Workshop Report

Mason-NSF
Virginia Cities and Counties
Cybersecurity Partnership Workshop

October 3, 2017
Richmond, VA

Mason – NSF Virginia City and County Cybersecurity Partnerships Workshop
Review, Recommendations and Resulting Initiatives

The report reviews the discussion, recommendations and initiatives resulting from the Mason – National Science Foundation Virginia City and County Cybersecurity Partnerships Workshop held on October 3rd, 2017 at Library of Virginia in Richmond.

Acknowledgements

Many thanks to the National Science Foundation for funding support for the the NSF City and County Cross Jurisdiction Cybersecurity Collaboration Capacity Building project (Award Abstract: #1623653) of which the October 3rd workshop is a part.

And thank you to the participants and speakers from city, county and town governments from across the Commonwealth (please see Appendix I) for their insights, recommendations, vibrant discussion and participation.

Special appreciation is extended to Secretary Moran for giving the opening speech and to Mr. Issac Janak, Cyber Security Program Manager, Homeland Security and Resilience Staff, Office of the Secretary of Public Safety and Homeland Security, Commonwealth of Virginia, for his talk and participation. Special gratutitude is given to Ms. Alexis Wales from DHS for her talk on cybersecurity governance and continuous support and contribution to Mason's cybersecurity projects. Great appreciation is also given to Mr. Tom Duffy, Chair of MS-ISAC, for speaking at the workshop and for highlighting resources and support that MS-ISAC provides to local governments to enhance their cybersecurity. Last but not least, many thanks to Dave Jordan, Arlington County's Chief Information Security Officer (CISO) for his partnership on this local government cybersecurity initiative and for his talk and many insights during the workshop.

Workshop Background

The workshop is one element of the Mason National Science Foundation Cybersecurity City and County Cross Jurisdictional Collaboration project having the goal of furthering U.S. city and county cybersecurity efforts by developing foundations and policies that enable and foster city and county cybersecurity partnerships. The motivation for the project is that many U.S. cities and counties have relatively limited budgets and expertise to address the major and rapidly changing cybersecurity threat. In addition, many cities and counties are increasingly adopting connected and smart city technology for administration and citizen services. Local governments also play a major role in critical infrastructure such as electric, water and transportation systems. Approximately 60% of the U.S. counties have less than 50,000 residents but "nearly all counties play a role in the nation's critical infrastructure" (Council of State Governments, 2015). Energy, water, communications and transportation provide the foundation for city and county

operations and urban life and cities and counties are critical to the nation's resilience and emergency response.

Given cybersecurity expertise and budget limitations, partnering among cities and counties in areas such as cybersecurity governance, staffing, procurement, leadership, training and information sharing, cities and counties are better able to address their cybersecurity needs.

The NSF project includes statewide workshops in four states with the first the October 3rd workshop Commonwealth of Virginia focusing on Virginia and held in Richmond. The objective of the Commonwealth of Virginia workshop was to develop Virginia specific policy and legislative recommendations to enable and further foster Virginia city, county and town cybersecurity collaboration The Virginia workshop has led to the planning and scheduling of regional Virginia workshops amongst cities, counties and towns to discuss steps they might take together. The first is planned for the Northren Neck and Middle Peninsula region in May 2018 and the second in the Loudoun, Leesburg and Purcellville region in June 2018.

The result of the four workshops will be the development and dissemination of a City and County Cybersecurity Partnerships Toolkit, associated Readiness Assessment and ongoing development and exchange of case studies and best practices on city and county cybersecurity partnering.

Workshop Next Steps

There are two main types of initiatives following on from the workshop:

- Developing city, county and town cybersecurity partnering initiatives, capabilities and sharable materials in the areas of Governance, Communications, Technology / Procurement, and Staffing (as shown in Figure 1 below);

- Fostering and facilitating partnering amongst Virginia cities, counties and towns on these and other cybersecurity partnering initiatives that are of most interest, priority and potential impact.

  Initial initiatives resulting from the workshop are:

  - Sharing and exchange of cybersecurity and privacy policies (providing by Arlington County)

  - Development of Commonwealth of Virginia city, county and town cybersecurity point of contact lists

  - Working with vendors for the development of packages of cybersecurity services that can be jointly procured by several or many cities, counties and towns.

- Holding regional workshops in the regions of the Commonwealth where there is an interest with the objectives of exploring possible areas of cooperation and building upon the workshop discussions.

As noted, Figure 1 depicts subject areas of potential city, county and town cybersecurity partnering as discussed and recommended in the workshop.

The subject areas are divided into the categories of:

Governance – Virginia's cities, counties and towns have developed a full range of cybersecurity policies, strategic plans and incident response plans and are continuing to develop policies in current focus areas such as industrial control systems and third party vendor security. Many of these are potentially adaptable to other cities, counties and towns.

- **Communications** - with the objectives including enhancing cybersecurity related communication amongst cities, counties and towns and Virginia government on an ongoing basis in cybersecurity strategy, governance and best practices in time of emergency by compiling (and then utilizing) a contact list of cybersecurity leads or points of contact for each of the Virginia cities, counties and towns

- **Technology / Technology** Procurement – in the areas of partnering on technology licenses and exchange of best practices in technology procurement.

- **Joint Staffing** – including for both cybersecurity leadership and management positions and shared amongst two or more cities, counties and towns; and also for cybersecurity staff.

- **Supplemental and Cybersecurity Partnering Seed Funding** – Supplemental cybersecurity funding for Virginia cities, counties and towns would be tremendously helpful especially as their operations and citizen engagement are becoming more reliant on IT in general and also due to increasing critical infrastructure connectivity and cybersecurity risk. As parallels the public schools have access to technology equipment grants through the Virginia Department of Education and also public safety through U.S. Department of Homeland Security. Cybersecurity Partnering Seed Funding might be of assistance in establishing regional cybersecurity partnerships and collaborations amongst cities, counties and towns.

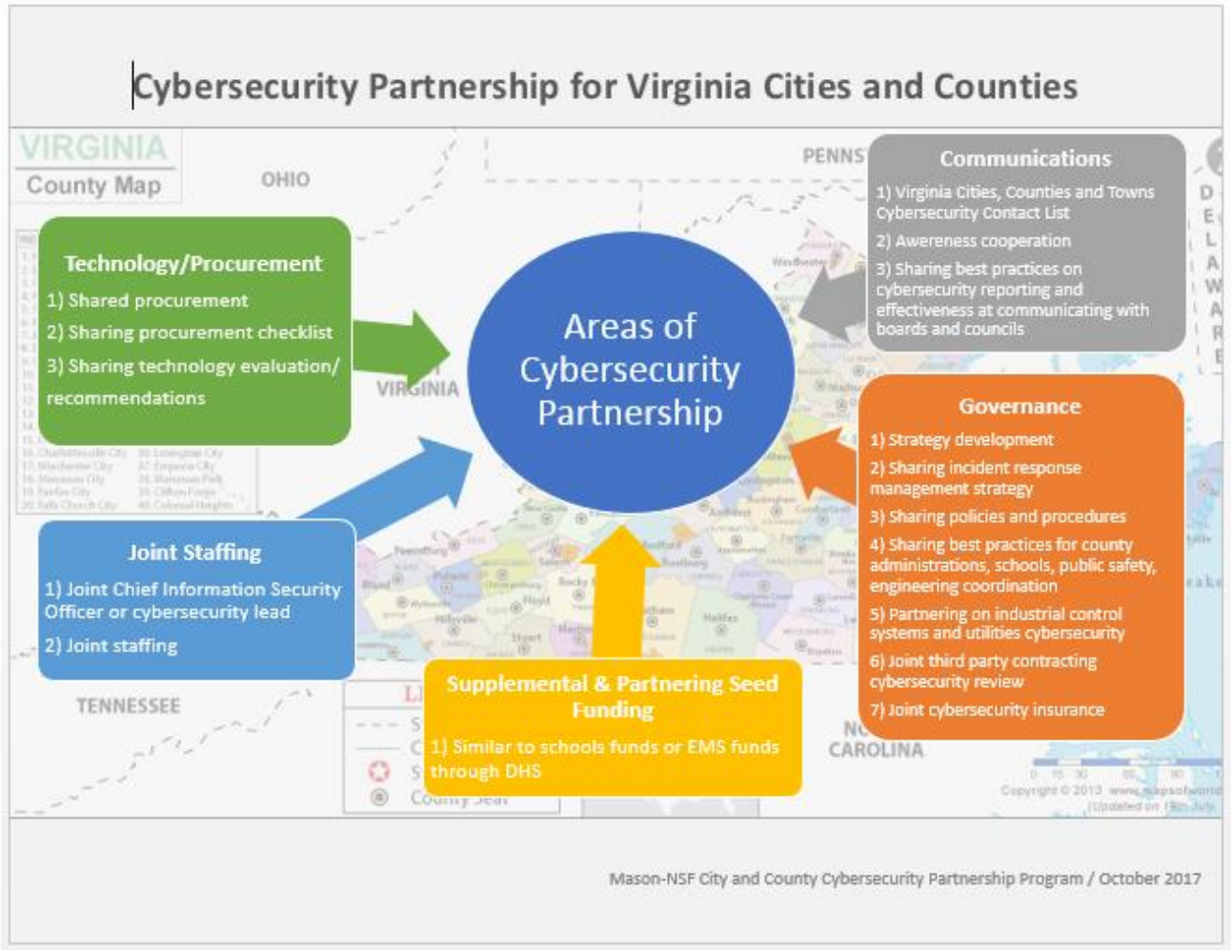

Figure 1 – Potential areas for cybersecurity partnering for Commonwealth of Virginia counties, cities and towns

Workshop Review and Notes

I. Secretary Moran's Opening Speech

Secretary Moran, Secretary of Public Safety and Homeland Security, Commonwealth of Virginia opened the workshop by highlighting the importance cybersecurity and the potential risks, vulnerabilities and cascading effects of a cyber attack on the nation's infrastructure. Secretary Moran pointed out,

> *"Cybersecurity is a key priority of the Commonwealth's security agenda."*

He noted that last year, as the Chair of the National Governor's Association, Governor McAuliffe chose "Cybersecurity" as the year's initiative. Secretary Moran discussed recent McAuliffe Administration and Commonwealth initiatives including the Virginia Cyber Security Commission which was established in 2014 by Governor McAuliffe's executive order, to bring industry leaders from across the Commonwealth as well as representatives from the McAuliffe Administration to make recommendations on how to make Virginia a leader in cybersecurity. Secretary Moran aslo highlighted the role and contribution of the Virginia Fusion Center and the National Guard and encouraged local participants to utilize these state resources.

II. Virginia County, City and Town Experiences

The attendees provided insights on the cybersecurity strategies, experiences and challenges for their counties, cities and towns which are organized below by major discussion topic area.

a. Interest in Partnering and Areas of Potential Partnership

There was a consensus that partnering among cities, counties and towns on cybersecurity has promise to overcome some of the challenges of limited cybersecurity budgets and expertise.

Large City
"There is a big gap between low level threat and high level action. There's the in-between level, where I can see partnering working. That's where policies and business plans come into play. These are things we all need to do and are probably doing right now. For example, there could be policy/procedure templates that most of us can use. There is a lot of commonality between what we are doing. We could all benefit from sharing in this area. It's just a question of how and what to share."

Large County
"We have 23 jurisdictions around the nation's capital region. The security executives of these jurisdictions formed a group, which convenes regularly to share threat intelligence and good practices. Conference calls are conducted regularly. I believe CISOs of these jurisdictions need to know each other and reach out to each other quickly if needed."

"As our local government operations matured, we started to accumulate documentation. For example, when we first started, people started going out and buying applications without asking important questions. We developed a 50 question questionnaire for vendors. This way, the vendors were asked questions early on and learned about what our expectations are. If they cannot answer "yes" to all the questions, their chance of getting this business is significantly less.

We also have documentation on Non-Disclosure Agreements for vendors and contractors. We started sharing this documentation with other jurisdictions."

Midsize City

"These incidents tell you that for a city of our size, we don't have the resources to deal with incidents like this. We don't have the man power to handle this. So my question is – Can we share expertise somehow? So we have some expertise we can all call on should we have problems like this."

Smaller County
"Most IT collaboration is informal. I'd love to see the state local government IT professionals community sharing information in a systematic manner. Next challenge is how to educate our city managers and build communications at the managerial level."

Midsize Town
"The County and Town IT work together under an MOU agreed ten year ago. We share resources, software. County and Town IT staffs meet monthly – benefit of learning what they are doing and what we are doing. A trust relationship is important - we are a good team."

Midsize Town
"We do not have sufficient policies. There should certainly be policies that can be used across the board. We need more priority on Data Loss Prevention (DLP). Data Loss Prevention tools would be another area of potential sharing. Another possible benefit of partnership is sharing the cost of training."

b. Scope of Responsibilities and Challenges

- *Many cities and counties are undertaking and plan to undertake "smart" city initiatives including multichannel service delivery for citizen services. These initiatives increase access and facilitate the transactions while at the same time increasing the role and importance of information technology and correspondingly increasing cybersecurity risk.*

- *In addition, many cities, counties and towns in Virginia own and operate critical infrastructure. These include water, water treatment, electric, traffic control systems and airports.*

- *The lack of financial resources and talent, and the ability to retain cybersecurity talent are a major challenge to Virginia cities, counties and towns. Most small to midsize local governments do not have their own or sufficient man power to develop cybersecurity strategy and policies, manage day to day cybersecurity and to address security incidents and breaches.*

  Midsize County
  "Major challenge is lack of resources and talent, and the ability to retain cybersecurity talent."
  Midsize City
  "We do not have a CISO. We do not have the funding yet. We have a risk manager in our finance department, who sort of has that responsibility."

  Midsize County

"Understaffed and underfunded. Bigger fish are getting protected. We are becoming the easy targets."

- *Decentralized IT operations not only make it challenging to implement standards and procedures, but also increase the cybersecurity staffing challenges for local governments. The IT collaboration amongst local government, school administration, fire and emergency departments, and utility authorities varies significantly from city to city, county to county, and town to town.*

  Midsize County
  "Our school IT is completely separate. I think it is not a good approach to resources and personnel. Especially as it is hard find IT professionals in general and given what we are able to pay in salaries."

- *Differences of technology and systems remain an obstacle to governments working together operationally.*

  Large City
  "We have a central IT group and have twelve to thirteen additional decentralized IT groups. Correlating standards and procedures across all these IT groups becomes a challenge."

- *Cybersecurity leaders need to be included in administration and board discussions on cybersecurity and cybersecurity risk. This can be especially challenging when a cybersecurity officer reports to the CIO instead of the board. To be successful, cybersecurity leaders should communicate with administration and the board in strategic and risk terms that the board understands and embraces.*

  Smaller County
  "For our elected officials, the key is to educate the Board – to create a compelling story. Make it in practical terms. From my perspective, it's about communications. Example - "This is our vulnerability and associated risks to our citizens. We need to do XYZ or something will happen." Of course, there are competing priorities. In my view, cybersecurity is on par with public safety. It may not be loss of life. You lose your identity, somebody has control over that. My advice – find a way to tell the story. Align your message with value to the elected local officials. You may still receive "nos". We are getting a better understanding on security and what we are facing. It's a bit easier – we are getting there."

- *For many city, county and town officials and board members, cybersecurity is not at the forefront of their agenda, especially given many competing priorities.*

  Smaller County
  "We are moving to the cloud and to increased citizen electronic involvement. We have one IT vendor that builds most of the systems and manages network needs. Some Board members don't see cybersecurity as important. They are not personally affected and don't see the risks. Diversifying the tax base is what's important for the Board."

- *Audits and assessments including by DHS and National Guard are very helpful as a snapshot and highlight focus areas for local governments including on cybersecurity policies and governance.*

- *Overall though, annual audits and assessments are not sufficient and ongoing governance requires assessments at machine speed and in real time.*

Smaller County
"We had DHS undertake an assessment. They did a vulnerability study for SCADA systems, water utilities, dams, and power. We were able to make some improvements. The Virginia National Guard did an assessment for us as well this year."

- *Cities, counties and towns are having success with training and awareness.*

Midsize County
"Recently we had a Virginia National Guard Cybersecurity team assess our system. It's a service that's worth $50,000 to $100,000 value. They did a fantastic job and some of the results were very revealing. They did social engineering testing along with penetration testing of the network. They traditionally find that 25% of staff respond to phishing emails. Our staff did better at xx%. In addition, we had open our email filters to let the phishing emails in. So normally many of the phishing emails wouldn't have reached to our staff. We try to balance that with our annual mandatory training and see how well the training improves our staff behavior. You are only good as your weakest link. People will always be our weakest link."

c. Cybersecurity Planning, Strategy and Initiatives and Recommendations

- *Since all governments, regardless of size, will need to have good policies and procedures in place, many believe sharing the language used in policies and procedures, especially contributions by more cyber mature and established governments, will be extremely beneficial to other local governments. A good example is the procurement questionnaire that can be shared among governments across the Commonwealth.*

Large City
"We tried borrow and adapt as much as possible. We started with NIST cybersecurity framework which we embraced. The framework provides a common language for communicating with upper management in describing priorities and the steps to protect the enterprise. The framework is written in business terms, rather than technical terms."

- *Security officers (or points of contact, if no security officer available) of each local government should form a network and connect regularly, and timely in time of emergency.*

- *As with policies and procedures, all governments need to provide timely and effective training to their employees to minimize human-triggered security breaches, the most common types local governments*

face today. It makes a lot of sense to standardize the curriculum and requirements of the training, and alleviate the burden many small and budget-stringent governments face to come up with their own training protocols.

- *Although sharing full-time staff can be difficult due to different retirement and benefit plans among different local governments, sharing the expense of hiring contractors could be a possible solution in alleviating personnel cost and availability. This applies both for hiring for cybersecurity management as well as staffing.*

- *Patch management is another area of potential partnership, where local government members can get together and collaboratively utilize contract benefits.*

- *Security managers would benefit from shared best approaches in communicating with senior management and the board in getting the understanding and support they need in advancing their security priorities, before major incidents happen.*

- *Several presenters mentioned the adoption of cybersecurity insurance, as an add-on to existing fire and other security insurance policies, in boosting their cyber defense.*

Large County
"We have insurance that covers county vehicles. When we bumped that insurance to $5 million, cyber insurance is covered."

Smaller County
"We don't have cyber insurance. This is a good question and another good area for sharing."

III. Critical Infrastructure

Many Commonwealth of Virginia counties, cities and towns own and operate electric, water and sewage facilities. In addition, some Virginia counties, cities and towns own and operate traffic systems and airports. With the convergence of information technology and industrial control systems for critical infrastructure, participants thought that partnering together on critical infrastructure cybersecurity has great potential.

IV. DHS, MS-ISAC and Commonwealth of Virginia

a. Department of Homeland Security

Alexis Wales, Branch Chief, Cybersecurity Governance, Federal Network Resilience, Office of Cybersecurity and Communications, Department of Homeland Security

DHS aims to help local governments to build their cybersecurity capacity through information sharing and incident response. In particular, DHS' National Infrustructure Protection Directorate (NIPD) works with local governments directly in their efforts to safeguard the nation's critical infrustructure. NIPD provides monitoring and technical assistance, as well as hosts regular workshops and foster the exchange of best practices.

Security will continue to gain attention from local government Boards in the near future as local governments continue to become more connected systematically and are going toward cloud computing. In the scenario of a smart city, security is as important as technology.

Good cybersecurity governance drives successful operations. It is important that local governments understand and adopt good governance practices, including but not limited to:

- Develop robust understanding of critical systems – how they operate, what they depend on, what depends on them, and what its failure looks like
- Performance management
- Early detection and continuous monitoring - identify the signs that information systems are not behaving as expected (as indications and warnings are critical to getting ahead of a crisis)
- Incident response plan to a wide variety of incidents, including those that may seem impossible
- Crisis communication – build deeper relationships with key players prior to crisis.

b. Commonwealth of Virginia

Isaac Janak, Cyber Security Program Manager, Homeland Security and Resilience Staff, Office of the Secretary of Public Safety and Homeland Security

National Guard, Virginia Chapter and Commonwealth of Virginia's Virginia Fusion Center (VFC) offer information sharing and operational support to local governments. These programs provide on-site evaluations on local governments' security operations. City and county governments should explore these resources if they have not already. Several presenters commented on the benefits such assessments provided their operations.

Virginia Cyber Commission. In two years, made policy recommendations focusing on cybercrime and infrastructure protection

Virginia Fusion Center (72 around the nation). Formed after September 11th to address the gap of information sharing at the state and local government level, the Virginia Fusion Center:

- Cybersecurity information sharing
- Coordination of incident response
- Investigative support.

Virginia National Guard
Virginia is home to the nation's 1st Cyber Brigade which does cybersecurity evaluations at the local level and augments support during cyber emergencies. The process to request incident response support is to call the Commonwealth emergency management office who will contact the National Guard team. They are usually on site for a week, and will usually interact for several weeks with the requesting government.

Virginia Cyber Incident Response Plan: responsibilities of threat asset, information coordination and network protection; notification including internal and external incident notification with thresholds forthreat to life and safety, physical impact; and data breach, impact to mission essential functions.

Notification process: Victim – Virginia Fusion Center; Asset Response (DHS, National Guard, Virginia Department of Emergency Management (VDEM)) and Threat Response (Virginia state police, FBI).

Available Cyber Grants from FEMA - State homeland security grant program. Managed by VDEM. Projects must be sustainable, map to reducing cyber risks, no technology procurement (preferred). Oriented towards policy development and training.

c. MS-ISAC

Tom Duffy, Senior Vice President of Operations, Chair, MS-ISAC, Center for Internet Security

Federally funded program, MS-ISAC, provides advisory and alert on vulnerabilities and attacks to state and local governments. MS-ISAC also offers network monitoring and sends out weekly newsletters. MS-ISAC also has an incident response team that goes out and respond to specific cases and offers distance learning opportunities. Their highly useful service is free of charge. Currently only 22 VA local governments, or governmental entities are members of MS-ISAC.
Any local authority is eligible to become a member of MS-ISAC. Current, MS-ISAC local members represent 60% of U.S. total local authorities. A large majority of the memberships is represented by large jurisdictions and authorities in major urban areas. The rest of smaller and rural government entities. Currently there are 22 MS-ISAC members in the Commonwealth of VA.

MS-ISAC offers and recommends a wide range of free resources to its local government members, including but not limited to:

- Through its Intrusion Detection Systems (IDSs), MS-ISAC has been able to monitor major systems, detect vulnerabilities, identify traffic patterns, track and cover attacks, and sent out weekly newsletter, with timely and actionable alerts and recommendations.
- MS-ISAC's Cybersecurity Intergration Center (NCCIC) has started to repond to incidents, about 200 cases a year. Last year, there was a lot of ransome ware. This year, rasome ware attacks decreased. About 90% of the incidents had to do with patching.

- MS-ISAC recommends the federal program, the National Cybersecurity Assessment and Testing Service (NCATS), which scans site and identified outdated servers; or the Vulnerability management Program, which profiles 1700 government websites every week and sends out daily advisories.
- National Cybersecurity Review, which was developed based on NIST cybersecurity framework, allows member governments to self-assess. Assessment report can be compared to the framework and to national peers.
- MS-ISAC also work on vendor discounts on behalf of local governments. For example, MS-ISAC members get 55-75% rates with SANs. A free online cybersecurity training program, Federal Virtual Training Environment (FedVTE) is also available for local government employees.

MS-ISAC also runs a mentoring program, where senior cybersecurity professionals mentor new staff.

Large City
"We've been member MS-ISAC for a while. They provide timely information on what's going on, current threats."

Midsize County
"Through MS-ISAC, we get alerts. But with a staff of four, it is challenging to process all that information."

Large County
"Each of the 130 Virginia local governments need to be members of MS-ISAC. Cybersecurity problems will arise. MS-ISAC has conference calls each month. And have hundreds of local government members."

Appendix A – Workshop Speakers and Participants

Speakers

Secretary Brian Moran, Secretary of Public Safety and Homeland Security, Commonwealth of Virginia
David Jordan, CISO, Arlington County
Andy Stein, Director of Information Technology, City of Newport News
Mike Goetz, Director of Information Technology, City of Lynchburg
Bill Hunter, Director Communications & Technology, County of Roanoke
Mike Culp, IT Director, Albemarle County
Sandra Graham, Information Security Manager, Chesterfield County
Larry Clement, IT Director, Orange County
David Moorman, Deputy County Administrator, Botetourt County
Julie Kaylor, Deputy County Administrator/Clerk, County of Mathews
Tim Grant, Director of Technology, Warren County Public Schools
Alexis Wales, Branch Chief, Cybersecurity Governance, Federal Network Resilience, Office of Cybersecurity and Communications, Department of Homeland Security
Tom Duffy, Senior VP of Operations, Chair, Multi-State ISAC, Center for Internet Security
Isaac Janak, Cyber Security Program Manager, Homeland Security and Resilience Staff, Office of the Secretary of Public Safety and Homeland Security

Participants

Mark Barham, Director of Information Technology, City of Williamsburg
Logan Blystone, Applications Support Specialist, Prince George County
Warren Bowman, Security Officer, Henrico County
Jesse Budd, Systems Technician, Warren County Public Schools
Dianna Catron, Director of Information Technology, Apps & RM, County of Culpeper
Kirsten Cherry, Director of Information Technology, County of Prince George
Larry Clement, IT Director, County of Orange
Andrew Crane, Information Systems Specialist, County of Nelson
Christie Crouch, IT Administrator, Town of Bedford
Mike Culp, IT Director, Albemarle County
Tonya Estes, Director of Information Technology / GIS, Town of Culpeper
James Finney, Protective Security Advisor, U.S. Department of Homeland Security
Ben Fox, Director of Information Technology, Accomack County
Harry French, Director, Information Technology and Telecommunications, Charles City County
Brian Gibbs-Wilson, CISO, Virginia Department of Education
Mike Goetz, Director, IT, City of Lynchburg
Timothy Grant, Director of Technology, Warren County Public Schools

Rodney Gray, Technology Services Manager, Botetourt County
Harry Guilford, Network Technician, Warren County Public Schools
Bob Hardy, Director, Information Technology, Louisa County
RobertHeadley, Director of Information Technology, Northumberland County
Bill Hunter, Director, Communications & Information Technology, County of Roanoke
Charles Huntley, Director, Information Technology, Essex
Isaac Janak, Cyber Security Program Manager, Virginia Office of Public Safety and Homeland Security
Julie Kaylor, Deputy County Administrator, Mathews County
Casey McCracken, IT, County of Augusta
Thomas McKnight, Assistant Director of Information Technology & GIS, Town of Culpeper
RobertMooney, Protective Security Advisor, U.S. DHS
David Moorman, Deputy County Administrator, Botetourt County
Mike Mullins, Information Technology, Loudoun County
Tom Owdom, Information Technology Director, Henrico County
Michael Pearse, Public Safety Technology Manager, City of Winchester
Don Spady, IT Manager, City of Manassas Park
Andy Stein, Director, Information Technology, City of Newport News
Hiram Tackett, Systems Engineer, City of Staunton
Jackie Vair, Director, Information Technology, Amherst
Sean Whitfield, Information Technology, Manager, City of Manassas
Jackie Zetwick, Director of Information Technology, County of Augusta

Mason-NSF Virginia City and County Cybersecurity Partnership Workshop Report
Oct. 3, 2017

Report is part of NSF Funded Project: City and County Cross Jurisdiction Cybersecurity Collaboration Capacity Building (Award #1623653)

Primary Contact:
Dr. J.P. Auffret
George Mason University
Phone: 703-993-5641 Email: jauffret@gmu.edu