WaTech
Washington Technology Solutions

Office of the Chief Information Officer

FY20-FY21 IT Biennial Report

Letter from State CIO

It would be difficult to overstate the technological change wrought by the COVID-19 pandemic during the past two years. The mass shift to remote work, the use of video conferencing in place of in person meetings, and the adoption of digital signing in lieu of physically handling documents are just some of the changes that have permanently altered the way we work and interact.

This report presents an overview of the state's information technology (IT) landscape during that time (the 2019-21 biennium), as well as a glimpse of what's ahead.

As the state's Chief Information Officer, I am focused on strategic, cost-effective technology investments that will build on the unprecedented change we have experienced and help transform state services for Washingtonians.

The state has already made tremendous strides, including the fast-tracked adoption of cloud-based technology which has allowed the state to modernize and rapidly scale access to online applications that deliver state services. We've also shown innovation in response to the pandemic, such as using geospatial information to help guide the state response and bringing in new technologies, including chatbots, to help meet demands for services.

The state has made progress on oversight of IT spending, with the Office of the Chief Information Officer providing independent oversight to 129 IT projects underway at more than 47 state agencies and valued at over $2.28 billion.

While there have been significant achievements, there also remain challenges. Cyberattacks are increasing exponentially on a global level, making it critical for everyone, including the state of Washington, to remain vigilant and keep pace with the escalating threats. The state also continues to see many retirements in its IT workforce. During FY20-21, more than 45% of the state's IT employee turnover was due to retirement. More needs to be done to recruit the next generation of IT workforce to support public sector technology.

Looking ahead, I also believe we need to do a better job to understand and reproduce the experience the public has at home in state government. This will be a strategic priority for me as state CIO in the upcoming biennium. I want Washingtonians to have a common portal for services – just as they have come to expect when working with the private sector.

As we improve the ability for residents to access services online, efforts through the State Broadband Office will continue to address the disparities in broadband access, which was highlighted as a significant issue during the COVID-19 pandemic.

The pandemic has shown us the importance of delivering government services through technology and ensuring equitable access to those services. Government must rise to the challenge to meet resident expectations in a way that is accessible, high quality, and secure.

William A. Kehoe

Table of contents

Executive Summary

The 2019-21 IT Biennial Report, required under RCW 43.105.220, documents a period of unprecedented technological change driven by the global COVID-19 pandemic.

The state's technology investment of more than $3.49 billion during the biennium helped fuel an ongoing transformation that is not only changing how state employees work, but also how the state delivers critical services to Washingtonians. This total IT investment includes both new acquisitions and ongoing maintenance and operations.

Significant changes seen during the past two years include a massive shift to remote work and dramatically increased digital access to government services as brick-and-mortar buildings were closed to the public. While these changes were made on an emergency basis in response to the pandemic, they have had a profound and lasting impact on how the state conducts business.

Examples include:

- Widespread use of video conferencing (Microsoft Teams, Zoom, etc.), which almost entirely replaced in-person meetings. In a matter of months, the technology not only became the primary way workers collaborate, but also how the public views and participates in many public meetings.
- Fast-tracked adoption of cloud-based technology which allowed the state to modernize and rapidly scale access to online applications that deliver state services.
- The adoption of digital signing for documents, which speeds transactions and negates the need for physically handling paper.
- Rapid development of applications to help the state respond to the pandemic including the state COVID dashboards and vaccine verification (WaVerify).

Structural changes, not readily apparent to the public, also quickly moved forward including the consolidation of licensing for Microsoft products at a statewide level and the adoption of enterprise-level security tools and services to safeguard the state's data.

This IT Biennial Report discusses those changes and also assesses state progress toward goals outlined by the state technology strategic plan during the past biennium.

Areas highlighted in this report include:

Innovation: COVID-19 forced rapid technological change by the state to respond to the pandemic. Some of this was a matter of taking existing technology such as geospatial information and applying it in new ways, but the state also adapted on the fly, bringing in new technologies, including chatbots, to help meet demand for services.

Effective and Efficient Government: Information on where the state's IT dollars were spent, how those decisions were made and why. For example, the COVID-19 pandemic accelerated the

adoption of cloud services including the statewide adoption of the cloud-based Microsoft Office 365 (M365). In addition, the pandemic forced state agencies to boost their ability to provide services online due to the closure of brick-and-mortar locations and having a remote workforce. Doing so required spending on faster, more robust technology to get data and information from one point to another.

Accountable IT management: Through the 2020-21 biennial cycle, the OCIO provided independent oversight to 129 IT projects underway at 47 state agencies and valued at over $2.28 billion from beginning to completion of the project. As Washington's business application portfolio ages, the state continues to take a hard look at legacy applications to ensure business needs are being met. By the end of June 2021, more than 73% of the major technology projects under OCIO oversight were dedicated to addressing legacy modernization and business transformation efforts.

IT workforce: Starting July 2019, a new IT Professional Structure (ITPS) became effective to realign state job classifications to accurately reflect work, enabling comparisons to local public and private sector jobs. Prior to the reclassification, over 80% of the positions in the state's IT workforce were in three job classifications (ITS 4 & 5, ITA/S 6) – the three highest paying Washington General Service (WGS) classifications. As a result of the reclassification, most positions (3,902) transitioned into one of the 12 ITPS job classifications. Less than 5% of the existing IT workforce was transitioned out of an IT job classification.

The state also continues to see many retirements in its IT workforce. Over the previous two biennia it was reported that a high percentage of the state's technology workforce was eligible to retire within the next five years. During FY20-21, more than 45% of the state's IT employee turnover was due to retirement. The average age of retirees was 64 years.

Enterprise architecture (EA): In FY20-21, the Enterprise Architecture program supported major business transformation initiatives within the Administrative and Financial (One Washington) and Health and Human Services Domains (via the Health and Human Services Coalition). The program also continues to drive a statewide approach to cloud migration, leading to the creation of the Enterprise Cloud Computing Program which supports the ongoing strategic adoption of cloud technologies and a statewide cloud brokerage strategy.

Security: With cyberattacks increasing globally, Washington is working to prevent and stop bad actors as early as possible. WaTech's Office of Cybersecurity has focused on four foundational areas at an enterprise (statewide) level: An endpoint protection system that detects, blocks and alerts when malicious activity occurs; a Vulnerability Assessment System that scans state systems for weaknesses and helps agencies to prioritize and remedy them; a Security Information and Event Management platform that improves the ability of security staff to detect and respond to signs of attacks on state assets; and a web application defense that protects the state's nearly 300 online public facing eServices including the unemployment benefits system, tax, and business licensing services against automated attacks.

Privacy: The state also is making steady progress in protecting privacy. The state Office of Privacy and Data Protection (OPDP) during the past biennium, for example, provided Washington State

Agency Privacy Principles that will help establish a common understanding to use when discussing, promoting, and implementing privacy practices as a priority among state agencies. The Privacy Office also conducted annual privacy reviews of state agencies and developed a breach assessment form template that helps agencies determine if an incident requires notification under Washington's breach notification law.

IT Strategy next biennium: Looking ahead, there will be an increased focus on the customer experience when accessing state services. The goal is to provide a common portal for services where Washingtonians can go right to what they need, just like what they experience when shopping online. They shouldn't have to understand the way the state is organized to figure out which department provides certain services.

There is a digital equity piece to this approach as well. As we grow the digital experience, we also must address the disparities in broadband access. This has been a significant issue, particularly in rural communities, and has impacted the ability of state residents to receive services.

Also, as part of this effort, we need to ensure we have the right identity and access management capabilities. We also need to reduce our digital footprint, so Washingtonians are not required to repeatedly provide the same information to obtain different services from government. The larger the data footprint, the larger the risk to data.

The COVID-19 pandemic has shown the importance of delivering government services through technology and ensuring equitable access to those services. Governments must rise to the challenge to meet resident expectations in a way that is accessible, high quality, and secure.

Technology Performance Report Structure:

The OCIO is legislatively mandated to prepare and lead the implementation of a strategic direction for information technology in state government. The 2017-2021 Washington state IT Strategic Plan serves as the framework for the five primary section headings of this report:

- Efficient & Effective Government.
- Accountable IT Management.
- IT Workforce.
- Enterprise Architecture.
- Security & Privacy.

Due to the heightened interest in 'Innovation', this topic has been elevated to a section header within the report.

Section topics also cover requirements within the following state RCWs:

- RCW 43.105.205
- RCW 43.105.220
- RCW 43.105.225
- RCW 43.105.235
- RCW 43.105.245
- RCW 43.105.265
- RCW 43.105.287
- RCW 43.105.341
- RCW 43.105.369

Section 1 - Innovation:

COVID-19 forced rapid technological change for the state to respond to the pandemic. Some of this was a matter of taking existing technology such as geospatial information and applying it in new ways, but the state also adapted on the fly, bringing in new technologies, including chatbots, to help meet demands for services.

Examples:

COVID-19 Case Mapping – Washington State Geospatial Program Office:

Geospatial information was crucial in the early stage of the pandemic for state response efforts. Maps and applications were created in real time to adjust to information needs from working with epidemiologists to map the spread of COVID-19, to mapping the locations of public Wi-Fi access for people working remotely and locations of childcare for first responders and identifying supplies of personal protective equipment.

Geospatial aid provided to state agencies and local governments during the pandemic include:

- The Washington Emergency Operations Center Intelligence Portal which used Geographic Information System (GIS) data to shed light on COVID cases, demographics, personal protective equipment and fatality management.
- The development of more than 50 maps, 52 applications and 75 data sets to support emergency management operations and response. Applications included mapping locations of publicly available Wi-Fi sites to support telemedicine, remote work and distance learning as well as food bank and childcare locations for essential workers.
- Converting state Department of Health (DOH) statistical information to an easy-to-view geographical format with nearly real-time COVID-19 data, displayed by county. The Geospatial team also assisted the Department of Military with the collection and display of other data critical to the state's response and became an integral part of the Emergency Operations Center response.

Figure-1 provides a highlight of the information available on the COVID-19 Case Map:

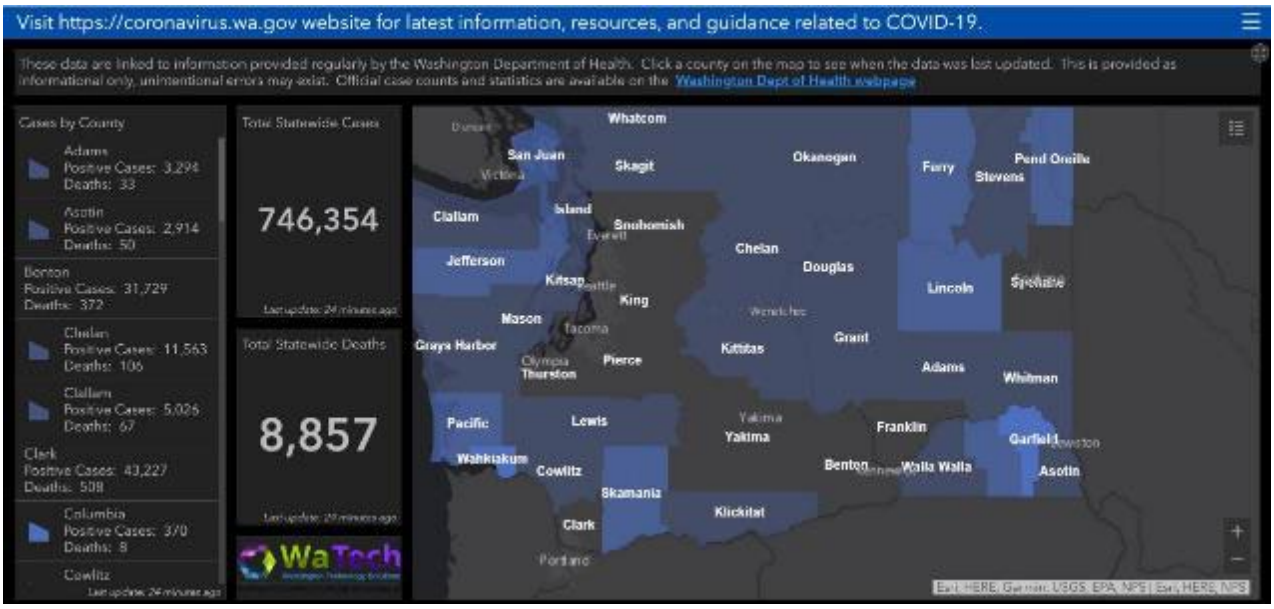


Figure 1 - Washington State COVID-19 case map.

Employment Security Department's (ESD) Unemployment Virtual Assistant:

With unprecedented demand for unemployment insurance benefits during the pandemic, ESD developed a virtual assistant in May 2020 that was used more than 450,000 times to help Washingtonians find information and answer basic questions. The technology freed up inundated call center staff to work directly with people with more complicated claims or who required more assistance due to technical literacy or other barriers. ESD, in partnership with Google, is now working to develop a more sophisticated virtual assistant that will serve customers by phone or chat. This project will also add the ability for customers to look up information about their claim, make changes to some preferences, and schedule a call if the virtual assistant is not able to resolve the issue.

In addition to innovative technology brought to bear on the pandemic, the state also forged ahead in other areas as well during the biennium – work that has earned the state top marks from the Center for Digital Government. (Washington received an A- in the 2020 Digital States Survey, which reflects a state that is trending sharply up, according to the survey.) Examples include:

Paid Family and Medical Leave (NASCIO Special Recognition):

The National Association of State Chief Information Officers (NASCIO) and the Center for Digital Government recognized Washington, among other things, for its Paid Family and Medical Leave project. Washington became the first state in the country to create a paid family and medical leave system from scratch, and only the fifth state to have such a program at all when Gov. Jay Inslee signed it into law in July 2017.

Starting Jan. 1, 2020, Washington workers no longer had to choose between a paycheck and taking time to give or receive care. In the first week alone, 10,000 Washingtonians

applied and the first month tally of 30,000 applications exceeded previous projections. By May 1, 2020, Employment Security Department had received a total of 65,072 applications for benefits and more than 38,000 claims, which resulted in benefits payments of nearly $114 million.

When creating the program, the state Employment Security Department used common platforms and technology which enabled the state to avoid a future over-reliance on vendor services.

The Paid Family and Medical Leave program has become a national model, with agency staff, advocates and lawmakers from other states regularly seeking updates on our implementation and advice on how to launch programs as successful as Washington's.

Washington has been charting a path for other states as well – including co-hosting a national forum to exchange lessons learned and best practices. Washington's experience provides important lessons on best practices for other states in terms of team culture, technology, policy, communications, outreach, collaboration, and innovation.

Key innovations that contributed to Washington's success include:

- Putting team culture first – embracing the sentiment that culture eats strategy for breakfast.
- Active and visible executive sponsorship at all levels.
- Customer insight, involvement and support – putting the customer at the center of our thinking.
- Applying Agile values and principles.
- Purpose driven system design – Launch and last, not launch and leave.

Invasion of the Murder Hornets: Using Communications Technology to Detect and Eradicate the Largest Hornet in the World:

The Asian Giant Hornet is the world's largest species of hornet. It can be up to two inches in length, with a quarter-inch long stinger. While the hornets generally don't attack pets or people, they do attack and destroy honey-bee hives. A few hornets can destroy a hive in a matter of hours.

Bees pollinate a third of U.S. crops, an important part of the food supply chain that contributes an estimated $15 billion in value to the agriculture industry. If it becomes established, the Asian Giant Hornet will have significant negative impacts on the environment, economy and public health of Washington state.

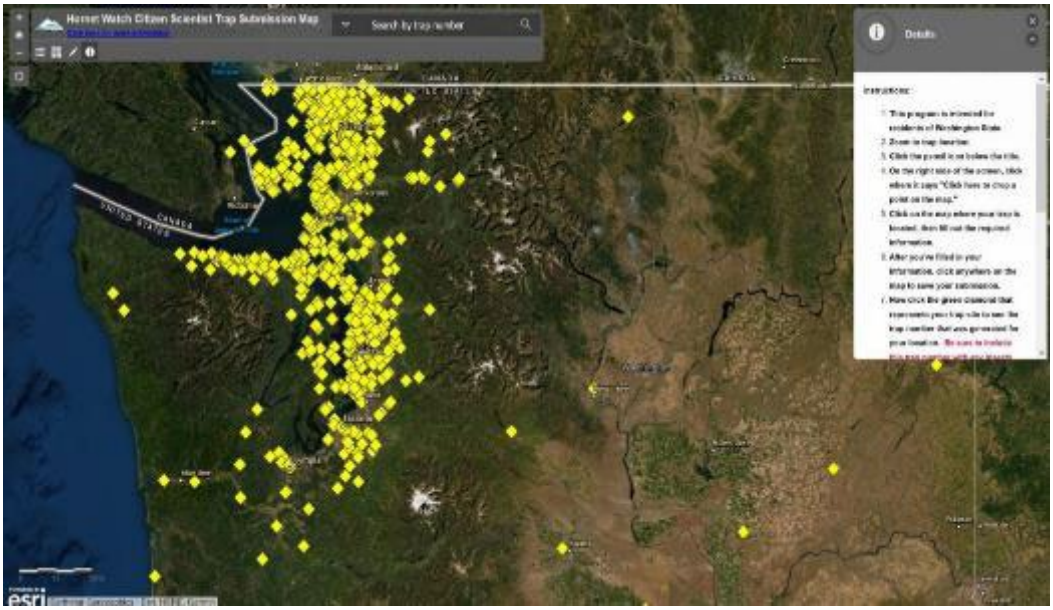
Honeybee vs. Asian Giant Hornet

The Washington State Department of Agriculture (WSDA) received and verified two reports of Asian giant hornet near Blaine, Washington in 2019. These are the first-ever sightings in the United States. After receiving additional reports in 2020, the WSDA conducted the first-ever eradication of an Asian Giant Hornet nest in the United States.

This effort involved an innovative use of technology – including social media crowd sourcing, geo mapping and live tracking using a radio tag tied to a hornet – to find and eradicate the only known nest of the hornets at the time. The destroyed nest contained 190 larvae, 112 workers and 76 queens.

The successful eradication of the nest would not have been possible without the support and hard work of 380 citizen scientists who placed and monitored more than 2,000 live hornet traps for months at a time and registered their traps using a WSDA web-based mapping application developed for the effort.

This work enabled the WSDA to narrow down possible locations of the nest over a large geographical area and ultimately destroy it. Although the first Asian Giant Hornet nest in the U.S. was eradicated, more nests were subsequently found in Whatcom County in 2021 using this same program. The WSDA believes early detection provides a fighting chance to continue to detect and fully eradicate this apex predator in the coming years. Until there are multiple years of negative survey seasons, it will never be fully deemed as a successful invasive pest eradication.



ArcGIS Online Cloud Based Mapping Web App used to allow Citizen Scientists to mark their trap locations throughout the state.

Central Washington University's (CWU) Academic Planning System 2.0 (CAPS+) project (Washington Digital Government Summit – Best of Washington Recognition):

After CWU upgraded its data system to the latest Oracle PeopleSoft, it became apparent that there were no compatible planning tools available to automate academic scheduling. A team of Central Washington University (CWU) professionals created a software application – Central's Academic Planning System 2.0 (CAPS+) – that alleviates the challenges of an antiquated nine-step manual degree planning system by developing an online, mobile first, academic planning tool for degree seeking students. CAPS+ was developed by CWU employees who are also alumni. The lead developer remembered the challenges associated with the manual degree planning method and wanted to make the process easier for today's students. Now, instead of working through nine manual degree planning steps, students using CAPS+ can schedule courses using only four mobile-friendly online actions, cutting the degree planning process by more than half.

Section 2: Efficient and Effective Government

The Office of the Chief Information Officer (OCIO) collects detailed information on the state's technology investments to show how they support state priorities. That data, collected from agencies on an annual basis, was used to build this report and validate alignment to the 2017-2021 strategic plan.

The following material in this section provides a high-level overview on the pursuit to support state priorities including where the IT dollars were spent, how those decisions were made and why. Priorities identified in the IT strategic plan include consolidating common technology and services, pursuing brokered service options, maximizing the state's buying power, creating constituent focused portals, and developing accessible and responsive designs, and increasing access to open data. This section also discusses major technological shifts during the pandemic including boosting the state's virtual private network (VPN) capacity, modernizing the state's network infrastructure, increased video conferencing and more.

IT Investment Financial Assessment:

"Cost Pools" and "Technology Towers" are standard terms used for benchmarking the state's IT spending against other public and private organizations.

State agencies invested close to $3.49 billion in 2020-21. Based on information submitted to the OCIO by state agencies, labor represents the largest proportion of overall IT spending.

2020-21 STATE IT INVESTMENT				
Cost Pool	**2020**	**2021**	**2020-21 Total**	**% Of Spend**
Internal Labor	$622,330,494	$645,088,579	$1,267,419,073	36%
Software	$205,148,141	$267,323,524	$472,471,665	14%
Hardware	$189,481,225	$260,533,751	$450,014,976	13%
Internal Services*	$185,350,242	$197,494,726	$382,844,968	11%
Outside Services	$172,091,400	$199,011,689	$371,103,090	11%
External Labor	$89,834,094	$115,539,607	$205,373,702	6%
Telecom	$75,003,821	$76,893,805	$151,897,625	4%
Facilities & Power	$58,901,216	$58,360,773	$117,261,989	3%
Other	$33,265,863	$40,217,247	$73,483,111	2%
Total	**$1,631,406,497**	**$1,860,463,703**	**$3,491,870,199**	**100%**

Table 1: (NOTE: "Internal Services" contain agency expenditures to central service agencies)

When benchmarking the state IT investment against 166 private and public sector organizations using industry Cost Pool standards, there are two categories that standout. The state internal labor investment is one of the highest and the software investment is one of the lowest. This is to be

expected given the high percentage of applications supporting agency missions are custom in-house built versus Commercial Off the Shelf (COTS) or Software as a Service (SaaS) solutions.

Hardware is 2% higher than the average of most organizations and is attributed to the amount of equipment in place to support the workforce. The remaining six cost pool categories remain within the median range.

When asked to assign cost pools to technology towers (see Figure 2), state agencies in the Technology Business Management program, reported "application" attracting the largest amount of IT investments followed by "end user," which includes support of workforce desktops, mobile devices, and desktop software. Investment in network technology rounds out the top three technology towers.

Looking at technology investment by governmental function, higher education continues to be the state leader (see Figures 3 and 4). However, statute exempts them from OCIO requirements to assign IT costs to technology towers.

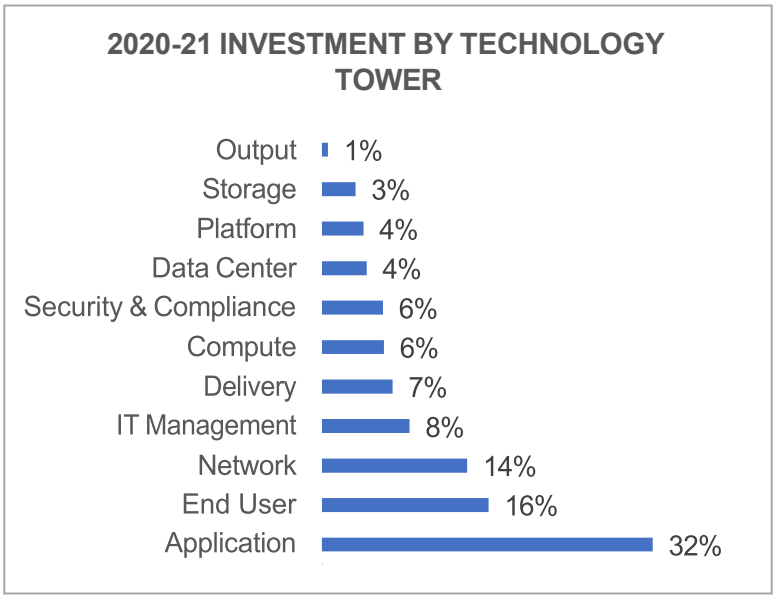


Figure 2 - Agency reported investment through the TBM Program.

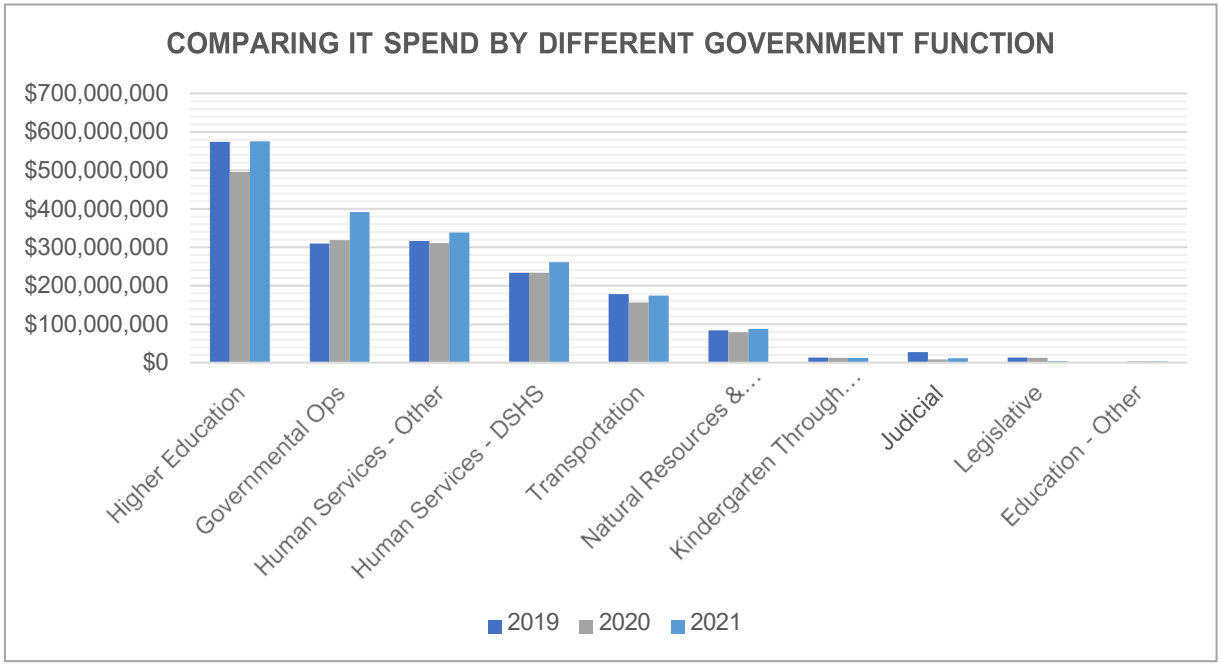


Figure 3 - Trending function of government IT spend over the biennium.

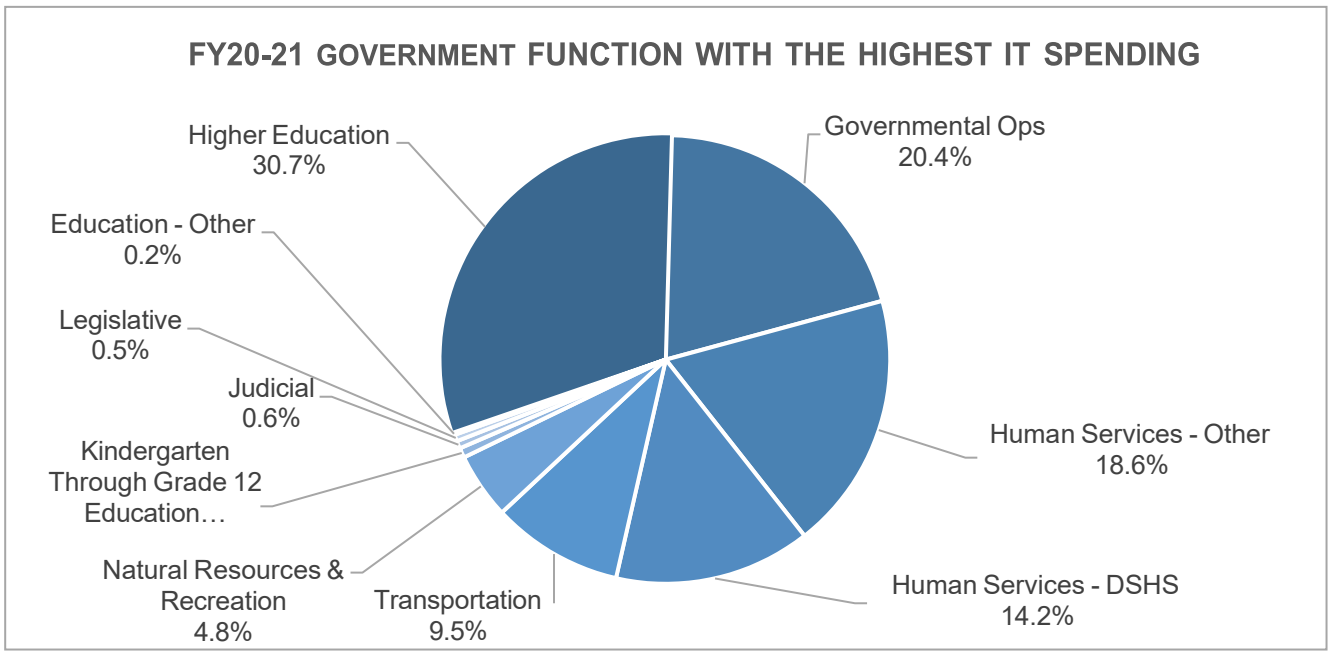


Figure 4 - Percentage of 2020-21 IT spend by different government function.

Agencies are required to report technology investments by new acquisitions development (i.e., new spend), and by maintenance and operations (M&O). Figure-5 includes itemization of expenditures by new acquisition, maintenance and operations, payments to central service agencies (classified as Data Processing Interagency) and unmarked IT spending. Unmarked IT spending includes hardware and software investments that agencies did not identify as IT when coding the payment information into the state Agency Financial Reporting System (AFRS).

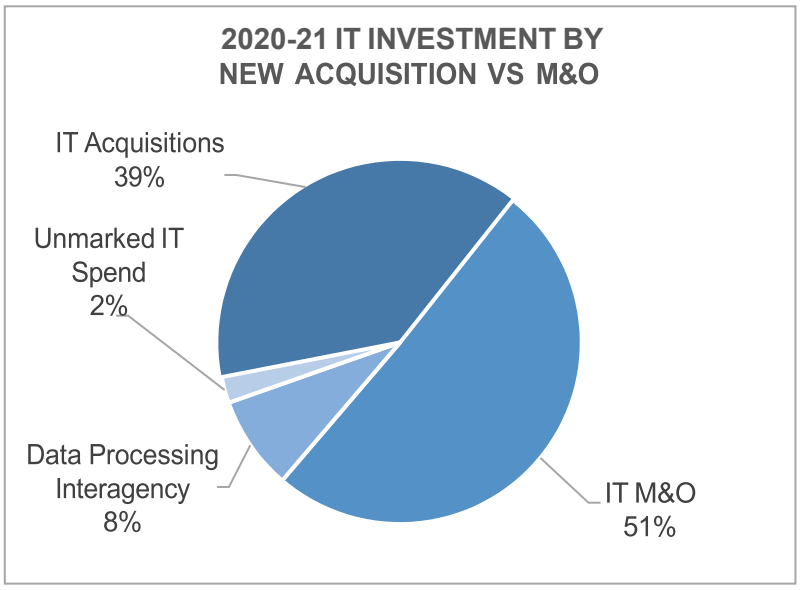


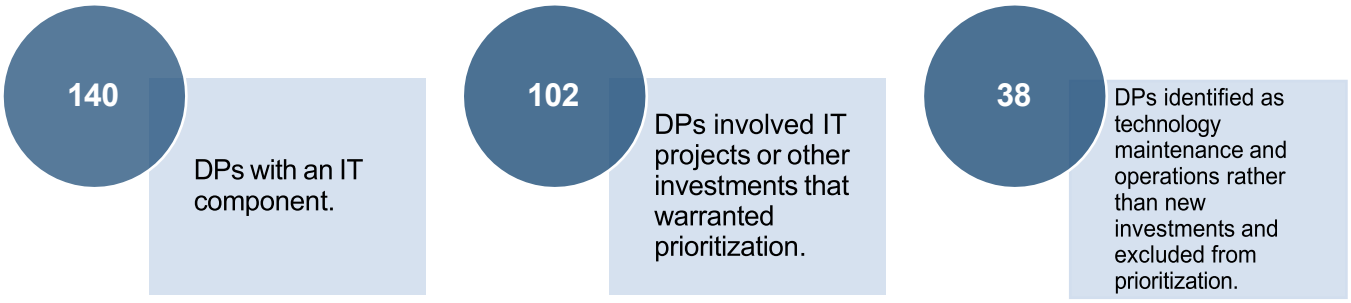
Figure 5 - Itemized IT investment by new spend and M&O.

Reviewing and ranking IT Decision Package requests:

The OCIO is required by law (RCW 43.105.235) to evaluate state agency IT budget requests and submit recommendations to the Office of Financial Management (OFM) regarding funding all or part of the request. The OCIO does this by reviewing and ranking agency submitted technology-related decision packages (DPs) on an annual basis.

In fall 2020, the OCIO analyzed 140 agency information technology DPs that were submitted to the OFM. Of those, 102 went through the review, scoring and prioritization process. The remaining 38 DPs were not prioritized because they were funding requests to maintain existing IT services (maintenance and operations).

DECISION PACKAGE REVIEWED AND SCORED FOR FUNDING RECOMMENDATION



For a copy of the comprehensive report submitted to the Legislature and available to the public, see OCIO 21-23 Biennium IT Decision Package Funding Recommendation Report.

Consolidating common services and technology with M365:

The COVID-19 pandemic accelerated the adoption of cloud services including the statewide adoption of the cloud-based Microsoft Office 365 (M365).

The mandatory shift to teleworking of state employees created an immediate need to onboard state agencies as quickly as possible. The state's central services provider, WaTech, onboarded more than 50 agencies and 83,000 users to Outlook in 2020. The move also included the use of multi-factor authentication (MFA) to increase security for additional state teleworkers.

The state also was challenged with a large-scale phishing attack in 2020, with attackers seeking to take advantage of the fear and uncertainty created by the pandemic. WaTech migrated customer agencies to an enterprise solution, Exchange Online Protection, to increase email security at the perimeter to mitigate the attack.

With those actions, Washington state deployed a modern Security Operations Center that leverages tools within the M365 suite of services, while achieving $30M in cost savings across telephony and redundant point solutions.

Microsoft M365 Platform - Shared Tenant

- Changes how agencies have historically managed their IT infrastructure.
- Shifts management of these resources to cloud providers.

Shared Tenant Benefits

- Enhanced security.
- Increased productivity.
- Improved IT efficiency.

Through the Enterprise Shared Tenant, the state is well positioned to support a remote workforce through 2021 and beyond.

The shift to telecommuting accelerated the workforce's reliance on Microsoft Teams. Figure-6 shows increased utilization of Teams group chat, calls, channels (private chat messaging) and meetings.

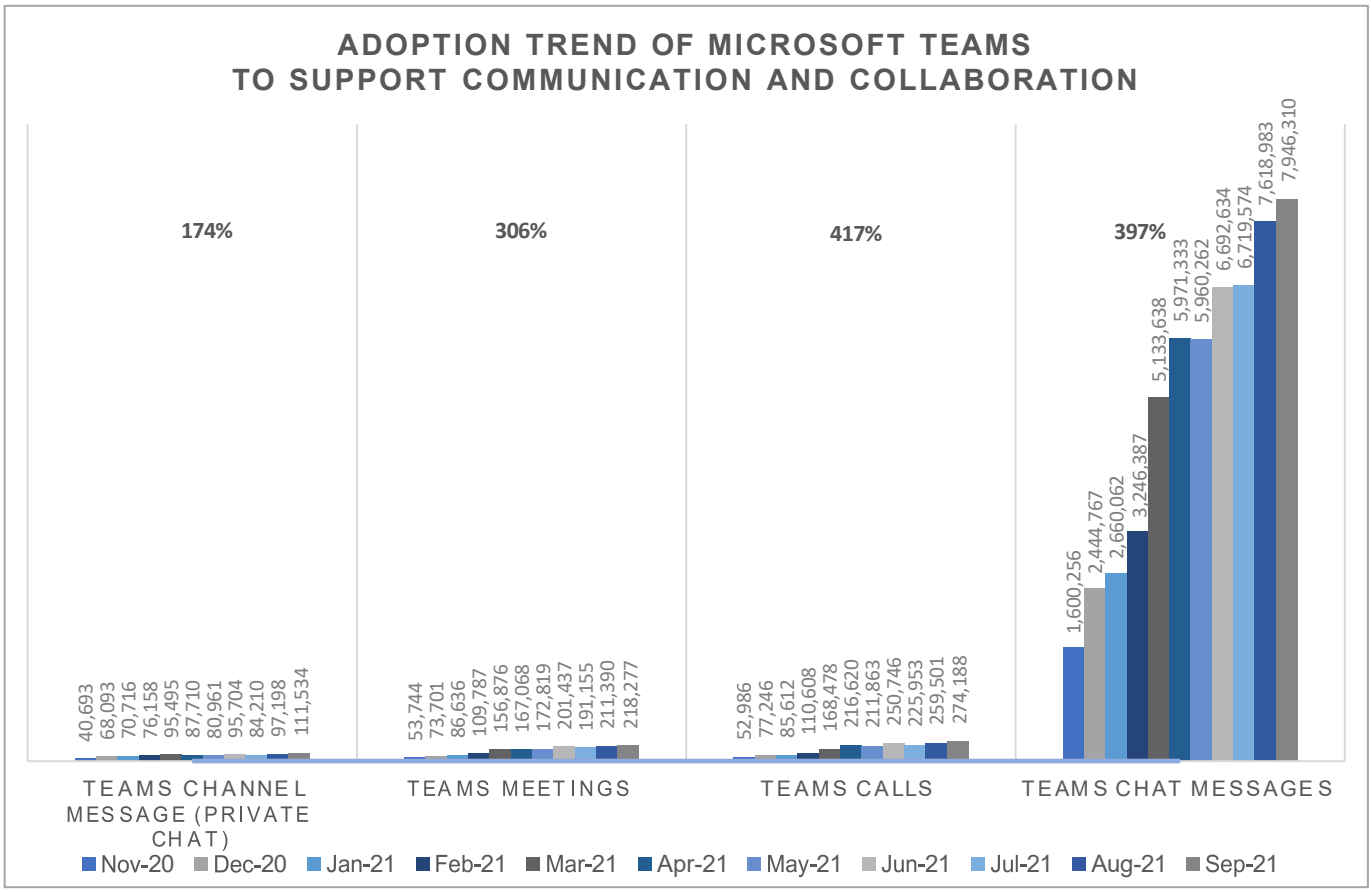


Figure 6 – Microsoft Teams utilization for agency business communication.

Maximizing statewide buying power - M365 Licensing:

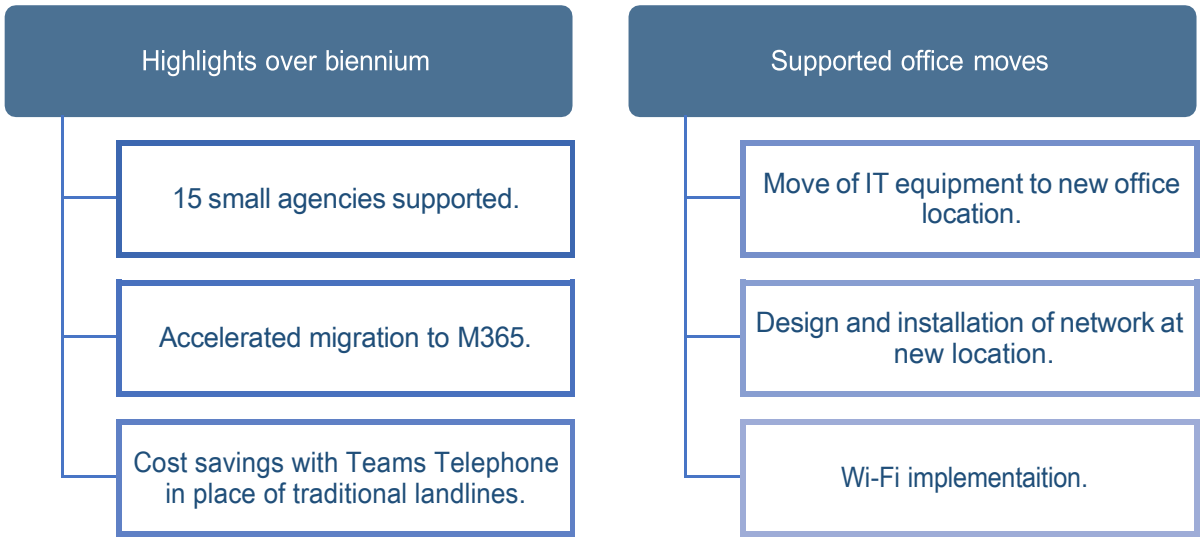
Several agencies submitted Decision Package requests to fund core M365 licensing investments. Because each agency had its own enterprise agreement, they received licenses at varying rates. An enterprise approach was needed to get the best value for the state and enhance the security posture.

WaTech, the Department of Enterprise Services (DES) and the Office of Financial Management (OFM) pursued an enterprise approach to M365 licensing at the G5 licensing level. In December 2020, the state consolidated 44 individual agency agreements with Microsoft into a single enterprise agreement to fund these base-level services. Work was done with Microsoft and OFM, in consultation with DES to enhance the master agreement.

Small agency support:

Many small agencies and commissions within Washington state do not have the technical staff to manage and administer technology needs to meet business requirements. A support model was established and is currently managed by WaTech so small agencies can focus on their primary mission with the confidence their technical needs are being met. Benefits of this approach to the state and small agencies include:

- Efficiency through reduced duplication of common purchasing activities.
- Improved control of asset and inventory with lifecycle management of hardware, software and other equipment.
- Enhanced protection of valuable agency information residing on the agency workstations, network, and mobile devices, including an improved security profile with protection from viruses and malware.
- Assistance accessing a more reliable network infrastructure to ensure quality delivery of voice, data and video conferencing going forward.
- Improved continuity of operation with the ability for backup and restoration of data in the event of a disaster.



Hardware Investments:

Agencies report the investment on end user hardware – which includes desktops, laptops and mobile devices – went up from 26% in the 2018-19 biennium to 30% in 2020-21 and represent their highest hardware costs followed by networks (see Figure-7).

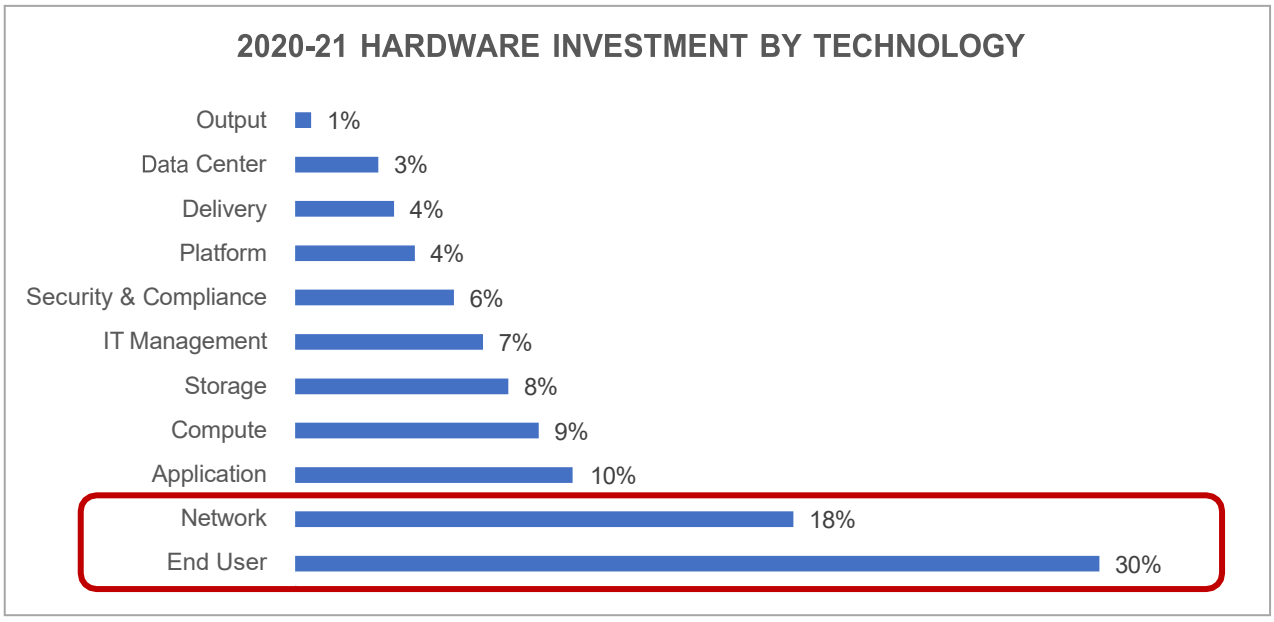


Figure 7 - 2020-21 Hardware investment by technology.

With the movement to a mobile work environment during COVID-19, support for end user devices represented a growing share of labor expenditures. In 2021, (the first-year agencies provided infrastructure inventory), executive branch agencies reported having more than 128,000 end user devices. Given desktops, laptops and mobile devices have a shorter lifecycle than other IT equipment, the state will likely experience increased spending on internal and external labor to support end users and their devices.

Network access to services and data:

Washington state constituents have significantly changed how they access state government services during the past five years, requiring movement to faster and more robust networks. COVID-19 accelerated this trend, with many agencies boosting their ability to provide services online due to the closure of brick-and-mortar locations and having a remote workforce.

Doing so required the introduction of faster, more robust technology to get data and information from one point to another. The increased demand for high-capacity network circuits has resulted in a steady increase in network investments (see Figure-8), with over 81% of the investment associated with the 10 agencies referenced in Figure-9.

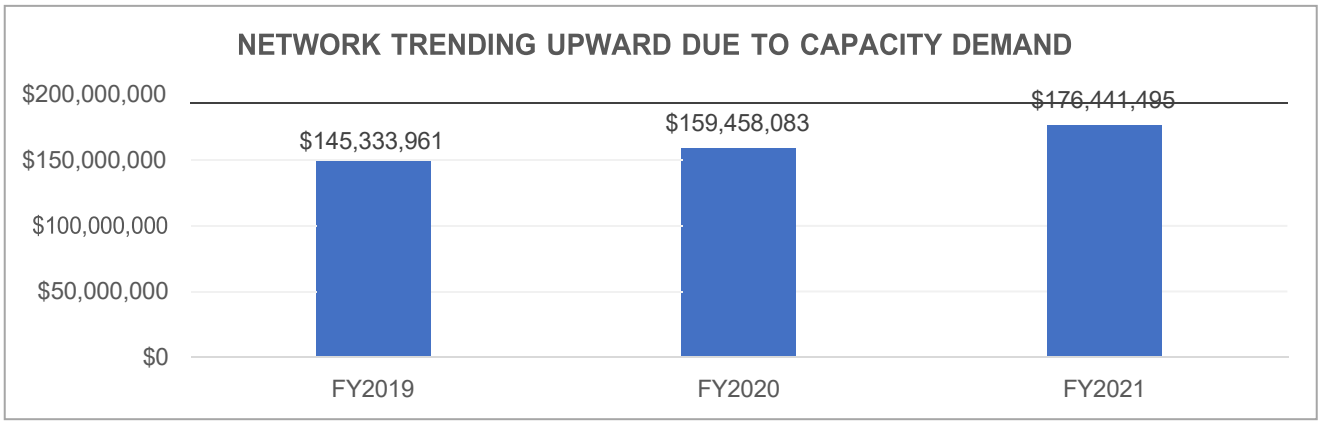


Figure 8 – Trending network investment.

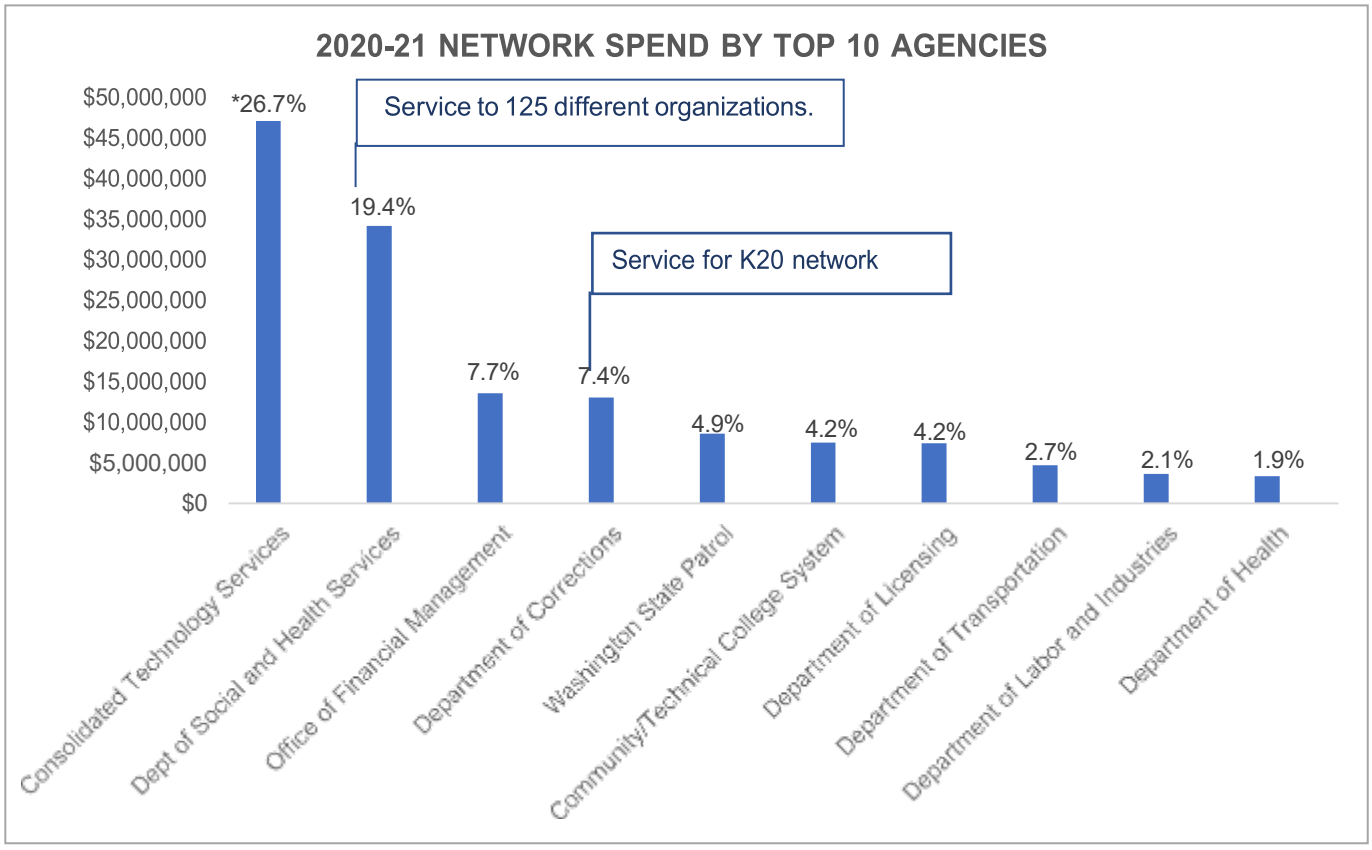


*Figure 9 - * WaTech makes up the largest portion of the 26.7% because it is the state's central IT services agency and provides network service to more than 125 organizations.*

The unprecedented push to provide online services has advanced the modernization of the state network. Agencies transitioned from leveraging lower capacity legacy infrastructure to higher speed network solutions.

Figure-10 shows state government movement from legacy solutions to the cloud for a more responsive solution.

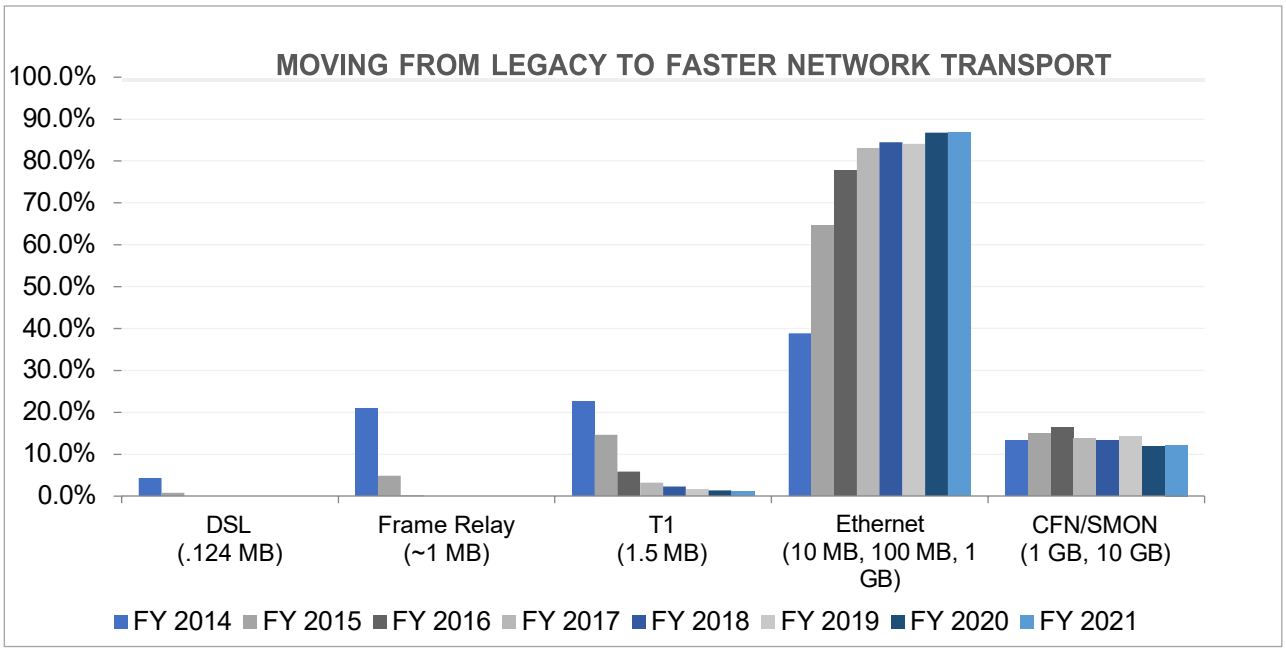


Figure 10 - Movement from slower legacy technology (DSL, Frame Relay and T1) to modern, faster network transport.

State agencies continue to depend on resources available through the internet. As shown in Figure-11, the state's internet use has increased more than 400% over the last two years indicating that agencies are requiring more internet capacity to deliver services than ever before.

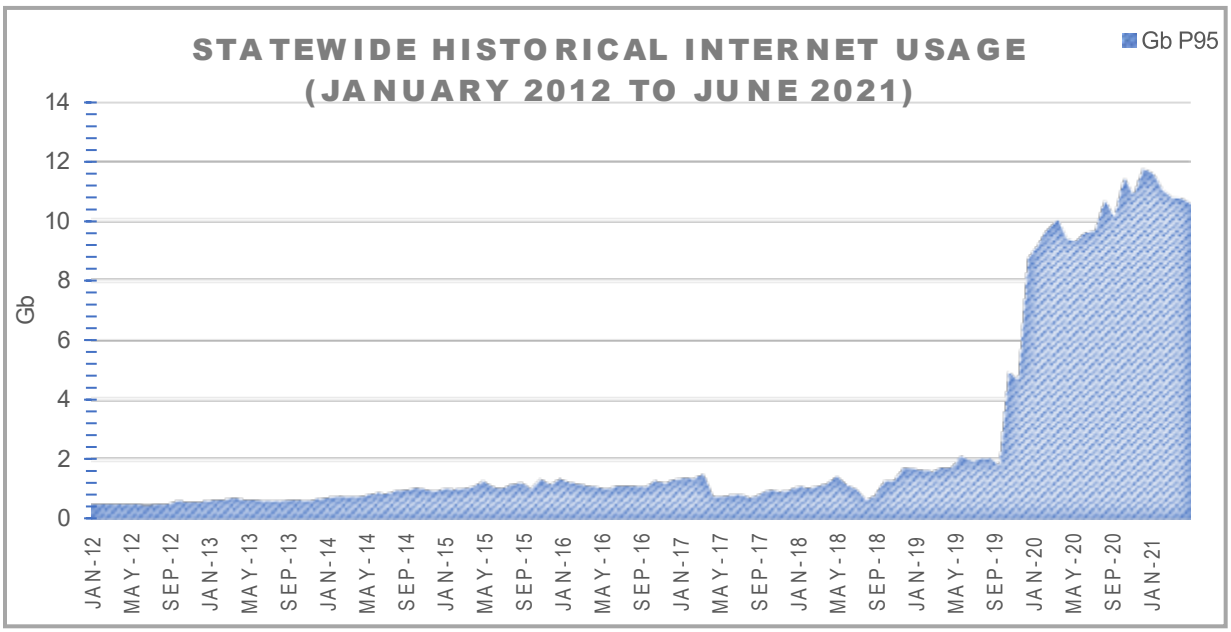


Figure 11 - Trending state Internet usage at 95 percentile (P95) Gigabit per second.

As agencies have become more dependent on the internet, there is consistent monitoring to determine when additional network investment is required. Currently, when the usage hits 70% of the maximum network capacity (P95 average gigabits) this requires state investment in more capacity. Figure-12 provides insight into the current internet usage compared to the threshold requiring an upgrade investment.

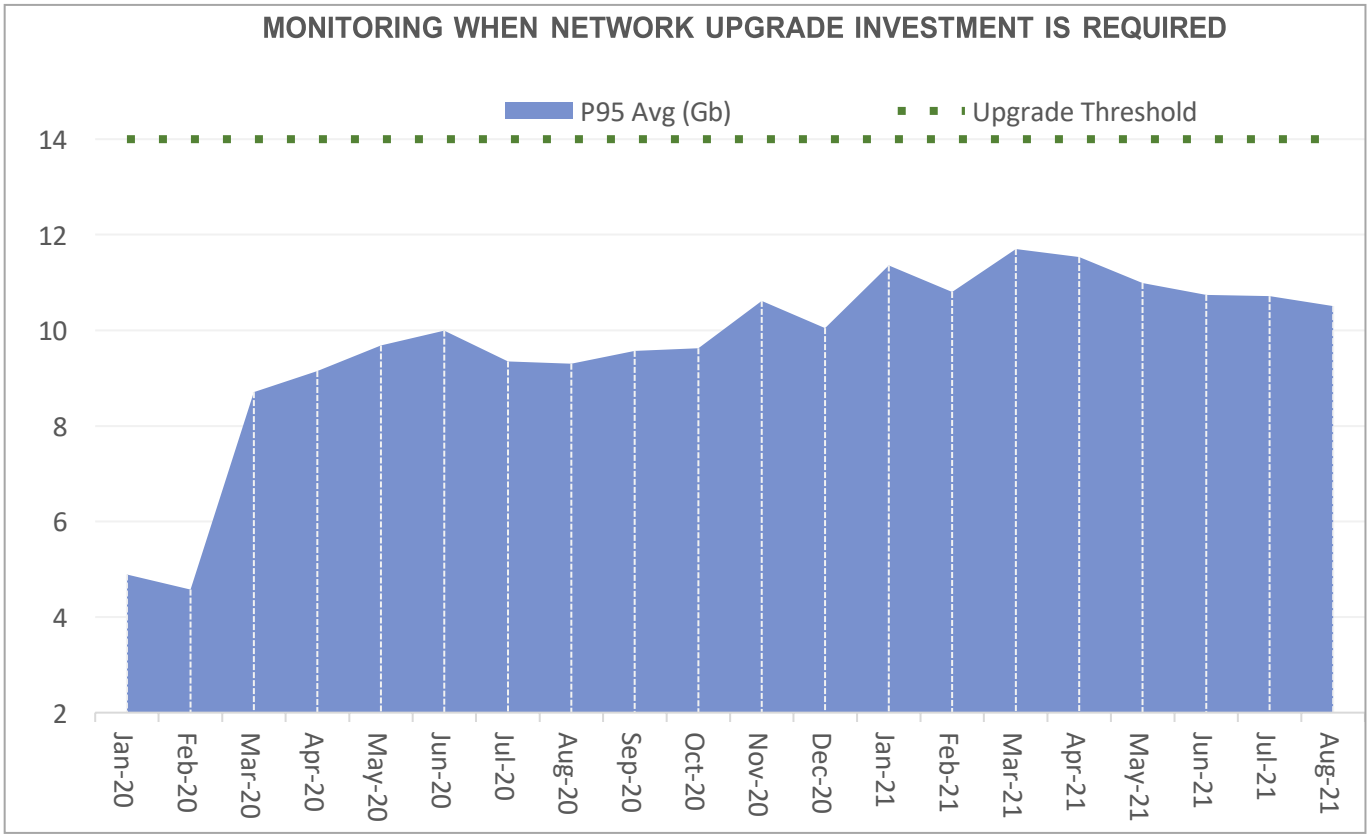


Figure 12 – 95 percentile (P95) is the established maximum gigabit burst that triggers investment decision.

Since the start of the COVID-19 pandemic, the state's reliance on broadband internet has drastically evolved how the state's workforce accesses state resources. Table-2 shows the top state government services driving the increase while providing a comparison before and during the pandemic. Many state services adopted certain technology over the internet due to the shutdown of public facing buildings and a remote workforce.

TOP SERVICES DRIVING INTERNET USAGE DURING COVID			
Business function	Average prior to COVID	Average Mar 20-Dec 20	Average 2021
DOC and AOC Replication for Disaster Recovery purposes.	116 TB	94 TB	None
Citizen access to Secure State resources through Secure Access Washington (SAW).	81 TB	278 TB	292 TB
VPN access to state resources (primarily state employees).	75 TB	330 TB	368 TB
Traffic to Washington Dept of Transportation. Increase after COVID due to WSDOT employee access.	20 TB	146 TB	129 TB
Traffic to AWS and Azure from state agencies adoption of cloud technology.	176 TB	276 TB	436 TB
Streaming.	12 TB	14 TB	19 TB
Other (unclassified).	359 TB	645 TB	857 TB

Table 2 - Detailed information on agency services that drove the increase in internet usage.

Access through Virtual Private Network (VPN):

WaTech's Virtual Private Network (VPN) provides mobile users secure internet access to agency networks from any location. The massive shift to remote work in early 2020 immediately tested the state's enterprise VPN system. However, the state was able to procure necessary hardware to rapidly scale the system. From February 2020 to May 2020, the VPN user count jumped 157%, from 14,000 to 36,000 unique users accessing the system. It has remained near that level, slowly increasing to 38,000 by the end of June 2021 (Figure-14). By comparison, VPN usage five years ago (in 2016) averaged about 4,000 users a day.

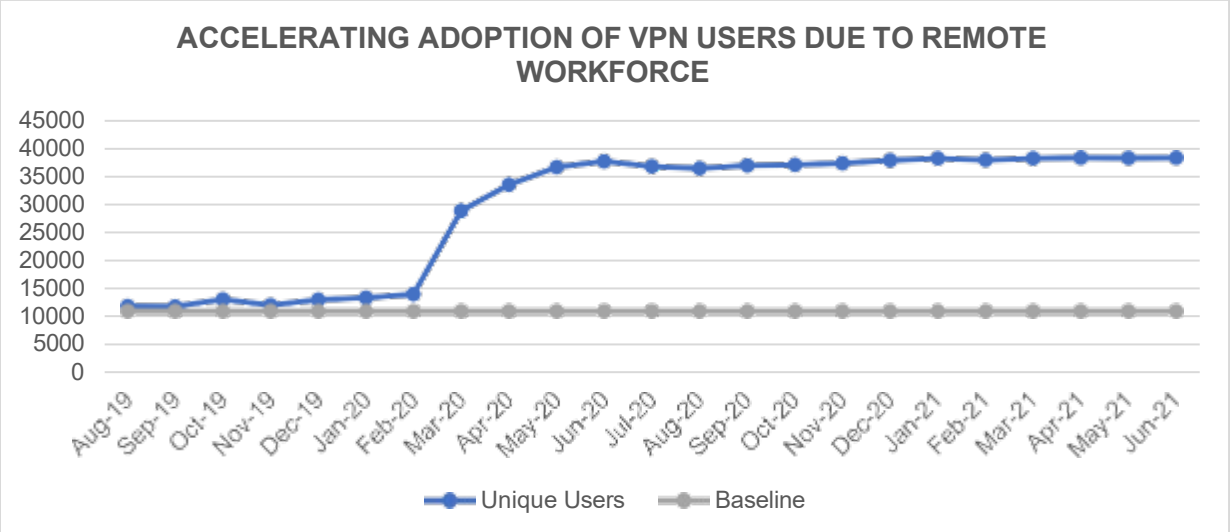


Figure 14 – Trending the increase in unique VPN users

Changing how we use telecommunication technology:

One of the capabilities within Microsoft Teams is the ability to provide telephone service (known as softphone technology) over the internet at a much lower cost than the current on-premises phone system. As the central service provider of phone service, WaTech was able to leverage existing phone network services and infrastructure to lower the cost of the service to members of the Enterprise Shared tenant.

The move to a remote workforce in response to COVID-19 increased adoption of softphone technology as reflected in Figure-15. Call centers that provide services and benefits to constituents converted from working in the office to being remote. WaTech was able to rapidly deploy remote agency software and monitoring tools to help maintain access to these important services. It is anticipated that most of these call centers will continue providing services with remote agents after employees are cleared to return to the office.

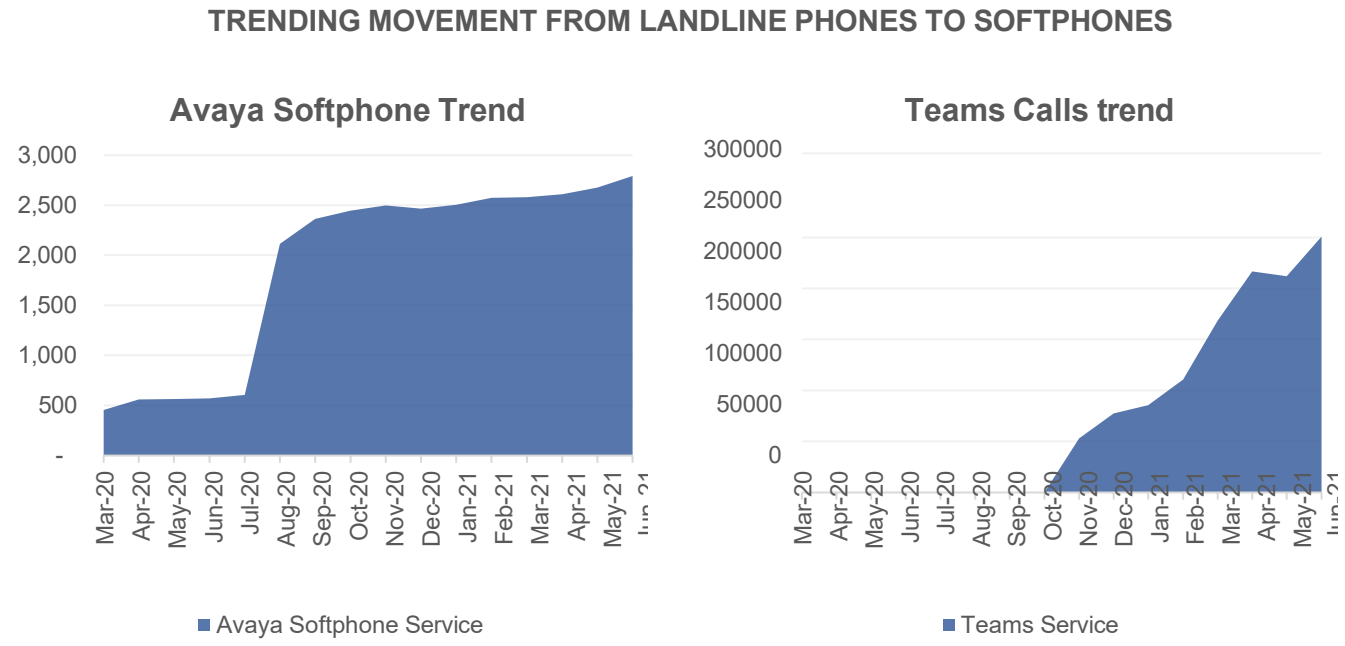


Figure 15 – Adoption trend of modern telephone (softphone) technology.

- Virtual Conferencing:
  With the state workforce move to remote work, agencies turned to conferencing services to meet, communicate, and collaborate. Across the state there was a 200-300% increase in the usage of conferencing services. Utilization of the services – including WebEx and the state's operator assisted Conference Bridge services – spiked at the beginning of the pandemic and then leveled and gradually decreased with the introduction and adoption of Microsoft Teams (Figure-16).

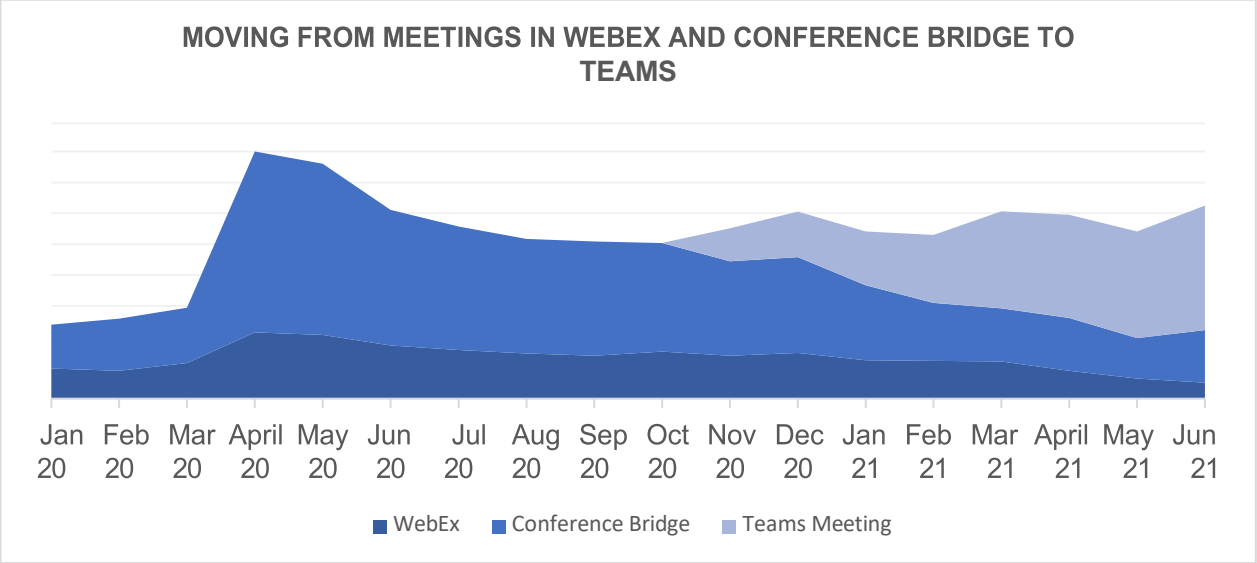


Figure 16 - Virtual meeting movement between 3 different statewide solutions.

- The future of on-premises communication system (Avaya PBX):

  Over the past two years, as users transition to cloud-based softphone technology, WaTech has continued efforts to provide a high-quality telephone service with the on-premises PBX telephone platform for the government services still requiring this technology. Efforts to reduce costs include:

  - Consolidating systems, upgrading older systems, and combining Public Network access from widespread individual circuits onto a centralized digital access which leverages the state's data network.
  - Sixteen PBX systems have been consolidated into two systems uniting offices and associated resources across the state.
  - All of Washington's prisons have been upgraded to modern, well managed communications systems as have the state hospitals (Western State and Eastern State).
  - In the movement to centralized Public Network Access, over 200 individual circuits have been eliminated so far.
  - A new 911 management system also was put in place with upgraded notification capabilities.

- Challenges to on-premises Avaya PBX:

  The sustainability of the on-premises PBX system faces challenges as users migrate to cloud-based telephone services, such as Microsoft Teams. Other services such as analog lines and conferencing services are expected to decline as they are replaced by cloud-based

or lower cost alternatives. It is anticipated the support cost for on-premises PBX will rise, potentially resulting in rate increases to remaining users.

Public access to data including those with disabilities:

By statute (RCW 43.105.220), state agencies must set priorities for making public records widely available electronically to the public. The state of Washington is committed to providing access to information technology to the public and Washington state employees, including individuals with disabilities.

Accessible design and development ensures both direct and equal access that is compatible with a person's assistive technology including screen readers, alternative input devices or screen magnification. Web accessibility services and solutions introduced during the biennium include a "Check Accessibility" feature in Microsoft Word and WaTech Web Accessibility services available to state agencies.

Agencies continue to report improvements in public access to data as well as accessibility to those with disabilities. Examples of accessibility, transparency and mobile access during the biennium includes:

- Washington Health Benefits Exchange Healthplanfinder:

  The Washington Health Benefit Exchange provides more than 1.8 million Washington state residents with quality, affordable health insurance coverage and is recognized as one of the nation's top state health insurance exchanges. Approximately 12.8% of Washington state's 7.1 million residents report having a disability, according to the U.S. Census Bureau's 2015 American Community Survey. People with disabilities need health care for the same reasons everyone else does – to stay well, be active, work and participate in community life. However, disability-related disparities in access to health care are prevalent.

  During the past two years, the Washington Health Benefits Exchange committed to making Washington Healthplanfinder accessible to people with disabilities. Metrics were developed to track, triage, and prioritize ADA issues in new development. As a result, there's been an 85% decrease in accessibility issues being introduced into production. Overall, ADA compliance improved, and the development system lifecycle costs of accessibility decreased. Most importantly, people with disabilities and

Web Accessibility services available to state agencies:

- Code review - Coding standards review with detailed code compliance report.
- Professional accessibility assessment – Assessment service-based criteria that meet accessibility standards and the Department of Homeland Security's Baseline Tests for Software and Web Accessibility.
- Coordinated user testing – Team of experts that coordinates and organizes testing with users of assistive technologies.

assistive technology users can now access, browse, and purchase health plans without barriers.

- Department of Health COVID-19 data through constituent focused dashboard:

  Washington state had the first documented case of COVID-19 in the United States. The Washington state Department of Health (DOH) quickly initiated a massive effort to understand and respond to the epidemic. A crucial part of the response was to collect and disseminate as much information about the disease as possible so that medical professionals, political leaders and the public could make informed decisions and save lives. The public is able to gain access to information on the DOH COVID-19 Data Dashboard.

- Washington Sales Tax Rate Lookup Mobile App:

  The redesigned and updated Sales Tax Rate Lookup mobile app launched in April 2019 for Android, and June 2019 for Apple iOS. The release of the app greatly enhanced the government-to-business experience by making all sales tax rates easily accessible for businesses working across multiple locations such as the construction industry, service and delivery businesses.

  Because Washington does not have an income tax, it relies heavily on sales tax as a primary funding source. In Fiscal Year 2019, Revenue distributed $5.6 billion in sales tax to local jurisdictions. This revenue is distributed based entirely on the local tax codes reported by businesses which is why accuracy in local sales tax rates and coding is so important.

  The new app features and improvements included allowing users the ability to find the combined state and local tax rate at their current location using GPS, or by typing in an address; download or share a spreadsheet (CSV file) with all their saved locations and charges for importing into account systems; and view confirmation codes generated by each search to save for audit purposes. The success of the Sales Tax Rate Lookup mobile app relaunch has been significant. Adoption and usage statistics continue to grow, with nearly 650,000 sessions from April 15, 2019, to April 21, 2020, and more than 1.8 million screen views.

Section 3: Accountable IT Management

Governance Activities to support business requirements:

IT Governance should be continually assessed and improved to reduce risk and meet business needs. A federated environment like Washington state's IT needs a strong governance structure. Several technology governance and advisory frameworks are in place that focus on state priorities, policies, strategies, and objectives (Figure-17).

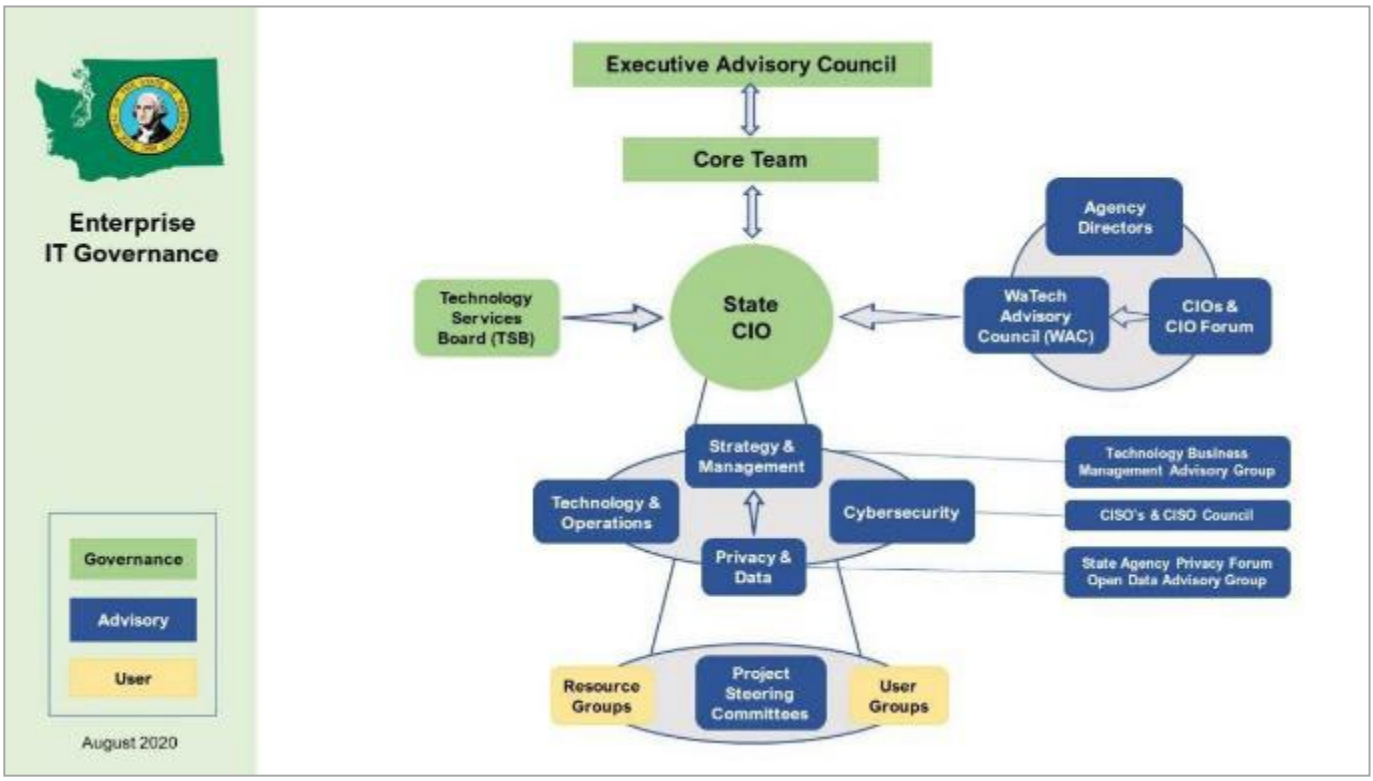


Figure 17 - FY 2020-21 Enterprise IT Governance and Advisory Structure.

The following groups and boards meet on a regular basis to provide the state CIO guidance and steering for strategic vision and planning for enterprise IT initiatives and projects. Additional governance improvements are targeted for next biennium to ensure business needs are being identified and met. Plans are in place to transform and strengthen the current governance model to gain additional input from the business area.

- Chief Information Officers (CIO) Forum:

  The Chief Information Officers (CIO) Forum is a monthly meeting of CIOs representing Washington state agencies. Meetings include discussions of new and trending technology initiatives that may impact the state enterprise, governance issues, updates on major projects, training opportunities and general information sharing. This group sponsored engagement with Microsoft regarding state accessibility and disability issues. The CIOs also had weekly check-ins at the onset of COVID that started as an emergency then attendees discovered value in continuing more frequent meetings. Topics expanded to adoption of Microsoft 365 and discussing uncertainty of moving to the cloud and the costs associated with it.

- Health and Human Services (HHS) Coalition:

  The Washington Health and Human Services Enterprise Coalition (HHS Coalition) is a collaborative that provides strategic direction, cross-organizational information technology project support, and federal funding guidance across Washington's HHS organizations. The HHS Coalition includes the following organizations: Department of Children, Youth, and Families (DCYF), Department of Health (DOH), Department of Social & Health Services (DSHS), Health Benefit Exchange (HBE), and Health Care Authority (HCA). The OCIO and the Office of Financial Management (OFM) are ex-officio members that advise on issues around compliance with statewide IT policies, and state financial budget and legislative processes.

- State Interoperability Executive Committee (SIEC):

  The State Interoperability Executive Committee (SIEC) works to ensure that all emergency responders, across all levels of government and jurisdictions can talk to each other and share data.

  During this timeframe the Washington Statewide Communications and Interoperability Plan (SCIP) was developed and approved by the committee. The purpose of the SCIP document is to use as reference for future planning and communications and applies to state agencies. The document benefits the SIEC, cities and local counties.

- Technology Services Board (TSB):

  The Technology Services Board (TSB) includes legislators, business leaders, agency directors and a union representative. The board acts as an advisor to the state CIO by providing strategic advice and guidance in carrying out responsibilities for strategic vision and oversight of technology in Washington state government. The TSB reviews and approves policies, standards, procedures and provide oversight of major technology projects.

- WaTech Advisory Council (WAC):

  The WaTech Advisory Council (WAC) represents the CIO community and provides guidance and recommendations regarding current and future services to be provided by WaTech. This includes recommending new services or decommissioning existing ones. The WAC helps identify challenges, gaps, and needs across all agencies to assist WaTech with its mission.

- Washington Recovery Group (WRG) to Coordinate COVID-19 Recovery Activities:

  The Washington Recovery Group (WRG) was established to coordinate the state's COVID- 19 pandemic recovery activities and set priorities that strengthen the resiliency of our state and all Washingtonians. Acting in an advisory capacity, board members representing state agencies, boards, commissions, tribal partners, and local agencies discuss recovery issues

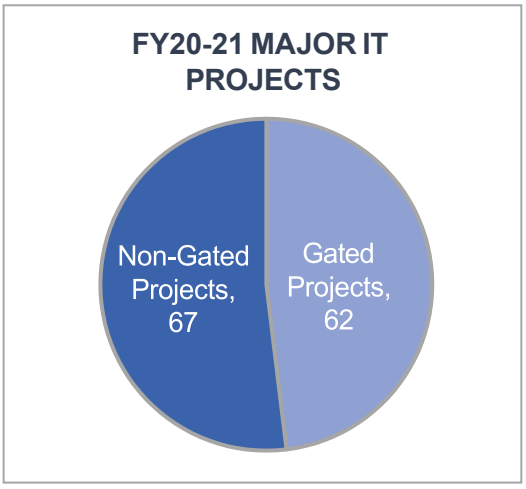
and efforts, establish unified objectives, and provide the governor's executive cabinet lead with recommendations to support state recovery operations.

Major IT Projects:

Through the 2020-21 biennial cycle, the OCIO provided independent oversight to 129 IT projects underway at more than 47 state agencies and valued at over $2.28 billion. Based on language in legislation, 67 projects were gated and 62 were non-gated. For projects assigned to the gated process, a percentage of total funding is retained and released to the agency only after successful completion of project stages. The OCIO evaluates and notifies the authorizing environment when a project is certified to proceed to the next stage.

Throughout the oversight lifecycle, the project health status is assessed monthly. Project health is assessed on the following green, yellow, red scale.

- Green Low risk – Project requires no action beyond management tools already in place.
- Yellow Elevated risk – Project requires action to reduce or avoid critical risks(s).
- Red High risk – Project requires immediate action to mitigate critical risks/issues.



By June 2021, 71 major projects were completed or closed. Figure-18 provides status on the projects at biennium end along with the closed projects final assessment.

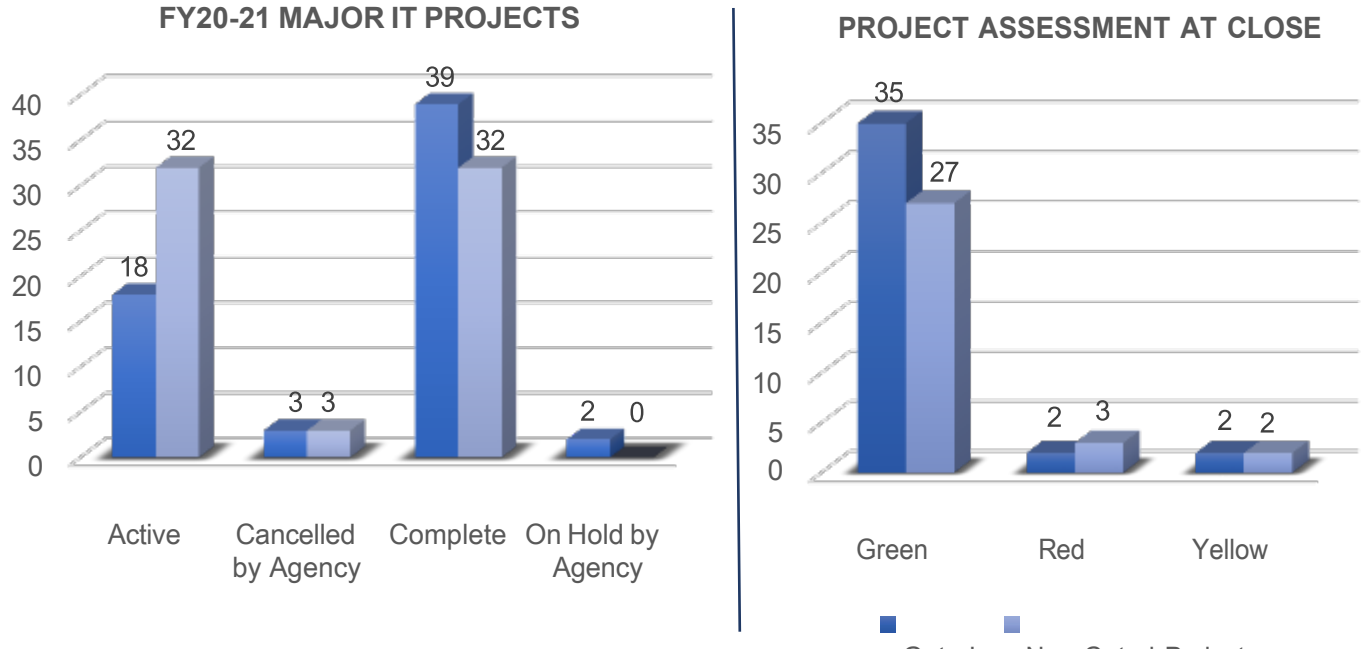


Figure 18 - IT Major project status at biennium close.

- Activities associated with improvements to IT Project Oversight practices:

  The OCIO engaged expert project managers in support of successful project outcomes. Implemented improvements include.

OCIO Project Management Partners	Provided over 4,000 hours of master level project management consulting and advisory services to more than 80 projects including sponsor and project management coaching, shared best practices and lessons learned, risk/issue management and mitigation and procurement and vendor management consulting and advice.
Project Management Community of Practice (CoP)	Established a statewide project management community of practice (CoP) for agency project managers to share experiences, best practices, advice and resources. The CoP hosts live discussion boards and monthly learning events. CoP membership is nearing 170 individuals representing 36 agencies.
IT Project Resource Website	Established an online IT Project Resources website that provides access to a lessons-learned repository for state agencies. This repository provides a tool for project managers and other project stakeholders to learn from the experiences of others to help reduce project risk.
IT Project Managers Guidebook	Published an IT Project Manager's Guidebook for state agencies. This guidebook provides a step-by-step process for managing projects from initiation through closeout. It also includes 24 associated best practice-based project management templates to aid project managers.
Reports	Shared observed IT project best practices for agency IT stakeholders and legislative fiscal staff in four separate quarterly reports. Delivered two annual reports on independent recommendations on oversight of IT projects, accountability and performance metrics to legislative fiscal committees.

- IT Project Dashboard Enhancements:

  The Washington State IT Project Dashboard provides the public with major IT project data in a graphical format as well as additional options for viewing information. During the biennium, noteworthy changes made to the dashboard include:

  - A standard technology budget template developed and used by all major IT projects under oversight to provide granular reporting. Additionally, the template meets statutory IT project reporting requirements by aggregating project financial information in a uniform manner.
  - Displaying financial data on gated funding projects with approved technology budgets.
  - A view of projects by agency along with associated financial data. Users can select the agency to be viewed and navigate to individual agency project pages.
  - Technology budgets showing the project planned spend along with a display of actual expenditures from the state financial system providing insight into the projects budget variance.

- Key documents are available and sorted by type to make it easier to find material. Status information is displayed to show a project's history. Users can hover over the status symbol for a description of the color and effective date of the status.

Investing in legacy application modernization:

The state has made progress with several business transformation and modernization projects currently underway. By the end of June 2021, more than 73% of the major technology projects under OCIO oversight were dedicated to addressing legacy modernization and business transformation efforts. The reported budget for these multi-year projects total over $2.05 billion.

For this report, analysis of funding legacy application modernization efforts is limited to the 140 IT decision package requests submitted by agencies in the 2021-23 biennium. As seen in Figure-19, 58% of the budget requests were to address modernization efforts. For submitted modernization funding requests, Figure-20 provides insight into the final amount funded.

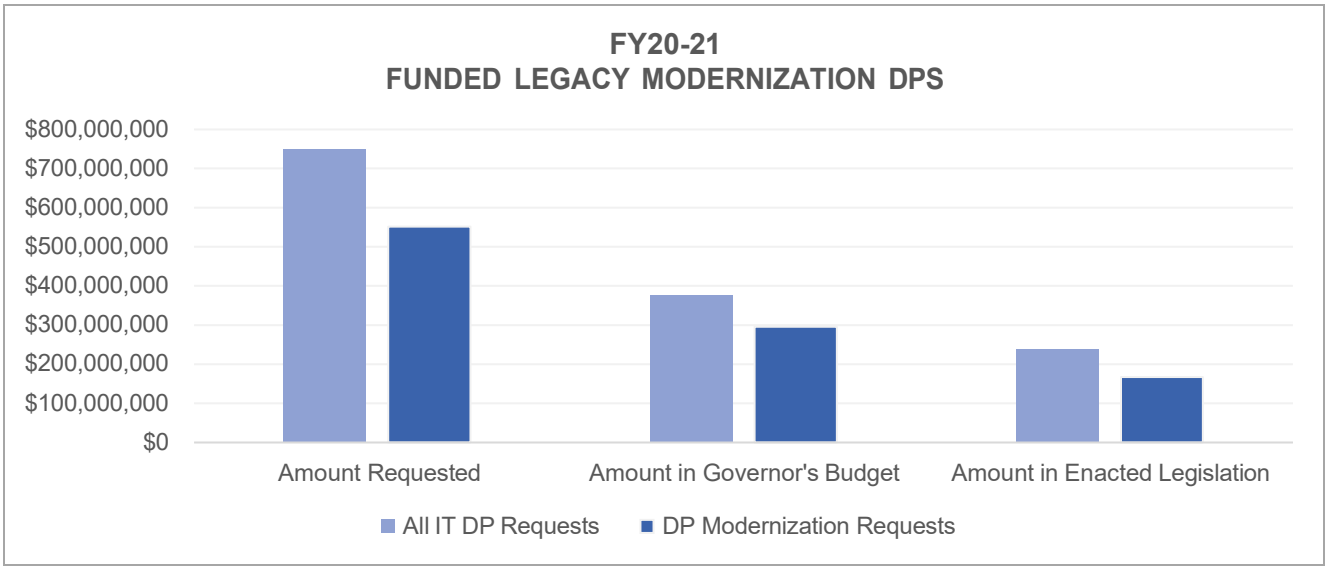


Figure 19 - 140 agency modernization funding requests submitted.

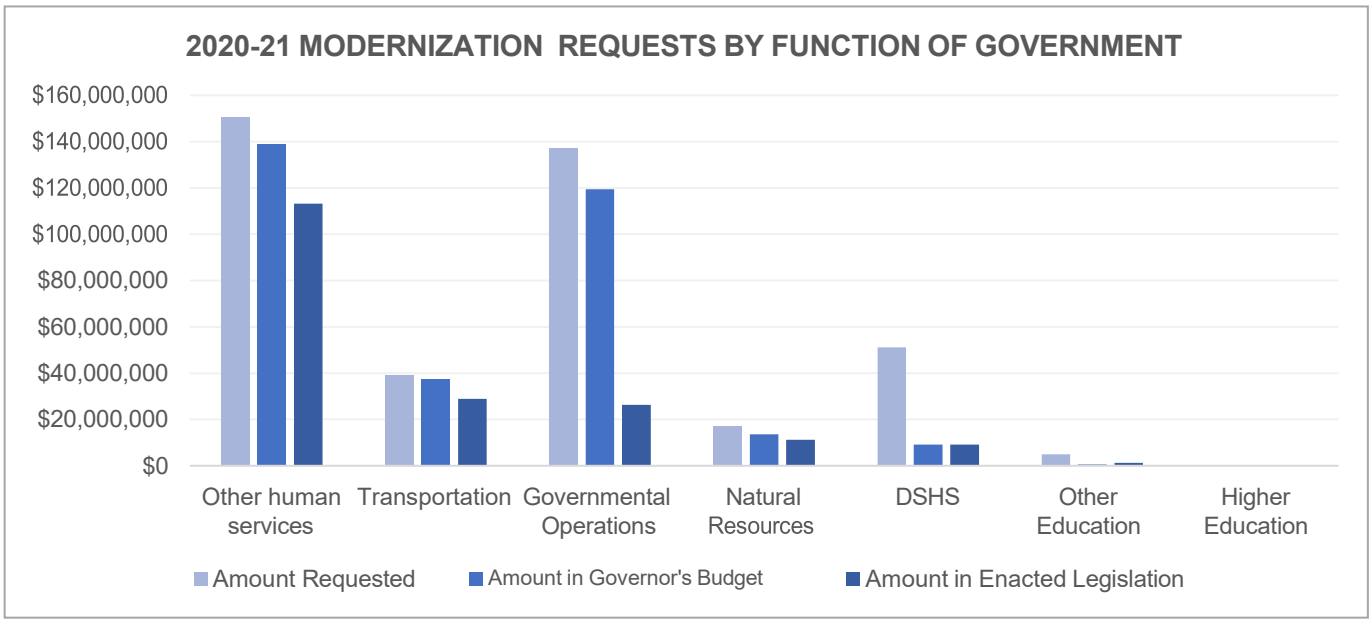


Figure 20 - Funding requests by function of government.

Statewide application portfolio - assessing modernization:

As Washington's business application portfolio ages, the state continues to take a hard look at legacy applications to ensure business needs are being met. This includes moving forward with a systematic plan to address legacy applications and technical debt.

With 5,935 applications registered with the OCIO, emphasis has been placed on modernization. Continued analysis provides insight into the number of state systems that will require future investment to modernize legacy characteristics. Agencies include responses to legacy questions in their annual application portfolio submittal. In FY2020 the application inventory system was end-of-life and replaced with an Excel template.

WHAT IS A LEGACY APPLICATION?

- The system cannot be easily updated due to complicated or unclear code, fragile interfaces, or lack of documentation.
- Maintenance or modification of the system depends on expertise that is hard to find or prohibitively expensive.
- The system depends on software no longer supported by the vendor.
- Other risks identified by agencies, such as vendor instability and lack of alignment with enterprise architecture or a lack of in-house expertise.

TECHNICAL DEBT

Technical debt is the backlog created when quick, lower-cost solutions are used to meet near term needs instead of pursuing a design or solution that may take more time to implement but is the better strategic choice. While this approach may be less expensive initially, the long-term costs can end up being much greater and pose increased financial and reputational risk.

Changing to the application template resulted in gaps in application data submitted by some agencies. While agencies improved the list of applications in their inventory, in many cases they neglected to respond to some legacy inventory questions. Figure-21 displays the legacy trend of the state application portfolio at the end of FY21.

Agencies also self-define how critical their applications are to the organization. Figure-22 provides a breakout by percentage of how they categorize their applications based on the following four definitions and potential results if the system is unavailable:

- Business Essential: If unavailable, there is direct negative customer satisfaction; compliance violation, public damage to organization's reputation; direct revenues impact.

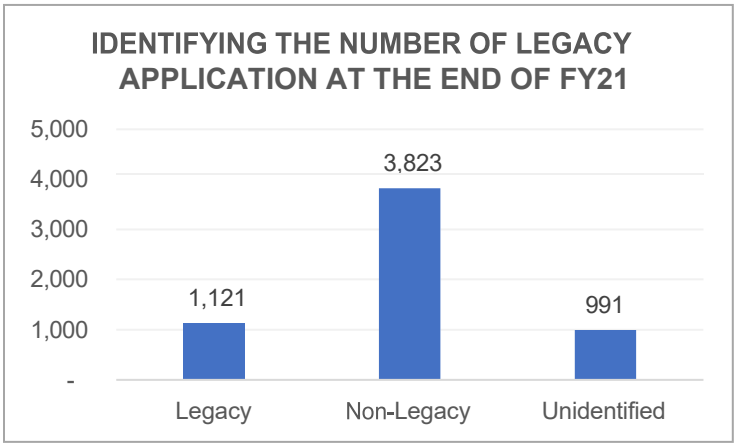


Figure 21 - 91% of the unidentified applications are associated with 3 agencies not responding to legacy questions in the inventory.

- Historical: Needed for historical purposes.

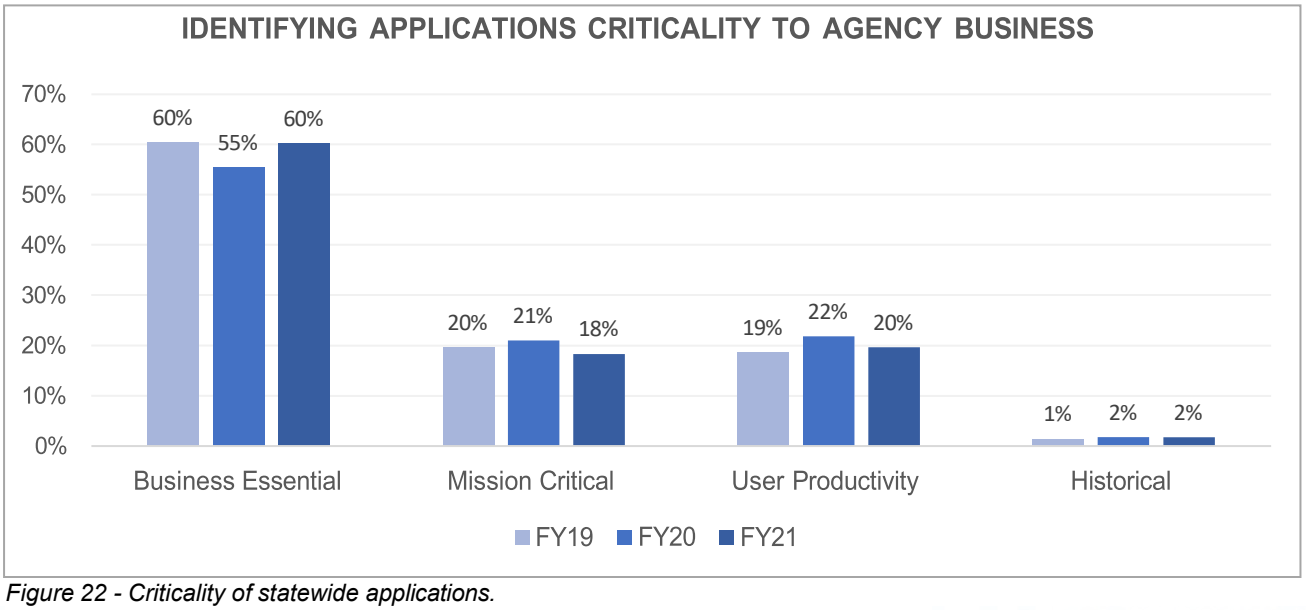


Figure 22 - Criticality of statewide applications.

- Mission Critical: If unavailable there is widespread business stoppage with significant revenue or organizational impact; risk to human health/environment; public, wide-spread damage to organization's reputation.
- User Productivity: If unavailable there is impact to employee productivity.

State agencies have reduced their use of legacy applications that are not critical to their mission. As a result, the mission critical and business essential applications – which are harder and more expensive to replace – account for a large share of the state's legacy applications as shown in Figure-23.

As noted in the Financial Assessment section, applications attract the highest percentage of internal labor support. Agencies report support and operations attracting the highest portion of internal labor followed closely by application development, then support of Commercial Off the Shelf (COTS) business software (Figure-24). A high percentage of internal labor is associated with custom-built applications listed in the state portfolio.

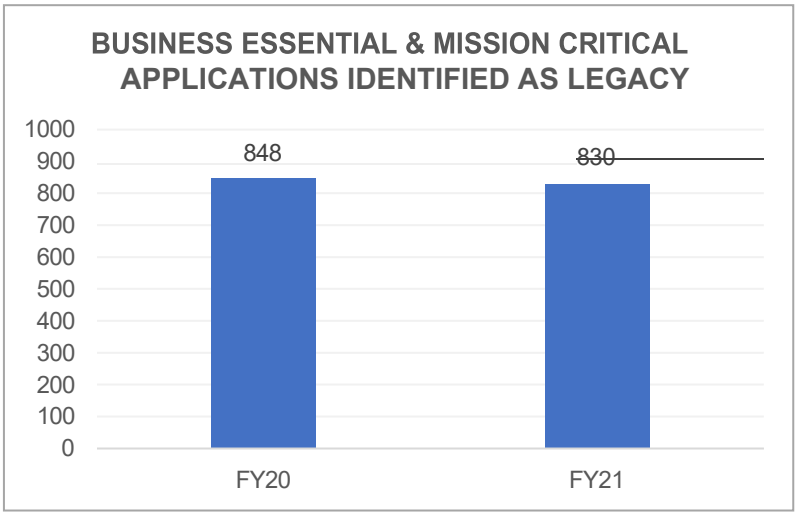


Figure 23 - Trending legacy applications over the biennium.

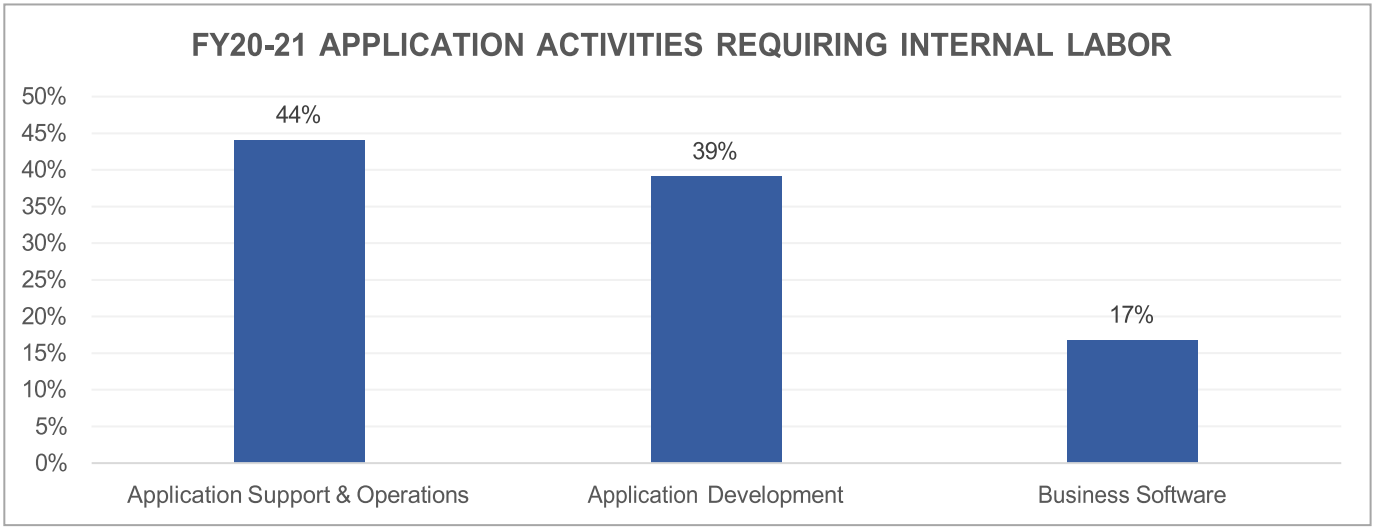


Figure 24 - Note: Business software support is for COTS business software.

Historically, custom applications lack scalability and make upgrades challenging. In many cases, changes to custom applications can take more time to implement which creates problems when speed is needed to adapt to fiscal and policy changes. Custom-built applications continue to dominate the state's application portfolio but have declined slightly over the last three years (Figure-25).

In Washington, like many states, tight budgets, business-driven deadlines and funding cycles have helped fuel a growth of technical debt. A mix of system changes have occurred over time as a result, with agencies building on top of existing applications to enable new capabilities.

These systems become harder to sustain and may need additional investment or replacement.

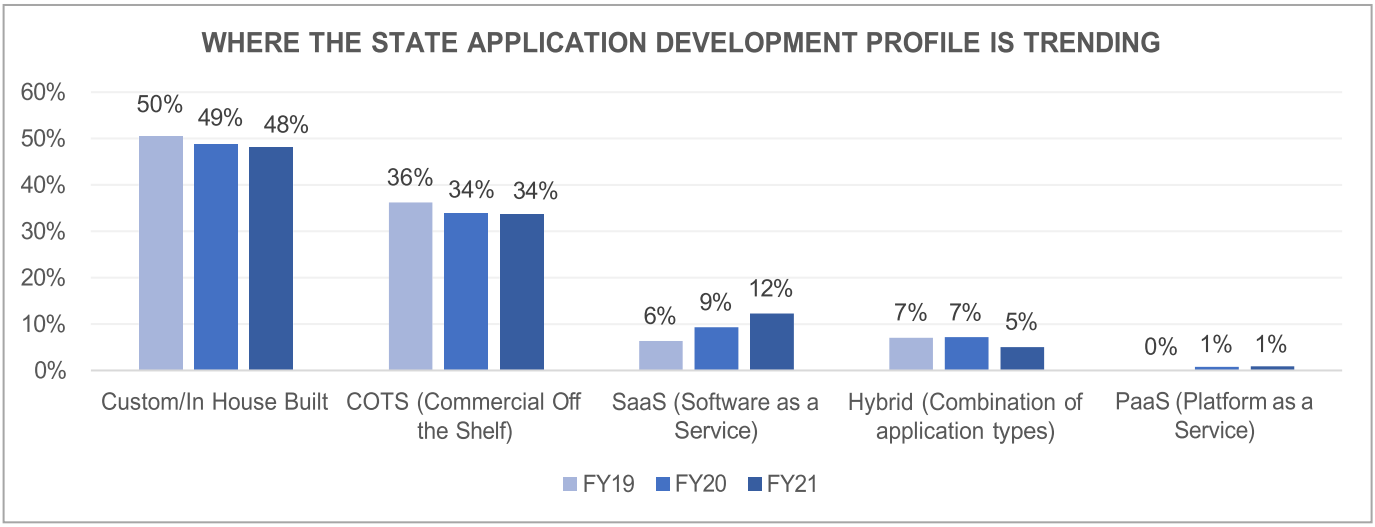


Figure 25 - Application portfolio development trends.

By the end of fiscal year 2021, 476 applications of the statewide application portfolio were identified as legacy custom-built systems supporting mission critical or business essential functions (see Figure-26). These applications surface as priority candidates for a modernization assessment.

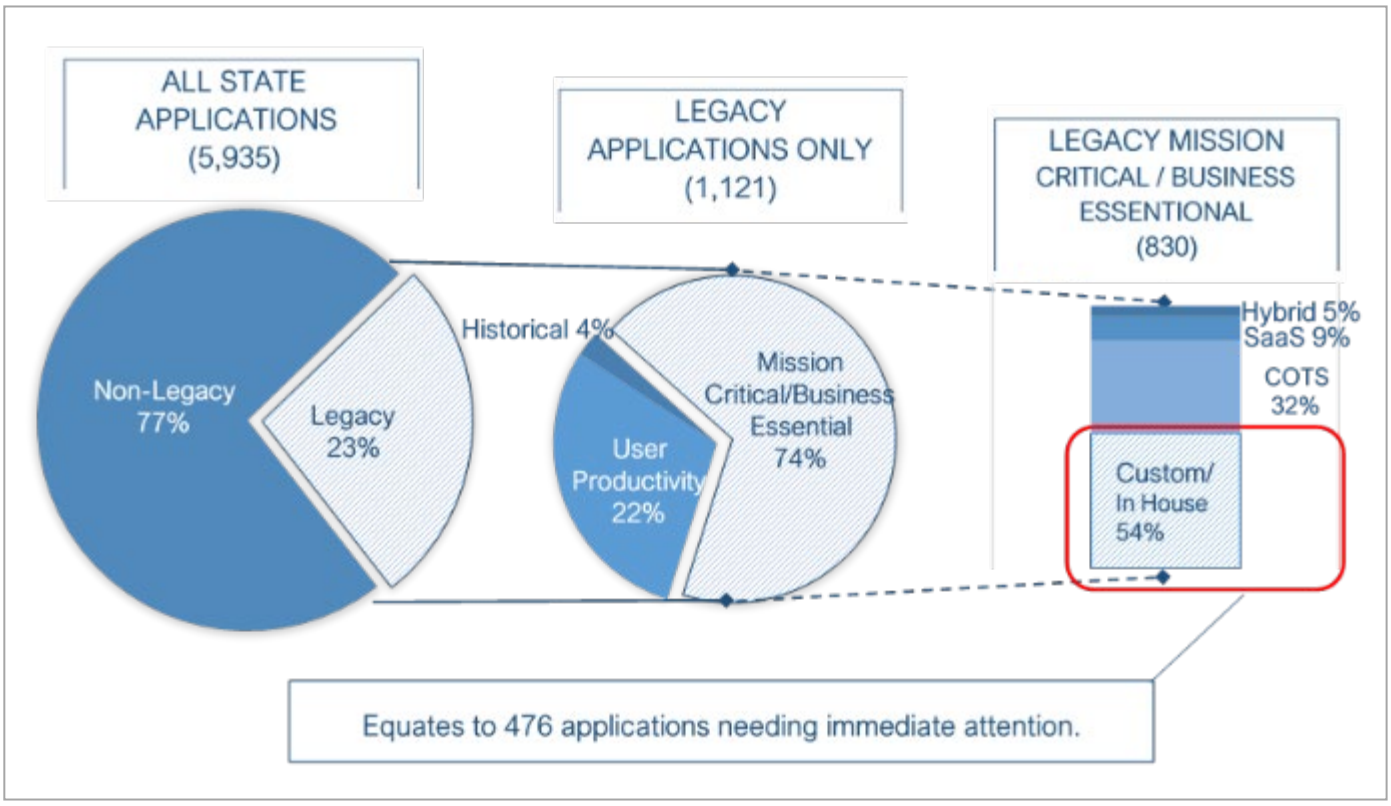


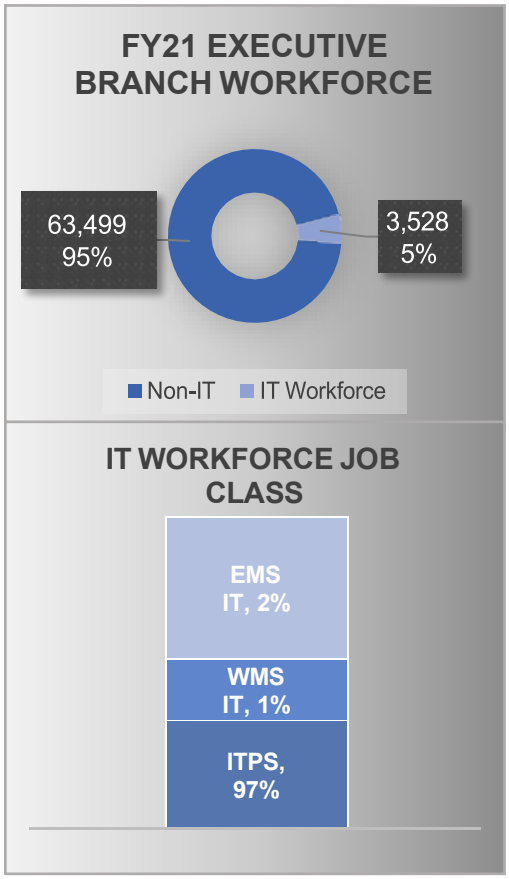
Figure 26 – Legacy application profile.

Section 4: IT Workforce

Starting July 2019, a new IT Professional Structure (ITPS) became effective. By the close of FY2021, the Executive Branch workforce numbered over 67,000 with 5% identified as IT.

The IT workforce data represented in this report is Executive Branch but:

- Excludes higher education.
- Washington Management Service (WMS) IT and Executive Management Service (EMS) IT is restricted to WMS and EMS jobs with Information Technology Market Segment.



Prior to the reclassification, over 80% of the positions in the state's IT workforce were in three IT Systems/Applications Specialist (ITS/ITAS) job classifications – ITS 4 & 5, ITA/S 6: and the three highest paying Washington General Service (WGS) classifications.

Business drivers for the change:

- Recruitment and retention problems.
- Misallocation of employees.
- Generic and outdated classification structure.
- Lack of alignment with industry and market definitions of IT work.
- Unable to compete for specific specialized skills in the job market.
- Legislative interest in the management of the IT workforce in state government.

ITPS CLASSIFICATION GOALS

- Industry-relevant job titles and job levels.
- Realign state job classifications to accurately reflect work, enabling comparisons to local public and private sector jobs.
- Ability to benchmark work internally and externally.

ITPS COMPENSATION GOALS

- Market-informed pay range alignment.
- State IT ranges vs local public and private sectors.
- Enhance state efforts to recruit and retain IT talent.

At the close of FY21, 57% of the ITPS workforce were within application development, IT system

administration and IT customer support (Figure-27).

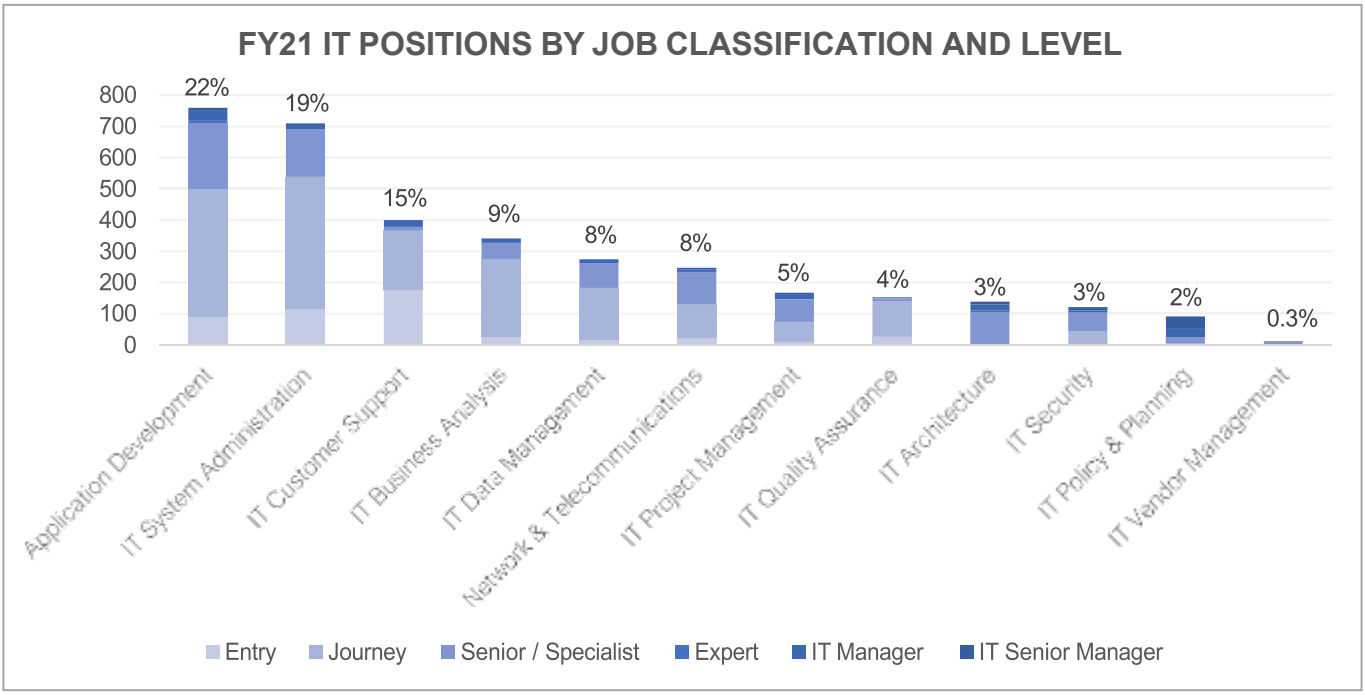


Figure 27 - FY 21 ITPS workforce by job classification and job level.

In the previous biennium there was a perception that positions reclassified out of IT would result in employees leaving for other positions that remained in higher salary IT positions. Other concerns surfaced related to salary compression issues where the IT classified positions pay became higher than their supervisors who are in Washington Management Service (WMS) or Exempt Management Service (EMS) positions. The data collected over the biennium shows a high percentage of workforce filing appeals due to the reclassification.

As a result of the reclassification 3,902 positions transitioned into the ITPS and 198 positions identified as not meeting requirements of ITPS reallocated into the appropriate job classification by the employer. Table-3 provides details on positions that remained IT and those no longer IT.

POSITION STATUS OR JOB RECLASSIFICATION AS OF JULY 1, 2019

		07/01/2019		Remained IT						No Longer IT			
Position Type	FY19 6/30/19	Active	Delimited	ITPS	New WGS IT	Old WGS IT*	WMS IT	No Job Class*	IT Subtotal	WMS Not IT	WGS Not IT	Exempt Not IT	Non-IT Subtotal
Classified IT	3,852	3,823	29	3,454	116	34		21	3,625	2	194	2	198
WMS IT	279	277	2	218			59		277				-
Total Classified IT Positions	4,131	4,100	31	3,672	116	34	59	21	3,902	2	194	2	198

**Positions with Old WGS IT Job Classification and positions not assigned a new job classification not considered to be "classed out" of IT as of July 1, 2019.*

Table 3 - IT Position reclassification in 2019.

Appeals related to ITPS reclassification:

The IT workforce encountered the following salary reclassification impacts:

- 2,117 employees with wage growth opportunity in new structure (progression through steps).
- 484 employees at Step M (top longevity step).
- 431 employees at Step L, approximately six years until progression to longevity step M.
- 414 employees Y-rated, total for positions included and excluded from ITPS.

A total of 1,041 appeal requests for Director's Review were filed to the State Human Resources (HR) office. State HR hired additional staff to manage the appeals and revised business processes to address this significant workload. It is anticipated that all appeals will be completed in FY22.

CHALLENGES TO ITPS RECLASSIFICATION	ITPS RECLASSIFICATION POSITIVE IMPACTS
• Adherence to evaluation standards and making consistent allocation decisions. • Employee appeals. • Potential inversion/compression with exempt and/or management positions. • Employee discontent with job class titles. • Employee Y-rating – salary above new pay range. • Employee positions excluded from the ITPS.	• Established foundation to assess market competitiveness of our pay ranges. • Enterprise and organizational alignment and equity. • Ability to implement targeted increases to address areas of concern. • Increased promotional opportunities. • Funding for progression increases (PIDs). • IT Governance Committee oversees management of the ITPS.

ITPS maintenance and operations activities implemented for ongoing support:

- Creation of the ITPS Governance Committee. The ITPS Governance Committee, co-chaired by the OFM Assistant Director for State Human Resources and the State Chief Information Officer, is a multi-agency collaborative responsible for effective and sustainable oversight and guidance for the administration of Washington's ITPS.
- Centralized review of all Expert level evaluations to be approved by the Assistant Director of State HR prior to allocation.
- All agencies and institutions required to follow the State HR consultation process. State HR reviews evaluations prior to allocations being finalized. Once the agency or institution have demonstrated they are meeting the established criteria they are released from the consultation process and can allocate positions without external review.
- Requirement in rule for each agency to have a designated ITPS Coordinator responsible for coordinating internal evaluations and participating in the statewide ITPS Coordinators Workgroup managed by State HR.
- Quarterly monitoring of ITPS usage by State HR.

Why are they leaving and where are they going?

Over the previous two biennia it was reported that a high percentage of the state's technology workforce was eligible to retire within the next five years. During FY20-21, 12% of the IT employees exited state service for various reasons with over 45% (421) leaving to retire (Figure-28).The average age of retirees was 64 years.

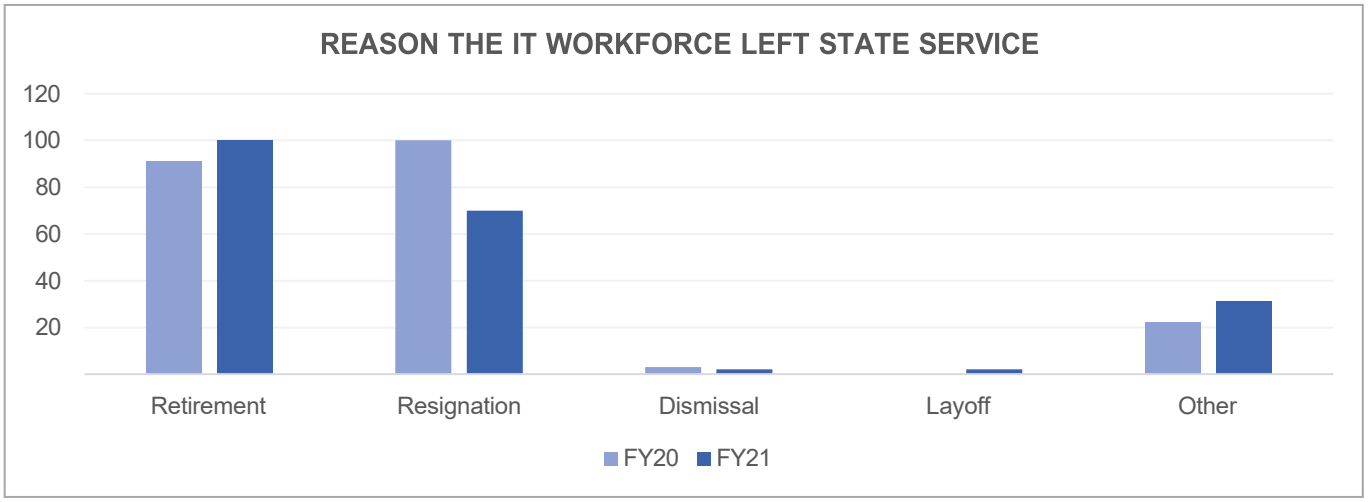


Figure 28 – Why the IT workforce are leaving.

Of the IT workforce exiting state service, 120 participated in an exit survey providing information on where they are going (Figure-29) and their years of state service (Figure-30).

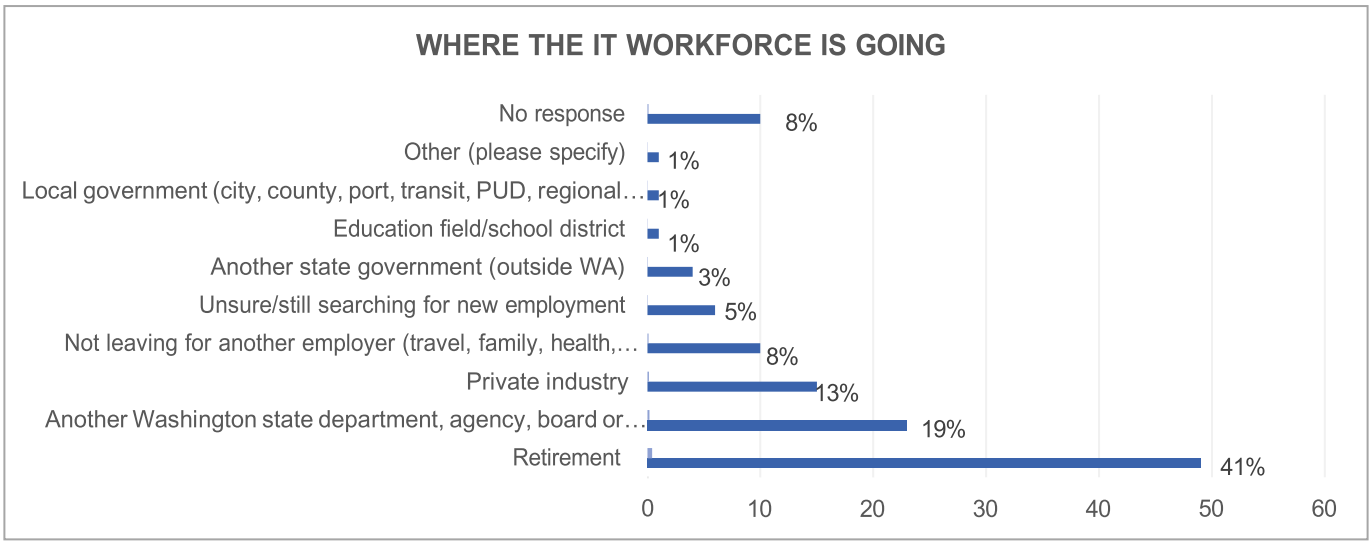


Figure 29 – Responses from the 120 IT workforce submitting exit survey.

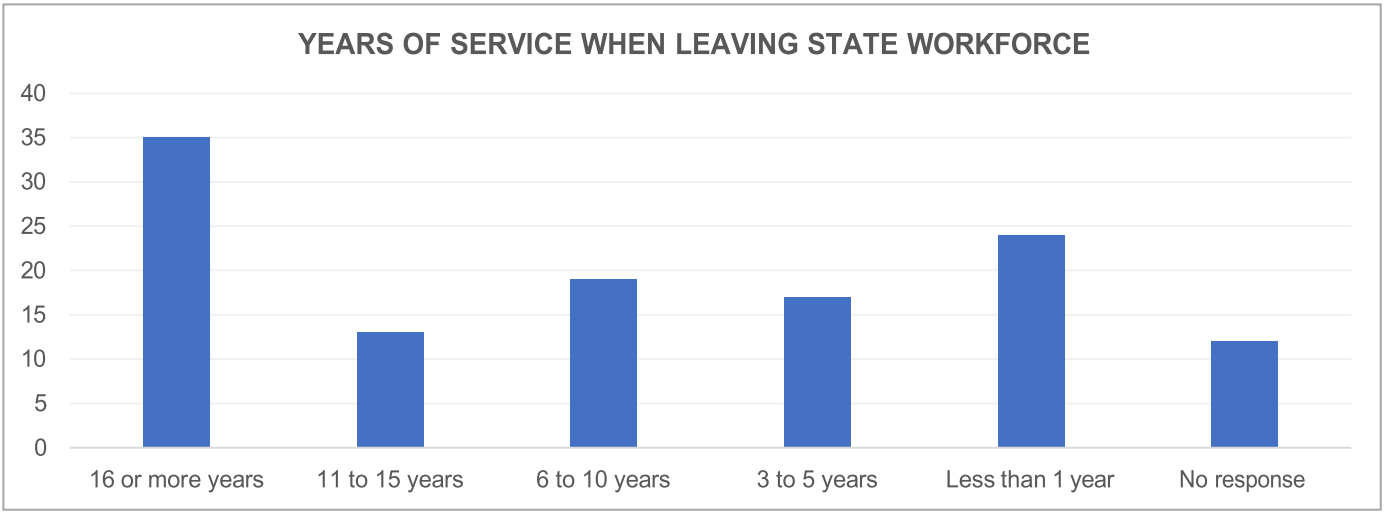


Figure 30 – Exit survey respondents' years of service.

IT workforce age and diversity:

At the end of June 2021, 3.5% of the IT workforce was under age 30, 46.3% are in the 30-49 age bracket and 50.3% are 50 and older. The percentage of the IT workforce over 50 years old runs higher when compared to the executive branch while the 30-and-under workforce is much lower (Figure-31).

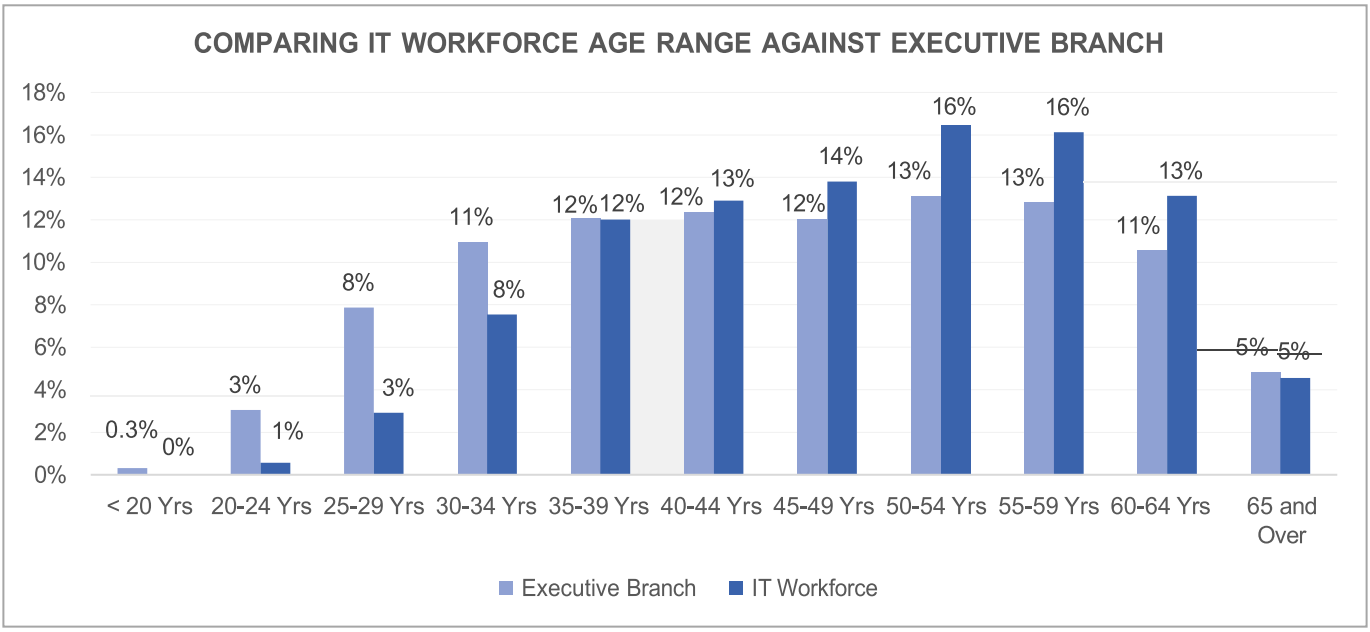


Figure 31 - Average age of Executive branch and IT workforce.

The IT workforce had 400 new hires during the biennium. At 14%, there is a limited number of hires in the under 30 age range while over 40% of the new hires were in the 45 and older age range. Figure-32 provides additional detail on the age of new hires.

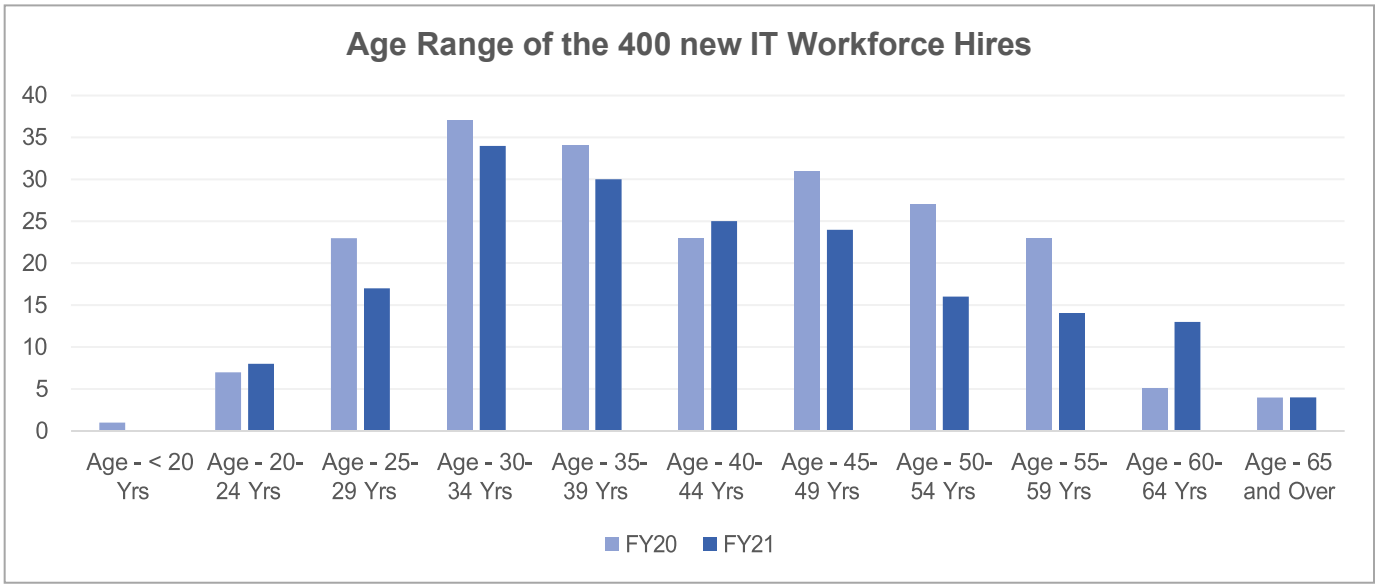


Figure 32 - Age of new hires to state IT workforce.

Within ITPS there are six progressive job class levels: entry, journey, senior specialist, expert, manager, senior manager. With the high percentage of the IT workforce in the 50 and over age category as indicated in Figure-33, work needs to be done to build a path that attracts, trains, and develops those in entry level positions to be the senior level experts of the future.

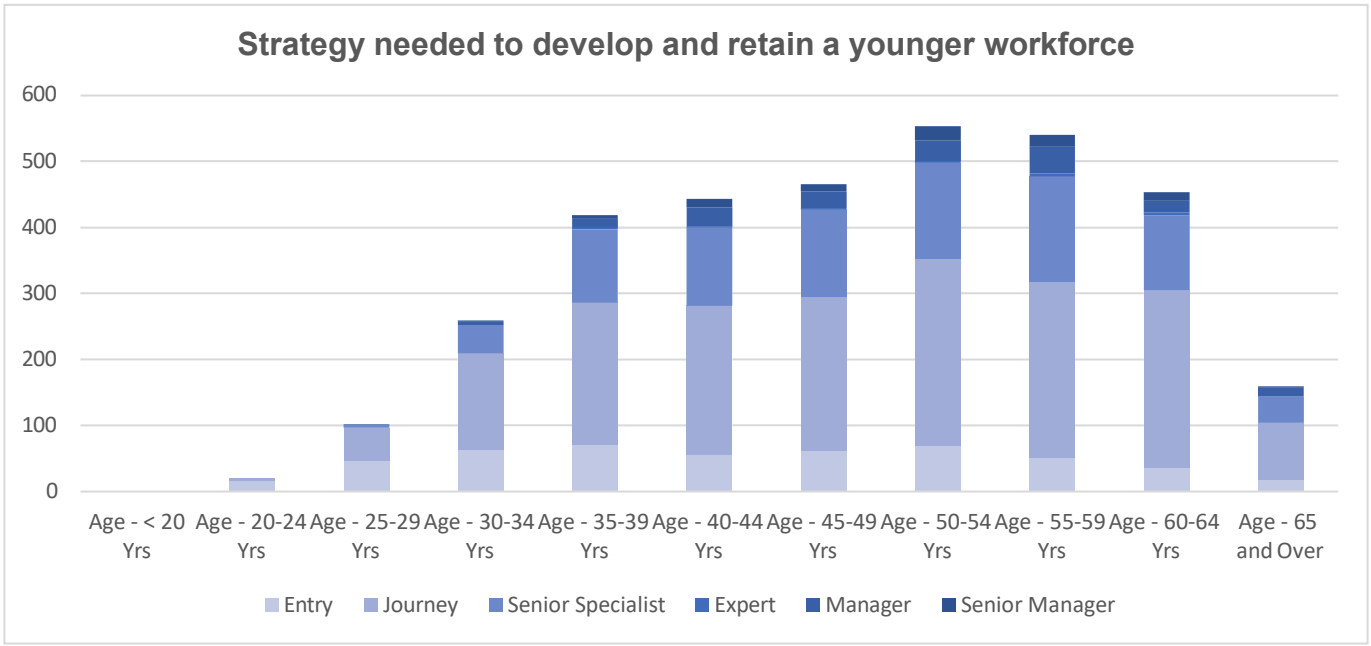


Figure 33 – IT Workforce job classes by age category.

Figure-34 compares the diversity level of the state IT workforce and the executive branch including insight into 2021 new hires.

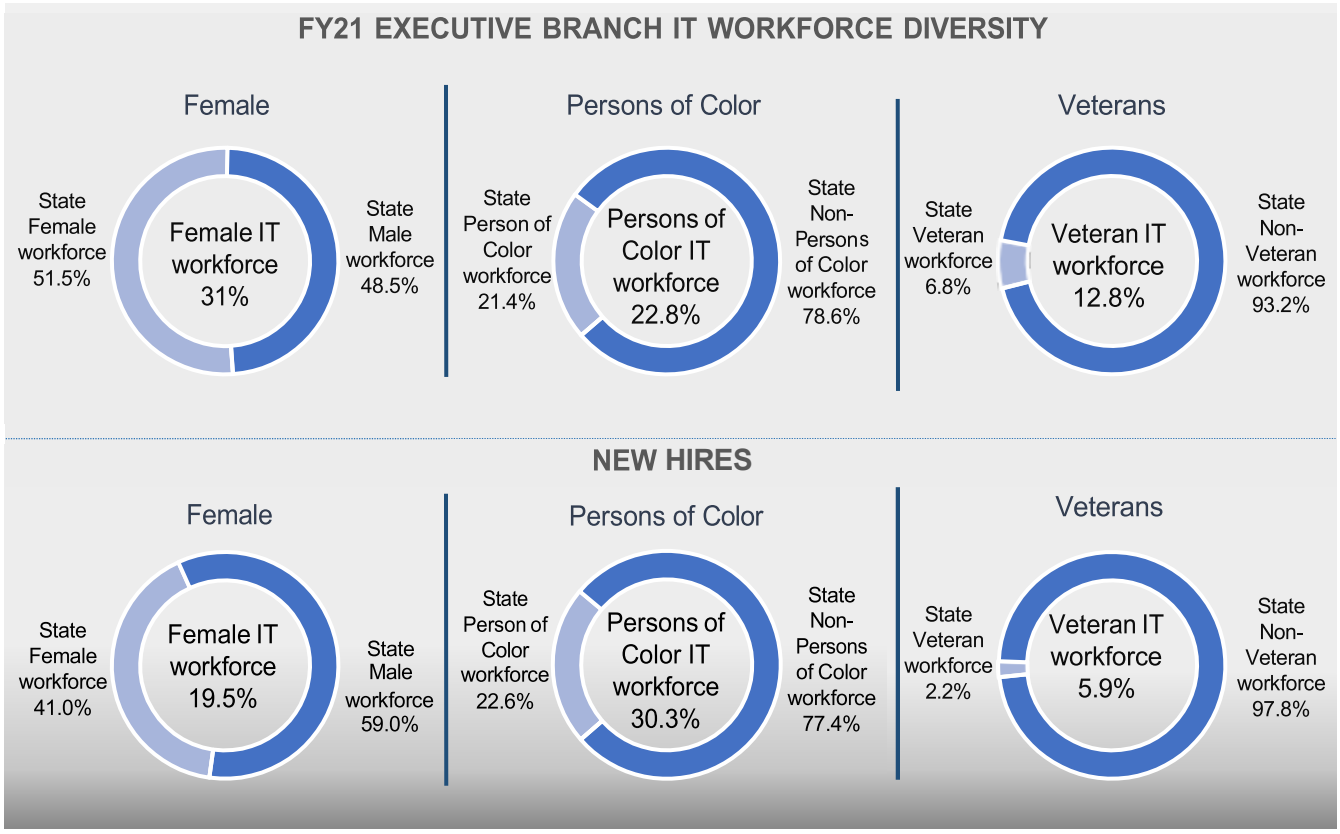


Figure 34 - FY21 Executive Branch and IT workforce diversity.

Cloud Transition Task Force:

The Washington State Legislature has determined that the state's information technology systems should move toward cloud services. To ensure the state can retain its current talent base and arm them with appropriate skills and tools to thrive in the cloud-based technology environment, the Legislature created the Cloud Transition Task Force to review and provide recommendations related to three key issues:

- Impacts on the state government's IT workforce of transitioning to third-party cloud computing services.
- Retraining needs that the existing workforce may require to maintain employment in the information technology sector and deliver cloud computing services effectively within state government.
- The optimal method for delivering such training.

The Cloud Transition Task Force is comprised of IT executive leadership, private and public sector subject matter experts and state labor union representatives. The task force will deliver recommendations to the Legislature addressing the key issues in the 2022-23 biennium.

Figure-35 from Gartner illustrates the new roles and skills that will be needed as cloud technology becomes the industry standard.

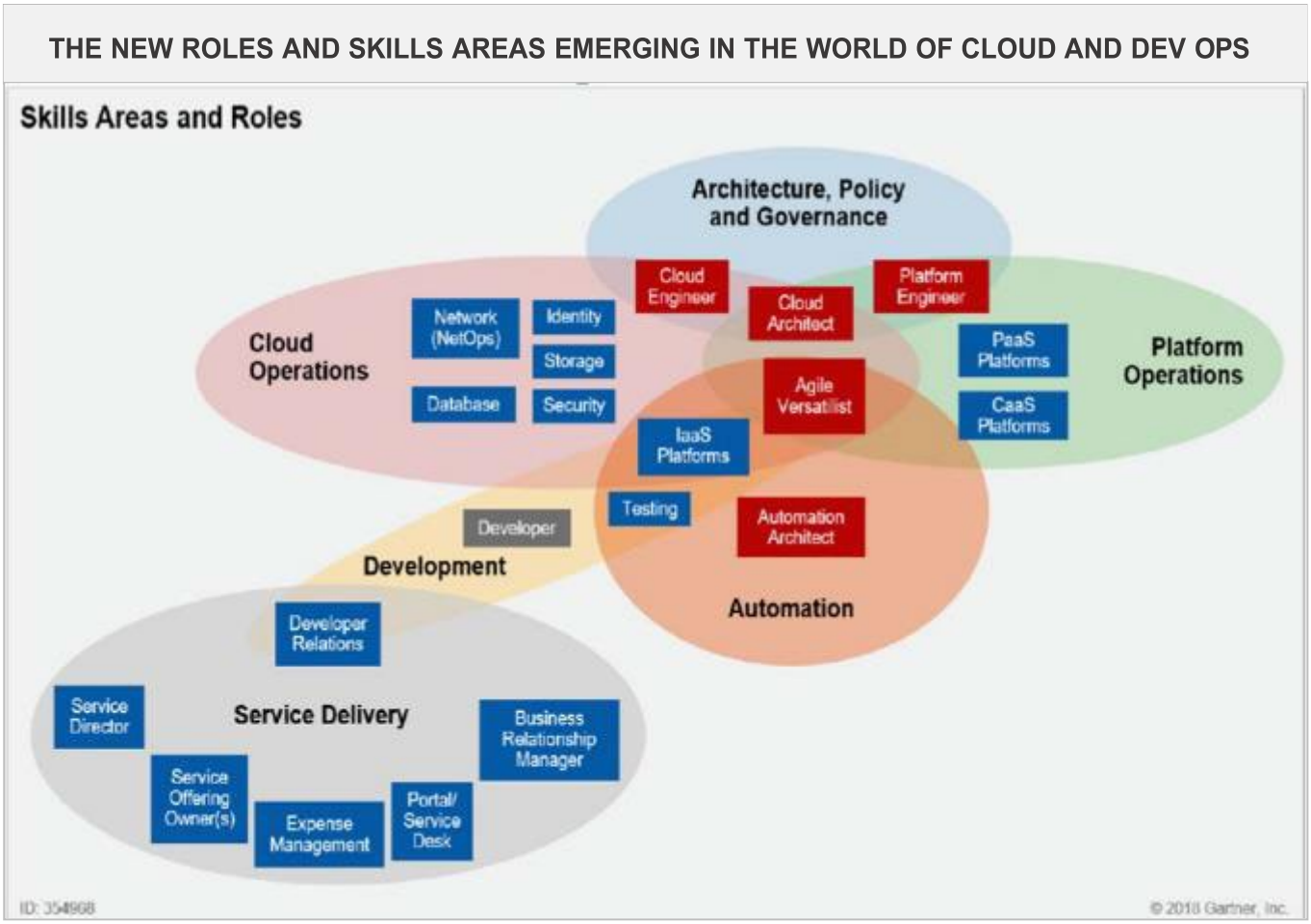


Figure 35 - New roles and skills emerge in the world of Cloud and DevOps, Gartner, 2021.

Section 5: Enterprise Architecture

Enterprise architecture (EA) (RCW 43.105.265) translates business vision and strategy into effective enterprise change. EA also shows how information, business and technology work together to accomplish the state's business objectives.

One of EA's major value propositions is that the enterprise achieves significant value by sharing and reusing common solutions and strategic resources. The EA model in Figure-36 depicts the architectural operating model that ensures state IT investments align with the State Technology Strategy and is the foundation supporting reuse across business services.

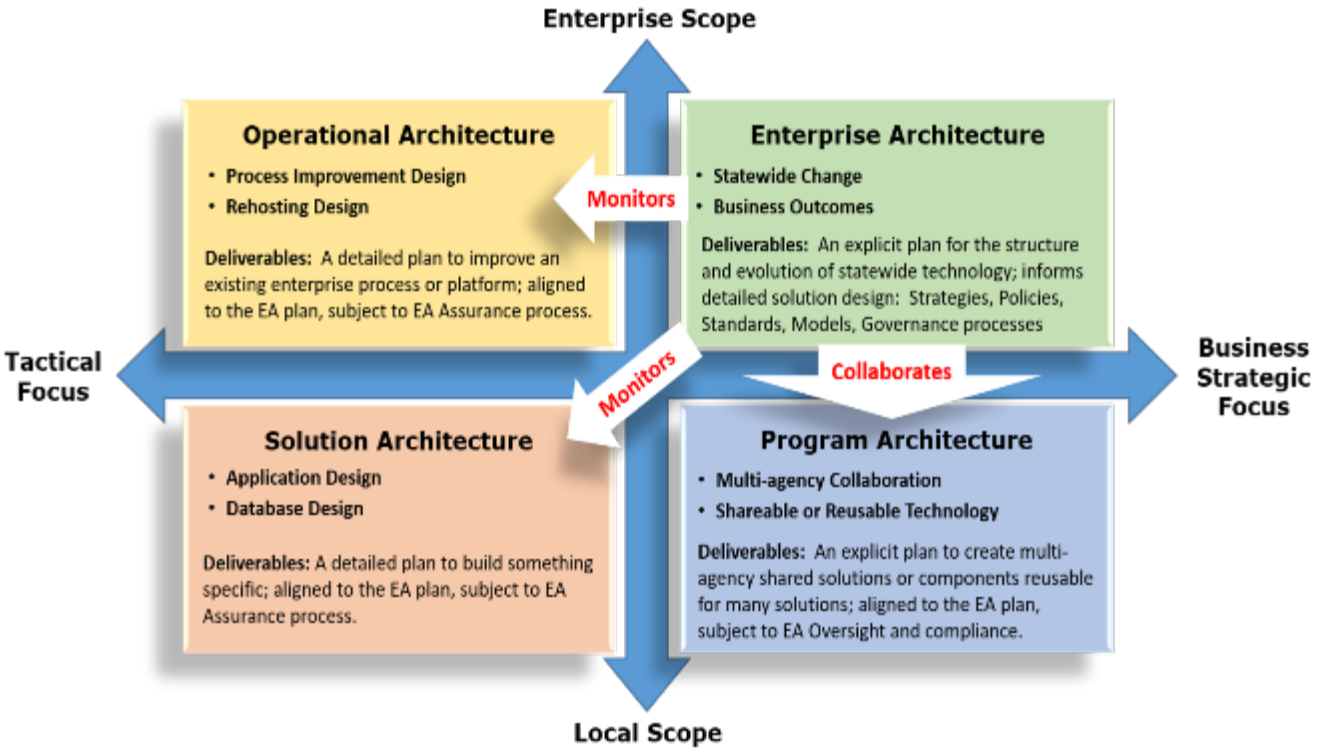


Figure 36 - Enterprise Architecture uses an operational model to ensure technology decisions align with the State IT Strategy and promote reusable components.

The EA program's FY20-21 priorities included:

- OFM - One Washington program to replace the state's decades old financial and administrative applications with a modern enterprise resource planning (ERP) solution.
- The Health and Human Services coalition priority projects developed as part of a strategic, modular architecture to provide reusable enterprise services such as:
    - Master Person Index project.
    - Integrated Eligibility project.
- Data architecture standards.
- Work to advanced data analytics.

- Government cloud computing and cloud office.
- Identity management; citizen digital ID.

One Washington:

One Washington, led by the Office of Financial Management, is an enterprise-wide transformation program focused on replacing 1960s-era technology with a cloud-based solution for finance, procurement, budget, HR, and payroll processes. Phase 1a of the program includes replacement of the Agency Financial Reporting System (AFRS) with a new, cloud-based enterprise resource planning (ERP) system. The program positions the state to move forward with the new Workday financial system in FY22-23. (Workday is an on-demand, cloud-based vendor that specializes in enterprise resource planning, financial management and human capital management applications).

Admin/Financial Investment Assessments promote re-use of One WA capabilities:

In FY 2020-21, the One Washington program and OCIO evaluated over 500 agency reported investments for strategic alignment with Workday (Figure-37). They were assessed to ensure they did not duplicate technology that will be implemented in the Workday solution.

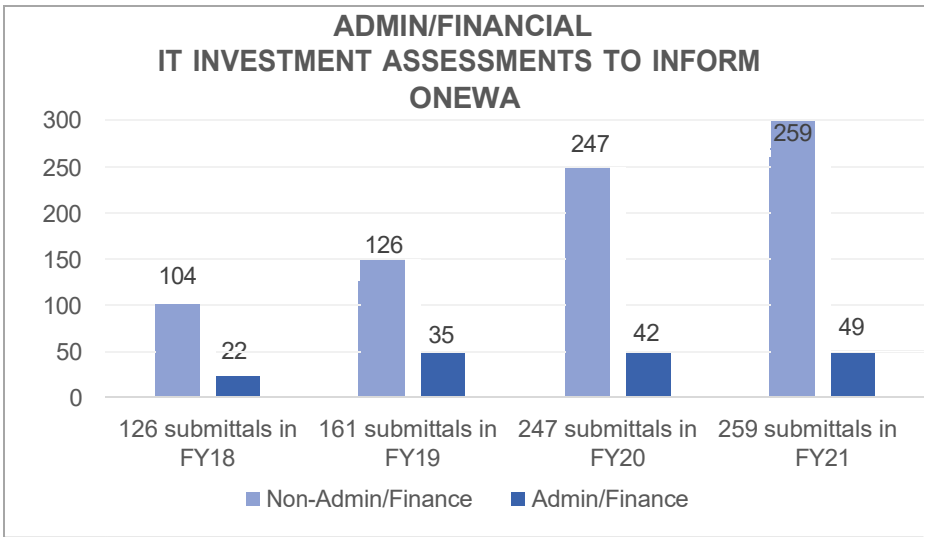


Figure 37 - Statewide project assessments to determine administrative or financial.

Cloud Readiness:

The OCIO initiated a statewide cloud readiness assessment in July 2019 as required by Engrossed Substitute House Bill 1109. The assessment included a survey of 79 agencies and a vendor-produced substantive deliverable in October 2020. Based on the assessment activities, OCIO published a summary and key insights for the Washington State Cloud Readiness report distributed January 2021. Key findings and recommendations of the report:

- Most agency applications appear to be good candidates for migration to cloud services.
- State cloud migration could result in significant financial return of investment, also recognizing challenges in the decentralized nature of IT operations across state agencies.
- IT staff need to be trained to fill cloud position requirements.
- WaTech should follow industry best practices to provide centralized cloud support service. Specific industry reference models include Cloud Services Broker (CSB) and Cloud Center of

Excellence (CCOE).

- Recommended nine major projects covering cloud operational readiness, enterprise architecture, governance and workforce preparation. Eight of the projects prepare the technical environments and organizations for cloud migration.

Based on the recommendations in the State Cloud Readiness Report, the Enterprise Cloud Computing (ECC) program was kicked off in March of 2021 to plan and execute cloud adoption across the state. With a steering committee that includes the state CIO and four agency CIOs, the program started with a discovery process that documented the needs of agencies, included insights from other states and cloud market leaders.

This resulted in a set of guiding principles for the program as well as strategic documents that will be iterated on an ongoing basis. The program prepared a Request for Proposal (RFP) to onboard a vendor to come alongside the program, adding critical expertise and the capacity to jump start the ECC program to support agencies on their cloud journey. The decision on the Apparently Selected Vendor is scheduled for mid-October. The program also started to hire ECC staff. The manager was onboarded July 2021 and other staff members are planned for late 2021 or early 2022.

In April 2021, Engrossed Second Substitute House Bill No. 1274 was signed by the Governor. The bill states that the Legislature intends to migrate the state's information technology toward cloud services. The law states that agencies shall locate all existing and new information or telecommunication investments in the State Data Center or within third-party, commercial cloud computing services. It also requires a task force on cloud transition to evaluate the impacts to labor, reporting findings and recommendations by November 2021. The Cloud Task Force has been established based on the legislative requirement. More information can be found on the Cloud Task Force website.

Work to minimize duplication and encourage reuse:

- Health and Human Services (HHS) Coalition:

  The Washington Health and Human Services Enterprise Coalition (HHS Coalition) provides strategic direction, cross-organizational information technology project support and federal funding guidance across Washington's HHS organizations. IT project collaboration results in better service coordination and public stewardship that improves the health and well-being of the people, families, and communities of Washington. The HHS Coalition submitted a report to the legislature in November 2021 as required by Engrossed Substitute Senate Bill 5092 (2021) providing an overview of its IT investment coordination.

  - Master Person Index: The HHS Coalition is developing a Master Person Index (MPI) that will support identity management across HHS programs and systems via an authoritative client identifier. The MPI will identify individuals across programs and systems, which is essential for effective program planning, development, delivery, and integrity. The MPI will improve services for Washingtonians by reducing the need to submit certain documents multiple times to different programs, reducing the time individuals and families spend applying for or maintaining services. People will be better served because

the information needed to deliver services is more readily available to the organizations that provide them. As the HHS Coalition embarks on modernizing its technology solutions, the MPI will be a critical tool to facilitate identity management and is integral to supporting modular system development.

- Integrated Eligibility & Enrollment: The HHS Coalition is developing an approach for a health and human services integrated eligibility and enrollment (IE&E) solution. A driving goal for these solutions is to facilitate eligibility determinations and benefits enrollment for multiple programs in a streamlined fashion due to the overlap in program eligibility for

  many low-income individuals and families. Washingtonians face barriers in accessing health and human services programs including having to provide the same information across multiple organizations to support their eligibility and enrollment, and limited hours to apply for benefits even with an online application. Caseworkers must access many systems to verify information about applicants. The HHS Coalition is delivering a report to the legislature in January 2022 describing the roadmap to an IE&E solution for over 75 Washington health and human services programs.

- Geographic Information System (GIS) technology:

  The state has a long-standing GIS coalition that supports multiple agencies. An example of the coalition's work include efforts last biennium when the Department of Natural Resources (DNR) reported 1,002 wildfires burning over 713,000 acres statewide.

  The fire season represented a worst-case scenario with weather, fuel and topography. DNR developed a publicly available, mobile-friendly map-driven web application providing users with a single source of current wildfire information compiled from all six DNR and interagency dispatch offices. Tapping into data feeds from the other interagency partners this solution provided situational awareness and focused on real-time intelligence from all available sources through the wildfire dashboard: http://Fireinfo.dnr.wa.gov/home.

  Features included:

  - A streamlined, interactive web map that displays a number of important GIS layers for wildfire managers.
  - A Situation Snapshot panel providing users an in-depth look at the current wildfire situation.
  - A Resource Status panel capturing the status of assigned/available ground and aviation resources throughout the state.
  - Year-to-Date Fire Statistics depicting statistical summaries aimed at providing a single, around-the-clock source for the total number of responses, fires, and acres burned in total and by month.
  - DNR Fire Twitter compilations using a live Twitter feed from WA State DNR Wildfire, allowing users to keep their "finger on the pulse" of wildfire in the state.

In addition, aviation experts (helicopters and fix winged aircraft) relied heavily on GIS for aerial support in 2020. This includes coordinating limited resources, used for daily briefings, determining how to shift things around each day and using hotspot analysis from 10 years of Fourth of July holidays to help state fire fighters prioritize where to put resources to be more effective. The information is publicly available and used by local fire managers and reporters. This supported consistent communications reporting with real time updates on lightning strikes.

- Identity Management:

  Market discovery activities started in the biennium to support advancing the state's identity and access management strategy included Gartner research, user story research and review and Request for Information (RFI). These activities will be used in the next biennium to inform recommended updates to the state identity management policy, technical solutions to meet identity internal (state employees) and external (public) management needs and a development of a comprehensive governance plan.

- Data Center waivers and SDC utilization:

  At the start of the biennium, 29 agencies had approved waivers to migrate equipment out of their facility to the State Data Center (SDC) or private cloud service and by July 2021 there are 11 agencies still working on their migration (Figure-38). Of the 11 agencies, four plan on moving to the SDC, four are moving to the cloud and three will have a hybrid of both the SDC and cloud.

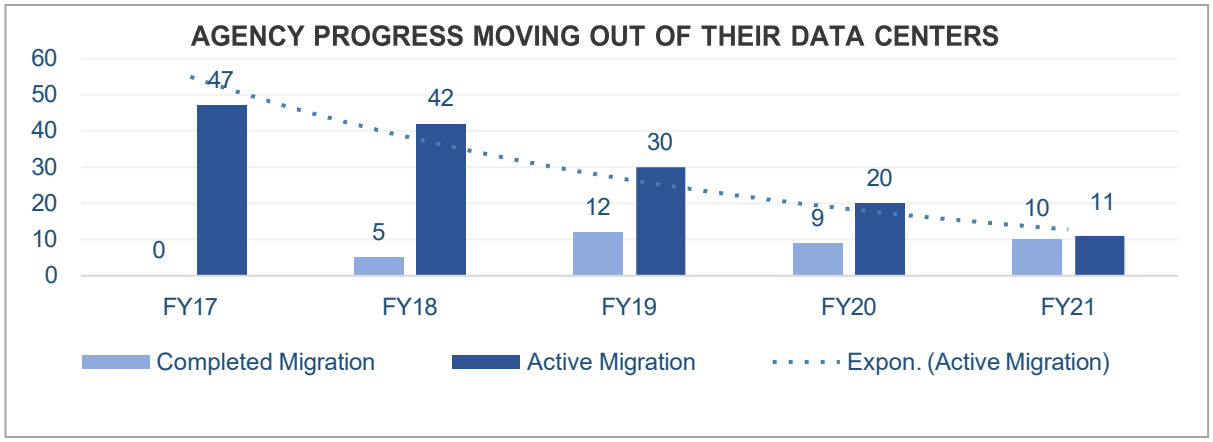


Figure 38 - Data center migration project trend.

At close of the biennium, there were 56 agencies having equipment located in the SDC. Of those, 40 are using colocation services, 16 are using the state private cloud and 15 have a presence in both services.

During the biennium the state Private Cloud service name was changed to Washington State Cloud (WS Cloud) to better reflect the service offering. The offering is for all agencies, boards, and commissions on the State Governmental Network (SGN).

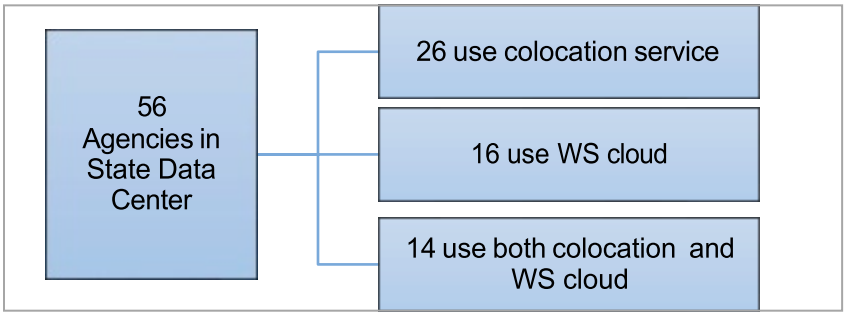


Figure 39 - State Data Center customer usage as of June 30, 2021.

Section 6: Security

How Washington state safeguards data:

With more than 100 state agencies serving a population of nearly eight million people, the state of Washington has one of the largest and fastest growing service delivery systems in the nation. The enormous amount of information generated by the enterprise is stored not only on the state government network (SGN) and within the confines of the state data center but also, increasingly, in the public cloud and third-party vendors' data centers.

The COVID-19 pandemic has accelerated this shift, broadening the state's digital footprint with a move to remote work by state employees and the scramble by agencies to provide services online instead of in brick-and-mortar buildings. This, in turn, has provided bad actors with more ways to attack the state. (More doorknobs to rattle).

Washington faces persistent and increasingly sophisticated cyberattacks – including targeted phishing email campaigns – that impact state agencies, their private vendor partners and ultimately Washingtonians.

Financial gain drives most threat actors. The Federal Bureau of Investigations' 2020 Internet Crime Report, reported a record number of complaints nationally in 2020, with 791,790 reported losses exceeding $4.1 billion. That represented a 69% increase in total complaints from 2019.

According to the Washington State Attorney General's Office 2021 Data Breach Report, the number of data breaches reported to the Attorney General's office by public and private organizations across the state skyrocketed to 280 in 2021 compared to the previous year's total of 60. The report found that more than 150 ransomware incidents were recorded in 2021.

Malicious actors focus on two main avenues for initiating an attack:

- One method is to trick users, through phishing emails, to click on a link that downloads malicious software that gives attackers a beach head in an organization's network.
- The second approach is for attackers to look for vulnerabilities in end user devices and enter an IT system by exploiting those weaknesses.

Once bad actors gain access to an organization's IT system they begin to methodically take steps that lead them to their goal – making money. For example, Personally Identifiable Information (PII) stolen by threat actors can be sold on the dark web, and then utilized to launch new cyberattacks. In Washington state, criminals used this type of recycled PII to fraudulently file unemployment benefits in 2020. Stolen credentials also can be used to enter and traverse an organization's network, encrypt all its data and then hold it for ransom.

With these types of attacks increasing, Washington is working to prevent and stop bad actors as early as possible. The State Office of Cybersecurity has focused on four foundational areas at an enterprise (statewide) level:

- Endpoint protection: When users click on a malicious link or attachment in a phishing email, a series of steps occur on the user's machine that could lead to a compromise if left unchecked. Microsoft's Defender for Endpoint system detects, blocks and alerts when those steps occur on all state endpoints – laptops, tablets, mobile phones and other wireless devices. The types of threats being blocked include attempts by bad actors to take control of the user's machine to perform malicious actions.
- Vulnerability Assessment System (VAS): The VAS scans for the same weaknesses in state systems that bad actors look for and helps agencies to prioritize and remedy those weaknesses before they can be exploited. There are more than a million programs running on state devices. Threat actors can exploit vulnerabilities to download malicious payloads – including ransomware – to conduct attacks. The VAS provides the state with an enterprise view of vulnerabilities, the risks associated with them and a path to prioritize remediation activity across hundreds of thousands of devices.
- Security Information and Event Management (SIEM): In 2021, the state deployed a new cloud based SIEM platform that improved the ability of security staff to detect and respond to signs of attacks on state assets. The SIEM provides the state with an enterprise view of all executive branch agencies and can detect threats across the state's nearly 10,000 infrastructure assets (servers, network devices, etc.), providing detailed intelligence needed to detect and mitigate threats.
- Web application defense: A common tactic by threat actors is to steal or obtain large quantities of credentials (usernames and passwords) from organizations and then use those credentials in attacks against others. This is because many people use the same usernames and passwords for many of their online services. Criminals use the credentials in automated attacks to try to gain access to accounts. In response to threats in 2020 and 2021, the state implemented a web application defense system that protects the state's nearly 300 online public facing eServices including the unemployment benefits system, tax, and business licensing services against automated attacks.

All the services described above are operated at WaTech's state Office of Cybersecurity (OCS) at an enterprise level. They are standard tools representing industry best practices and are

fundamental to any enterprise information security program. Their value has been repeatedly demonstrated in recent and ongoing cyberattacks.

In addition to the creation of enterprise services, the state – through Senate Bill 5432 (2021) – also made OCS the state's lead organization in combatting cyber threats and created a clear mandate for the development of centralized services and functions across state government.

The bill creates several new ongoing requirements for OCS in the next biennium including a confidential annual report submitted to the governor and appropriate legislative committees; confidential quarterly reviews of any unmitigated risks identified by OCS (also with the governor and certain committees); and a catalog of services provided by OCS at an enterprise level.

- National Governors Association (NGA):

  Washington is one of five states selected by the National Governors Association (NGA) in 2021 to work on policies to advance whole-of-state cybersecurity postures.

  Representatives of the five states convene in-state workshops to create action plans for strengthening state cybersecurity; participate in regularly scheduled convenings with NGA staff on their progress and plans; and build relationships with and learn from peers in other states facing similar challenges.

  The intent is for the selected states to serve as pilots through which best practices relevant for all state and territorial governments are developed. The NGA uses outcomes, promising practices, and lessons learned from Policy Academies as the basis for the promulgation of best practices to all 55 state, commonwealth, and territorial governors across the country, featuring the work of these states in its national technical assistance efforts.

- SecureAccess Washington (SAW):

  Multiple agencies use SecureAccess Washington (SAW) to help shield state services from harmful activity by providing secure external access, while allowing self-administered access to registered users. SAW, on average, has over three million logins per month. Usage of SAW more than doubled during the pandemic as Washingtonians accessed vital state services such as unemployment benefits.

  Additionally, there were improvements to the state's security profile by implementing Multifactor Authentication (MFA) on all SAW accounts and increasing the number of state applications that can only be accessed by using SAW.

Privacy:

The Office of Privacy and Data Protection (OPDP) efforts have focused on expanding the volume of available resources on privacy and increasing engagement with public agencies. Examples of key initiatives include:

- Expanding and rebranding the existing Privacy Working Group into a new State Agency Privacy Forum (SAPF). The SAPF, which meets quarterly, is open to any agency that wants to participate and includes privacy, data sharing and cybersecurity experts.
- Hosting privacy webinars each month there is not a quarterly SAPF meeting. Topics have included data breach notification, facial recognition, contact tracing, de-identification, data classification, and the intersection of privacy and the Public Records Act, and the Keep Washington Working Act. These webinars are recorded and available on the OPDP's webpage.
- Creating and distributing draft Washington State Agency Privacy Principles to state agencies during the summer, with the final version published in November 2020. The principles will help establish a common understanding to use when discussing, promoting, and implementing privacy practices as a priority among state agencies.
- Launching a new OPDP website and Privacy Points, a monthly blog/newsletter, to help improve the distribution of privacy information and give additional access to OPDP trainings and presentations.

Figure 8 – Calendar of ongoing Privacy education activities.

- Conducting the annual privacy review of state agencies. The number of agencies responding, the importance of privacy, and the maturity of privacy programs across state agencies has steadily increased over time. Specific details about the privacy assessment survey findings are included later in this report and the full report is posted on our website at https://watech.wa.gov/privacy/newsinformation.
- Developing a breach assessment form template that helps agencies determine if an incident requires notification under Washington's breach notification law. This tool is also useful to local governments.
- Representing OPDP on several committees working on important initiatives in the state including the Bluetooth Exposure Notification Advisory Committee, Systems Technology and Data Security Subcommittee for the Washington State Autonomous Vehicle Workgroup, Washington All-Payer Claims Database Data Release Advisory Committee (DRAC), and the Open Data Advisory Group.

Figure 41 – Agency Privacy principles.

- In partnership with the Office of Cybersecurity, creating resources for safely using Wi-Fi and video conferencing during the pandemic. In addition, to increase accessibility, OPDP's Tips for safely using public Wi-Fi publication was translated into 35 languages spoken by communities across Washington.
- Automated Decision-Making Workgroup:

  OPDP is currently leading and facilitating the Automated Decision-making systems Workgroup. The purpose of the ADS workgroup is to develop recommendations for changes in state law and policy regarding the development, procurement, and use of automated decision systems by public agencies. The workgroup will examine how automated decision-making systems can best be reviewed before adoption and while in operation and be periodically audited to ensure such systems are fair, transparent, and accountable and do not improperly advantage or disadvantage Washington residents.

Section 7: IT Strategy Next Biennium

In 2021 the OCIO and agencies collaborated on the Statewide IT Strategic Plan for 2021-2025 (Figure-42). This plan will serve as an anchor for the 2022-2023 biennium.

Figure 42 - 2021-2025 Statewide Information Technology Strategic Plan.

The state IT strategy needs to support, improve and modernize the way government services are delivered to Washingtonians. Maturing the state's strategy helps support the commitment to use innovative and transformative solutions that enable the state to provide essential government services in an efficient manner. IT strategic priorities to optimize and transform government services during the next biennium include:

Common constituent portal: An IT priority for the next biennium is to work toward a common portal for services– just as constituents have come to expect in their experience with the private sector. Improving the digital experience includes working with the State Broadband office to address disparities in broadband access. This has been a significant issue, particularly in rural communities, and has impacted the ability of state residents to receive services.

IT Governance Assessment: Work over the next biennium includes transforming existing IT Governance activities with the intent to adjust and strength practices going forward.

Enterprise Cloud Computing: Targeted for the next biennium is an Azure Express Route that connects the WS Cloud – Infrastructure as a Service (IaaS) – to Microsoft's Azure IaaS. Future activities include a proof of concept that should allow existing WS Cloud customers to provision new compute workloads in Azure or on-premises using the existing WS Cloud portal. With this connection to Azure, the WS Cloud staff should also be able to migrate customers' existing compute workloads from the WS Cloud on-premises IaaS to Azure IaaS and back on-premises if needed.

Major Project Oversight: Improve major IT projects outcomes by updating policies and refining oversight processes for project management, transparency and technical architecture.

Enterprise Architecture: In the coming biennium, the EA program will be focusing on advancing the state's identity and access management strategy, as well as the state's maturity in the data, business, and governance architectural domains.

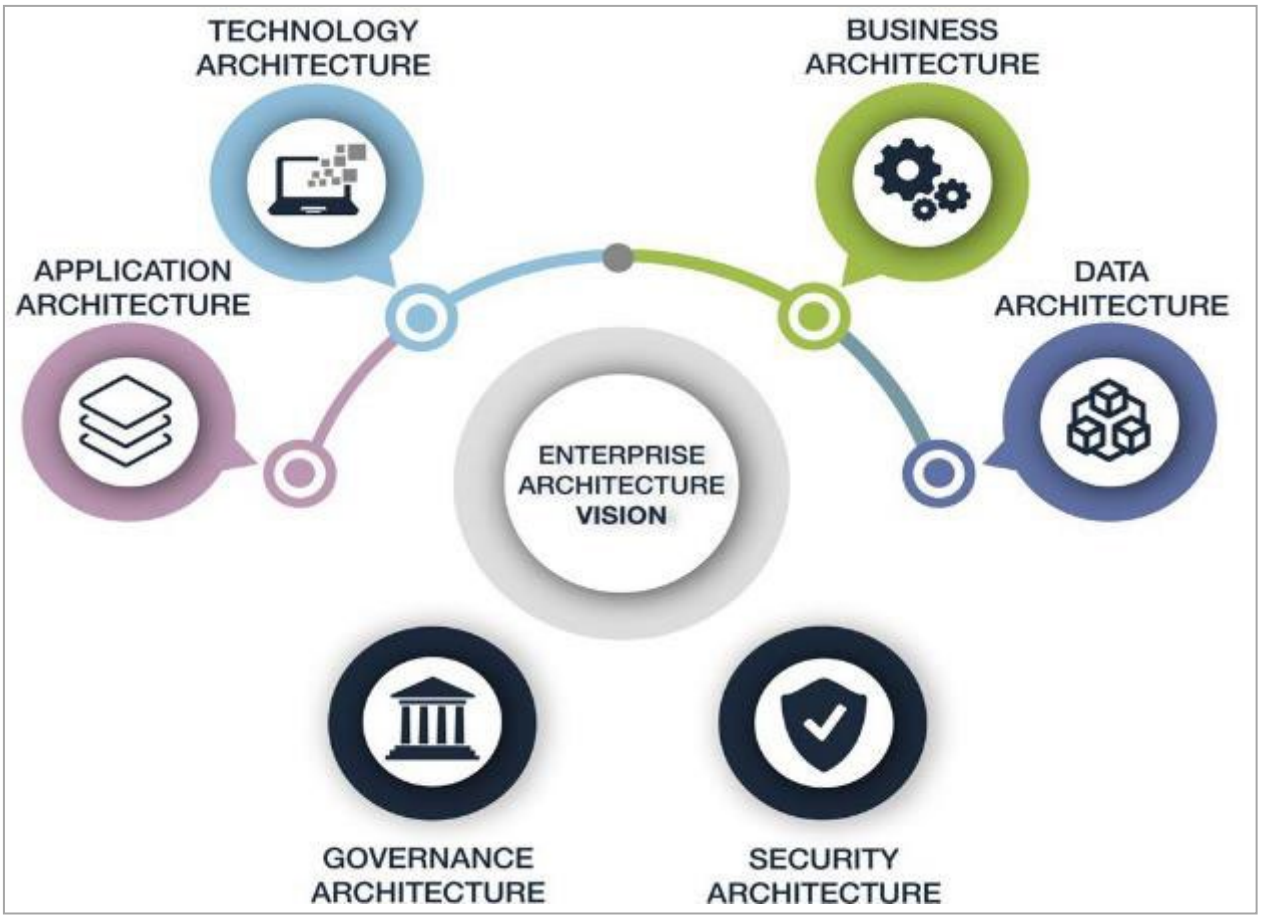


Figure 43 - - Enterprise Architecture focus on several key domains to advance the State IT Strategy.

Standardization Efforts: Expanding a common platform for sharing GIS data to support hazard mitigation, emergency response, Puget Sound recovery, renewable energy initiative and state equity. The strategy includes working towards a single accurate dataset using standardized data for:

- Counties.
- Legislative districts.
- Census tracts.
- Zip codes.
- School districts.
- Homeland security regions.
- Tax location code boundaries.

Additional efforts to support workforce return to workspace and projects with low effort and high impact will be prioritized. Work on a "national to local level" is required to benefit state efficiency such as the National Hydrography Dataset where data is used for:

- Mapping.
- Scientific Analysis.
- Monitoring.
- Decision-making.
- Permitting.

Security and Privacy: As outlined in Senate Bill 5432 (2021) OCS will continue development of centralized services and functions across state government to combat cyber threats. An ongoing requirement for OCS includes a confidential annual report submitted to the governor and appropriate legislative committees by December 2021. Other requirements in the new law include:

- Data Governance Report: OCS, along with WaTech's state Office of Privacy and Data Protection and the state Office of the Attorney General, must research and examine best practices for data governance, and data sharing and protection, including model terms for data-sharing contracts and adherence to privacy policies. (This report is due to the Legislature December 2021.)
- Independent Security Assessment: OCS is required to hire a vendor to do an assessment of cybersecurity audits of state agencies completed since July 1, 2015. The assessment must evaluate the efficacy of the audits performed and the state's ability to act based on the results. (This report is due in August 2022.)
- Quarterly Reviews: Confidential quarterly reviews of any unmitigated risks identified by OCS with the governor's office and appropriate legislative committees.
- Annual Report on Audits: This confidential report includes audit findings and risks identified in the quarterly reviews, along with mitigation steps being taken.
- Model Incident Response Plan Policy: OCS is required to develop a model incident response plan related to the management of security incidents and to define a "major cybersecurity incident" within policy. The legislation requires state agencies to inform OCS of any business needs to improve security on an annual basis.

Contact

Questions regarding the FY20-FY21 IT Biennial Report can be directed to:

Cammy Webster
Cammy.webster@ocio.wa.gov
(360) 407-8912