WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

Office of Privacy and Data Protection

National Governors Association Cybersecurity Policy Academy Washington State Report

July 2, 2022

Table of contents

Participants

Core Team

- Team Leader: Vinod Brahmapuram, former state Chief Security Information Officer – WaTech/OCS
- Administrative Contact: Sarah Colvin – WaTech Office of Cybersecurity
- Katy Ruckle - WaTech Chief Privacy Officer (state and local privacy).
- Lisa Brown - WA Department of Commerce (Broadband, Workforce Development).
- Adjutant General Bret Daugherty - WA Military Division | Mark Glenn - CIO (Emergency Management).
- David Danner - Utilities and Transportation Commission Chair (Critical Infrastructure).
- Pat McCarthy - WA State Auditor (Cybersecurity assessment/evaluation).

Home Team

- Eli King - WA Director of Energy Emergency Management
- Justin Burns - WA Secretary of State CISO
- Robin Lang - WA-EMD, Cyber and Infrastructure Manager
- Dr. Barbara Endicott – University of WA Exec. Dir.- Center for Information Assurance and Cybersecurity.
- Zack Hudgins - WaTech Privacy Manager for local government

Introduction

The National Governor's Association (NGA) Whole of State Cybersecurity Policy Academy convened state and local government stakeholders during 2020-21 to address common challenges. This report summarizes the discussions and highlights recommendations.

Cyber threats are a proliferating hazard to state, local, and tribal governments, as well as private industry and operators of critical infrastructure systems. A "whole of government, whole of community" approach is needed for response to significant cyber events to mitigate the risks and protect critical infrastructure.

The state of Washington engaged with the National Governor's Association in a cybersecurity policy academy to address three key questions:

- What recommendations do local governments have to prevent, mitigate and recover from cybersecurity incidents?
- What can the state government do to help increase the flow of talent into the technology workforce, and cybersecurity workforce in particular?
- Which entities are working towards these goals?

The WaTech Office of Cybersecurity (OCS) and the WaTech Office of Privacy and Data Protection (OPDP) invited stakeholders together to discuss these issues in a series of meetings. Guided by the NGA Cybersecurity Policy Academy – in conjunction with local, state and tribal partners – recommendations were collected and discussed.

Over the course of a year, discussions and virtual meetings were held to examine roles of entities within cybersecurity, needs of various organizations, models of governance from other states, challenges faced that were seen to be common to many organizations, and recommendations for consideration or implementation towards an improved cybersecurity posture in Washington state.

During the COVID-19 pandemic, the NGA helped to convene state and local leaders for ideas on addressing challenges. An initial assessment of state agencies and others addressing the cybersecurity challenges of the day was an agreed upon first step. During this assessment, recommendations were gathered.

This report is a snapshot, or inventory of roles, and recommendations offered to policy makers, as the concept of 'whole of state' cybersecurity is explored for implementation for better defense against cyberattacks.

None of the recommendations should be seen as a reflection of current preparedness, but rather suggestions for a more robust system of defense and recovery based on best practices. Cybersecurity, like privacy, is a journey and not a destination. This report offers suggestions for possible steps forward.

Areas highlighted in this report include:

Recommendations from Local Governments: With the wide diversity of size and resources within local governments, recommendations centered on better communication, utilizing market power for services and creating services that could be scaled to other entities.

Workforce Development: One consistent theme that came from discussions across many sectors was the need for attention to workforce development. The need for general technologists, cybersecurity specialists, entry level positions, and a more robust pipeline of workers was echoed by state, local, tribal governments as well as non-profits and educational institutions. The need for these workers is not limited to the technology sector in our state.

Other recommendations: There were many other general recommendations that focus on general cyber hygiene, cyber and data governance. This was an area where discussions and models from other states proved most interesting to many in the NGA meetings as many states have encountered similar challenges with cybersecurity oversight or implementation.

Stakeholders: This report takes a snapshot of many stakeholders that are trying to address some aspect of cybersecurity or privacy issues in our state. Continued communication across these many stakeholders will enhance any cybersecurity responses that may be needed.

In conclusion, cybersecurity threats are not going away. Continued attention, resources and communication will be required to successfully protect residents' data, infrastructure, and services.

Recommendations from Local Government

State training assistance: Local governments would greatly benefit from standardized training in privacy policy, as well as cybersecurity policy, laws and best practices. Developing standardized training would assist all jurisdictions large and small across the state.

Sample preparedness checklist: The state could provide a checklist of common issues or pitfalls, based on risk assessment processes, that may cause a breach or security threat. This checklist, plus relevant, actionable information can be on a cybersecurity state hub for easy and scalable access from local governments. Information can also be sent out via regular newsletters, podcasts, videos, and a local government guidebook.[1]

Stay familiar with resources: All government entities should be constantly improving their cybersecurity profile, awareness and programs. This can be done in an affordable way by staying up to date on available resources from trusted organizations like Homepage | CISA. [2]

Sample contract / vendor checklist: The state could provide a preferred vendor list and a general or standard contract for IT vendors. The state could also provide a contract checklist for hosted systems. This could include a developed framework that can be adopted by all agencies, consistent with statewide policy and CJIS

Develop communication plans: The state could offer templates for sample communication plans developed with local government in mind for security and privacy incidents. Plans could be synchronized with incident response plans, checklists for who to contact, and what information should or should not be shared with stakeholders during different points of an incident.

Develop a local government privacy framework: As privacy policy becomes more important, local government would benefit from the state standardizing and developing a model privacy framework and then supporting privacy capacity in implementation.

[1] cybersecurity-plan-2021.pdf (in.gov)

[2] As an example of a resource from CISA, here is a briefing tip sheet on ransomware: Protecting Against Ransomware | CISA

High level expertise availability: Local governments know their networks better than anyone else, but they still need access to more expertise. Audits, assessments and policies provide great roadmaps, but local governments often lack high-level expertise and funding to implement necessary changes. The state could provide this temporary assistance.

Standard playbooks: The state could help local governments with standard playbooks for cybersecurity incident response, e.g. ransomware, data breach, email compromise, website defacement, etc. In the same way the state could provide a checklist for prevention of incidents, the state could provide a playbook for reacting to a cybersecurity incident.

Monitoring: While local governments will continue to monitor and maintain their networks, the state could assist with implementation of cyber hygiene and penetration testing protocols to prevent security incidents. This could take the form of memorandums of assistance or mutual aid, access to expertise and state agency resources.

A more robust partnership: As the state builds out a more robust 'whole of state' cybersecurity and privacy standard, the partnership between state, local and tribal governments should be made more formal. A primary focus of the partnership should be better pooling of resources and capabilities. This relationship can focus on:

1. Providing coordinated responses to cyberattacks at all levels of government.
2. Providing statewide access to cloud-based phishing and security awareness training.
3. Expanding cyber audits to assist local and other governments.
4. Provide penetration testing if requested by local or other governments. A penetration test (pen test) is a simulated attack that uses the same methods as attackers to find and remediate weaknesses in a system.

A mutual aid framework: The state could develop a system framework for mutual aid of different jurisdictions to assist with urgent needs for support from technical personnel throughout the state. This framework should consider costs, amount of access, insurance liability, decision-making processes, and other complexity that comes with cyber incidents.

Response help: The state should formalize response assistance for local governments. The state could provide a temporary mitigation response team partnership. This could take the form of a hotline to call, potential receipt of onsite services – assistance, support, monitoring, coordination with other jurisdictions or insurance companies.

Practice: The state can both provide tabletop exercises (e.g. ransomware response) and review and improve existing response procedures directly for other jurisdictions.

Broad plan access: Local governments should have access and updates to cyber incident response plans to address gaps, including local government components of the Washington State Comprehensive Emergency Management Plan. Other critical infrastructure planning should include local governments.

Expand the network: The state, through existing work at the Department of Commerce and the IT community, can identify resources for workforce development for local governments through partnerships with institutions of higher education, apprenticeship programs, and the private sector.

Cybersecurity Insurance: Insurance costs and requirements continue to escalate for many governments. Operating without proper cybersecurity insurance is difficult to contemplate for most government agencies and jurisdictions.[3] The state could help with the preparation of increasingly difficult requirements for cyber insurance, and work to bundle service for state and local governments to assist with cost containment.

Recovery: The state could allow for the use of the State Data center for network recovery.

Recommendations for Work Force Development

Standardize and sync IT job descriptions: State government should strive to adopt the national NIST/NICE standards and incorporate the associated skills into existing security classifications and position descriptions. Current jobs classifications should be mapped to skills required and training required for that job function.[4] The public sector should collaborate with the private sector and industry partners to improve and update security related job classification and position descriptions.

Create entry level positions and career ladders within state government: State government should recognize that entry level positions will lead to future talent. More entry level positions should be created within and across state government. The state and local governments are perfect places to give hands-on experience and build these professional networks. These networks will also benefit government and other professionals in the cybersecurity ecosystem.[5]

Create an entry level IT paid internship or apprenticeship program: While there is some work being done at state agencies to create a paid internship program, this could be an excellent source of future government talent. Agencies need to work through the structure, supervision, and duties of paid interns, and could foster career paths for entry level employees. A robust program that coordinates across state agencies and utilizes past intern programs could benefit both individuals and state government.

Recruit talent to public sector with two approaches: benefits of public service and updated pay bands: The multitude of benefits of public sector service should be highlighted in job descriptions and recruiting. These benefits include flexibility in work location, ability to telework, generous leave options and an emphasis on a work/life balance. Pay scales and pay bands should be as competitive as possible with the private sector and updated on a yearly basis to adjust to changes in the marketplace.

Focus recruiting on specific groups of people with talent: Many organizations are training IT professionals and technologists with an eye towards under-represented communities. The state should continue to reach out to these communities that are highly sought after, including military veterans, women, and communities of color. By partnering with organizations producing IT talent, the state may get first access to public sector recruitment.

State government can harmonize training with job skill needs: Educational institutions need to be clear about the skills they are imparting, while employers need to be transparent about the abilities they need. This harmonization should include certifications often listed as desired qualifications, instead of requirements in job announcements. Adoption and implementation of national job classification standards would help.

[3] Is Cybersecurity Insurance Out of Reach for Government? (govtech.com)
[4] The Workforce Framework for Cybersecurity (NICE Framework) | NIST
[5] Executive Partnerships Are Critical for Cybersecurity Success (darkreading.com)

Conditional scholarships for high demand jobs: State government can offer public service scholarships at all levels to recruit technology talent. Scholarships could take the form of re-training for a specific job, additional training for certifications, initial training and education, or capacity with NGO programs. The scholarships would be forgiven after a period of public service in the high demand job. These models exist in other sectors. This should be part of the expanding talent pipelines approach that considers applicants with nontraditional experience. This can also be part of engaging more K-12 students in cybersecurity while reaching beyond usual sources of recruiting.[6]

Mid-level up skilling is a must: Instead of focusing solely on competition with the private sector for new talent, government organizations should also work to retain their current workforce. Many IT professionals can be up skilled and cross trained. State assistance for local governments to retain their workforce while cross training on the many needs facing smaller jurisdictions would have enormous benefit.

Establish a single point of cybersecurity coordination and outreach: A single point of coordination to help all jurisdictions utilize available state and federal resources would benefit the people of Washington. Often, in local government, many IT professionals are unable to explore a new federal program, or NGO resource that would benefit them. Capacity is stretched so thin in many jurisdictions they are unable to benefit from free trained interns, or Department of Defense (DOD) funded cybersecurity assistance.

Look for new ways of attracting talent: The public sector needs to differentiate the pitch for cybersecurity and privacy talent and look for a different set of skills. Public service, a clear mission, regular work hours all contribute to quality of life for workers in a way the private sector can't always deliver on. The future of recruitment also requires looking for new skillsets as well. Instead of simply looking for products of four-year programs, public sector recruiting needs to seek people with technical abilities and soft skills. As IT and cyberthreats evolve, being able to embrace the unknown will help solve problems. An ability to connect with elected leaders and tell a compelling narrative will assist with budgets and project funding. And a natural curiosity will help see over the threat horizon as information comes from many non-IT sources. [7]

Provide 'a la carte' privacy and cybersecurity assistance to local governments: Local governments have such varying needs and capacities across the state that one size of assistance rarely helps everyone. The state can organize its assistance in a way that allows local governments to decide what best benefits them and compare to options they already are aware of or utilize.

Expand broadband access – close the digital divide: Many Washingtonians are unable to benefit from online access due to unavailable or slow internet connections. Expanded broadband access will increase economic opportunities as well as individual talent.

Prepare for jobs and demands of the future: The state must not only look at filling its current IT, privacy and cybersecurity needs, but also to future talent requirements. This means looking broadly at cloud adoption, artificial intelligence use (and human support), and machine learning (with human oversight and interaction.) Governments at all levels should begin to nurture and recruit or train for its future needs.

[6] Did the Cybersecurity Stakes Get Even Higher in 2021? (govtech.com)

[7] https://media.erepublic.com/document/GT20_HANDBOOK_ATT_SecuringNetwork_Slides_v.pdf

General Recommendations

Suggestions for better performance and efficiency were discussed in depth and those recommendations are reflected below:

Start with an assessment: Local governments should start their process with a self-assessment of their cybersecurity program. The Cybersecurity and Infrastructure Security Agency (CISA) has a free assessment tool - Cyber Security Evaluation Tool (CSET®) | CISA.

Local Emergency Managers: One lesson learned during the COVID-19 pandemic was that the same people responsible for natural disasters were often called upon to deal with other kinds of emergent needs. Providing for some surge assistance for local jurisdictions would assist responses.

Cybersecurity Annex: The Washington State Comprehensive Emergency Management Plan (CEMP) was written in 2015, and while policies and procedures have evolved in a dynamic way to address the ever-changing threat landscape, there is general agreement that the response plan could use a refresh.

Government continuity and recovery: State and local governments should design continuity of operations and data recovery strategies around recovery time and data loss reduction. These strategies should include building and documenting policies and procedures, testing data recovery and continuity of operations plans, adapting those plans and sustaining plans into the future.

Pass a data protection law with enforcement: Privacy laws like the General Data Protection Regulation in Europe and the California Consumer Privacy Act, as well as orders from the Federal Trade Commission, feature more notice and rights to access, correct, move, and delete data.[8] Washington state can offer similar protections with a consumer-focused law including proper enforcement mechanisms.

Notification requirements: Local governments, state agencies and companies that provide critical infrastructure should be required to notify authorities of data breaches, and to increase collaboration, proactive response and defenses against cyberattacks.[9]

Cover the basics: All organizations should make sure they are covering the basics of cyber hygiene – training, patch management, least privilege implementation, and data backup.

Stakeholders

The NGA work groups identified stakeholders in two tracks. The first track examined the current status and need for cybersecurity workforce development. The second track discussed broader, collaborative efforts, and specific needs of stakeholders focusing on local government needs and requests.

From these parallel discussions a list of stakeholders was developed and invited to participate in various aspects of the NGA policy work. Each stakeholder below contributed ideas and offered context for a broader discussion of needs within cybersecurity:

State government agencies: One benefit of the NGA work group was the ability to work across many state government agencies. Participants included the State Auditor's Office, Washington State Fusion Center, the

[8] How Big Tech turns privacy laws into privacy theater. (slate.com)
[9] America's Cyber-Reckoning | Foreign Affairs

Military Department (including Emergency Management), Department of Commerce, Washington Technology Solutions (including the Office of Privacy and Data Protection, and the Office of Cybersecurity), the Utilities and Transportation Commission, Secretary of State's office and the Governor's Office.

State Auditor's Office (SAO): The SAO performs independent cybersecurity audits of state agencies and local governments under its performance audit authority. SAO audits assess implementation of certain security controls and test for vulnerabilities in security. The office also develops, curates and promotes cybersecurity resources designed for local governments in Washington based on best practices and common issues highlighted in audits.

Washington State Fusion Center: In Washington, the mission of the Fusion Center (WSFC) is to support the public safety and homeland security missions of state, local, tribal governments and private sector entities. This includes cybersecurity education, and assistance across multiple levels of law enforcement.

Military Department: The Washington State Military Department works to prepare the state for cyber emergencies. Extensive outreach and program development efforts by the National Guard and other state agencies culminated in the creation of a cybersecurity program within the Emergency Management Division. The manager of the program functions as the state's cybersecurity policy leader and strategist for emergency management.

The Department of Commerce: The Department of Commerce Energy Emergency Management Office (EEMO) is the primary agency for engaging with the Federal Department of Energy (DOE) and the state's energy critical infrastructure providers including but not limited to; electric and natural gas utilities, pipeline owners and operators, petroleum industries, and generation facilities for cybersecurity protection through all phases of emergency management and continuity of operations.

Washington Technology Solutions: WaTech supports state agencies that serve the public. Within WaTech two offices have taken a lead – the Office of Privacy and Data Protection (OPDP) and the Office of Cybersecurity (OCS): .

- Office of Privacy and Data Protection (OPDP): The state Office of Privacy and Data Protection (OPDP) was created by the state Legislature in 2016. The office, overseen by the state Chief Privacy Officer, serves as a central point of contact for state agencies on policy matters involving data privacy and data protection, and to serve as a resource for consumer privacy issues.

- Office of Cybersecurity (OCS): The state Office of Cybersecurity provides strategic direction for cybersecurity and protects the state government network from growing cyber threats. OCS, and its team of cybersecurity experts, detect, block and respond to cyberattacks on state networks. The office helps prevent and mitigate threats before they can cause significant damage.

The Utilities and Transportation Commission: The UTC is a three-member commission appointed by the governor and confirmed by the state Senate. The UTC ensures that the services of regulated companies are safe, available, reliable, and fairly priced. These regulated companies often provide important services that overlap with the definition of critical infrastructure – especially in the discussion of cybersecurity.

Washington State Attorney General: The Office of the Attorney General provides independent legal services to the state of Washington and protects the rights of its people. This includes work within the developing world of cybersecurity, cybercrime, and data breach protections. The office is committed to protecting people's data security and online privacy. The Washington Attorney General produces an annual Data Breach Report as a public service to help individuals better safeguard data through awareness of threats.

The Secretary of State's office: The Secretary of State's office protects elections as part of the state's critical infrastructure. This takes the form of both supervising state and local elections and certifying the results of state primaries and general elections, but also in overseeing an Information Sharing and Analysis Center (ISAC).

Governor's Office: "[Cybersecurity] is a matter of public safety, not just embarrassment or inconvenience. It requires a total community effort to stay ahead of those, who want to do us harm." — Gov Jay Inslee. Governor Inslee has consistently prioritized Cybersecurity and Data Privacy during his tenure as governor. He has hosted a Governor's Summit on Cybersecurity and Privacy in the past and has offered policy directives to better prepare and protect Washington state governments and individuals.

Educational entities

Four-Year Research Institutions: Traditional four-year universities provide opportunities to build and expand on innovative solutions to both technical and workforce challenges. Examples of the work being done at four-year institutions include:

- The University of Washington's Center for Information Assurance and Cybersecurity (CIAC).
- The Washington State University has been selected as a recipient of a $1.5 million Department of Defense (DOD) grant to establish a new cybersecurity education and research program.
- The Northwest Virtual Institute for Cybersecurity Education and Research (CySER)[10] program establishes a cyberoperations research and teaching center at WSU, one of the first three funded in the United States. This includes Central Washington University (CWU).

Washington State Workforce Training and Education Coordinating Board: Washington's Workforce Training and Education Coordinating Board (Workforce Board)[11] is a governor-appointed partnership of labor, business and government that is dedicated to helping Washington residents obtain and succeed in family-wage jobs, while meeting employers' needs for skilled workers. The Workforce Board acts as an advocate on all issues and programs related to workforce development, which includes 16 education and training programs. The Workforce Training and Coordinating Board is fully integrated with the work of the Career Connect Washington[12] initiative and the State Board of Community and Technical Colleges (SBCTC) initiatives to promote training in the cybersecurity field.

[10] Northwest Virtual Institute for Cybersecurity Education and Research | Washington State University (wsu.edu)
[11] https://www.wtb.wa.gov/
[12] Home | Career Connect Washington

SBCTC: The board is integrated into the work of the Career Connect Washington[13] initiative and promotes the cybersecurity training programs in 15 of its colleges around the state. Two examples of the work begin done in cybersecurity workforce development by the state community and technical colleges are from Big Bend College and Whatcom Community College.

The largest cybersecurity program in Washington, based on the number of enrolled students, is at Big Bend College. Whatcom Community College recently won a national grant to develop curriculum for other schools around the nation through its National Center of Academic Excellence in Information Assurance and Cyber Defense.

Local Government partners

Local governments are true partners in providing services to residents of Washington. Working in collaboration with various organizations, and jurisdictions can result in better "whole of state" cybersecurity coordination, preparation, response and recovery. Some organizations that have already engaged in this partnership work include:

Association of County and City Information Systems (ACCIS): is an organization composed of the chief information systems officers of counties and cities from within the state of Washington.

Public Utilities Districts (PUDs) (and their association WPUDA): PUDs are not-for-profit, community-owned utilities providing energy, water, sewer, and wholesale telecommunications services. PUDs are created by the people to serve the people. Within a cybersecurity discussion, they often fall within the category of critical infrastructure.

Water and sewer districts: The Washington Association of Sewer and Water Districts is composed of "special purpose" sewer, water, or combined sewer/water districts.

The Municipal Research and Services Center (MRSC): MRSC is a non-profit organization that helps local governments across Washington state better serve their communities by providing legal and policy guidance on any topic. MRSC serves all 281 cities and towns in Washington, 39 counties, and hundreds of special purpose districts, state agencies, and other government partners.

The Association of Washington Counties (WSAC): WSAC serves the counties of Washington state. Members include elected county commissioners, councilmembers, and executives from all of Washington's 39 counties. WSAC provides a variety of services to its member counties, including advocacy, professional development, public-private business partnerships, and a forum to network and share best practices.

The association also serves as an umbrella organization for affiliate organizations representing: County Road Engineers; Local Public Health Officials; County Administrators; Solid Waste Managers; County Human Service Administrators; Planning Directors; Clerks of County Boards.

Association of Washington Cities (AWC): AWC is a private, non-profit, nonpartisan corporation that represents Washington's cities and towns before the state legislature, the state executive branch and with regulatory agencies. Membership is voluntary. However, AWC consistently maintains 100% participation from Washington's 281 cities and towns.

[13] Home | Career Connect Washington

Federal and Tribal partners

Under the Federal Cybersecurity framework, State Local Tribal and Territorial (SLTT) partners are included in discussions for "whole of state" cybersecurity work and collaboration. Communication with federally recognized tribes within our state is ongoing. Here are some of the highest profile federal partners:

Federal Bureau of Investigations (FBI): The FBI is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities, including cybercrime through the Internet Crime Complaint Center (IC3), and the National Cyber Investigative Joint Task Force (NCIJTF). The IC3 receives complaints crossing the spectrum of cybercrime matters, including online fraud in its many forms. The NCIJTF is comprised of over 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization's mission from a whole-of-government perspective.

Federal Department of Homeland Security (DHS): DHS is focused on securing the nation from the many threats it faces, including those from cybersecurity. The Washington State Military Department is the point of contact for protecting critical infrastructure for DHS. The Fusion Center network, including the Washington State Fusion Center is also a point of state contact with DHS. Cybersecurity Infrastructure and Security Agency (CISA) operates out of the U.S. DHS and focuses on critical infrastructure protection from cyber threats. The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

The National Institute of Standards and Technology (NIST): NIST, as part of the U.S. Department of Commerce, develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. NIST cybersecurity frameworks[14] are rapidly becoming one of the most adopted policies for governments and organizations to protect their infrastructure from the threat of cyberattacks. The National Institute for Cybersecurity Education (NICE) within NIST has worked to build a framework for standardizing the needs, skillsets and competencies needed for a cybersecurity workforce. NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development.

Center for Internet Security (CIS): The Center for Internet Security (CIS) is another widely adopted cybersecurity framework[15] that assists many organizations, including local governments, manage, maintain, monitor, and respond within their networks to cybersecurity threats. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. state, local, tribal, and territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

Non-Governmental Organizations

Many non-governmental organizations stepped into the workforce development space to create new programs that addressed the lack of diversity and the workforce challenges identified by both the public and private sector. These are some of the highest profile organizations doing workforce development in the non-governmental sector:

[14] Cybersecurity Framework | NIST

[15] CIS Critical Security Controls (cisecurity.org)

Ada Developers Academy: ADA prepares women and gender expansive adults to be software developers while advocating for inclusive and equitable work environments. It has recently expanded nationally.

Washington Technology Industry Association (WTIA) / Apprenti: The Apprenti program, created within the WTIA[16] has adapted the time-tested model of apprenticeship to create a quicker path to qualified and certified talent.

The Public Infrastructure Security Cyber Education System (PISCES): PISCES works with students and local governments to both protect local governments and train students with the skills of cybersecurity work. PISCES provides qualified students with curricula and supervised experiences to act as entry-level cyber analysts. Students analyze streaming data for small communities or municipalities who may otherwise not be able to obtain cybersecurity to the extent needed.

Technology Access Foundation (TAF): TAF is a Seattle-based non-profit leader redefining K-12 public education throughout Washington state for all students and teachers, particularly those who identify as a person of color and are from traditionally underserved communities.

iUrbanTeen: The program was founded in 2011 to expose "non-traditional STEM learners" to STEM careers and opportunities. Based in Portland, Oregon, with outreach to Vancouver, WA and the Seattle metro area, iUrban Teen Tech introduces middle schoolers and high school-aged black and Latino young people to tech tours, mentorship and job shadowing opportunities.

Technology Alliance: The Technology Alliance is a statewide, non-profit organization of leaders from Washington's technology-based businesses and research institutions united by the vision of a vibrant innovation economy that benefits all of Washington's citizens. Through programs, events, data analysis, and policy activities, the alliance advances excellence in education, research, and entrepreneurship to support the growth of high-impact industries; the creation of high-wage jobs; and economic prosperity for our entire state. [17]

Information Professional Management Association (IPMA): The IPMA (Information Professional Management Association) is dedicated to promoting Washington state's status as the nation's premier hub for information technology. Its events and seminars are designed to bring together the state IT community for professional development opportunities. IPMA fosters collaboration, leadership, and innovation so that members are prepared to find solutions to tomorrow's challenges in the field of information technology.[18]

Contact

Questions regarding the Washington State National Governor's Association Inventory and As-Is Report can be directed to: zack.hudgins@ocio.wa.gov with the Washington State Office of Privacy and Data Protection or Andrew.garber@ocs.wa.gov with the Washington State Office of Cybersecurity.

[16] Apprenti Program - WTIA (washingtontechnology.org)
[17] Technology Alliance (technology-alliance.com)
[18] Networking for IT Professionals | Washington (ipma-wa.com)

Where to report cyber incidents:

- State agencies and local governments may report cybersecurity incidents to the Office of Cybersecurity here: https://cybersecurity.wa.gov/state-agency-cyber-incident-reporting. They may also call 360-407-8800 (option #2).
- Individuals may contact the Washington State Attorney General at: https://www.atg.wa.gov/internet-crime.
- The Internet Crime Complaint Center operated by the FBI may be contacted here: https://www.ic3.gov/Home/ComplaintChoice.
- The local Fusion Center which partners with the US Department of Homeland Security is also helpful and can be contacted here: http://www.wsfc.wa.gov/ (Primary) – 877-843-9522.
- You may also report cybercrime to your local law enforcement.