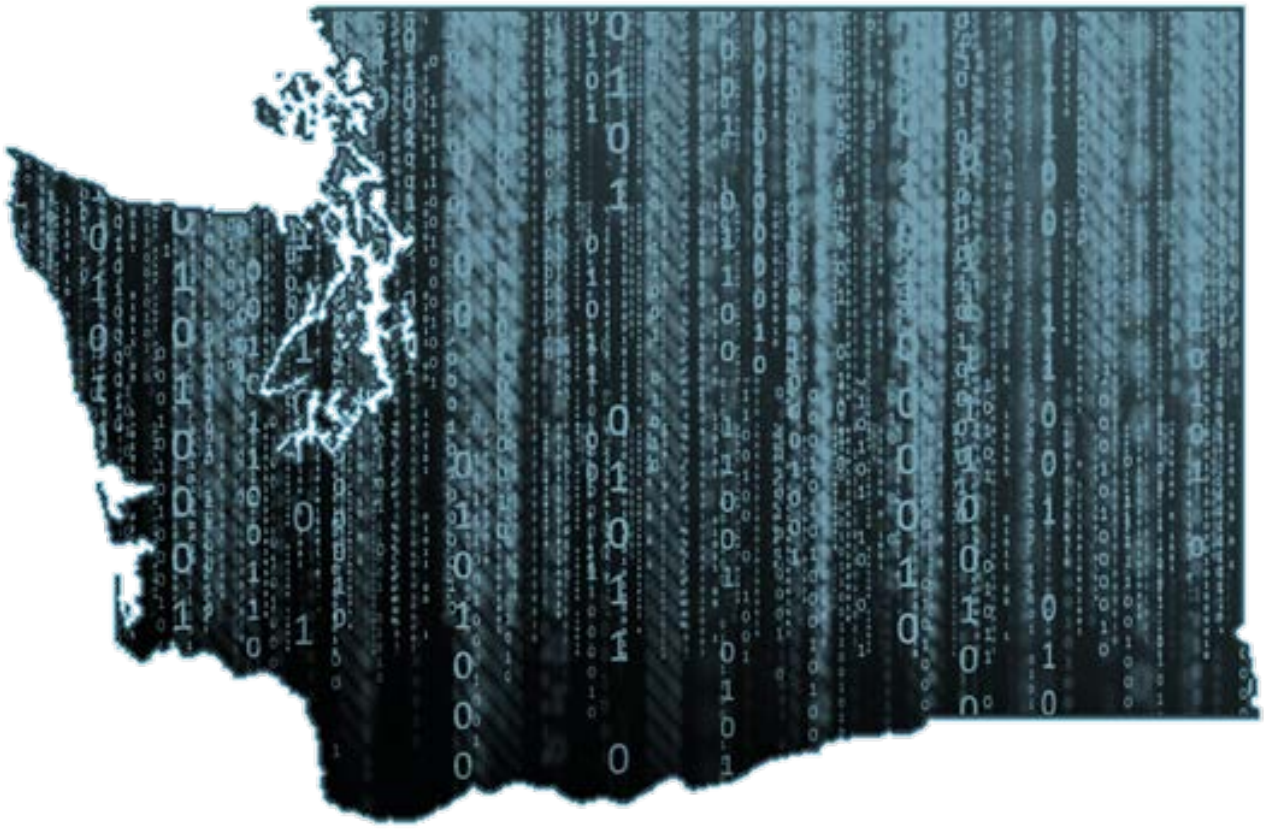
Cybersecurity Governance in the State of Washington

A CASE STUDY

December 2017



Homeland Security

NASCIO
Representing Chief Information Officers of the States

Washington State Fast Facts[1,2]

ELECTED OFFICIALS:

- Governor Jay Inslee
- WA House of Representatives: 98 Representatives
- WA State Senate: 49 Senators

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Officer (CIO) Michael Cockrill
- Chief Information Security Officer (CISO) Agnes Kirk
- Major General Bret D. Daugherty (Adjutant General, WA National Guard)

STATE DEMOGRAPHICS:

- Population: 7,288,000
  Workforce in "computers and math" occupations: 4%

EDUCATION:

- Public with a high school diploma: 48.6%
- Public with an advanced degree: 41.4%

COLLEGES AND UNIVERSITIES:

- 34 community colleges
- 6 public universities
- 15 private colleges

KEY INDUSTRIES:

- Information and communication technology
- Agriculture/food manufacturing
- Aerospace
- Clean technology
- Forest products
- Life science/global health
- Maritime
- Military/defense
- Sciences
- Logistics
- Manufacturing
- Technology

Executive Summary

The Overall Challenge:

How to address a range of cybersecurity challenges that cut across multiple government, public, and private sector organizations?

Overall Lessons Learned from Washington's Governance Approach:

- **Leadership Matters.** Leaders across multiple government, public, and private organizations make cybersecurity, and cybersecurity governance, a priority.
- **Leadership Is Not Everything.** Laws, policies, structures, and processes instantiate and align cybersecurity governance with cybersecurity priorities so that focus does not change as personalities change.
- **Governance Crosses Organizational Boundaries.** The distributed nature of cybersecurity requires a range of governance mechanisms that connect across multiple organizations and sectors.

This case study describes how Washington used laws, policies, structures, and processes to help govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. It explores cross-enterprise governance mechanisms used by Washington across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education.[*]

This case study is part of a pilot project intended to demonstrate how states have used governance mechanisms to help prioritize, plan, and make cross-enterprise decisions about cybersecurity. It offers concepts and approaches to other states and organizations that face similar challenges. As this case study covers a broad range of areas, each related section provides an overview of Washington's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Washington to better understand how to tailor solutions to their specific circumstances.

In recent years, the Washington executive and legislative branches have taken a series of deliberate steps to govern cybersecurity as an enterprise-wide strategic issue across both state government and a diverse set of private and public-sector organizations. (In this case study, "agency" refers to executive branch agencies.)

[*] For purposes of this case study, governance refers to the laws, policies, structures, and processes that enable people within and across organizations to address challenges in a coordinated manner through activities such as prioritization, planning, and decision making.

In 2015, the state Office of CyberSecurity, OCS, was consolidated into Washington Technology Solutions along with all other state IT services. OCS, led by the state Chief Information Security Officer sets statewide cybersecurity strategies and planning activities. The state CISO reports to the state CIO, who oversees WaTech.[3] To incorporate private sector perspectives into the state's strategic planning process, the legislature created the WaTech Technology Services Board (TSB).[4] The TSB is an oversight body to the Office of the Chief Information Officer (CIO) that provides input regarding the state's strategic vision and planning process for information technology (IT) and security issues, as well as oversight of major IT projects.[5] This body allows the CIO to incorporate emerging trends, issues, and industry best practices as part of the deliberative policymaking process. The TSB actions include, but are not limited to, advising the CIO regarding data center investments, IT disaster recovery planning, business application/system governance, and quality assurance for IT projects.[6]

To respond to a declared "significant cyber event," the state established formal procedures and processes among various federal, state, local, and private sector entities. A significant cyber incident is defined "as an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture."[7] The Cyber Annex to the Washington State Comprehensive Emergency Management Plan (CEMP) defines a significant cyber event and provides formal processes and procedures to coordinate various parties. The formal CEMP is needed because all the "required resources, authorities and execution responsibilities do not reside in one department, agency, organization or company within the State of Washington."[8]

The Governor formally designated the Homeland Security Advisor (HSA), who reports directly to the Governor, with the responsibility to lead response efforts across the state and engage with federal, local, and private sector stakeholders in response to "significant" cyber-events. The HSA partners with a Cyber Unified Coordination Group (UCG), which consists of representatives from federal, state, and local governments, academia, private industry, and critical infrastructure owners/operators, to have a coordinated response to a significant cyber event. As noted in the Cyber Annex Washington State CEMP, Cyber UCG participants, in turn, act and provide assistance upon request from the HSA.[9] The Cyber Annex Washington State CEMP specifies that "during a significant cyber incident triggering state-level coordination," the HSA coordinates activities through the Cyber UCG.

To address the challenge of cyber workforce shortages, the state has a multi-threaded approach that has used a variety of governance mechanisms to bring together public and private organizations. State officials worked across the business community and a not-for-profit organization to modify the education curriculum and standards to strengthen science, technology, engineering, and math (STEM) subjects. Leaders from two- and four-year colleges worked together to create a cybersecurity academic path for students who begin in community college and want to continue to earn a degree from a four-year college. To address cybersecurity workforce training needs, officials worked across the business community, government, and not-for-profit organizations to develop an apprenticeship program that will train, certify, and place people from underrepresented groups in the technology industry.

These, and other efforts described in the rest of this case study, were the result of many years of concerted, diligent effort by many individuals. Several key officials across government worked for years to understand cybersecurity risks and

build relationships to enable stronger state-wide efforts to address cyber threats. Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Washington uses a range of governance mechanisms to work across different public, private, academic, and nonprofit organizations. Leadership on the part of individuals who made cybersecurity and cybersecurity governance a priority across government, public, and private organizations was very important. However, leadership was not everything. As Washington demonstrates, the priority must be translated into tangible laws, policies, processes, and structures that instantiated and aligned cybersecurity governance with broader cybersecurity priorities.

Table of Contents

Background & Methodology

This case study was developed as part of a pilot project to identify how states have used laws, policies, structures, and processes to help better govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. This project emerged as a result of the *Department of Homeland Security (DHS) Advisory Council Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT*), which recognized the importance of governance in addressing a range of cybersecurity technology and operational challenges.[10]

The case study explores cross-enterprise governance mechanisms used by Washington across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education. It is not intended to serve as a formal evaluation. Instead, the case offers concepts and approaches that may be useful to other states and organizations that face similar challenges. As this case covers a broad range of areas, each related section provides an overview of Washington's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Washington to better understand how to tailor solutions to their specific circumstances.

DHS' Office of Cybersecurity and Communications (CS&C) initiated and leads the project in partnership with the National Association of State Chief Information Officers (NASCIO). NASCIO is a nonprofit association "representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia."[11] The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS owned Federally Funded Research and Development Center (FFRDC), developed the case studies.

Candidate states were identified to participate in the pilot project based on:

- analysis of third party sources,
- diversity of geographic region, and
- recommendations from DHS and NASCIO with awareness of SLTT cybersecurity practices.

Candidate states that agreed to participate in the DHS-led pilot project did so on a voluntary basis. Researchers used open source material and conducted a series of interviews to gather the necessary information to develop each state case study.

I. Strategy & Planning

The Challenge:

How to set direction and prioritize cybersecurity initiatives across multiple organizations?

Features of Washington's Governance Approach:

- The state Chief Information Officer (CIO) develops a statewide strategic information technology (IT) plan that sets direction for how the state will use and secure technology.
- An oversight board, which includes public and private sector representatives, advises the CIO about cybersecurity investments, risks, and policy changes.

Washington State's cross-government cybersecurity strategy and planning activities are led by the state's CIO and informed by the Chief Information Security Officer (CISO). As shown in Figure 1 below, both the CIO and CISO functions reside within Washington Technology Solutions (WaTech). The CIO, who is also the Director of WaTech, is appointed by the Governor and "is charged with preparing and leading the implementation of a strategic direction and enterprise architecture for information technology for state government."[12] WaTech was created in 2015, after a change in state law consolidated IT services to serve all state agencies and departments.[13]

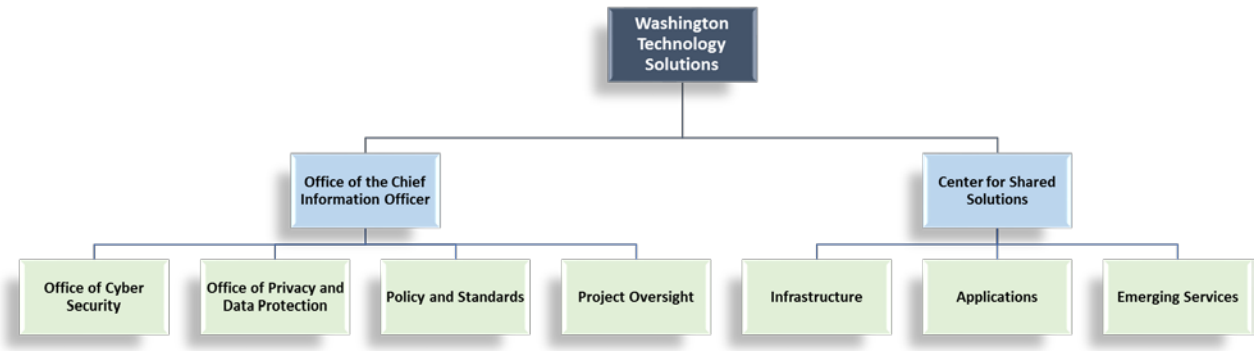


Figure 1. WaTech Organizational Chart (September 2017)

As part of this responsibility, the law directs the CIO to prepare a state strategic IT plan every two years.[14] This plan, called the Strategic Roadmap, identifies priorities for moving the state forward both in using technology to enable mission delivery and in securing and protecting those technologies.[15,16] For example, the most recent roadmap identifies initiatives (e.g., enhanced

identity management and integrated cloud-based identity services) to address sophisticated cyber threats emanating from the increased use of cloud computing and mobile devices over the next several years. To track progress on the impact of cybersecurity-related initiatives, the CISO publishes a biweekly cyber health report and distributes it to departments and agencies. This health report provides a snapshot of information security measures, such as types of attacks, trends, measures of effectiveness and mitigations, and allows for ongoing adjustments to key initiatives.

The CIO and CISO advise state legislators and the Governor's office on a range of cyber-related strategic issues. Current CIO Michael Cockrill notes, "technology is involved in everything our citizens do, especially related to privacy and cybersecurity, so I spend a lot of my time consulting with state legislators and the governor's office about public policy issues related to technology and cybersecurity."[17]

II. Budget & Acquisition

The Challenge:

How to manage investments in strategic cybersecurity priorities as part of budget and acquisition processes across multiple organizations?

Features of Washington's Governance Approach:

- The CIO evaluates and approves IT and cyber-related spending requests across state departments and agencies.
- The CIO creates IT acquisition policies and procedures to evaluate and manage risks associated with proposed IT acquisitions across state departments and agencies.

For both budget and acquisitions, the CIO has authority to evaluate department and agency IT and cybersecurity budget requests and recommend which investments should be included in the annual state budget process. The annual budget process is used to identify, propose, and fund cybersecurity investments at a variety of levels:

1. Within WaTech operations,
2. Within the Office of Cybersecurity, and
3. Investments at each agency.

Each state department and agency prepares an annual IT budget as part of a centralized budgeting process. The CIO evaluates current IT spending and prioritizes new IT and cyber-related spending requests against portfolio-based IT management and cyber-related criteria developed by the CIO.[18] The CIO establishes priority ranking categories for the proposals based on several categories of risk and other factors, with no more than one-third of the submitted proposals ranked in the highest priority category.[19]

Based on this prioritization, the CIO recommends to the Director of Washington's Office of Financial Management (OFM) to fund all or part of submitted agency IT budgets and additional IT or cyber-related budget proposals.[20] (The OFM has final approval authority over the development and submission of the Governor's budget request to the state legislature.) This prioritization informs the final funding decisions by the Governor and the legislature. In addition, as mentioned above in the Strategy & Planning section, the TSB plays a role in setting the criteria and the weighting for those criteria on IT budget and planning activities.[21]

The CIO also formulates IT acquisition policies that apply to all state agencies. These policies establish that the CIO review, approve, and oversee all major IT investments.[22] The CIO determines what constitutes a major IT investment, but size of the investment and potential type and severity of risks to the state's network are always considered as part of the evaluation process. To aid in the evaluation process, the CIO provides departments and

agencies with a standardized IT Project Assessment tool to "assess the cost, complexity, and statewide significance of an anticipated [IT]" and the corresponding risk profile of proposed projects.[23] Projects with higher risk profiles receive varying levels of direct oversight.

The CIO considers severity in terms of "impact on citizens, visibility to the public and Legislature, impact on state operations, and the consequences of doing nothing."[24] Risk is evaluated according to "impact of the IT investment on the organization, the effort needed to complete the project, the stability of or familiarity with the proposed technology, and the agency preparedness."[25] In addition, the TSB plays a role in the acquisition process by reviewing major IT policy changes and providing oversight of major IT investments. The CIO is chair of the TSB.

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of Washington's Governance Approach:

- The CISO sets standards to govern information security that apply to all state government systems and conducts security assessments.
- For every project, departments/agencies are responsible for producing a risk assessment that guides the implementation for security controls for that project.
- The CISO oversees a design review and reviews agency risk assessments. All departments and agencies must go through that process prior to launching a new system or service.
- The Military Department collaborates with critical infrastructure owners and operators to develop plans that address cybersecurity threats and risks to critical infrastructure.
- The Military Department identifies risks that would require a coordinated emergency response from the state.

Governance for cross-organizational risk identification and mitigation is shared by the CISO and the Military Department. The CISO focuses on risks to state networks, while the Washington Military Department focuses on risks that could impact critical infrastructure and that would require an emergency response.

The Office of Cyber Security (OCS), which is located within the WaTech Office of the Chief Information Officer and led by the CISO, is charged with identifying and mitigating cyber risks to state government networks.[26] The CISO, who reports to the CIO, sets information security standards for state systems and advises the Governor and state legislators on various cyber issues.

The OCS is responsible for identifying potential risks to the state government's network, managing the state's Security Operations Center (SOC), conducting risk assessments, implementing data controls, and determining the appropriate data architecture based on risk profiles of various types of data. The risk identification process starts when departments/agencies produce a risk

assessment for new information technology projects (see Budget and Acquisition section).

These assessments guide the implementation for security controls for that project. The CISO oversees a design review and reviews agency risk assessments prior new systems or services being launched. For example, in 2016, the OCS conducted 225 design reviews and discussions of major systems to ensure that they met security standards prior to being installed on the network and conducted 17 security assessments at state agencies, which identified mitigated vulnerabilities to the state's network.[27,28] The OCS also reviews "annual attestation reports from all state agencies detailing their level of compliance with state security guidelines and best practices."[29]

In addition to risk identification and mitigation actions of the OCS, the Washington Military Department plays a role in identifying risks that could require a coordinated emergency response from the state. The Military Department is focused on identifying risks, such as hazards that cause injury and/or damage from natural and technology disasters, that could necessitate an emergency response, and planning for a coordinated emergency response.[30] The Military Department maintains the State Threat and Hazard Identification and Risk Assessment, a Federal Emergency Management Agency risk assessment that identifies risks and emergency plans and capabilities available to respond in an emergency.

The Washington Military Department also leads efforts to coordinate with private sector owner/operators of critical infrastructure and key resources (CIKR) to develop plans to address cybersecurity threats to CIKR. In 2008, the Military Department developed the State of Washington Infrastructure Protection Plan in collaboration with public agencies and the private sector.[31] The plan articulates "an all-hazards approach to identify and protect CIKR with statewide, regional or national implications that if lost or disrupted," while acknowledging that "protection of CIKR is primarily the responsibility of its owner/operators with government support as necessary."[32] (See Incident Response section for additional information about how cyber incidents are addressed.)

For example, as part of its coordination role, the Military Department facilitated meetings of the Washington State Energy Coordinating Council (ECC) as it developed the Washington State Sector Specific Plan for Critical Energy Infrastructure.[33] The ECC, which includes private sector owner/operators of energy critical infrastructure (i.e., oil, natural gas, electric utility), is part of the standing Infrastructure Protection Subcommittee of the Washington Committee on Homeland Security.[34] The plan identifies key issues and mitigation programs and measures across issue areas including data and information sharing, critical infrastructure mapping, interdependencies, out-of-state infrastructure critical to Washington operations, and emergency response, restoration, and recovery.

IV. Incident Response

The Challenge:

How to prepare for and respond to cyber incidents that require coordinated action across multiple organizations?

Features of Washington's Governance Approach:

- The CIO, in coordination with the CISO, develops policy and leads response to cyber incidents that could pose a threat to the state's data architecture and/or systems.
- The Military Department leads the response to significant incidents that could impact the public and private sectors.
- A Cyber UCG, which includes public and private sector organizations, helps manage significant incidents.

Governance for cross-organizational cyber incident response is shared. If the threat is to the state government network, it is led by the CIO, in coordination with the CISO. If the Governor declares a significant cyber incident, it is led by the HSA.

The CIO develops the incident response policy to address possible IT security incidents that could pose a threat to the state's data architecture and/or systems.[35] The law defines a security incident as an accidental or intentional event resulting in "an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources."[36]

The OCS, which reports to the CISO, is the central point of contact for state government agencies to report and respond to suspicious activity and security incidents on the state network.[37] OCS staff includes a cadre of cyber professionals who are on call 24 hours a day, seven days a week, and are trained to identify, respond to, and mitigate cyber threats.[38] In 2016, OCS staff blocked more than 100 million malicious activities each week, blocked more than 12 distributed denial of service attacks on the state's network, and responded to 47 major cybersecurity incidents involving 19 state agencies.[39] In addition, to mitigate potential risks, the OCS trains state agency leaders by conducting exercises to help them identify and respond to cyber attacks. The office also hosts regular technical and policy training sessions with IT security professionals from across the state enterprise to remain current with the latest security tools and best practices.

As shown in Figure 2 below, the incident response policy sets forth a five-step response process that articulates the roles and responsibilities of the CIO, CISO, and agencies.

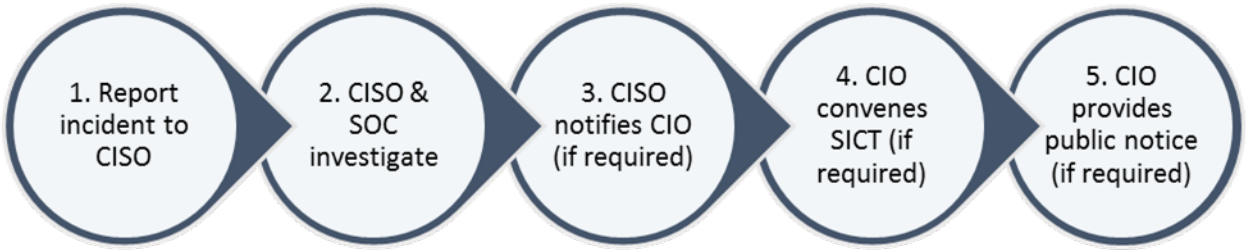


Figure 2. Five-Step Response Process to an IT Security Incident on the State Network[40]

Once an agency notifies the CISO, through the OCS, of an IT security incident, the CISO and OCS staff work with the agency IT staff to determine the scope, severity, and cause of the incident, as well as to determine what corrective actions are needed to rectify the situation.[41] The CISO can provide specialized capabilities to agency IT staff to assist in response efforts. For example, the OCS Computer Emergency Readiness Team (CERT), comprised of digital forensic experts, investigates malware intrusions on state-owned computers to determine method and origin of infection. In addition, the CERT provides statewide incident response for state agencies.[42]

Next, the CISO determines whether to notify the CIO and the Assistant Attorney General for the CIO. The CISO and the Washington State Attorney General determine whether public notification is warranted and provide the CIO with that determination.[43] The CIO may then convene the Security Incident Communications Team (SICT) if public notification of the IT security incident is required by law. The SICT may include heads of the agency or agencies impacted, legal counsel, the CISO, and members of law enforcement, among others.[44] Finally, the CIO may authorize public notification of the IT security incident if required under law.[45]

If the Governor declares a significant cyber incident, the HSA, who is also the Adjutant General, leads the response at the state level and coordinates at the federal level.[46] The Adjutant General is head of the Washington Military Department and as such oversees the Emergency Management Division and the Army, Air, and State National Guards. A significant cyber incident is defined as "an event likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture."[47] Cyber incidents that impact CIKR sectors would be deemed significant.[48] The Governor also directs the CIO to coordinate with the HSA if the significant cyber incident involves state agency IT systems.

The HSA reports directly to the Governor in the event of a significant cyber event and coordinates response efforts with the support of the Cyber UCG, which is organized through the State Emergency Operations Center (SEOC). Formal coordination is needed because all the "required resources, authorities and execution responsibilities do not reside in one department, agency, organization or company within the State of Washington."[49] The HSA partners with the Cyber UCG (which consists of representatives from federal, state, and local governments, academia, private industry, and critical infrastructure owners/operators) to respond quickly to a significant cyber event.

The SEOC provides a dedicated space to organize Cyber UCG members from across government and the private sector to address "incident prioritization, critical resource allocation, and situational awareness for issues arising as a result of a significant cyber incident."[50] Representatives from CIKR sectors are encouraged to communicate and coordinate

with the Cyber UCG and are "integrated physically and virtually into the UCG" during a significant cyber incident affecting CIKR sectors."[51] Cyber UCG participants have the authority to act and assist upon request from the HSA.[52] In addition, the Washington State Fusion Center (WSFC) "may host the Cyber UCG when activated and generate cyber alerts to notify federal, state, regional, local, tribal, and private sector partners with early warning indicators and potential actionable intelligence measures."[53]

Also, state law provides that the Governor may activate the National Guard to help with incident response.[54] The Washington National Guard is equipped to address certain cyber threats because of its expertise in industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems. Many members of the Washington National Guard are trained by the federal government to respond to security incidents impacting ICS and SCADA, and therefore are well prepared to deploy in response to cyber incidents that require this expertise.

V. Information Sharing

The Challenge:

How to engage across multiple organizations to share cybersecurity-related information?

Features of Washington's Governance Approach:

- The SOC supports information sharing across state departments and agencies.
- The state participates in cross-state information sharing bodies (e.g., the Multi-State Information Sharing and Analysis Center [MS-ISAC], the DHS National Cybersecurity and Integration Center [NCCIC].
- The state is in the process of developing a SLTT-ISAC to strengthen sharing with SLTT partners.

Washington State uses a range of governance structures to promote sharing of different types of information within state government and between the state government, federal government, and private sector. David Morris, the Washington State CTO for Cyber Security, characterizes information sharing in terms of trusted relationships, where "security is all about building trust relationships" and that those "relationships need to be in place *before* they are needed."[55]

Within the state government, the OCS SOC is "the nerve center for information sharing and monitoring enterprise security."[56] The SOC gathers a variety of threat information from monitoring state networks and from engaging with several information sharing bodies: the Cyber Incident Response Coalition and Analysis Sharing, a regional information sharing body; the MS-ISAC; and the DHS NCCIC. The SOC communicates threat information to state, local, and/or tribal government representatives and/or critical infrastructure partners. Stakeholders use this threat information in different ways to inform operational adjustments to network defenses.

In the event of a significant cyber event, the WSFC plays a role in facilitating incident-related information sharing, leveraging the "Homeland Security Information Network, a national secure and trusted web-based portal for information sharing and collaboration…"[57] The WSFC is designed to organize cyber alerts, notifications, and updates emanating from the Cyber UCG, NCCIC, and Seattle Federal Bureau of Investigation Joint Cyber Task Force, as well as to communicate with the SEOC and WSFC cyber stakeholders.[58] "In addition, the WSFC engages with other national homeland security fusion center cyber programs through the Cyber Intelligence Network (an outreach network of corporate security, information security and intelligence community professionals) to augment the SEOC common situational awareness of a significant cyber incident."[59]

At the regional level, officials are expanding information sharing beyond the federal, state, and regional levels to include local partners. The OCS is in the process of establishing a Washington State-level Information Sharing and Analysis Center (ISAC).[60] The Washington-specific ISAC will provide actionable threat information to SLTT partners. The CTO and CISO, in collaboration with the CIO, are "highly focused" on establishing the state ISAC to build the trusted relationships necessary to identify and respond to cyber threats within the context of regional Washington environments.[61]

In addition to the federal information sharing resources listed above, the Washington CISO participates in national-level information sharing with peers through NASCIO. NASCIO is a nonprofit association "representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia."[62] The Washington CIO sits on the executive board of NASCIO and the CISO sits on the cyber advisory board. NASCIO plays a significant role and builds trusted relationships with fellow state CISOs, trading best practices and emerging trends across the threat landscape.

VI. Workforce & Education

The Challenge:

How to work across multiple organizations to shape responses to cybersecurity workforce shortages and education needs?

Features of Washington's Governance Approach:

- K-12 curriculum standards were changed to include computer science and STEM graduation requirements and enabled public school districts to award college credits for Advanced Placement computer science classes.
- Community colleges and four-year universities have partnered to enable community college graduates in cybersecurity programs to transfer credits to four-year universities.
- A public-private partnership, led by the WTIA, offers an apprenticeship program to train underrepresented groups in the technology industry.
- The state is developing a program that would fund cybersecurity training and certifications for individuals in exchange for a paid position in a government organization.

Washington used a variety of governance mechanisms to bring together public and private organizations to address cybersecurity workforce shortages and education needs. These organizations included business, K-12 public education, community colleges, four year colleges, and not-for-profit organizations.

State officials worked across the business community and a not-for-profit organization to modify the K-12 curriculum to address the need for greater student understanding of STEM subjects. Starting in 2013, the state legislature, Governor, and business community worked together to address the need to include computer science classes in the K-12 curriculum. The Governor signed a bill to allow Washington public school districts "to award a math or science credit to students who enroll in an AP Computer Science class" to encourage more students to enroll in computer science classes, reduce the STEM skills gap, and "provide more opportunities for students to gain real-world experience and knowledge in a cutting-edge industry."[63] This legislation was an early step toward strengthening STEM-related education and was supported by Washington business leaders, including Microsoft, as well as the nonprofit code school code.org.[64]

Building on these first steps, in 2015 the Governor announced that the Washington K-12 public school curriculum would include new computer science education standards. The new *Washington State Computer Science K–12 Learning Standards* address the need for graduates in STEM. "The new standards map out computer literacy goals for students in elementary and middle schools, while also mandating levels of proficiency a student needs to pass a high school computer science course."[65] According to Governor Inslee, in 2016 "roughly 11 percent of Washington's schools meet these standards." However, by 2019, the Governor's goal is "to bump that up to 50 percent."[66]

Education changes were also made at the postsecondary levels. Leaders from select two-and-four year colleges worked together to create a cybersecurity academic path for students who begin in community college and want to continue to earn a degree from a four-year college. Typically, four-year colleges accepted few, if any, academic credits from community colleges. However, a partnership between select community and four-year colleges allows eligible students to transfer all credits to a four-year college. This structural change is enduring, allowing for a pipeline of students to transition smoothly from community college to four-year college. For example, students who complete a two-year degree in one of the cybersecurity-focused programs at Whatcom Community College can transfer all of their credits to either the University of Washington or Western Washington University.[67]

To address cybersecurity workforce training needs, officials worked across the business community, government, and nonprofit organizations to develop an apprenticeship program. This program is training existing workers to qualify for IT and cyber-related jobs. Washington leveraged an existing nonprofit organization, the Washington Technology Industry Association (WTIA), and a federal grant to launch an apprenticeship program to respond to "technology companies in Washington…struggling to fill their growing number of vacant, skilled positions."[68] As a private industry-led nonprofit entity, Apprenti can respond more quickly to changes in market-based workforce demands across a number of businesses. The WTIA, whose membership includes private technology and communications companies, manages and operates the apprenticeship program. The WTIA is expected "to provide training and jobs for up to 1,000 people, 600 of them in the technology industry."[69] As of 2015, there were "more than 240 registered apprenticeship training programs in the state with more than 10,000 active apprentices."[70]

In the future, the CIO, CISO, and Governor are working to establish new paths to fill the workforce gap. One initiative is a plan to launch Cyber Washington, a dedicated effort to try to bridge the gap between academia (education providers) and the private sector (job providers). Cyber Washington will launch a program to attract top talent to state and local IT vacancies. In exchange for state funding of training and certifications, individuals participating in the program will agree to work for the government for a period of time. This will provide participants with both education and professional experience to be competitive candidates for hire among the many Washington-based technology firms. While the details are still being developed among all parties, this program already has the support of key government officials, as well as private sector leaders such as Amazon, Microsoft, and Expedia.[71] Additionally, the state is partnering with higher education to expand online cybersecurity educational programs that will result in certifications for specific cyber skills that both public and private companies have agreed meet their workforce needs. This program will build on the cyber defense

programs offered by the cyber centers of academic excellence programs.

Washington leaders are now focused on measuring the outcomes of these many policy initiatives. In 2016, the Washington legislature passed a law directing the CIO and Director of WaTech to collaborate with community colleges, universities, the Washington Department of Commerce, and other stakeholders to "evaluate the extent to which the state is building upon its existing expertise in information technology to become a national leader in cybersecurity."[72] The law requires the WaTech Director to periodically evaluate the state's performance in achieving a variety of policy objectives, such as number of students graduating in the STEM fields.[73] The OCS must report its performance with regard to these policy objectives, as well as recommendations to the state legislature, before December 1, 2020. This baseline study will likely guide future cybersecurity investments in education and training, as well as a host of other matters.

VII. Deep Dive: Apprenti

Introduction

The purpose of the "Deep Dive" is to provide a more in-depth look at how Washington applied a cross-sector solution to address a specific cyber governance challenge.

The Challenge

The demand for a trained, diverse cybersecurity workforce outstrips supply. Traditional models (e.g., recruiting graduates from select undergraduate and graduate schools) have not kept up with the demand. Workforce training, especially of those from a more diversified ethnic and socioeconomic background, is needed to address the demand for talent. The demand for a cybersecurity workforce cuts across multiple companies and industries. One company or industry alone cannot fully address the challenge.

The Solution

Create a public-private partnership, led by a single not-for-profit institution (called Apprenti), that offers an apprenticeship program to train underrepresented groups, such as women, minorities, and Veterans, in the technology industry. Once accepted, applicants receive a certification and are placed among several different participating businesses.[74]

Background

While community college and four-year university programs serve various workforce and education needs, the demand for a diversified cybersecurity workforce continues to outstrip supply. Workforce training, especially of those from more diverse ethnic and socioeconomic backgrounds, is needed to address the demand for talent. Several years ago, some members of the WTIA took the initiative to evaluate and gather consensus regarding how to address persistent market demand for a larger skilled workforce in various cybersecurity-related fields, such as data analysts, front-end software developers, and network administrators, among others.

The WTIA, founded in 1984, is a not-for-profit 501(c)6 organization industry trade association comprised of 600+ information and communications technology companies. Members include Microsoft, Amazon, Nordstrom, and Expedia, to name a few. The WTIA's three strategic priorities are to (1) help small and medium-sized firms attract and retain technical talent; (2) advocate for more private and public investments in computer science education at all education levels; and (3) "help create a long-term, sustainable technology industry by developing technical and entrepreneurial talent directly through programs and indirectly through partnerships."[75]

In 2015, the WTIA established the Washington Technology Workforce Institute (WTWI) and the pilot tech apprenticeship program Apprenti. Apprenti is a 501(c)(3) not-for-profit, whose mission is to serve as the tech sector's apprenticeship intermediary, connecting industry, government, and education using public/private partnerships to close the talent and diversity gaps.[76]

Apprenti represents a public/private partnership and is funded in part by a federal grant from the American Apprenticeship Initiative, the U.S. Department of Labor, the State of Washington's Department of Labor and Industry, and private sector partners. Hiring partners and private funders include Microsoft,

Amazon, Accenture, JP Morgan Chase, Comtech, Silicon Mechanics, and F5.

The federal grant provided Apprenti with initial seed capital to launch the program. State and local Department of Labor officials will continue monitoring the progress of Apprenti over the next several years in accordance with requirements outlined in the federal grant.

Applicants accepted into the Apprenti program receive a certification paid for by the WTWI worth approximately $15,000 in various occupations, such as database administrator, project manager, network security administrator, web developer, software developer, Windows systems administrator, Linux systems administrator, or IT support professional.[77]

Apprentices are hired by a partner company prior to beginning classroom training and receive a salary and benefits while learning on the job. Typically, companies spend approximately $75,000 in direct (salary) and indirect (benefits) costs to train an apprentice for the year. The goal is for the employer to cultivate the talent to a level where, at the end of the one-year apprenticeship program, the apprentice will be retained at entry-level market wage for that job. The goal is to train 600 women, Veterans, and/or minorities over the next five years. To date, 76 Apprenti graduates have been placed in apprenticeships, and the program is on track to place a total of 130 by the end of December 2017.[78]

One of the lessons learned from the Apprenti program is that how the entity is legally organized matters in terms of governance and funding issues. As a 501(c)3, Apprenti is allowed to receive funds from private foundations in addition to state and federal funds (to train workers, for example). This allows the program to draw from multiple funding streams. As a private industry-led nonprofit entity, Apprenti has direct access to tech companies for hiring and can respond more quickly to changes in market-based workforce demands.

VIII. Acronyms

Acronym	Definition
AP	Advanced Placement
CERT	Computer Emergency Readiness Team
CIKR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
DHS	Department of Homeland Security
ECC	Energy Coordinating Council
FFRDC	Federally Funded Research and Development Center
HSA	Homeland Security Advisor
HSSEDI	Homeland Security Systems Engineering
ICS	Industrial Control Systems
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NCCIC	DHS Cybersecurity and Communications Integration Center
OCS	Washington State Office of CyberSecurity
OFM	Washington's Office of Financial Management
SCADA	Supervisory Control and Data Acquisition Systems
SEOC	State Emergency Operations Center
SICT	Security Incident Communications Team
SLTT	State, Local, Tribal & Territorial
SOC	Security Operations Center
STEM	Science, Technology, Engineering, and Math
TSB	WaTech Technology Services Board
UCG	Unified Coordination Group
WaTech	Washington Technology Solutions
WSFC	Washington State Fusion Center
WTIA	Washington Technology Industry Association
WTWI	Washington Technology Workforce Institute

[1] All statistics taken from the Statistical Atlas, Overview of Washington, data based on US Census Bureau 2010 census. Available: http://statisticalatlas.com/state/Washington/Overview except the population data which is taken from US Census Bureau, Population estimates, July 1, 2016, (V2016). Available: https://www.census.gov/quickfacts/fact/table/WA#viewtop. Retrieved August 2017.
[2] Information regarding elected officials and state cybersecurity executives was validated in September 2017. "Fast Fact" details were collected in August 2017.
[3] WaTech unifies the former Office of the Chief Information Officer, the original Consolidated Technology Services, and the enterprise applications division of the Department of Enterprise Services. *See* WaTech, "WaTech Re-inventing the Everyday Public Service Experience." Available: http://watech.wa.gov/about. See also RCW 43.105.006, http://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.006.
[4] RCW 43.105.287. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=43.105.287.
[5] WaTech Technology Services Board. Available: http://ocio.wa.gov/boards-and-committees/technology-services-board-tsb-0. *See also* RCW 43.105.287 for a complete list of powers and duties of the Technology Services Board. For a current list of members, *see* http://ocio.wa.gov/technology-services-board-tsb/technology-services-board-tsb-board-members.
[6] WaTech Technology Services Board, "Policy Actions." Available: http://ocio.wa.gov/sites/default/files/public/policy%20actions_120616.pdf.
[7] Washington State Comprehensive Emergency Management Plan (CEMP), Annex D (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[8] Ibid.
[9] Ibid.
[10] Department of Homeland Security Advisory Council, "Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT)." (2016, June). Available: https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_SLTT_FINAL_Report.pdf.
[11] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[12] Ibid.
[13] WaTech unifies the former Office of the Chief Information Officer, the original Consolidated Technology Services, and the enterprise applications division of the Department of Enterprise Services. *See* WaTech, "WaTech | Re-inventing the Everyday Public Service Experience." Available: http://watech.wa.gov/about. See also RCW 43.105.006, http://apps.leg.wa.gov/RCW/default.aspx?cite=43.105.006.
[14] RWC 43.105.220. Available: http://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.220.
[15] Ibid.
[16] WaTech, Consolidated Technology Services Roadmap. Available: http://watech.wa.gov/sites/default/files/ctsroadmap.pdf.
[17] Interview with Michael Cockrill, Washington State CIO (2017, March 13).
[18] RCW 43.105.240. Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.240.
[19] Agnes Kirk, Washington State CISO. (2017, September 14).
[20] Interview with Agnes Kirk, Washington State CISO. (2017, March 14).
[21] RCW 43.105.287. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=43.105.287.
[22] WaTech Policy 121: Procedures: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/policy/it-investments-approval-and-oversight-policy.
[23] WaTech, Office of Chief Information Officer, Agency Preliminary Assessment Tool, https://stofwadeptofenterpriseservices.formstack.com/forms/agency_preliminary_assessment_tool.
[24] WaTech Policy 121: "IT Investments - Approval and Oversight - Appendix A: Severity and Risk Assessment." (2014, January 8). Available: https://ocio.wa.gov/policy/appendix-severity-and-risk-assessment.
[25] Ibid.
[26] Washington State Office of Cyber Security, "About Us." Available: http://www.soc.wa.gov/about-us.
[27] Ibid.
[28] Office of CyberSecurity by the Numbers, Office of CyberSecurity Year in Review. (2017, February 16). Available: https://cybersecurity.wa.gov/cybersecurity-by-the-numbers-bb05664d7477.
[29] Office of Cybersecurity, "Highlights 2016: Monitoring of agencies' compliance with security standards and best practices." Available: https://cybersecurity.wa.gov/office-of-cybersecurity-highlights-2016-816d54e6565d.
[30] This 2015 plan includes a strategic overview of risks to people, property, the economy, and the environment from potential cyber events, a characterization of the level of response needed by federal, state, and local entities, and a brief overview of types and likelihood of cyber-attacks. Available: https://mil.wa.gov/other-links/enhanced-hazard-mitigation-plan; https://mil.wa.gov/uploads/pdf/hazplancyber.pdf.
[31] Washington State Military Department, "Washington Infrastructure Protection Plan." (2008). Available: http://mil.wa.gov/uploads/pdf/PLANS/2008%20washington%20infrastructure%20protection%20plan.pdf.
[32] Ibid.
[33] Washington State Energy Coordinating Council, Washington State Sector Specific Plan for Critical Energy Infrastructure. (2011, November 2011). Available: http://www.commerce.wa.gov/wp-content/uploads/2016/05/Energy-WA-State-Energy-Sector-Specific-Plan-

2011.pdf.
[34] Ibid.
[35] WaTech CIO Policies, 143 - IT Security Incident Communication. Available: https://ocio.wa.gov/policy/it-security-incident-communication.
[36] RCW 43.105.020 (19). Available: http://app.leg.wa.gov/RCW/default.aspx?cite=43.105.020.
[37] Washington State Office of Cyber Security, "About Us." Available: http://www.soc.wa.gov/about-us.
[38] A. Kirk, "IT security staff needed to battle hackers," Office of Cybersecurity, State of Washington. (2017, May 30). Available: https://cybersecurity.wa.gov/agnes-kirk-96b464e57a5a.
[39] Office of CyberSecurity by the Numbers, Office of CyberSecurity Year in Review. (2017, February 16). Available: https://cybersecurity.wa.gov/cybersecurity-by-the-numbers-bb05664d7477.
[40] Image derived from information included in WaTech CIO Policies, 143 - IT Security Incident Communication. Available: https://ocio.wa.gov/policy/it-security-incident-communication.
[41] Ibid.
[42] Correspondence with Agnes Kirk, Washington State CISO. (2017, June 29).
[43] Ibid.
[44] Ibid.
[45] RCW 42.56.590. Available: http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.590.
[46] State of Washington, Office of the Governor, "Designation as Senior Official and Homeland Security Advisor for the State of Washington." (2015, July 29). Available: https://mil.wa.gov/uploads/pdf/emergency-management/hsa-tagcyberletterfromgovernor.pdf.
[47] Washington Military Department, Emergency Management Division, "Washington State Comprehensive Emergency Management Plan." (2016, June). Available: https://mil.wa.gov/uploads/pdf/PLANS/final-wacemp-basic-plan-june2016-signed.pdf.
[48] Washington State CEMP, Annex D. (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[49] Ibid.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] The power of the Governor to declare a state of emergency may be found at RCW 43.06.010(12), while the power of the Governor to order the National Guard to active status may be found at RCW 38.08.040.
[55] Interview with David Morris, CTO. (2017, April 25).
[56] Office of CyberSecurity, Security Operations Center, What We Do. Available: http://soc.wa.gov/node/481.
[57] Washington State CEMP, Annex D. (2015, March 4). Available: https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf.
[58] Ibid.
[59] Ibid.
[60] Interview with David Morris, CTO. (2017, April 25).
[61] Ibid.
[62] The primary state members are senior officials from state government who have executive-level and statewide responsibility for IT leadership. *See* NASCIO, "About NASCIO." Available: https://www.nascio.org/AboutNASCIO.
[63] Governor Jay Inslee's Communications Office, "From coding to creating cool apps: Governor Inslee signs bill to promote computer science in schools." (2014, May 13). Available: http://www.governor.wa.gov/news-media/coding-creating-cool-apps-governor-inslee-signs-bill-promote-computer-science-schools.
[64] Ibid.
[65] State of Washington Office of the Superintendent of Public Schools, "Computer Science K-12 Learning Standards." (2017, March 21). Available: http://www.k12.wa.us/ComputerScience/LearningStandards.aspx.
[66] J. Stang, "Washington Gov. Inslee pushes for broad adoption of new computer science education standards," Geekwire.com. (2016, December 8). Available: http://www.geekwire.com/2016/washington-gov-inslee-pushes-broad-adoption-new-computer-science-education-standards/.
[67] Washington State has four state colleges and universities designated by the National Security Agency as National Centers of Academic Excellence in Information Assurance/Cyber Defense: (1) Whatcom College in Bellingham; (2) City University in Seattle; (3) the University of Washington in Bothell; and (4) Highline College in Des Moines. *See* https://cybersecurity.wa.gov/agnes-kirk-96b464e57a5a.
[68] Governor Inslee, Office of Governor Inslee, "Federal apprenticeship grants will help Washington high-tech workers," Press Release. (2015, September 9). Available: http://www.governor.wa.gov/news-media/federal-apprenticeship-grants-will-help-washington-high-tech-workers. Washington won a $5 million U.S. Department of Labor grant under the American Apprenticeship Initiative in 2015.
[69] Ibid.
[70] Ibid. Information on apprenticeships is available at www.lni.wa.gov.
[71] Apprenti, About. Available: https://apprenticareers.org/about/.
[72] RCW 43.105.801. Available: http://app.leg.wa.gov/rcw/default.aspx?cite=43.105&full=true#43.105.285.
[73] Ibid. The new law specifically requires the WaTech Director to track how the state develops "future leaders in cybersecurity, as evidenced by an increase in the number of students trained, and cybersecurity programs enlarged in educational settings from a January

1, 2016, baseline"; and (2) develops "broad participation in cybersecurity trainings and exercises or outreach, as evidenced by the number of events and the number of participants."

[74] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).

[75] Apprenti, Members. Available: https://www.washingtontechnology.org/about/#members.

[76] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).

[77] Apprenti, Careers. Available: https://apprenticareers.org/. *See also* Apprenti Tech Apprenticeship Update, July 20, 2017, provided by Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute.

[78] Interview with Jennifer Carlson, Director of Executive Director of the Washington Technology Industry Association Workforce Institute. (2017, May 3).