Chief Information Officers (NASCIO). McAuliffe placed emphasis on the link between their need for improved cyber governance and efforts around budgeting, the economy and workforce development.

"We've created 166,600 new jobs since I became governor," McAuliffe said. "We've tried diversifying into those new areas. […] We're creating a lot of jobs, but what's happening is a lot of the baby boomers are now retiring and younger folks are coming in, they're working part-time, they're not at the pay wage, so while more jobs are being created … new jobs are not being paid [the same wages] as the old jobs. How do you fix that? Twenty-first century technologies, data analytics, all this cyber activity, and it's a huge opportunity for us going forward."

McAuliffe also pointed to new cyber programs in higher education as a key component of the commonwealth's economic and technology planning.

"We increased by three times the number of centers of academic excellence in our Virginia community colleges," McAuliffe said. "I would recommend to all of the states the number one focus is to go out and get one of your community colleges to become a center of excellence. You cannot get any federal work, you can not build that cyber workforce [without one]. Most of these jobs do not

require a four-year degree. [...] Our community colleges are the sweet-spot and we have totally turbo-charged our education system in Virginia to begin to meet the need of all these cyber warriors we need in the Commonwealth of Virginia."

Virginia's recently-approved $109 billion budget includes a first-of-its-kind scholarship program that gives the recipient a free education if he or she agrees to work for the state once they have attained the needed cybersecurity credentials. Programs that generate new pathways for employment allow states to compete with the federal government and private sector while bolstering the economy, McAuliffe said

Veterans programs are also a boon to the cyber-economic effort, he said.

"We just expanded a new veterans pathway program for cybersecurity, something I'm very proud of," McAuliffe said. "We have more veterans per capita than any state in America. [...] If you want to come to Virginia, I can get a veteran to work for you. [...] You hire a veteran, they're highly motivated, they're highly disciplined, they show up on time and they work their heart and soul out each and every day."

Virginia's program accelerates veterans' path to technology credential and employment. Between McAuliffe inauguration in Jan. 2014 and this past Jan., the state doubled its goal and hired more than 20,000 veterans.

Other efforts in Virginia include the Virginia Cyber Range, an online obstacle course for high school and college students, and the inclusion of Northern Virginia Community College as an National Security Agency Regional Resource Center, which McAuliffe called a "big deal."

"How did we get one of these? It's everything I just talked about," he explained. "Leaning in on education and showing the federal government we are invested and building this pipeline of cyber workers."

The summit was the first in a series, which will facilitate in-person information sharing along with the building of an online resource library, which can be found on the initiative's website.

A new podcast series, also to be found on the initiative website, will disseminate the expertise of those working in the cybersecurity sector, while Virginia's recognition of October's designation as National Cybersecurity Awareness Month and further development of the state's Fusion Center further support the state's position as a thought leader in the sector. NASCIO also announced support of National Cybersecurity Awareness Month and is showcasing the organization's designation as an official "cybersecurity champion." Later this month, the association will release updates to its cybersecurity readiness guide

Participating states include Alabama, Arizona, Arkansas, Colorado, Connecticut, Indiana, Kansas, Kentucky, Maine, Maryland, Massachusetts, Minnesota,

Mississippi, Missouri, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Utah and Virginia.

Future updates on Meet the Threat can be found via the the initiative's official Facebook page and Twitter hashtag, which is #MeetTheThreat.

http://statescoop.com/virginia-governor-terry-mcauliffe-recruits-26-states-for-regional-cybersecurity-initiative

Meet the Threat: States Join Forces to Develop Innovative Cybersecurity Strategies
GovTech
October 6, 2016

On Oct. 5 in Boston, Virginia Gov. Terry McAuliffe unveiled an initiative aimed at developing state strategies for strengthening cybersecurity practices — and nearly 30 states have joined the cause.

At the first of several National Governor's Association (NGA) regional summits dedicated to furthering Meet the Threat objectives, McAuliffe's initiative as chair of the NGA, he said the goal is to replicate the work done in Virginia to best position all states and territories for meeting the cyberthreat — and to connect policy leaders from every state with private-sector experts and federal partners to highlight innovative practices and identify ways state-driven solutions can be replicated nationwide.

"I know firsthand from my work in Virginia that governors and states play a critical role in confronting the ever-growing and sophisticated challenge of cyberattacks," he said at the summit, adding that the Meet the Threat website will serve as a library of resources for states. "As the year progresses, we will add to the library and encourage state policymakers to use it."

The next regional summit will be held in San Jose, Calif., in spring of 2017, and the initiative will conclude in Virginia with the National Summit on State Cybersecurity. This final summit, McAuliffe said, will bring together representatives from each state, commonwealth and territory to share best practices and lessons learned.

"These are ambitious goals. With your engagement, however, I know we can succeed," he said. "The initiative has the potential to shape the nation's response to the growing cyberthreats we face by underscoring the critical role state leaders play in securing the cyberenvironment."

http://www.govtech.com/security/Meet-the-Threat-States-Join-Forces-to-Develop-Innovative-Cybersecurity-Strategies.html

Morning Cybersecurity

Politico
by Tim Starks
October 6, 2016

YOU'RE IMPORTANT — Virginia Gov. Terry McAuliffe, the chairman of the National Governors Association, wants his fellow state officials to know that they're a vital part of U.S. cyber defense efforts. "I know firsthand from my work in Virginia that governors and states play a critical role in confronting the ever-growing and sophisticated challenge of cyberattacks," McAuliffe said Wednesday while kicking off the first summit for his state cybersecurity initiative. Thirty states attended the event, and Suzanne Spaulding, the DHS undersecretary for the National Protection and Programs Directorate, delivered a briefing. McAuliffe — or "Governor Cyber," as MC likes to call him — urged other governors to follow his lead in declaring October "National Cybersecurity Awareness Month," which the president has done for 13 straight years.

http://www.politico.com/tipsheets/morning-cybersecurity/2016/10/the-hits-keep-coming-for-nsas-hacking-team-216715

Del. Ken Plum: Cybersecurity in Virginia

Reston Now
by Del. Ken Plum
October 6, 2016

October is National Cybersecurity Awareness Month as designated by the U.S. Department of Homeland Security. The purpose of the month is "to engage and educate public and private partners through events and initiatives to raise awareness about cybersecurity, provide them with tools and resources needed to stay safe online, and increase the resiliency of the Nation in the event of a cyber incident."

Certainly the news of cyber attacks and hacking almost daily have made the public more aware of the reality of cybersecurity. One campaign — Stop.Think.Connect.– sponsored by the Department of Homeland Security, is designed to promote safe online behavior and practices by members of the public.

Virginia Gov. Terry McAuliffe, who is serving as chairman of the National Governors' Association, has made cybersecurity a centerpiece of his leadership of the organization. The Governor reported that since Jan. 1 of this year, the state of Virginia has experienced 53 million cyber attacks — roughly four attacks per second.

According to Gov. McAuliffe, there are 650 cybersecurity companies in Virginia, and the estimates are that cybersecurity jobs will increase 25 percent by 2022.

He said there were 17,000 cyber jobs open in the state of Virginia alone and the starting salaries are $88,000.

A recent edition of The Voice of Technology published by the Northern Virginia Technology Council (NVTC) indicated that 55 percent of its members are hiring cybersecurity professionals this year. Of the 33,000 tech sector job openings in Virginia, 17,000 are in cyber. NVTC also reported that 46 percent of the 2015 Greater-Washington venture capital funding supported cyber solutions.

Training for the cyber field is close at hand in Northern Virginia. Northern Virginia Community College has the highest recognition as a trainer for cyber workers. It has a two-year Associate Applied Science degree in cyber security, and George Mason University has a Bachelor's degree program.

The two institutions of higher education have one of the most successful articulation agreements in the country permitting students to move from one school to another.

The need for attentiveness toward cybersecurity extends beyond this month of organized awareness. Each individual has a role to play in securing their information. Simply, do not click on links that are suspicious. There is a high

likelihood that they are phishing for your information. Be sure you know who that e-mail is from.

Additionally, for individuals seeking better paying jobs, a career field, or new challenges, the field of cyber security offers many possibilities. Check with the staff at NOVA or GMU to discuss those possibilities. Virginia has recently introduced an apprenticeship program in cyber security. You can help keep vital information safe for businesses, organizations and individuals. That makes for fulfilling work.

To learn more about the Virginia programs, go to cyberva.virginia.gov or the Northern Virginia Technology site nvtc.org/techtalent.

https://www.restonnow.com/2016/10/06/del-ken-plum-cybersecurity-in-virginia/

Voting Cybersecurity Concerns Some State Officials
Bloomberg BNA
By Adrianne Appel
October 7, 2016

Voters should avoid filling out their ballots online due to cybersecurity threats and risk of harming confidence resulting from an election data breach, state election officials said at a recent gathering of governors.

But the officials said that the climate for adopting long distance means of casting ballots—including voting online—has cooled in reaction to hacking incidents.

After the breaches, demand for online voting has decreased, Connecticut Secretary of State Denise Merrill, said in Boston Oct. 5 at a meeting of the National Governor's Association focused on cybersecurity, called "Meet the Threat, States Confront the Cyber Challenge." Many states faced "increasing pressure but that has slowed down," she said.

Although most states allow those not present to cast their vote on paper ballots through the mail, some states allow them to be sent through the internet, Pam Smith, president of Verified Voting, a non-profit voting advocacy organization in Carlsbad, Calif., said.

"Sending a voted ballot over the internet is fraught with risk" because "the internet is a dangerous place," Smith said. "If you don't have to put it online, don't," she said.

Early this year, state election boards in Arizona and Illinois suffered cybersecurity incidents. The hackers had various success in their attacks—no voter records were stolen in Arizona but election records were tampered with in Illinois. Regardless of the hacks' success, congressional hearings (189 PRA, 9/29/16) and national coverage of voting-system data breach risks have caused the public to question the integrity of the ballot box.

Voting Systems Secure

Although voters may have lost some confidence in the voting system, there is little risk to states that employ methods that don't connect to the internet.

There is little actual risk that states' existing voting systems will be hacked, Merrill said. This is because most states use voting systems that aren't connected to the web, she said.

Even if a ballot box of one state is hacked it doesn't mean the whole U.S. will feel the affects of the hacking attack.

The nation's election system is highly decentralized, and made up of thousands of local voting precincts, Merrill said. "When people talk about the hacking of the election system, there is no one system," Merrill said. Instead, it's a collection of 9,000-10,000 election jurisdictions by local communities, she said.

The decentralized voting system allows for a hack in one state to not affect the voter roles and outcomes in another state, she said.

Voter Confidence at Issue

The lack of perceived risk of a cybersecurity attack against a state election system doesn't seem to quell voters confidence that their ballot will remain secret.

"I'm most concerned about the panic surrounding cybersecurity" of the ballot box Merrill said.

There is little risk that other state's voter registration systems, which are online, will be hacked, Matthew Masterson, commissioner of the U.S. Election Assistance Commission, said. Most election officials around the country don't feel their systems are at risk, Masterson said.

"When you talk to election officials about threats to voting, they're worried about the janitor not opening up the gym in time for voting," Masterson said.

'Trying to Scare People.'

Not all state election officials agreed that state voting systems are immune from cybersecurity attacks.

Arizona Secretary of State Michele Reagan said Oct. 5 at a separate event that all state voter registration systems are vulnerable to intrusion and tampering.

"We need to take our heads out of the sand," Reagan said. State officials need to be made aware of the threat that voter registration systems will be hacked, she said at the Cambridge Cyber Summit, hosted by the Massachusetts Institute of Technology, the Aspen Institute and CNBC.

At the end of the day, the hackers may not have wanted the voter information but wanted to scare potential voters to lower their confidence in the U.S. system.

"They weren't after information they were trying to scare people," Reagan said. "And it did have the intended effect," she said.

The state has fortified its voter registration data, to make it less vulnerable to manipulation. "We got lucky and they couldn't get into our database," Reagan said.

http://www.bna.com/voting-cybersecurity-concerns-n57982078237/

McAuliffe: States central in thwarting cyber attacks
Augusta Free Press
October 8, 2016

National Governors Association Chair Virginia Gov. Terry McAuliffe delivered a keynote address as part of the first regional summit for his chair's initiative, Meet The Threat: States Confront the Cyber Challenge. The initiative focuses on developing state strategies for strengthening cybersecurity practices as they relate to state IT networks, health care, education, safety, energy, transportation and critical infrastructure, and economic development and the workforce. Nearly 30 states and territories were represented at the summit.

"The aim of my initiative as NGA chair is to replicate the work we have done in Virginia to best position all states and territories for meeting the cyber threat," Gov. McAuliffe said. "I know firsthand from my work in Virginia that governors and states play a critical role in confronting the ever-growing and sophisticated challenge of cyber attacks."

In his remarks, Gov. McAuliffe also highlighted the recent roundtables held on education and workforce, health, critical infrastructure, autonomy and internet of things (IOT). The roundtables were attended by nearly 40 cyber CEOs and experts in the various areas from the public and private sector.

On Monday, Gov. McAuliffe challenged all of his fellow governors to issue a state proclamation declaring October Cybersecurity Awareness Month, as he has done in Virginia.

One session at the summit, "Threat Briefing: Scope of the Threat," examined threats confronting states and the need to improve state cybersecurity postures to mitigate those threats. That session was led by Suzanne Spaulding, the Under Secretary for National Protection and Programs Directorate at the Department of Homeland Security. The summit, which concludes Friday, will also include plenary sessions on health, education sector and election security.

"Our aggressive approach to grow our cyber sector is a central part of our work to build a new Virginia economy that is diverse and capable of withstanding the uncertainty of sequestration and federal budget fluctuations," Gov. McAuliffe said.

The goal of the regional summits is to bring together policy leaders from every state, as well as private sector experts and federal partners, to highlight innovative practices and identify ways in which state-driven solutions can be replicated nationwide. The next regional summit will be held in San Jose, California, in the spring of 2017.

To learn more about Gov. McAuliffe's initiative, visit nga.org/MeetTheThreat

http://augustafreepress.com/mcauliffe-states-central-thwarting-cyber-attacks/

States Play Central Role In Thwarting Cyber Attacks

Business Solutions
By Christine Kern
October 10, 2016

October is National Cyber Security Awareness Month (NCSAM), a widespread initiative led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security (DHS) to highlight the need for tighter security in the fight against cyber attacks. In its 13th year, NCSAM chose the theme Our Shared Responsibility to emphasize the role every individual plays in creating a safer internet.

"As every one of us, our families and our communities become increasingly connected, it becomes even more critical to practice good cybersecurity habits," said Michael Kaiser, NCSA's executive director. "Each October is the commencement of a new effort to help every digital citizen and business across the globe learn how to take simple security precautions to protect themselves and their personal information and share the responsibility of protecting others online."

The FBI is one agency working to target the most dangerous and malicious cyber activity — high-level intrusions by state-sponsored hackers and global cyber syndicates — and the most prolific botnets, working collaboratively with domestic and international partners and the private sector.

In testimony before Congress recently, Director James Comey said, "The pervasiveness of the cyber threat is such that the FBI and other intelligence, military, homeland security, and law enforcement agencies across the government view cyber security and cyber attacks as a top priority."

And that shared responsibility extends to the state level as well.

In a recent keynote address at the first regional summit for his initiative, Meet The Threat: States Confront the Cyber Challenge, National Governors Association (NGA) Chair and Virginia Gov. Terry McAuliffe said, "The aim of my initiative as NGA chair is to replicate the work we have done in Virginia to best position all states and territories for meeting the cyber threat. I know firsthand from my work in Virginia that governors and states play a critical role in confronting the ever-growing and sophisticated challenge of cyber-attacks."

The initiative focuses on developing state strategies for strengthening cybersecurity practices as they relate to state IT networks, health care, education, safety, energy, transportation and critical infrastructure, and economic development and the workforce. Nearly 30 states and territories were represented at the summit.

Gov. McAuliffe also challenged his fellow governors to follow his lead in issuing state proclamations declaring October Cybersecurity Awareness Month. "Our aggressive approach to grow our cyber sector is a central part of our work to

build a new Virginia economy that is diverse and capable of withstanding the uncertainty of sequestration and federal budget fluctuations," McAuliffe said.

http://www.bsminfo.com/doc/states-play-central-role-thwarting-cyber-attacks-0001

Data Nugget: Going on Defense
Association Now
October 11, 2016

One state—and the association that represents it—is particularly aware of the number of cyberattacks taking place at any given moment.

Cybersecurity breaches remain a massive concern for everyone from political organizations to industry associations. The issue is a top priority for the National Governors Association, whose current chair, Virginia Gov. Terry McAuliffe, has some experience in the arena. His state, home to the Central Intelligence Agency and the Pentagon, has suffered a slew of cyberattacks this year.

53 million

The number of cyberattacks in Virginia since January—roughly one attack every four seconds

http://associationsnow.com/2016/10/data-nugget-going-on-defense-cyberattacks/