FY18-FY19
IT Biennial Report

Technology performance report

WaTech
Washington Technology Solutions

Washington's Consolidated Technology Services Agency

Office of the Chief Information Officer

LETTER FROM THE STATE CIO

This report presents an overview of the state's information technology (IT) landscape during the 2017-19 biennium, as well as a glimpse of what's ahead.

A year since my appointment, my focus continues to be on strategic, cost-effective technology investments that will modernize and transform state services for Washingtonians.

While there is still much to be done, I can point to great progress.

The state has made tremendous strides in providing government services 24/7 through online access, saving both time and money. Government spending on IT also is more transparent than ever through online dashboards. In the area of information security, the state has worked to stay abreast of evolving cyber threats and expanded its efforts to educate employees about best practices.

Washington state has won national recognition for its efforts, including recent top honors from the National Association of State Chief Information Officers (NASCIO) for two Washington State Patrol (WSP) projects.
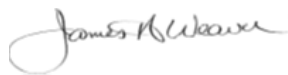
The WSP was recognized for its use of drones to expedite forensic mapping of collision and crime scenes – resulting in a 75% reduction in road closure time. The WSP also completed an initiative that allows sexual assault victims to track their sexual assault kit through the criminal justice process.

In addition, the Office of the Chief Information Officer was recognized by NASCIO for its Technology Business Management (TBM) program, resulting in improved data collection and reporting of statewide technology investments. My office now captures data on all technology investments in the state. This information is available to the public online on the OCIO website.

The state also is paving the way for vastly improved IT services and connectivity by moving to the cloud. For example, WaTech is working with state agencies to migrate to the cloud-based Washington Enterprise Shared Tenant. With the ability to serve multiple tenants from Microsoft 365 using a common, cloud-based service, agencies can benefit from shared resources such as existing data centers, computers, operating systems, software applications and maintenance. That is just one of many efforts underway.

We live in a time of tremendous technological change, which presents an enormous opportunity for the state to improve its services. The state has put a priority on modernization that does more than keep government running, but actually changes the way the state works, and the ways public servants can innovate.

I look forward to working with lawmakers and our partner agencies to make this vision a reality and transform state technology.

James Weaver, State Chief Information Officer

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of the Chief Information Officer (OCIO) is required by RCW 43.105.220 to submit a state performance report on information technology (IT) each biennium.

This IT Biennial Report assesses state progress toward goals outlined by the state technology strategic plan during the 2017-19 biennium. The report is organized to show the alignment between the state strategic plan and corresponding RCWs.

The state invested more than $3.4 billion in technology during the biennium. Those investments helped the state make progress on many fronts including increasing public access to government data while at the same time enhancing privacy protections for Washingtonians. The state also made headway in finding shared IT solutions for multiple agencies, which will ultimately allow for efficiencies and improved services. In addition, the state has advanced its understanding of the statewide technology portfolio through reporting and updated practices, which provides improved oversight of major IT projects and reduces risk.

This report also provides insights on the state's strategic investments to help secure state assets and information, an increasingly important issue in light of recent ransomware attacks that have affected state and local governments across the country.

Information also is included on application risk associated with the buildup of technical debt related to 420 legacy applications in the state portfolio identified as mission critical/business essential and custom in-house built.

Other areas highlighted in the report include:

- **Efficient and effective government:** Washington received national recognition for the innovative use of technology to increase efficiency and help state residents. This includes two national awards received by the Washington State Patrol – one for an initiative that allows sexual assault victims to track their sexual assault kit through the criminal justice process and another that uses drones to expedite the forensic mapping of collision and crime scenes.

- **Accountable IT management:** The OCIO now captures data on all technology investments in the state. The data became accessible to the public online in January 2019. It includes budget decision packages and the ranking of agency funding requests.

- **Project Oversight:** Over the biennium, 100 major IT projects received oversight from the OCIO. This includes 40 projects assigned to the IT Investment pool. By June 2019, 86% of projects were active. Of the remainder, 12% were closed, 1% canceled and 1% placed on hold.

- **IT workforce:** The OCIO and Office of Financial Management (OFM) State Human Resources office collaborated on a multi-year job class study for IT classifications aimed at building a more modern, competitive job class structure.

The study concluded June 30, 2019, and a new IT professional structure became effective in July 2019.

- **Enterprise architecture (EA):** The OCIO expanded the state Enterprise Architecture program to lead a collaborative, business outcome driven approach that focuses on value and enabling statewide digital transformation. Progress made during the biennium includes an estimated $500,000 in cost avoidance to agencies by advancing the Washington Master Addressing Services (WAMAS), so street, building, parcel, etc. addresses used by agencies now meet the United States Postal Service (USPS) standard. The state also adopted a shared state model for Office 365 and related cloud-based technologies, advancing Health and Human Services enterprise coalition and ensuring secured external access to agency applications by using Secure Access Washington (SAW). Enhancements to SAW improved user experience and reduced calls to the help support desk by 70%.

- **Security and privacy:** The state of Washington made strategic investments and leveraged federal dollars during the past biennium to help secure public data entrusted to government agencies. This includes a federal grant to help protect and safeguard the 2020 elections. The state Privacy Office expanded education activities to bring awareness to privacy issues.

The state also faces ongoing IT challenges that will require continued attention in the coming biennium, including:

- **Technical debt:** Tight agency budgets, business-driven deadlines and funding cycles have helped fuel a growth in technical debt in state government due to the practice of building on top of existing application architecture to enable new capabilities. This has resulted in systems that are harder to sustain and may need additional investment or replacement. Technical debt is the backlog that occurs when quick and easy solutions are chosen to meet the immediate burning need versus selecting a better design that will take more time to implement.

- **Tracking of IT spending:** The IT project assessment (ITPA) process was changed in an effort to gain earlier insight into the number of IT projects occurring statewide. However, gaps remain in the number of projects submitted. Fewer projects were reported to the OCIO than anticipated with only 161 agency ITPAs submitted in 2019. Of those, 32 were submitted as part of the 2019-21 funding request cycle.

- **IT workforce:** According to the state Human Resources Office, the state's technology workforce is aging and retiring in greater numbers. Data captured in the 2019-21 biennium will inform the outcomes of the IT position restructure and determine if the changes in compensation improves recruitment and retention efforts. Recruitment and retention efforts are important given that more than half of the state's technology workforce is eligible to retire within the next five years.

TECHNOLOGY PERFORMANCE REPORT STRUCTURE

The Washington state IT Strategic Plan (page 8) 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.

Section topics also cover requirements within state RCWs. To make a tie between the RCW and IT Strategic Plan a reference is included in the section header to the following corresponding RCWs:

- RCW 43.105.215

- 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

Due to the heightened interest in 'Accessibility' and 'Project Oversight,' these topics have been elevated to section headers within the report.

SECTION 1: STRATEGIC INFORMATION TECHNOLOGY PLAN (RCW 43.105.220 (1))

The OCIO is legislatively mandated to prepare and lead the implementation of a strategic direction for information technology in state government. The Office is responsible for:

- Providing enterprise architecture for state government.

- Supporting standardization and consolidation of technology infrastructure.

- Establishing standards and policies for efficient and consistent operations.

- Creating and nurturing a cohesive operating technology community.

- Providing technology expertise to improve the business of government.

- Fostering innovation and experimentation to bring modern capabilities to government.

- Educating and informing policy leaders about emerging technology.

- Creating technology investment clarity and alignment, while identifying opportunities for savings and efficiencies in technology expenditures.

The Technology Services Board (TSB), as described in RCW 43.105.287, reviews, approves, and provides oversight of major information technology projects. The board focuses on IT strategic vision and planning, enterprise architecture, policy and standards, and major project oversight. Members include legislators, business leaders, agency directors, a representative from local government and a labor representative.

Published by the OCIO in July 2017, the state Enterprise Technology Strategic Plan (see Figure 1) provided guidance through the 2018-19 biennia.
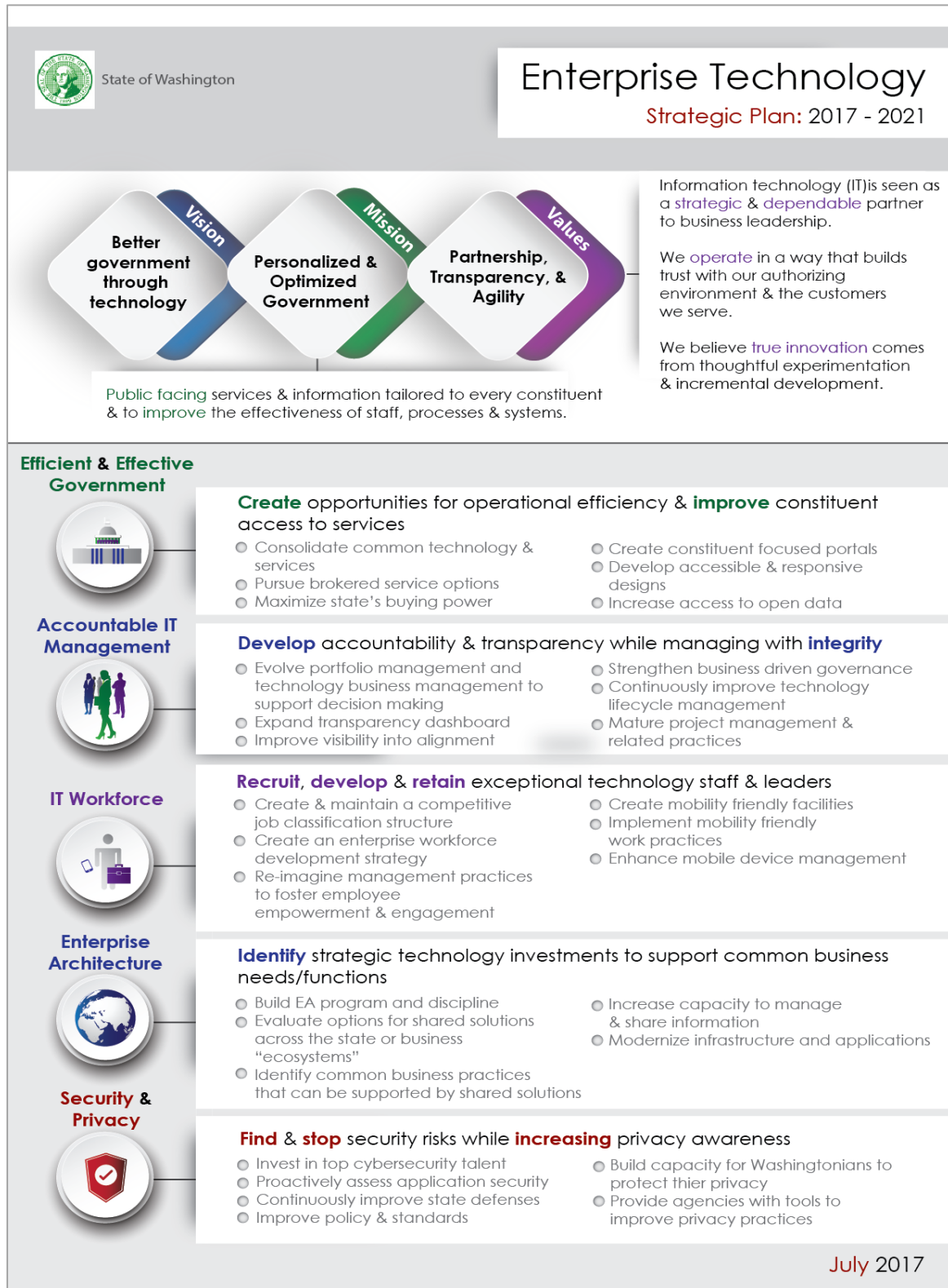
Figure 1: Strategic Plan 2017-2021.

SECTION 2: EFFICIENT & EFFECTIVE GOVERNMENT
(RCW 43.105.220 (2A), RCW 43.105.225, RCW 43.105.230, RCW 43.105.235 & RCW 43.105.341)

Information technology portfolio

IT portfolios detail existing and planned technology investments. The portfolio should show how investments support an organization's priorities.

In the 2017-19 biennium, the state worked to close gaps in technology portfolio practices. The application portfolio was modified to include information to support 'One Washington' enterprise resource planning efforts and minimize the number of times agencies request application information.

Chief information officers (CIOs) from 15 different agencies collaborated to create an IT portfolio conceptual model for use at both the agency and enterprise level. This was the first review in over 20 years. One of the key goals was to fully integrate technology business management financial disciplines as a component of the state's portfolio program. The model serves as a framework in support of several statutory requirements:

- RCW 43.105.341 - IT portfolios
- RCW 43.105.235 - State agency IT portfolio
- RCW 43.105.230 - State agency IT portfolio - Basis for decisions and plans
- RCW 43.105.225 - Managing IT as a statewide portfolio.

Portfolio Management Conceptual Model

- Establish goals, mission & objectives
- Develop business & technology plans
- Define Enterprise Architecture
- Identify key portfolio value indicators

- Compile business capabilities
- Understand resource availability
- Balance & align based on priorities
- Collect & communicate adjustments
- Track current & proposed projects & operations

Strategy

Inventory & Review

Governance

- Record progress towards meeting key portfolio value indicators
- Collect, analyze & report outcomes
- Measure business & technology plan advancement

Performance & Results

Monitor & Control

- Review performance indicators
- Manage portfolio risks
- Evaluate technology Investments
- Assess business & technology plan modifications
- Confirm alignment

Version 1 December 2018
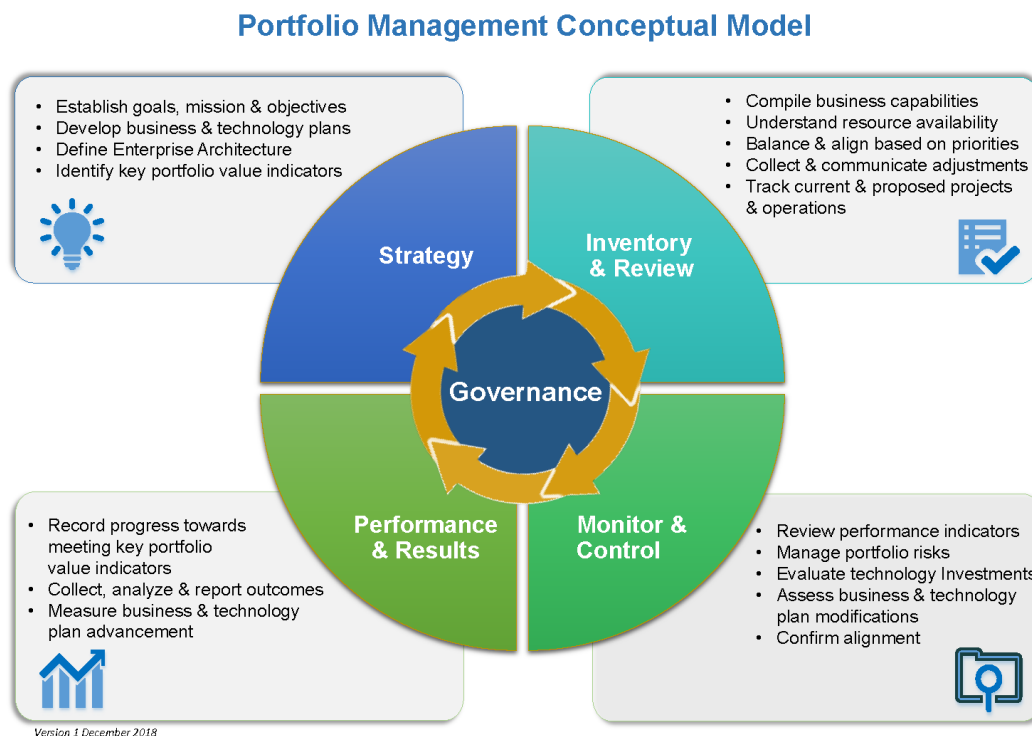
Figure 2: Technology Portfolio Conceptual Model.

Following development of the conceptual model, representatives from small, medium and large agencies collaborated to identify a shared minimum set of foundational elements that all agencies must collect to support their technology portfolios. These foundational elements – with requirements to have a technology plan along with standards on collecting applications, infrastructure and projects data – are documented in technology policy, standards and architecture.

Collection and review of the foundational IT elements – such as determining the number of applications, servers and projects – allows organizations to measure and understand the overall health of its existing technology assets and make informed decisions about the relative priority of each investment.

The information being collected improves the state's ability to set strategic priorities and make informed decisions about technology direction and architecture.

Washington state national recognition

Washington state is earning national recognition for its innovative use of technology to increase efficiency and help state residents:

Government Technology Digital States Survey: Washington continued to receive top marks in 2018 from the Center for Digital Government, earning an A- in the 2018 Digital States Survey. The survey, conducted every two years, evaluates states' use of

WASHINGTON DIGITAL STATE GRADE	
2018	A-
2016	A-
2014	B+

technology. Under the Digital States criteria, a grade of A reflects a state that is trending sharply up. The report, among other things, recognized Washington for its One Washington project, "a wide-reaching effort to modernize and improve Washington's aging administrative and business processes." The report also highlighted the state's new Driver and Vehicle System (DRIVES) – part of a $60 million multi-year business and technology modernization project.

Technology Business Management Program, National Association of State Chief Information Officers (NASCIO) recognition: The Washington state Office of the Chief Information Officer received a special recognition award in 2018 as a finalist in the annual NASCIO Awards for its Technology Business Management (TBM) program. The TBM program, first launched in 2011, experienced a major "reboot" in 2016 that more closely aligned technology investments in 44 state agencies through a consolidated system. This resulted in an improved reporting system that streamlines the state's overall ability to track investments in technology.

Washington State Patrol (WSP) Security Assault Kits Tracking System, (NASCIO) recognition: The WSP was a recipient of a 2019 NASCIO award for an initiative that allows sexual assault victims to track their sexual assault kit (SAK) through the criminal justice process. Sexual assault victims may undergo a forensic exam to collect evidence including biological material. The doctor or nurse conducting the exam preserves the evidence in an SAK. The new WSP system tracks the location of the kit and provides visibility and metrics regarding the overall status. The system is publicly accessible and hosted in the Microsoft Azure Government Cloud.

Figure 3: The WSP was a NASCIO award recipient for its use of drones to expedite the forensic mapping of collision and crime scenes in Washington state.

Washington State Patrol Use of Drones for Collision and Crime Scene Reconstruction (NASCIO) recognition: The WSP also was a recipient of a NASCIO award for its use of drones to expedite the forensic mapping of collision and crime scenes in Washington state. Traditional methods that used hand measurements, total stations, and 3D laser scanners resulted in lengthy road closures on heavily traveled highways. Using drones for the work has dramatically reduced the amount of time needed to map scenes. From January through September 2018, the use of drones in 126 investigations resulted in a 75% reduction in road closure time (a

STUDY: IMPACT OF USING DRONES IN 2018

- 126 accident investigations.
- Amount of time roads closed reduced by 200.5 hours (a 75% reduction).
- Saved more than $4 million ($350 per minute).

total of 200.5 hours). The Washington state Department of Transportation estimates that each minute of state route and interstate road closure time has a negative economic impact of $350.

Assessment and ranking of technology project funding request

The OCIO is required by law (RCW 43.105.235) to evaluate state agency IT budget requests and submit recommendations to 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 2018, the OCIO completed a major overhaul to the criteria used in order to provide a prioritized list assessing the proposed investment against 12 criteria in three key areas:

- Agency readiness/solution appropriateness.

- Architecture/technology strategy alignment.

- Business outcomes and customer focus.

In addition to the prioritization, the OCIO made funding recommendations for each item:

- **Fully fund as written:** The agency demonstrated adequate project planning and readiness in the DP documentation.

- **Fund with considerations:** The DP indicates many factors for success but may be lacking in key areas. DPs receiving this type of recommendation fit into roughly two categories: packages that lack sufficient funding in key areas (such as resourcing), and packages that require additional detail to evaluate or would benefit from more project planning or feasibility work ahead of full funding.

- **Partially fund:** Packages with this recommendation have stand-alone portions that appear to be well planned if funding is secured, or if a more incremental approach has been recommended for funding.

- **Do not fund as written:** Packages with this recommendation lack evidence of key success factors and strategic alignment indicators and, in the opinion of the OCIO, should not be funded as written.

Because of the changes, budget development staff and decision makers report improved recommendations that contain critical information to support more informed decisions.

In fall 2018, the OCIO analyzed 173 agency information technology DPs that were submitted to the OFM. Of those, 109 went through the review, scoring and prioritization process. The remaining 64 DPs were not prioritized because they were funding requests to maintain existing IT services (maintenance and operations).

For a copy of the comprehensive report submitted to the Legislature and available to the public, see Finalized IT Decision Package Funding Recommendations.

Financial assessment

Industry terms from the Technology Business Management (TBM) Council taxonomy are used for reporting on statewide technology investments. These standard reporting terms known as 'Cost Pools' and 'Technology Towers' allow benchmarking the state's IT spend against other public and private organizations.

State agencies invested close to $3.4 billion in 2018-19 and based on agency portfolio information submitted to the OCIO, labor represents the largest proportion of overall IT spending.

2018-19 STATE IT INVESTMENT				
Cost Pool	**2018**	**2019**	**2018-19 Total**	**% of Spend**
Internal Labor	$611,558,604	$626,968,592	$1,238,527,196	36%
Hardware	$179,249,044	$197,550,424	$376,799,468	11%
Internal Services	$182,201,614	$187,725,958	$369,927,573	11%
Software	$168,258,622	$195,711,921	$363,970,543	11%
Other	$115,779,656	$151,430,368	$267,210,024	8%
Outside Services	$110,907,294	$154,375,575	$265,282,870	8%
External Labor	$147,470,876	$114,497,752	$261,968,628	8%
Telecom	$70,728,897	$66,486,787	$137,215,684	4%
Facilities & Power	$59,009,410	$56,130,013	$115,139,423	3%
Total	**$1,645,164,017**	**$1,750,877,392**	**$3,396,041,409**	**100%**

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

When asked to assign cost pools to technology towers (see Figure 4), state agencies reported "application" attracting the largest amount of investments followed by "end user," which includes support of desktop, mobile devices and desktop software.

Higher education continues to be the state leader in IT spending (see Figures 5 and 6). However, statute exempts them from OCIO requirements to assign IT costs to technology towers.

2018-19 INVESTMENT BY TECHNOLOGY TOWER

Technology Tower	Percentage
Output	1%
Storage	3%
Security & Compliance	5%
Data Center	5%
Delivery	6%
Compute	7%
IT Management	9%
Network	13%
End User	15%
Application	36%
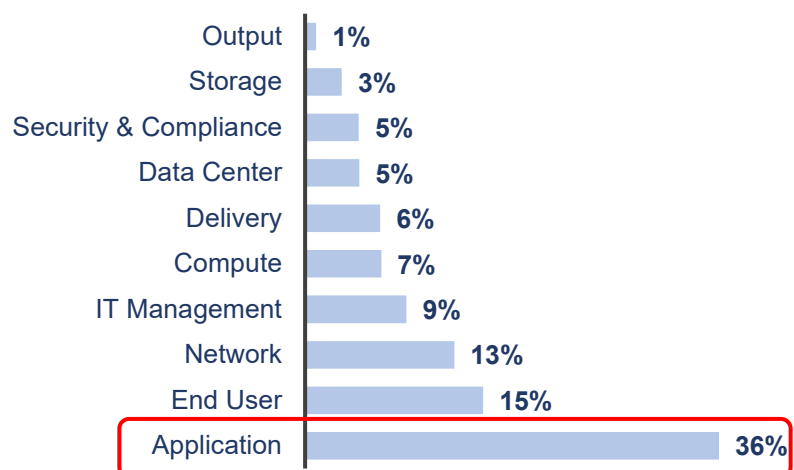
Figure 4: Percentage of expenditure by technology tower.

IT SPEND BY GOVERNMENT FUNCTION
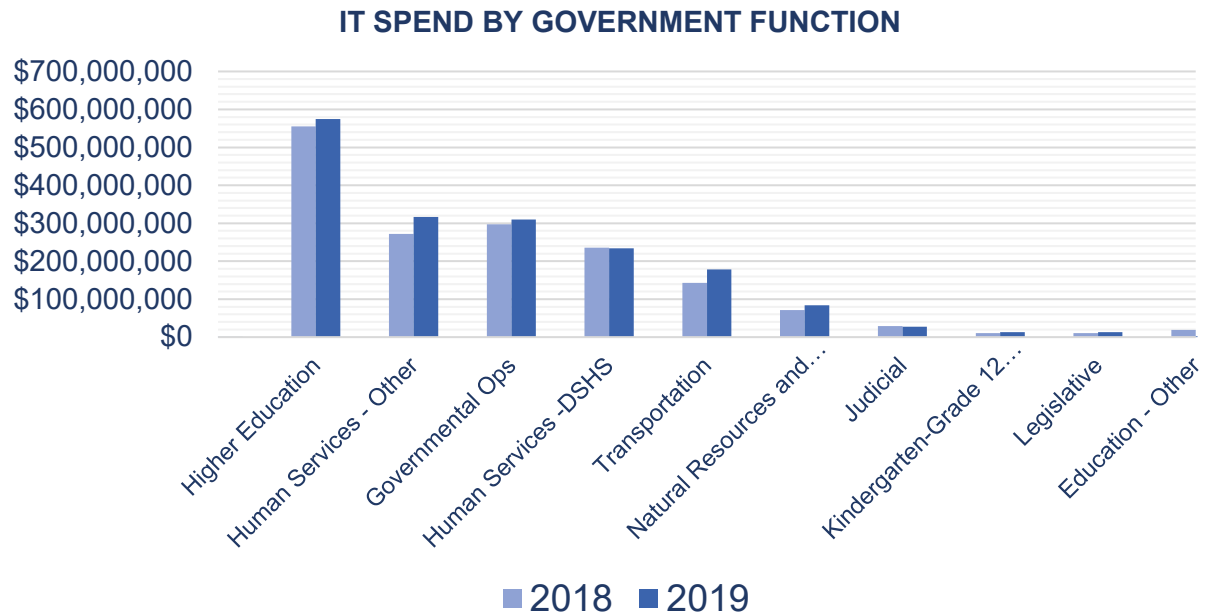
Figure 5: Comparing IT spend by different government function.

PERCENTAGE OF IT SPEND BY GOVERNMENT FUNCTION
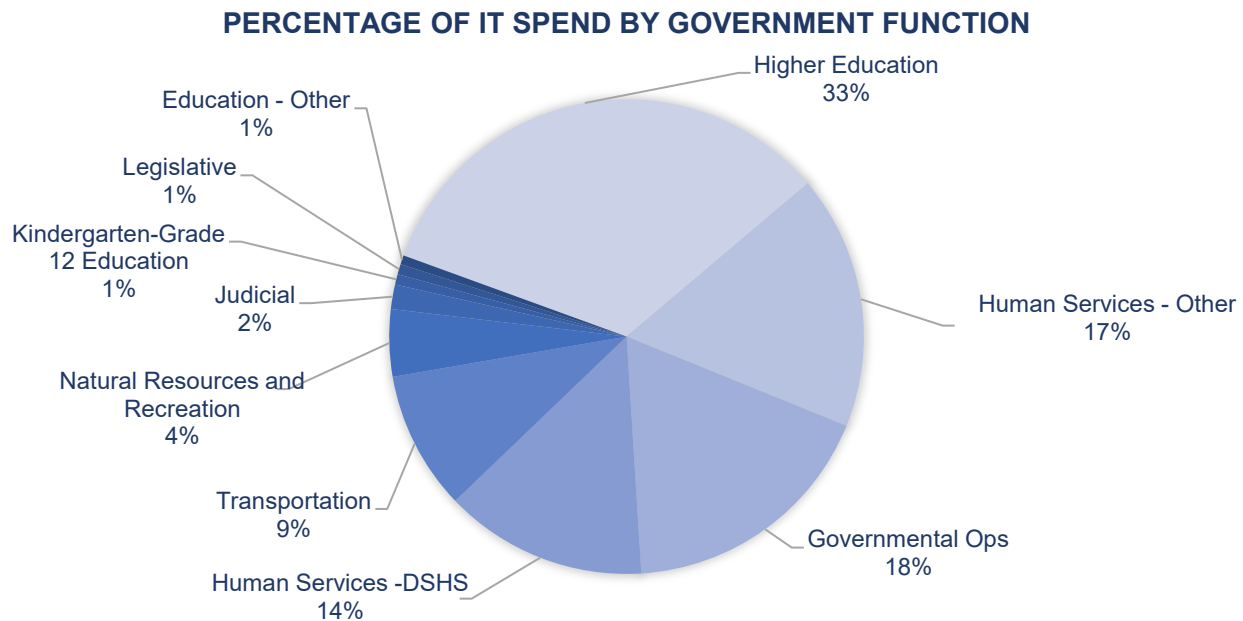
Figure 6: Percentage of 2018-19 IT spend by different government function.

Agencies are required to report technology investments by acquisitions/new development (i.e., new spend), and by maintenance and operations. Figure 7 includes itemization of expenditures by new spending, 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 Agency Financial Reporting System (AFRS).

2018-19 IT INVESTMENT - NEW VS MAINTENANCE & OPERATIONS

Maintenance & Operations 49%

Data Processing Interagency *(Payment to Central Service agencies)* **8%**

Unmarked IT Spend *(Includes hardware and software expenditures that agencies neglected to mark as IT)* **3%**

Aquisiton/New Development 40%
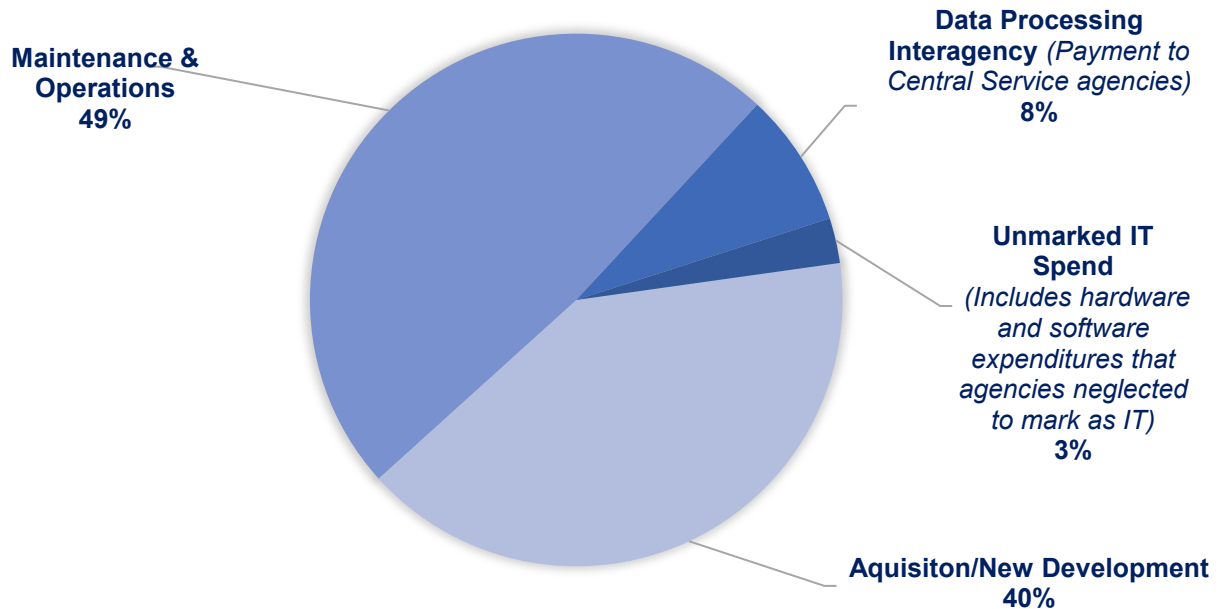
Figure 7: Itemized IT investment by new spend and M&O.

A trend began emerging related to cloud-based subscription services in 2019. Many new cloud-based subscriptions were being marked as maintenance and operations instead of "acquisitions/new development."

With current financial coding practices, a steady increase in the number of new cloud-based software and hardware investments being reported as maintenance and operations (OpEX) is anticipated. Given strategic emphasis on "buy rather than build," this practice will affect agencies that historically use depreciation (CapEX) as a cost saving measure. This cost savings is accomplished by extending hardware and software use-life past the depreciation end date.

FY19 CLOUD SUBSCRIPTION INVESTMENT PROFILE

- **6%** IT Acquisitions/New Development
- **94%** Maintenance & Operations

Application/software assessment

To gain insight into the number of legacy applications in the state portfolio, agencies covered under OCIO statute began submitting an application inventory starting in 2014 as part of the annual certification process.

As Washington's application portfolio continues to age, the state will continue 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 technical debt and better understand its relationship to legacy applications.

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 in-house expertise.

Analysis of the state's application portfolio provides insight into the number of state systems that will require future investment to address legacy characteristics and/or technical debt.

WHAT IS 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.

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. (See Figure 8 for trend.)

LEGACY APPLICATION TREND

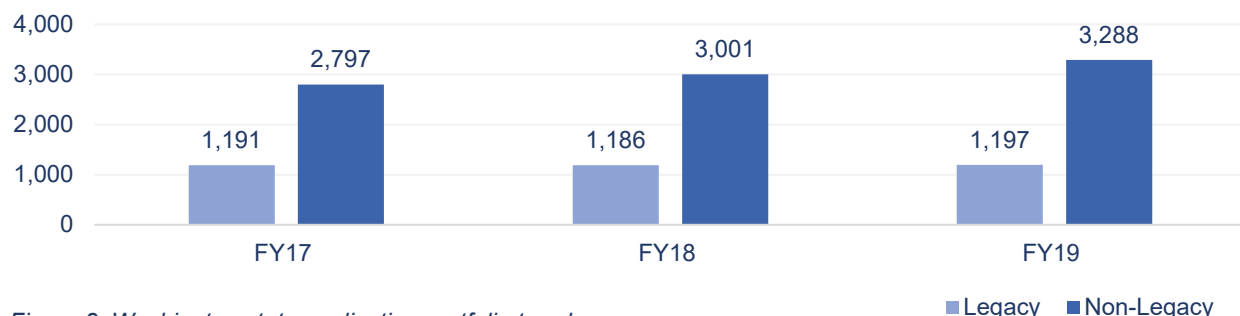|	FY17	FY18	FY19
Legacy	1,191	1,186	1,197
Non-Legacy	2,797	3,001	3,288

■ Legacy ■ Non-Legacy

Figure 8: Washington state application portfolio trend.

Agencies also self-define how critical their applications are to the organization. Figure 9 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**: Direct negative customer satisfaction; compliance violation non-public damage to organization's reputation; direct revenues impact.

- **Historical**: Needed for historical purposes.

- **Mission Critical**: Widespread business stoppage with significant revenue or organizational impact; risk to human health/environment; public, wide-spread damage to organization's reputation.
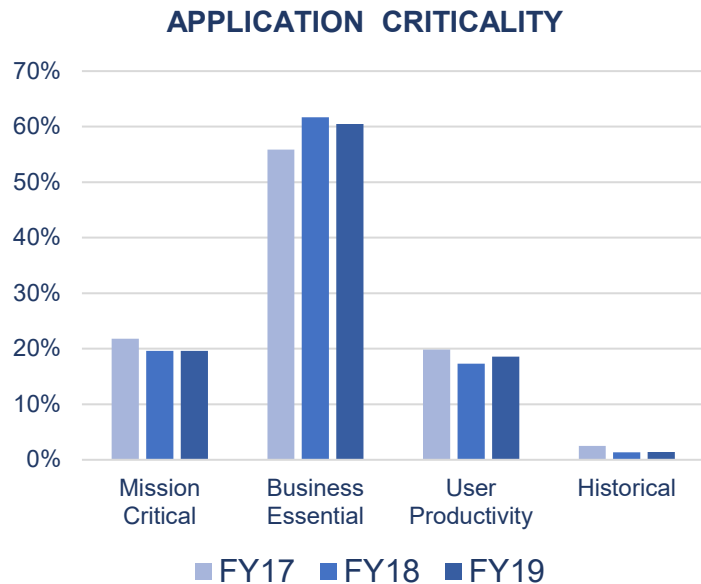
Figure 9: Trending application criticality.

- **User Productivity:** Impact to employee productivity.

State agencies have reported a reduction in legacy applications, but not those identified as critical to their mission. The proportion of legacy applications identified as mission critical or business essential to the agency has seen an increase as trended in Figure 10.
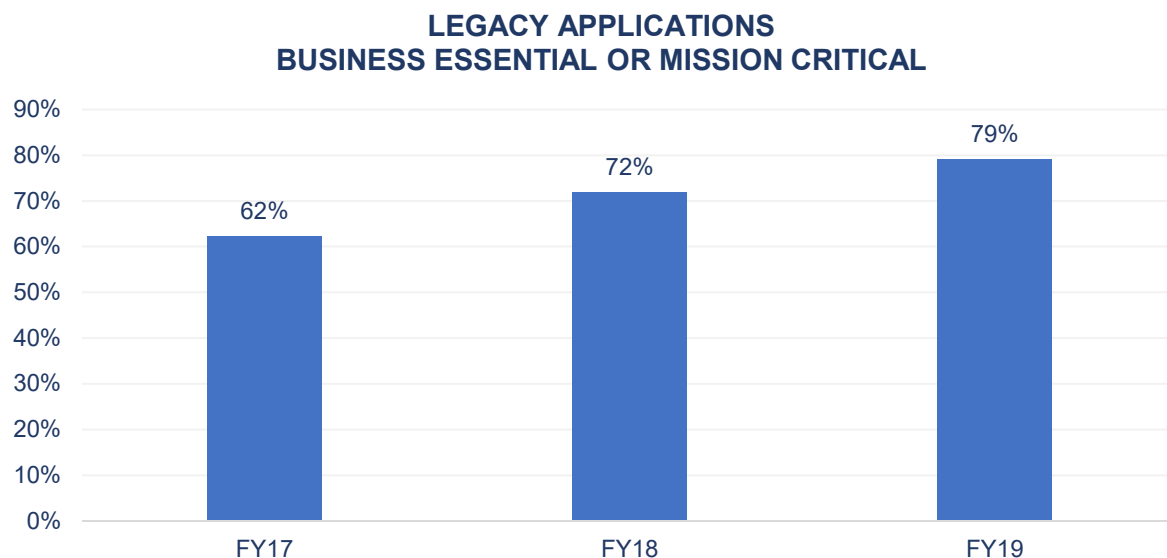
Figure 10: Trending mission critical/business essential applications.

Legacy custom-built application trends

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 and account for 50% of the state's applications (see Figure 11).

APPLICATION PORTFOLIO DEVELOPMENT TYPE
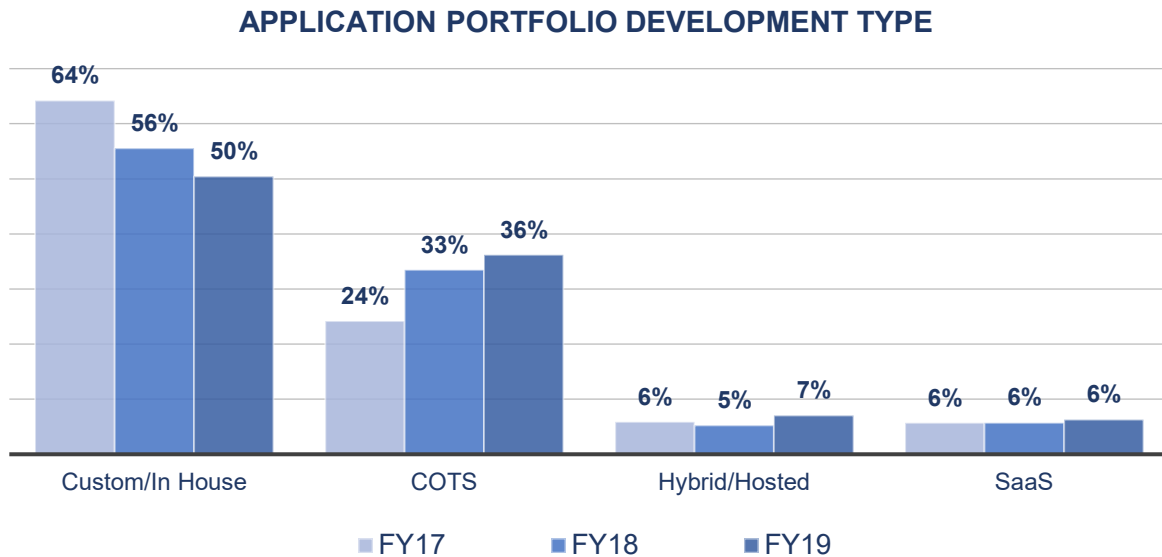
Figure 11: Trending the state application portfolio by development type

Looking at the past three-year trend, the number of custom/in-house built legacy applications that support mission critical or business essential functions has trended downward as seen in Figure 12.

**LEGACY - CUSTOM-BUILT
MISSION CRITICAL/BUSINESS ESSENTIAL**
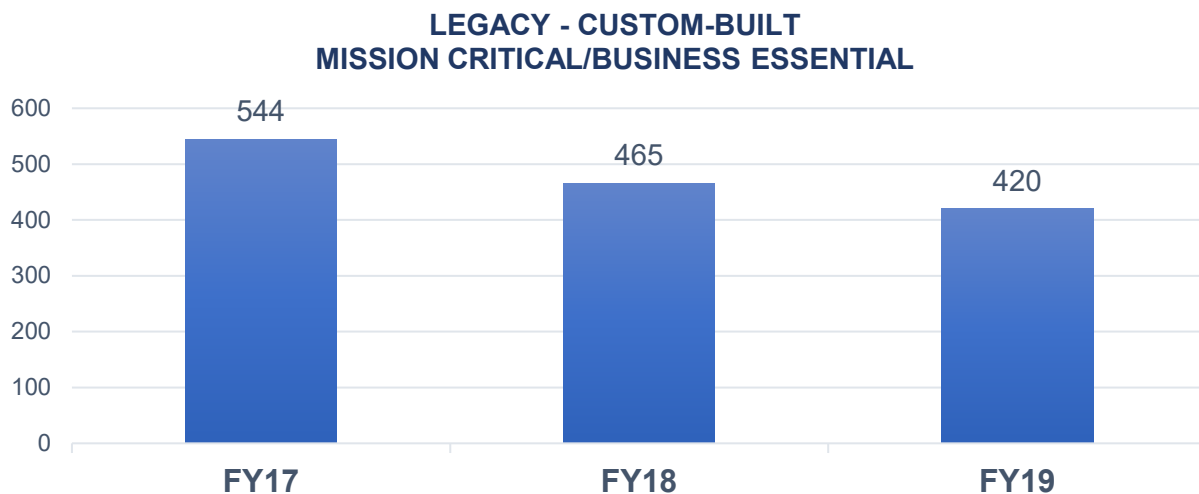
Figure 12: Legacy custom-built mission critical/business details.

Data in Figure 13 demonstrates that agencies were able to reduce the number of custom-built legacy applications classified as business essential while the number of mission critical applications remained constant.

LEGACY - CUSTOM BUILT
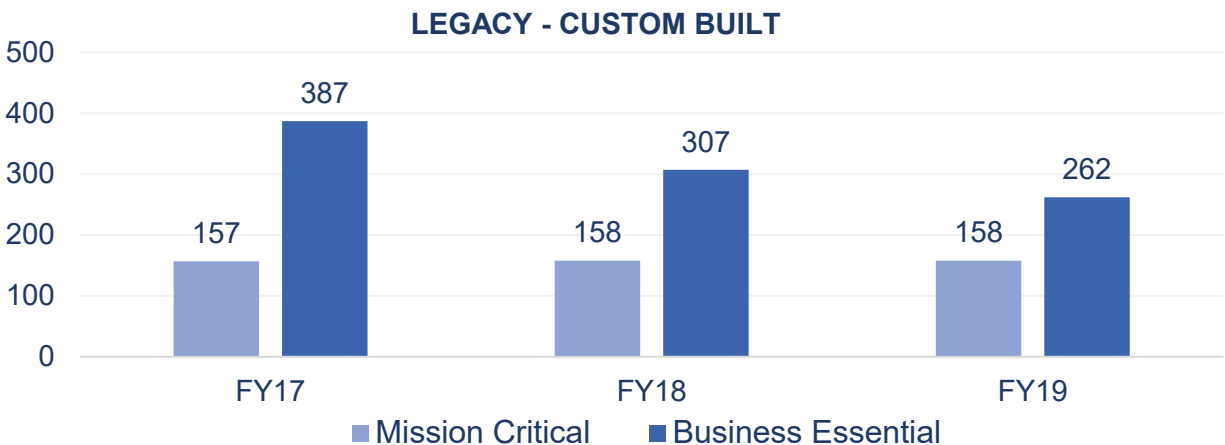
Figure 13: Legacy custom-built mission critical/business essential details.

In summary, by the end of fiscal year 2019, the statewide application portfolio contained 420 legacy systems identified as custom-built and supporting mission critical or business essential functions (see Figure 14). These applications surface as priority candidates for a modernization assessment.
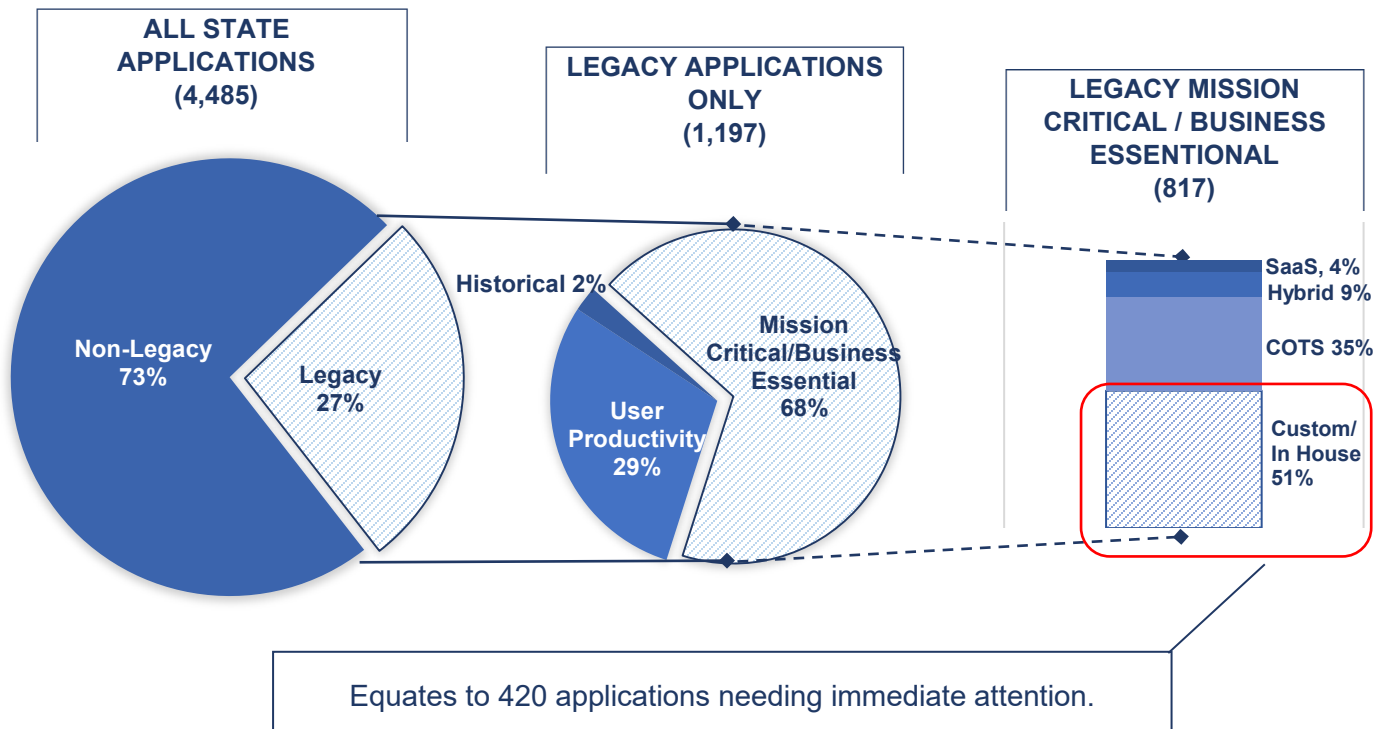
Figure 14: FY19 Legacy application profile.

Addressing legacy applications – tracking progress and cost

Agencies report using both decision package requests and their base budget to initiate projects that address legacy applications. The state has made progress with several large enterprise resource planning (ERP) and business transformation projects currently underway. By the end of June 2019, more than 60% 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 $1.39 billion.

> **LEGACY MODERNIZATION PROJECT LIFESPAN**
>
> **3 Years** – project average
> **1.5 Years** – shortest project
> **5.5 Years** – longest project

LEGACY & BUSINESS TRANSFORMATION PROJECTS UNDER OVERSIGHT

Project Status June 2019	Project Budget	Number of Projects
Closed	$148,578,048	18
Active	$1,245,056,228	33
TOTAL	**$1,393,634,276**	**51**

Table 2: Budgeted costs for 51 legacy modernization projects under OCIO oversight.

For this report, analysis of funding legacy application modernization efforts is limited to the 183 IT decision package requests submitted by agencies in the 2019-21 biennium. As seen in Figure 15, 25% of the budget requests to address legacy modernization were funded. For submitted legacy modernization funding requests, Figure 16 provides insight into the final amount funded.

2019-21 FUNDED LEGACY MODERNIZATION REQUESTS

Legend: ■ Amount Requested ■ Amount in Governors' Budget ■ Amount Enacted in Legistlation
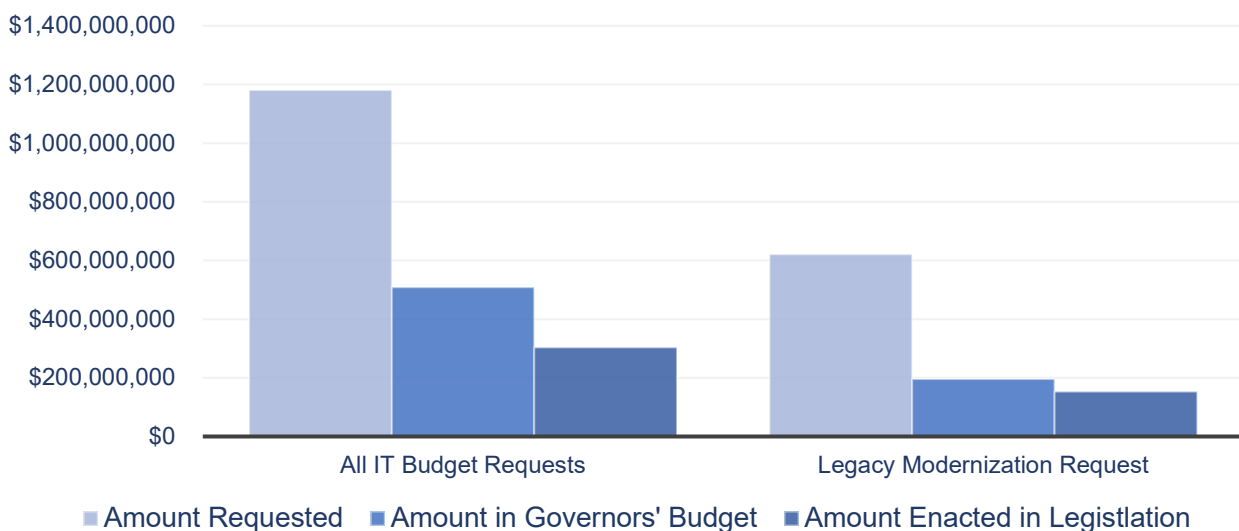
Figure 15: Legacy modernization request funding trend.

LEGACY FUNDING REQUESTS BY FUNCTION OF GOVERNMENT

■ Amount Requested   ■ Amount in Governors' Budget   ■ Amount Enacted in Legislation
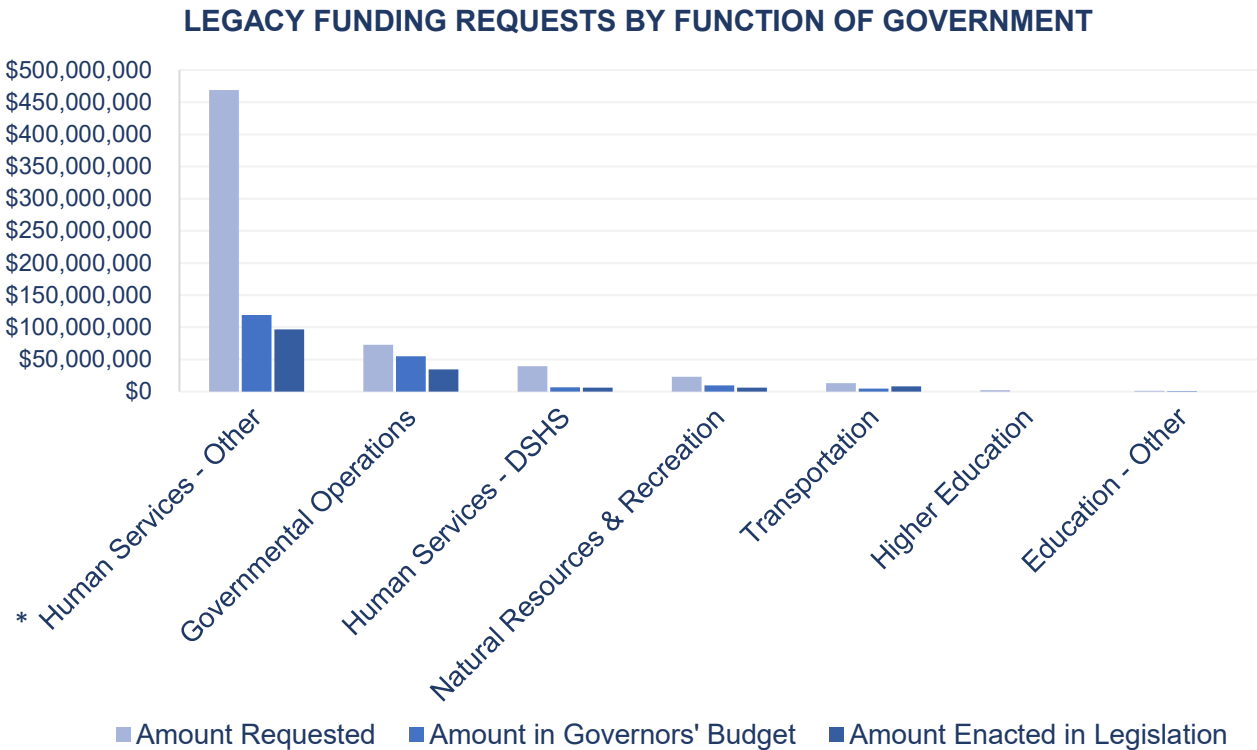
*Figure 16: * The significant variance between amount requested and in the budget is attributed to a single request.*

For requests that secured funding, Figure 17 provides data on the number of projects funded for system modernization and the percentage of funding received.

2019-21 SYSTEM MODERNIZATION FUNDING REQUESTS
Percent of request funded
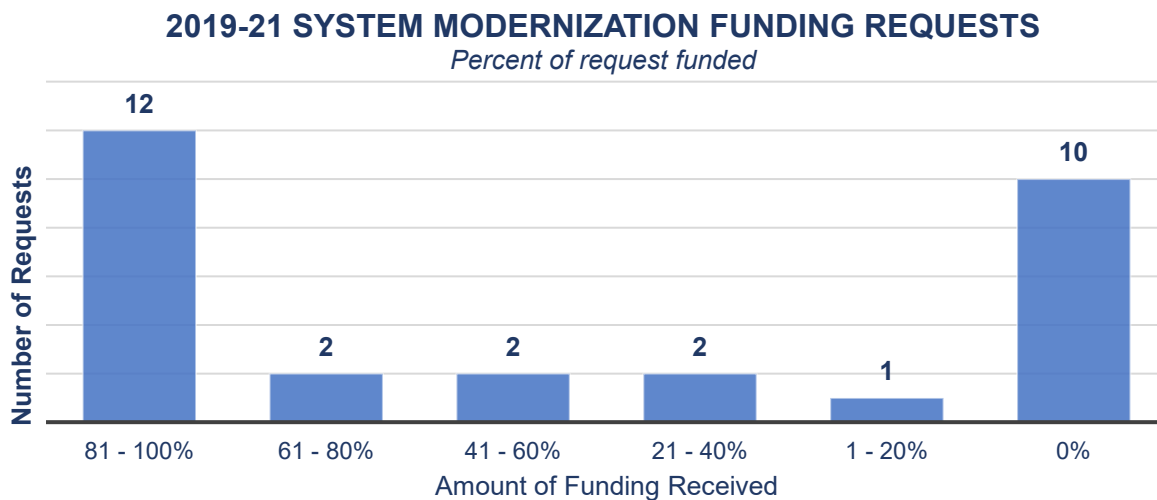
Figure 17: System modernization funding requests for 2019-21.

Application modernization projects are multi-year projects that can span multiple budget cycles. Recognizing that agencies must make tough decisions when prioritizing funding with tight budgets, legacy application modernization and business transformation

requests need to be based, going forward, on risk mitigation and benefits provided to Washingtonians.

Hardware assessment

Mirroring the hardware investment trend of FY16-17, state agencies report that end user hardware – which includes desktops, laptops and mobile devices – represent their highest costs followed by networks.

Compute hardware trended downward, from 11% of the hardware investment in FY16-17 to 9% in FY18-19.

2018-19 HARDWARE INVESTMENT BY TECHNOLOGY
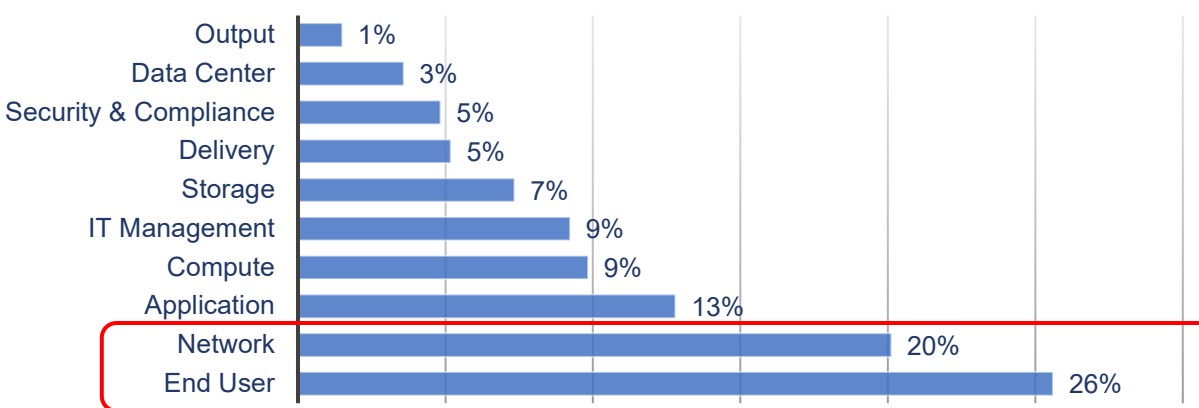
Figure 18: Hardware investment by technology.

The state recognizes mobile devices for many employees are valuable tools that aid in conducting business in an effective and timely manner. By spring, 2019 executive branch agencies reported having more than 23,600 mobile devices in use to access the state system and records.

With the continued movement to a mobile work environment and proliferation of mobile devices, support for end user devices is expected to represent a growing share of labor expenditures. Given the shorter lifecycle of desktops, laptops and mobile devices, the state will likely experience increased spending on internal and external labor to support end users and their devices.

Network assessment

Over 80% of network expenditures are associated with nine agencies. WaTech makes up the largest portion at 29% because it is the state's central IT services agency and provides network service to more than 125 organizations. The Department of Social and Health Services (DSHS) represents the largest share for a single agency at 18%. The OFM K20 network accounts for 9% of expenditures.

2018-19 NETWORK SPEND

Service to 125 different organizations.

Service for K20 network
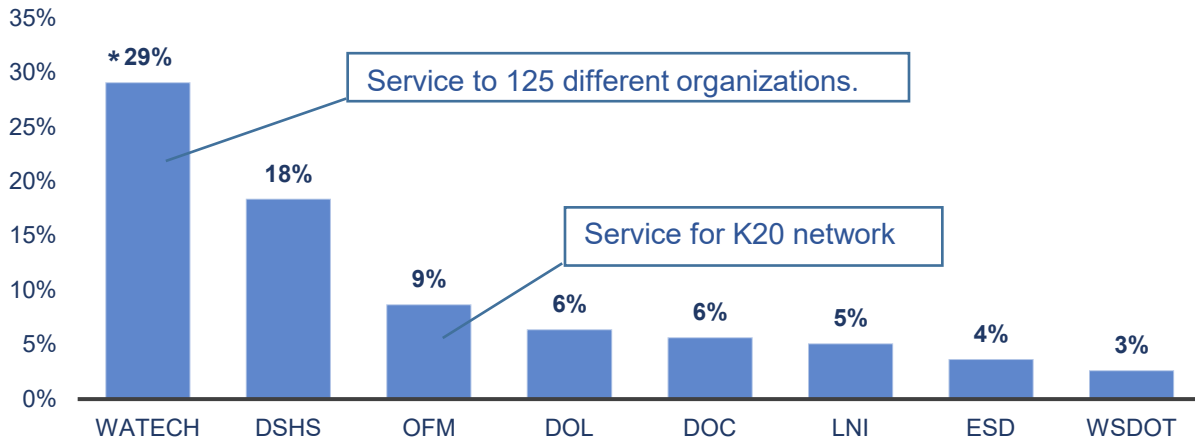
*Figure 19: * WaTech makes up the largest portion at 29% because it is the state's central IT services agency and provides network service to more than 125 organizations.*

WaTech, DSHS and OFM identify telecom circuits and labor as the majority of their network spend. Figure 20 provides a breakdown of the expenditures for these three agencies.

BREAKDOWN NETWORK SPEND
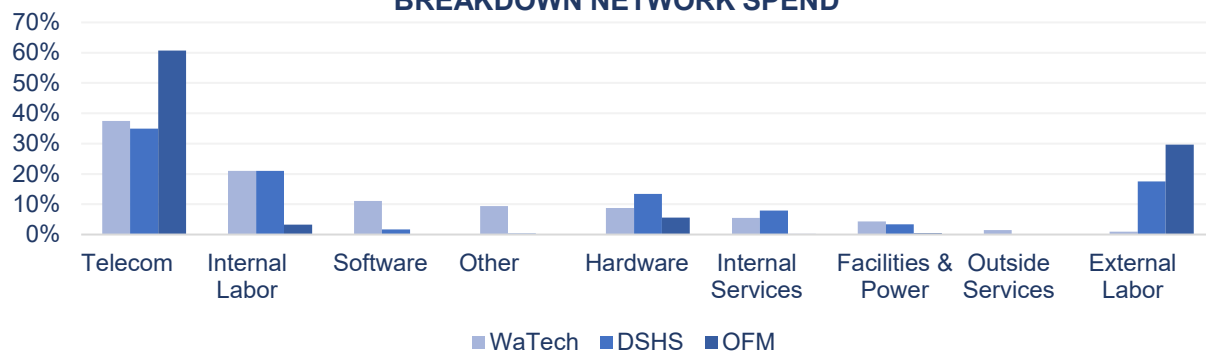
■ WaTech ■ DSHS ■ OFM

Figure 20: WaTech, DSHS and OFM network expenditures by cost pool.

During this time period, WaTech executed a new master services agreement (MSA) with more than a dozen telecommunication service providers to create a more efficient procurement approach that scales to meet the state's evolving needs. This resulted in both lower costs and improved services for the state.

Another benefit of the new MSA is resiliency. Under the new MSA, telecommunications service providers must have two redundant pathways in each of Washington's two centrally managed data centers. The primary center is located in western Washington and the secondary in eastern Washington. Additionally, providers are required to configure circuits as a point-to-multipoint – providing multiple paths from a single location to multiple locations. This greatly increases resiliency and helps ensure continuous service in the event of a disruption.

The State Metropolitan Optical Network (SMON) – a high-speed fiber optic network established between select areas of Olympia, Tumwater and Lacey – was expanded to support 10 Gigabit service. Redundant circuits also were added to connect the state's secondary data center. These improvements help ensure agencies have the bandwidth needed for cloud-based computing and ensure maximum survivability in the event of a disaster.

Other improvements include:

- Voice and network services made improvements that allow for increased state agency use of Voice over Internet Protocol (VoIP) technologies. VoIP uses the internet to transmit phone calls. As of FY19, about 20% of customer endpoints were VoIP and demand is accelerating. Customers benefit from improved service and a reduction in telephony costs.

- WaTech also is implementing LTE cellular technology as a cost-effective backup solution for state agencies that support critical sites such as prisons, hospitals and emergency services requiring 24/7 telephony and data connectivity.

- WaTech is implementing a "cloud highway," which is a dedicated, high speed, scalable model that provides all agencies with secure connectivity to public cloud providers.

Intergovernmental Network (IGN)

Improvements to the Intergovernmental Network (IGN) – including enhanced security, increased capacity and uniform pricing – were completed for counties, which represent the IGN's primary customers. The IGN enables over 100 Washington state counties, cities, federal agencies, tribes, health districts, and other authorized customers to securely connect to managed gateways and applications owned by the state within multiple agencies.

Labor assessment

Application support dominates the state's IT workforce investment, trailed by end user support, IT management, delivery (project and client management) and other technology services (see Figure 21).

2018-19 INTERNAL LABOR INVESTMENT

Output	1%
Data Center	2%
Storage	2%
Security & Compliance	6%
Compute	7%
Network	8%
Delivery	10%
IT Management	14%
End User	16%
Application	33%

0% 20% 40% 60% 80%

2018-19 EXTERNAL LABOR INVESTMENT

Output	0.2%
Data Center	3%
Storage	1%
Security & Compliance	1%
Compute	2%
Network	9%
Delivery	3%
IT Management	6%
End User	5%
Application	71%

0% 20% 40% 60% 80%
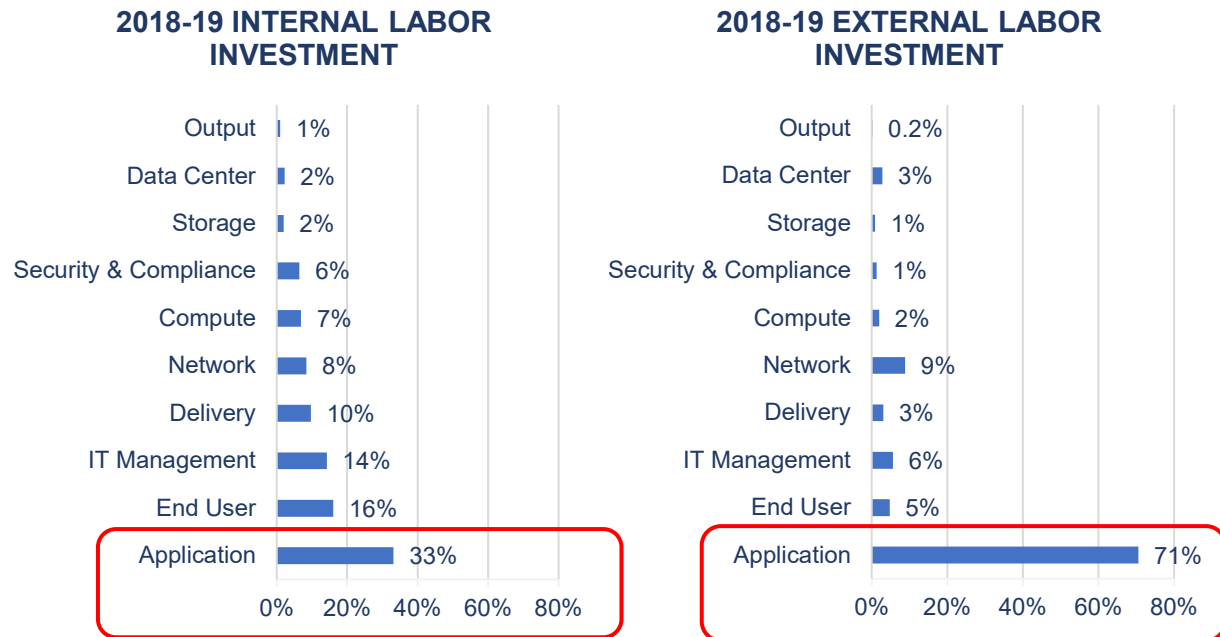
Figure 21: Internal and external labor investment by technology tower.

The data in Figure 22 shows the largest proportion of labor costs dedicated to maintenance and operations efforts. This trend is anticipated to remain the same going forward due to new and old systems running in parallel during modernization activities. Generally, the new system movement is to maintenance and operation while the decommissioning of the legacy system applications is still in progress.

IT LABOR - SUPPORT BY NEW & EXISTING TECHNOLOGY

	FY17	FY18	FY19
New Acquisiton	45%	39%	40%
Maintenance & Operations	55%	61%	60%

■ New Acquisiton   ■ Maintenance & Operations

Figure 22: Trending labor investment by new acquisition/development and M&O.

As mentioned in the hardware assessment, labor support for end user devices is expected to increase. Since desktops, laptops and mobile devices, have a shorter lifecycle there will likely be increased spending on internal and external labor to support end users and their devices.

Enabling continuity after a disaster

Washington state is working to strengthen system resiliency during a disaster. Efforts include the operation of a continuity data center in eastern Washington, using geo-mapping to help first responders during disasters and improving emergency communications.

Key areas being addressed include:

Data center: The operation of a continuity data center in Eastern Washington, which ensures redundancy and high-availability for the state's essential communications, security and network systems, as well as resilience and backup for critical business applications and data.

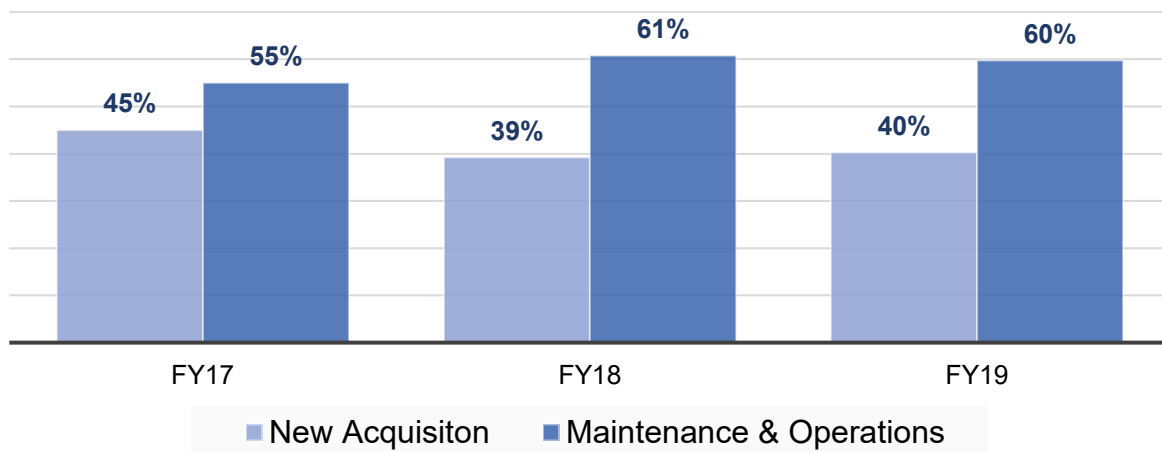**Interoperable communications:** Emergency responders in Washington state have a variety of wireless network options available for emergency communications including satellite and cellular services. For the most part, responders in Washington subscribe to one or more wireless providers (depending on network availability in their area of operations): FirstNet Built with AT&T, Verizon, T-Mobile, and Sprint all provide public safety wireless voice and data services. FirstNet and Verizon advertise priority of network services for responders for situations of decreased/degraded network capacity.

The wireless providers also have critical incident teams imbedded in the Washington Military Department/Emergency Management Division to ensure that communication services for responders and the public are restored as quickly as possible.

All wireless providers have pre-staged communications equipment strategically placed in Washington so they can be deployed within 14 hours of request. Washington OneNet (WON) is a federally, grant funded program to coordinate with the Federal First Responder Network Authority and public safety responders in Washington state. WON assisted FirstNet with the design of FirstNet Build with AT&T in Washington state.

Collaboration: The Washington Emergency Communications Coordination Working Group (WECCWG), composed of public, private, tribal and non-profit sector professionals involved in emergency communications across the Pacific Northwest are working together to provide reliable and resilient emergency communications throughout the state in times of crisis.

In addition, the Federal Emergency Management Agency's Regional Emergency Communications Coordination Working Group (REECWG) provides a forum to address the survivability, sustainability, operability, and interoperability of emergency communications systems at all government levels. The working group spans 14 states (including Washington, as well as 271 tribes, and the Pacific Islands.

Next generation 911 service: Washington state has moved most Public Safety Answering Point (PSAP) systems - responsible for answering emergency telephone calls - to the next generation Emergency Service Internet Protocol Network (ESInet). The ESInet will enable the public to transmit text, images, video and data to the 911 center.

There are 92 PSAPs in Washington: 52 primary systems, 29 secondary ones and 11 others that include backups and test systems. Of those, 64 have been connected to ESInet. No more systems are expected to be connected. The remainder can still receive 911 calls.

Remote Access: WaTech's Remote Access service has been improved to allow for robust VPN connections, including during emergencies.

For example, when an Amtrak train derailed on Interstate 5 in 2017, the VPN allowed large numbers of state workers to telecommute until the highway was reopened.

Mapping Technology: The state can map locations of wireless access points and telephone service sites using existing systems, such as

WaTech's Remote Access service hit a new record during the Amtrak derailment, allowing large numbers of state workers to telecommute until the highway was reopened.

WaTech billing information. It also purchases cell phone towers and fiber route locations from third-party vendors. This information can be compared to natural hazards data such as wildfires, which is then shared with state agencies and the public through a geographic information portal (geo.wa.gov). The maps below show how information can be combined to help inform first responders during emergencies.
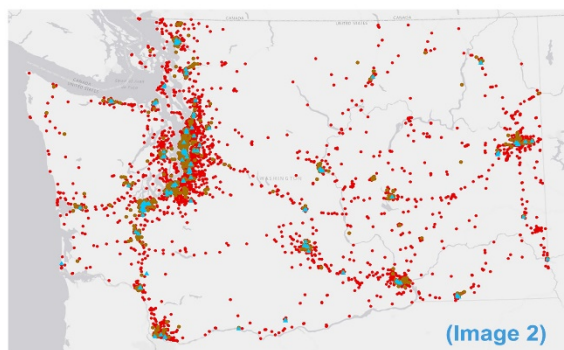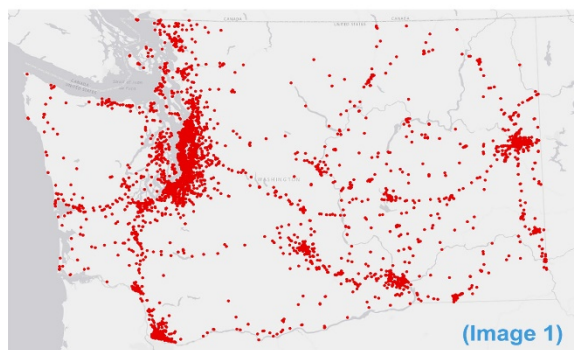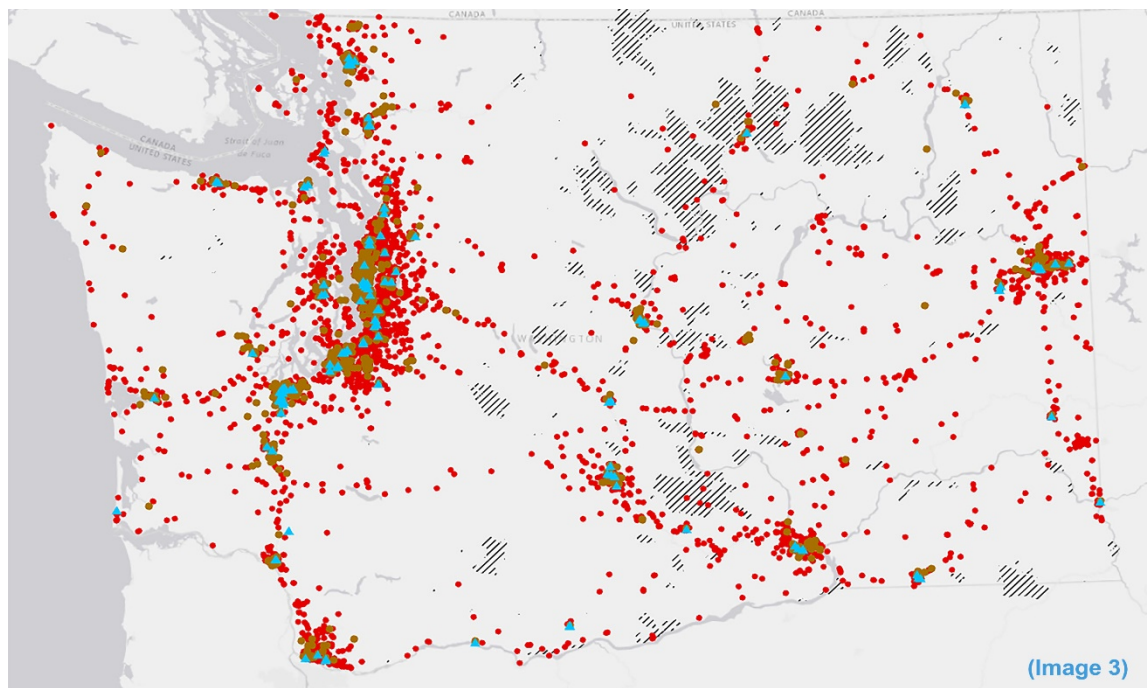
The state is able to use mapping technology to aid first responders during disasters. For example, in the maps above, Image 1 shows cell towers (in red) and Image 2 shows wireless access (in blue) and telephones sites (in brown). This information was combined in Image 3 to show where those sites were in relation to wildfires (in black).

SECTION 3: ACCESSIBILITY (RCW 43.105.220 (2C))

Access to public information and services

By statute RCW 43.105.220, state agencies are to set priorities for making public records widely available electronically to the public. Agencies continue to report improvements in public access to data as well as accessibility to those with disabilities.

Accessibility for those with disabilities

Washington state is committed to making technology accessible to everyone including those with disabilities. Agencies have matured and continue to ensure people with disabilities have equal access and use of state services and content.

For example, the Department of Social and Health Services - Aging and Long-term Support Administration (ALTSA) is working on a project to provide awareness, guidance, and recommendations regarding the creation of websites in order to address the challenges faced by those with disabilities. The goals of this project are to:

- Spread awareness that accessibility considerations are a priority when creating new websites.

- Make accessibility awareness a part of annual required training.

- Recommend the creation of an accessibility resource team, whose purpose is to provide guidance and review of website content to assure it meets accessibility guidelines.

Other examples:

- The Office of Financial Management hosted the sixth Annual Global Accessibility Awareness Day in May 2019. The purpose of the event was to create discussion about digital access and inclusion for people with different disabilities.

- Policy 188 and accessibility also were the topic of a panel discussion at an International Project Management Association forum held at Saint Martin's University, also in May.

- In August, the Washington State Department of Health held an Accessibility Awareness Day with information on Policy 188 and an assisted technology lab coordinated with Washington State Services for the Blind.

These efforts are making an impact. For example, a recent report by the Utah-based nonprofit WebAim, scanned the most popular 1 million homepages on the internet and found only 2% were free from accessibility errors available to their scan. The Washington State Department of Ecology homepage was one of those 2%.

Expanding access to data statewide

During the past biennium, there was a trend toward making more data available to the public along with publication of larger data sets. Open data remains a priority for the state of Washington.

Today there are 30 agencies publishing data on Data.wa.gov, resulting in approximately 1,700 assets available for use in a wide variety of formats. Based on web browser statistics the site is accessed 10,000-15,000 times per week. There is access to state data by developers using the Data.wa.gov programming interface, allowing custom queries and high-volume analysis for developers and data scientists. Other areas statewide where data has been made available:

Department of Health

Health Care Provider Credential dataset is currently the most used dataset in the collection with over a million views.

Public Disclosure Commission

Principal campaign finance reporting datasets like the Lobbyist Compensation and Expenses dataset, are updated continuously and viewed over 150,000 times.

Department of Licensing

Electric vehicle licensing data has recently been added to the portal, with automated updating for visualizations such as showing the top 10 electric car models titled in the past 12 months.

Office of Financial Management

Census, population and housing data are available on the portal in a variety of formats, such as the table of 2000 and 2010 census figures.

Liquor and Cannabis Board

Provides Open data portal https://data.lcb.wa.gov

Traffic Safety Commission

Commission's website includes a dashboard for Research & Data.

WSDOT

Maps & data offerings include maps, tables, and API interfaces.

Fiscal.wa.gov

Data on state budgets, spending, revenue, staff and other activities.

In addition, the OCIO makes information on major projects technology transparent and publicly available through the IT Project Dashboard. This website contains project investment approval materials, independent project quality assurance and project status reports. Data derived from project materials and supporting information is used for analytics related to project outcomes.

The state of Washington and California collaborate on [Data Equity for Main Street](#). The project mobilizes 26 libraries and a variety of civic technologists to write, test and improve open educational resources for use in training public library patrons and staff to understand and use open data.

The project, which concluded in the summer of 2019, published online courses and helped launch open data initiatives in Everett and Asotin County. Full curriculum materials and promotional models are available for free on [GitHub](#).

SECTION 4: ACCOUNTABLE IT MANAGEMENT
(RCW 43.105.220(2B))

Capturing technology performance

The state made headway over the biennium to capture metrics related to the statewide technology performance. Areas of improvement include:

- Starting in January 2019, data on all technology investment in the state became publicly accessible online on the IT Spend Dashboard for 19-21 Biennial Report. Stakeholders report moving the information from a paper-based format to online access saves time.

- Improvements in capturing technology decision package data enables reporting and ranking 100% of agency funding requests. The Finalized IT Decision Package Funding Recommendation is publicly available and final analysis on the proposed requests.

- With increased progression to a mobile workforce, emphasis was placed on securing and protecting state records on mobile devices. By the end of fiscal year 2019, 93% percent of executive branch agencies had all mobile devices protected with an approved mobile device management solution.

Data driven analytics

The state Technology Business Management (TBM) program continues to mature and help agencies gain additional insight into their IT investments.

UNMARKED IT SPENDING

* The majority of the unmarked IT spending in 2019 was for higher education projects, which are unable to be tracked in their financial system that feeds AFRS.

Based on data analysis, for example, many agency IT investments were not being properly flagged in the statewide Agency Financial Reporting System (AFRS). This resulted in millions of dollars of technology expenditures not being accurately reported statewide. Collaboration between the OCIO and Statewide Accounting resulted in OFM making changes to the chart of accounts, starting in fiscal year 2018, to improve capture of IT spending.

In 2018, over $63 million invested in technology was not identified as IT. By the end of 2019, agencies made improvements in properly marking hardware and software investments. As a result, unmarked IT spending dropped 53% to $29.6 million. The majority of the remaining unmarked IT spending in 2019 is attribubted to higher

education institutions with legacy systems that are unable to call out hardware and software expenditures.

Data center migration - updated progress

State agencies have made progress moving their equipment and services out of their data centers, following the enactment of RCW 43.105.375.

The biennium started with 42 agencies having projects to migrate equipment and services from 47 different agency specific facilities. Between FY17- FY19, 17 projects were completed and 30 were still active.

AGENCY DATA CENTER MIGRATION TREND
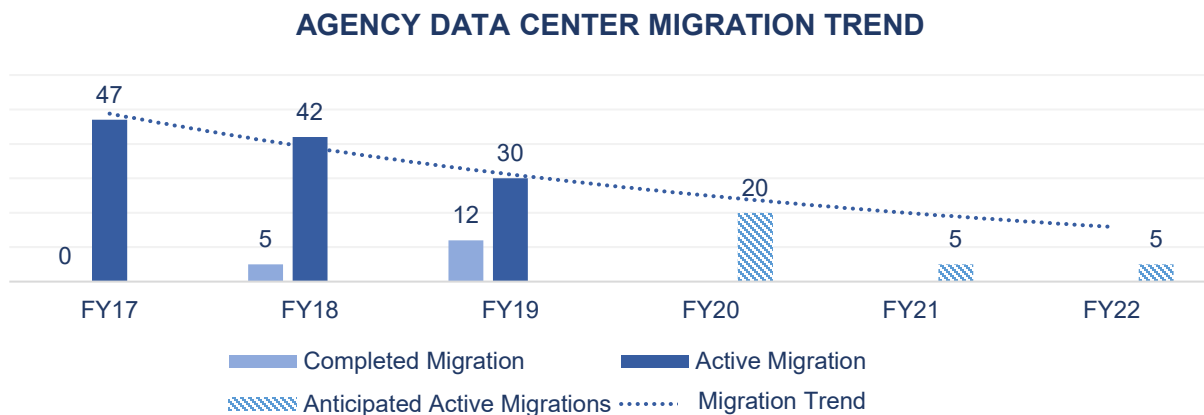
Figure 23: Trending current and future agency migrations.

Agency migration projects continue to be tracked on a monthly basis. Several complex migration projects, classified as major projects, are under OCIO oversight. Some of those are subject to gated funding for added accountability.

Of the remaining 30 migration projects, 16 are moving to the State Data Center, six projects are moving to an external cloud solution and eight have a hybrid solution that uses both the State Data Center and external cloud solution.

State Data Center utilization

At biennium close, there were 48 agencies with server workloads in the State Data Center. Of the 48 agencies, 35 are using colocation services, 26 are using the state private cloud and 13 have a presence in both services.
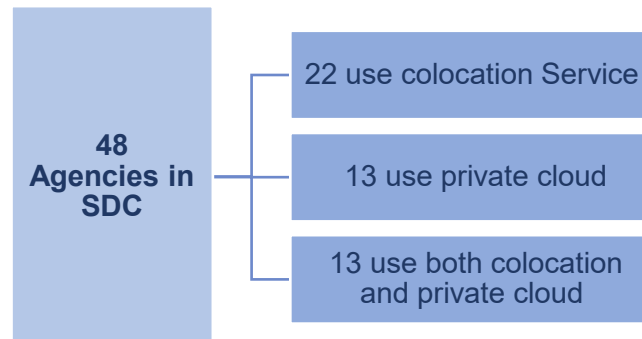
Figure 24: State Data Center customer usage as of June 2019.

SECTION 5: PROJECT OVERSIGHT (RCW 43.105.220 (2D) & RCW 43.105.245)

Practices related to projects

In Washington state, IT investment equates to any money spent on IT. An important first step for any IT investment, is to determine whether or not it is considered "major." A project is considered major based on the risk and impact score from an IT Project Assessment, if gated or otherwise noted in a budget proviso or occasionally at agency request. All major IT investments are subject to the approval and oversight of the Office of the Chief Information Officer (OCIO).
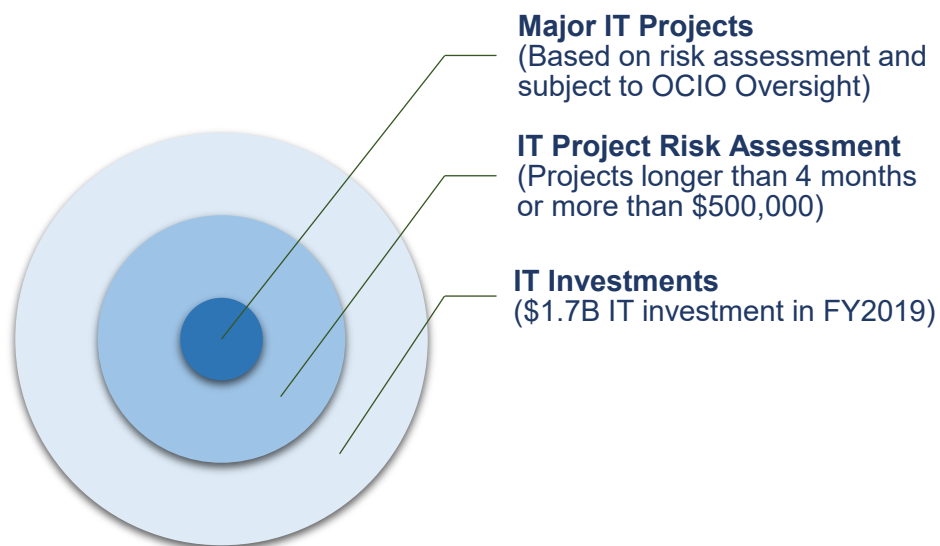

Major IT Projects
(Based on risk assessment and subject to OCIO Oversight)

IT Project Risk Assessment
(Projects longer than 4 months or more than $500,000)

IT Investments
($1.7B IT investment in FY2019)

With more than $1.7 billion in IT spending during fiscal year 2019, it is important to understand the makeup of the IT investments, determine which investments need to perform a project risk assessment and identify those that rise to the level of major IT project.

The IT project assessment (ITPA) process is a risk and impact evaluation of a proposed investment. Changes were made to the ITPA process in an effort to gain earlier insight into the number of IT investments occurring statewide. Guided by technology policies, agencies were asked to submit a risk assessment using the ITPA tool for all IT investments. Additionally, an ITPA submittal was required for all 2019-21 biennium IT funding requests.

Even with these changes, gaps remain in collecting information. Fewer investments were reported to the OCIO than anticipated with only 161 agency ITPAs submitted in 2019 from 42 agencies. Of those, 32 were submitted as part of the 2019-21 funding request cycle. For additional detail on 2018-19 submittals, please see Appendix A.

As part of their OCIO annual certification process, agencies were asked to share what barriers prevented the submittal of IT investment assessments. Agencies also were

asked to show what action was being taken to ensure all IT investments are being assessed. While 70% of agencies reported no barriers, the remaining agencies supplied information about changes to internal agency processes along with obstacles to submitting assessments.

During this time the OCIO worked on changes to policies, standards and existing oversight and approval processes. One example: The Project Go-Live Readiness Decision Governance standard better positioned the project steering committee and executive sponsor decision to determine if the organization is ready to go live with a new IT solution.

In early 2019, the OCIO engaged consulting firm Plante Moran to supplement additional analysis work by conducting an independent assessment and collecting oversight best practices. Plante Moran recommendations would provide additional insights along with recommendations based on best practices in other states.

Plante Moran focused on the following key questions and proposed recommendations the OCIO can use to inform oversight reform efforts targeted for the 2019-21 biennium:

PLANTE MORAN PROJECT APPROVAL AND OVERSIGHT ASSESSMENT	
QUESTIONS:	**RECOMMENDATIONS:**
1. How can the OCIO gain earlier visibility into agency projects? 2. How should the state determine if a project is to be considered major and subject to oversight? 3. How can the process of assessing projects and associated risks be made more consistent? 4. How can the Information Technology Project Assessment (ITPA) tool be improved to better assess project risks and identify major projects? Are the right risks highlighted and are the risk scales appropriately assigned?	• All state agencies should submit annual IT strategic plans aligned with their business plans. • These IT strategic plans should include specific planned projects, providing the OCIO earlier insight into agency projects and a comprehensive inventory of statewide projects. • RCWs 43.105.007, 43.105.054 and 43.105.205 already have content that supports this process. • In the future, agencies could submit IT strategic plans and projects through an online agency portal. • Define required technical deliverables to support improved architecture reviews and technical oversight.

Major project oversight

Through the 2018-19 biennial cycle, the OCIO provided oversight to 100 major projects. Of those projects, 60 were included based on risk/severity and 40 based on budget proviso that placed them in the Information Technology Investment Pool (IT Pool). Projects in the IT Pool are subject to gated funding. As part of the gated process, the

OCIO evaluates and notifies the authorizing environment when a project is certified to proceed to the next stage.

Estimated costs for the 100 major projects totaled over $1.6 billion. By June 2019, 33 major projects were completed or closed. Table 3 provides information on the 100 projects at biennium close.

MAJOR PROJECTS STATUS DETAIL - JUNE 2019

Project Status	Non-Pool Projects	Pool Projects	Total Projects
Active	28	24	52
Complete/Closed	23	10	33
Canceled	7	5	12
On-Hold	1	1	2
Proposed – not started	1	0	1
Totals	60	40	100

Table 3: IT Major project status at biennium close.

Each major project receives a regular independent assessment by the OCIO during the project lifecycle. As a result of that assessment, an overall health rating of green, yellow or red is assigned and a narrative provides more information about the assessment.

At project close out, the OCIO oversight consultant provides a final assessment. If the scope schedule or budget differed significantly from the approved investment plan then the project changes to red, yellow or green with the oversight consultant adding closing comments reflecting the reason behind the color designation. Figure 25 provides details on health check assessment at project close.

PROJECT LIFECYCLE HEALTH STATUS

- **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.

FY18-19 CLOSED PROJECT FINAL HEALTH CHECK ASSESSMENT
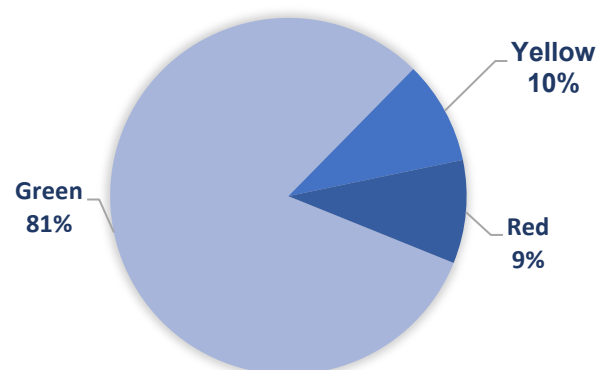
Green 81%
Yellow 10%
Red 9%

Figure 25: Health of 2018-19 major projects at close.

Having an independent and experienced Quality Assurance (QA) provider on major projects has proven successful. QA providers offer valuable insight into project and oversight activities. The QA provider helps project teams, sponsors and the OCIO anticipate risks and issues before they occur.

In 2017, vendors providing QA on major projects attended a QA Summit sponsored by the OCIO. Based on feedback at the QA Summit, the OCIO made changes to the project executive sponsors training. QA providers, agencies, and OCIO oversight consultants report that improvements to the executive sponsors training has resulted in more leadership support and engagement in projects.

Grounded on success of the 2017 QA Summit, another summit was held in spring 2019. The OCIO engaged Plante Moran to facilitate the summit, which was attended by 13 QA professionals from 10 firms. The OCIO plans to use the findings from the 2019 QA Summit to inform additional project oversight improvements in the 2019-21 biennium.

Identifying major project lessons learned and critical success factors

Major projects, when finished, complete a Post Implementation Review Report that includes lessons learned from both project teams and external quality assurance providers. When analyzing lessons learned, the ensuing common themes emerged from projects that were completed this biennium:

- Agency readiness to start the project.

- Emphasis on contract/vendor management.

- Right-sized/skilled resources and budget.

- Responsive and clear business requirements.

- Attention to organizational change management.

- Transition to operations.

OCIO implemented process improvements that promote effective assessment of and reporting by projects. Many of the enhancements to oversight practices this biennium were focused on the following areas:

- OCIO offering Executive Sponsor Training for all new and existing state project executive sponsors. The executive sponsor training continues in the 19-21 biennium.

- Ensuring that projects have effective governance in place to promote timely decision making.

FY18-19 EXECUTIVE SPONSOR LEADERSHIP TRAINING

- **10** training sessions.
- **20** participating agencies.
- **159** state leaders trained.

- Updated quality assurance standards requiring monthly assessment and agency response to QA Findings.

- Bringing projects to the TSB for briefing and guidance when assessed red (see project lifecycle health status definitions on page 36) for more than three consecutive months.

- Establishing readiness assessments decision governance to be based on several factors including data, technology, organization, internal and external users.

- Agencies determine go-live readiness criteria and factors during the project planning stage.

- The gated funding process for IT projects to create deliverables-based performance gates that are relevant to each project and facilitates opportunities to gauge lessons learned.

- Using project gates to log and track lessons learned at the gate and monitor improvements throughout the project and biennium.

PROJECT CRITICAL SUCCESS FACTORS

- Engaged and appropriate sponsor.
- Effective & timely governance.
- Appropriately staffed project management.
- Organizational readiness.
- Quality procurement & vendor management.
- Independent quality assurance as trusted advisor.

Major project cost tracking

Major projects previously were not consistent in either level of detail or formatting when reporting on project budgets, making comparisons difficult. As mentioned earlier, projects in the IT Pool are subject to gated funding and require OCIO and OFM approval to move through project stages. The gated funding practice brought an improved level of accountability to project cost reporting.

Several agencies under gated funding implemented dedicated coding to monitor project costs in the state enterprise financial system. For some agencies, meeting federal reporting requirements was the motivating factor for the dedicated coding. It became clear a foundation existed within agencies to standardize on reporting processes using dedicated coding.

A standard technology budget template was developed that incorporated dedicated coding. Projects at the Department of Fish and Wildlife (DFW) and Office of Financial Management (OFM) served as the initial use case. Based on DFW and OFM test results, the new technology budget template and process proved to be a viable solution for granular and gated reporting on all major IT projects under oversight. Additionally, the template meets statutory IT project reporting requirements by aggregating project financial information in a uniform manner.

All gated funding projects in the fiscal 2019-21 biennium will use the new process. These changes will improve the state's ability to capture accurate financial information

about projects, increase the confidence in agency data collected, and position the state for greater detail and analysis on the funding lifecycle for major projects.

Tracking progress of 2018-19 IT pool projects

Approximately 57% of the $1.6 billion approved for major IT projects during the biennium was assigned to 40 projects in the IT Investment Pool.

By the end of 2019, four of the 40 projects in the Investment Pool went past their end date and fiscal year funding. Two of those received funding in the 2019-21 biennium. Funds for the remaining two are coming from agency base budgets. Figure 26 provides IT Pool project status as of June 2019.

Ten of the IT Pool projects closed by June 2019. As demonstrated in Figure 27, the average completion time was 1.4 years less than projects not in the pool. The completed pool projects represented 30% of all closed major projects under OCIO oversight.

Ninety percent of IT pool projects closed in green status (see Figure 28).

IT POOL PROJECTS - JUNE 2019

Canceled 12%
Closed 25%
On-Hold 3%
Active 60%
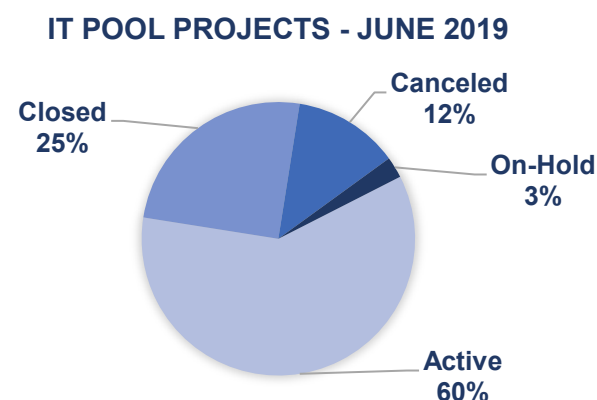
Figure 26: IT pool project status at the close of 2019

TIME TO CLOSE MAJOR PROJECTS

YEARS

IT Pool Project   Non IT Pool Project
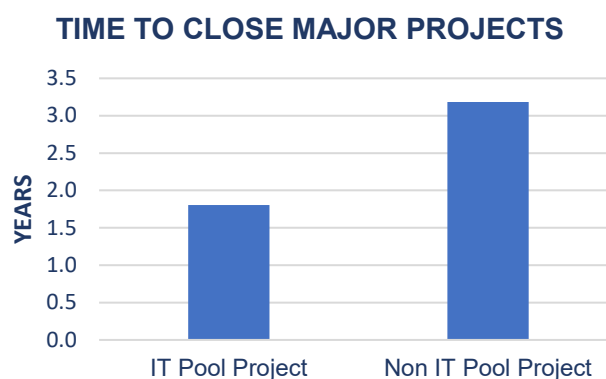
Figure 27: Major project time to close

**STATUS
CLOSED IT POOL PROJECTS**

Red 10%
Green 90%

**STATUS
ACTIVE IT POOL PROJECTS**

Green 32%
*No Color 8%
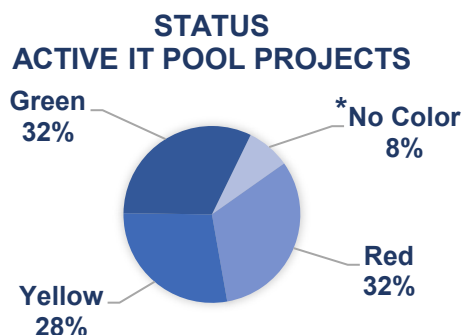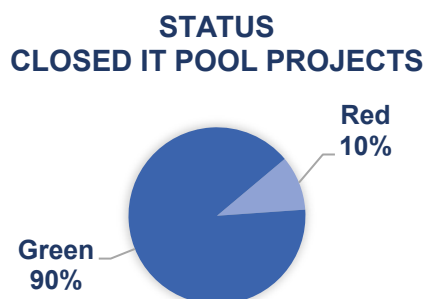Red 32%
Yellow 28%

Figure 28: Closed and active IT pool project status as of June 2019

* No Color represents projects that initiated activity near biennial end.

Outcome from major IT projects

Historically, information has been collected on how well projects stay on scope, schedule or budget. However there have been gaps in capturing data on project outcomes. There have been incremental improvements during this time period with more targeted for the 2019-21 biennium.

The following section highlights outcomes submitted from several major IT projects that closed in 2017-19 biennium.

AGENCY: PROJECT NAME	PROJECT REPORTED OUTCOMES
Department of Children, Youth and Family/Department of Early Learning: Time & Attendance aka Procure Time and Attendance System	The goal of this project is to increase the accuracy of a child's reported attendance and reduce a provider's opportunity for deliberate fraud. • The project has increased the accuracy of a child's reported attendance and for families receiving subsidy to review child attendance records through an online portal. • Over 99% of licensed providers in the state now have online access and no longer need to keep manual records to support the subsidy process. • With the ability for compliance reporting, less than 1% of licensed providers are out of compliance with the state requirements.
Department of Corrections: IT Business Solutions	With organization change on the horizon, this project supports efforts to address staff retention in advance. This project instituted a governance model and process to better support the business technology including staff training resulting in service delivery improvements.
Department of Licensing: Drive vehicle system (DRIVES)	With millions of licensed drivers in the state, this new modern system reduces downtime when licensing due to improved system reliability. Additional outcomes include: • Improvements in data reports which include providing more accurate records to law enforcement. • Improved business processes and interfaces between employees and WSDOT business partners. • The ability to collect new and increased fees more quickly.

Department of Social and Health Services: Background Check System (BCS)	A functioning background check system is critical to the states' ability to meet its responsibilities to protect the most vulnerable citizens of Washington state. DSHS processes over 330,000 background check requests per year for agency programs, service providers, licensees, and the Department of Children, Youth and Families (DCYF). • This system reduces the average turnaround time on fingerprint checks as well as name and date of birth background checks. • BCS also provides results of long-term care background checks to the Department of Health.
Department of Social and Health Services: Forensic System	This project facilitates compliance with federal court orders by creating a new data system that replaces two outdated legacy systems at both state hospitals. By creating one data system, the Department is able to produce more timely and accurate data reporting for the federal court and the legislature. • This project reports improved overall data accuracy resulting in improved compliance with court ordered requirements, and improved provision of data to courts, patients and others. • Improved data accuracy promotes better informed program policy decisions. • Improved data accuracy facilitates deployment of evaluators to complete evaluations within requirement time constraints and improves the referral process to inpatient beds.
Employment Security Department: Unemployment Tax and Benefits System (UTAB) enhancements	Studies consistently show that early intervention in reemployment effort is one of the single largest drivers of getting people back to work. • The enhancements made connections between systems making it possible for claimants to search for work opportunities once they have completed filling out their weekly claim. • The objective of this project is to reduce the number of weeks a claimant is on unemployed from 14.9 week in 2017 to 12 weeks by June 2020.

• Reemployment Trade Assistance payments are now made inside the system that automatically checks/prevents improper payments.	
Office of Financial Management: All Payer Claims Database (APCD)	Provided a public website ([Washington Health Care Compare](#)) that allows citizens to see and compare healthcare plans, price and quality to determine what is right for them. Along with improved transparency of health care services by describing access, price, utilization and value of services captured within the WA-APCD.
Superintendant of Public Instruction: Website Upgrade to ADA Compliance aka K12 Website Upgrade	This upgrade provides the K-12 public education community with a better experience when accessing information on the website. The site is fully ADA compliant and with improved navigation, access to information is intuitive for students, teachers and parents interested in Washington state public education.
Pollution Liability Insurance Program: Loan and Grant Portfolio Management System	This project allows the new loan and grant program to provide up to $2 million in funding per facility to underground storage tank (UST) owners and operators across Washington state to replace or upgrade fuel storage tanks, clean up historical or ongoing fuel contamination, or install alternative fueling equipment. PLIA administers the loan and grant program in coordination with the Department of Health (DOH). All loan and grant applicants must use the online system to apply which is more efficient as the demand increases.
Department of Fish and Wildlife: Network Infrastructure Rebuild	Agencies' networks are the foundation needed to provide services to clients and constituents. Network outages hinders the organization's ability to communicate between locations and prevents access to critical agency information. • This project reduced the number of unscheduled network outages resulting in improvements to staff productivity and communication with constituents. • The upgrades support improved enforcement officers' safety by making it possible to remain in contact with WDFW headquarters.

Washington State Patrol: Sexual Assault Kit Tracking System	This web-based program provides sexual assault survivors the ability to anonymously access and track location and status of their kit from collection, through forensic analysis, to final storage location. It further empowers survivors with information, assists law enforcement with investigations and crime prevention, creates transparency and fosters public trust.

SECTION 6: IT WORKFORCE

Attract and retain high-skilled technology staff in state government

With an aging state IT workforce, attracting and retaining highly skilled IT personnel continues to be a high priority, especially in a region where the state competes for talent with some of the biggest technology companies in the world.

The state CIO has prioritized workforce development and recruitment. The state CIO and OFM's State Human Resources office collaborated on a job class study for IT classifications. This multi-year effort, aimed at building a more modern, competitive job class structure, concluded June 30, 2019.

The new IT professional structure, which became effective in July 2019, was developed to:

- Ensure enterprise and organizational alignment and equity.

- Improve opportunities for career growth.

- Keep pace with the rate of IT industry change.

- Improve the state's ability to benchmark work internally and externally.

> **6.3%** of the Executive Branch Workforce are Technology Professionals.
>
> (*Classified, EMS and WMS*)
>
> *HRMS data as of 6/30/2019*

Table 4 shows the number of classified positions by job family (rows) and job level (columns) identified as part of the study:

Job level	Entry	Journey	Senior / Specialist	Expert	IT Manager	IT Senior Manager	Job Family Totals
Application Development	176	629	190	6	34	4	1,039
IT System Administration	145	573	141	1	18	3	881
IT Customer Support	374	243	12	N/A	25	N/A	654
IT Business Analysis	53	307	44	-	12	1	417
IT Data Management	39	254	79	-	23	1	396
Network & Telecom	47	190	95	-	14	7	353
IT Project Management	5	132	61	1	25	7	231
IT Quality Assurance	61	130	12	-	3	-	206
IT Architecture	N/A	17	98	11	22	6	154
IT Security	N/A	76	49	3	9	6	143
IT Policy & Planning	1	10	18	-	35	37	101
IT Vendor Management	4	5	3	-	3	1	16
Total	905	2,566	802	22	223	73	4,591

Table 4: Statewide classified IT professional structure profile.

Over 56% of the classified IT positions align with three job families; application development, system administration and IT customer support. At 55.9% the journey job level has the highest percentage of all position classifications.

IT POSTION BY JOB FAMILY
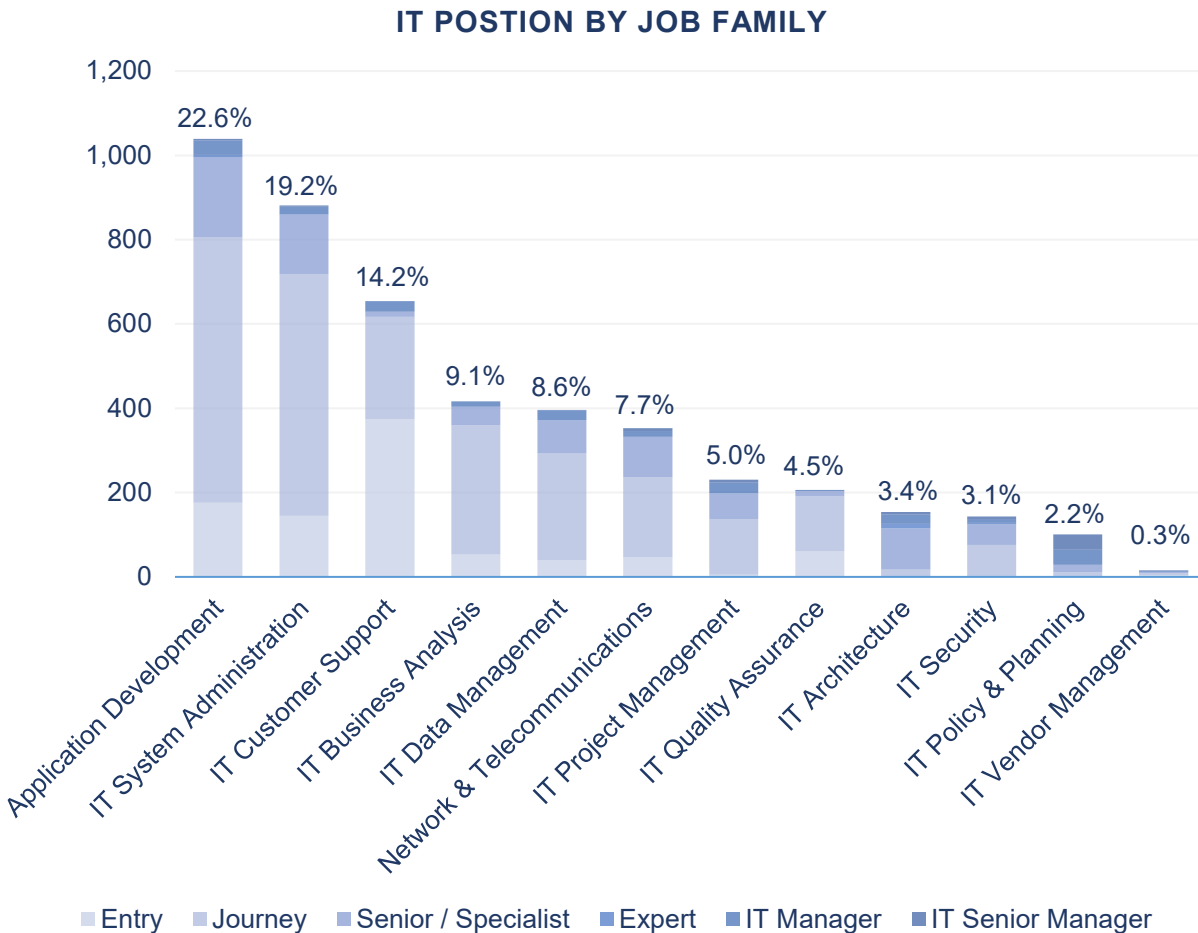
Figure 29: IT positions by job family and job level.

As the reclassification work was concluding, mixed results for state technology professionals began to surface across the state. In some cases, there is a perception that positions reclassified out of IT will result in employees leaving for other positions that remained in higher salary IT positions.

Other examples surfacing pertain to salary compression issues where the IT classified positions pay is higher than their supervisors who are in Washington Management Service (WMS) or Exempt Management Service (EMS) positions. With the new classification in place, it will be important to continue reviewing the state's ability to recruit and retain qualified IT professionals.

Data captured in the 2019-21 biennium will inform the outcomes of the IT position restructure and determine if the changes in salary improve recruitment and retention efforts. This is especially important given that more than half of the state's technology workforce is eligible to retire within the next five years, according to the state Human Resources office, which reports that the state's technology workforce is aging and

retiring in greater numbers (see Figure 30). Only 46 IT employees responded to the optional exit survey and Figure 31 captures their responses to where they are going and why they are leaving.

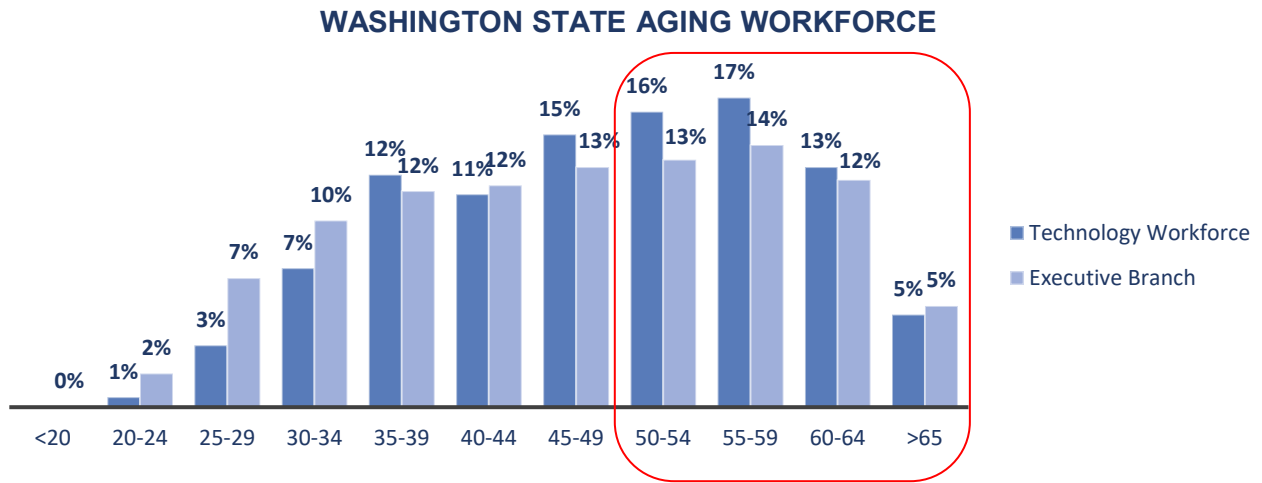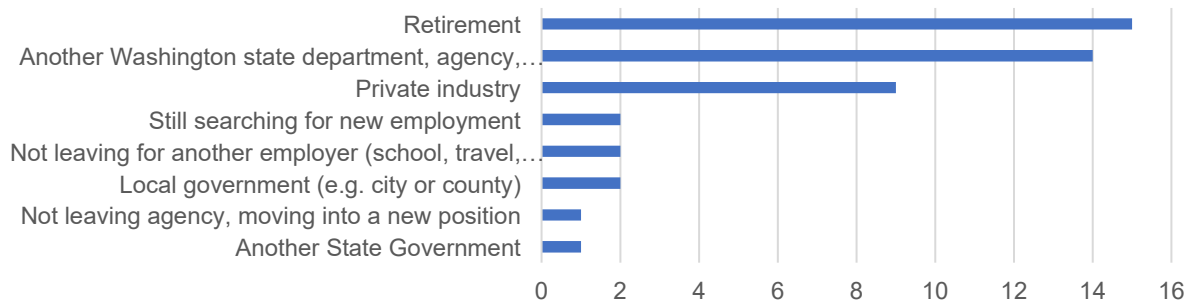**WASHINGTON STATE AGING WORKFORCE**

Figure 30: Washington state workforce by age.

IT Exit Survey Responses from 46 employees
2018 - 19

Where are they going?
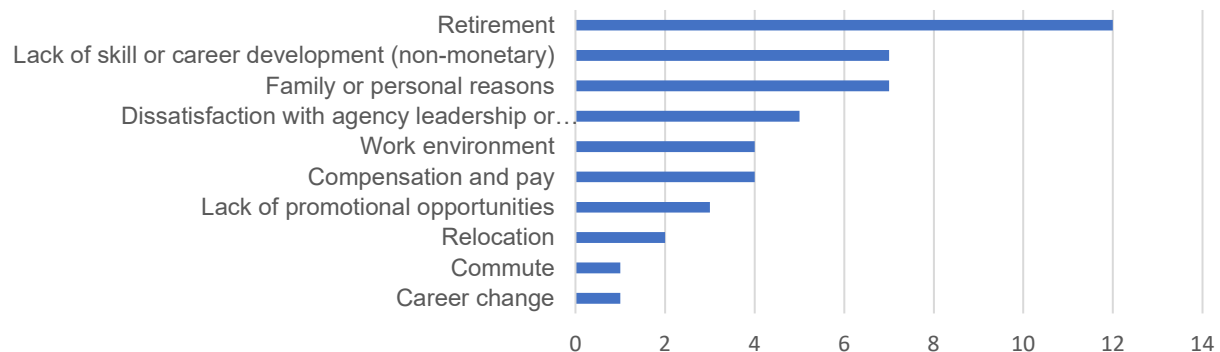

Why are they leaving?

Figure 31: Exit survey responses captured at state HR.

Figure 32 compares the state IT workforce diversity to the executive branch and Washington's civilian workforce doing similar work.

Female

21%

0%   **33%**   100%

Women are well represented in the technology workforce (33%). This is higher than the 21% doing similar work in Washington state's civilian labor force.

People of Color

27%

0%   **23%**   100%

People of color comprise 21% of the technology workforce compared to 20% for the executive branch. However, this is less than the 27% doing similar work in Washington state's civilian labor force.*

Veterans

7%

0%   **13%**   100%

Veterans comprise 13% of the technology workforce compared to 8% for the executive branch. Both are higher than the 7% available in Washington state's civilian labor force.*

US Census Bureau, 2006-2010 American Community Survey

People of Color and Veteran New Hires

People of Color 28%

People of Color IT Workforce 21%

Caucasian 72%

Veteran 19%

Veteran IT Workforce 13%

Non-Veteran 81%

The percentage of people of color hires at 21% and veterans at 13% was lower in the technology workforce than the executive branch.

Female New Hires

Female 29%

Female IT Workforce 33%

Male 71%

The percentage of female hires at 33% is higher in the technology workforce than the executive branch.
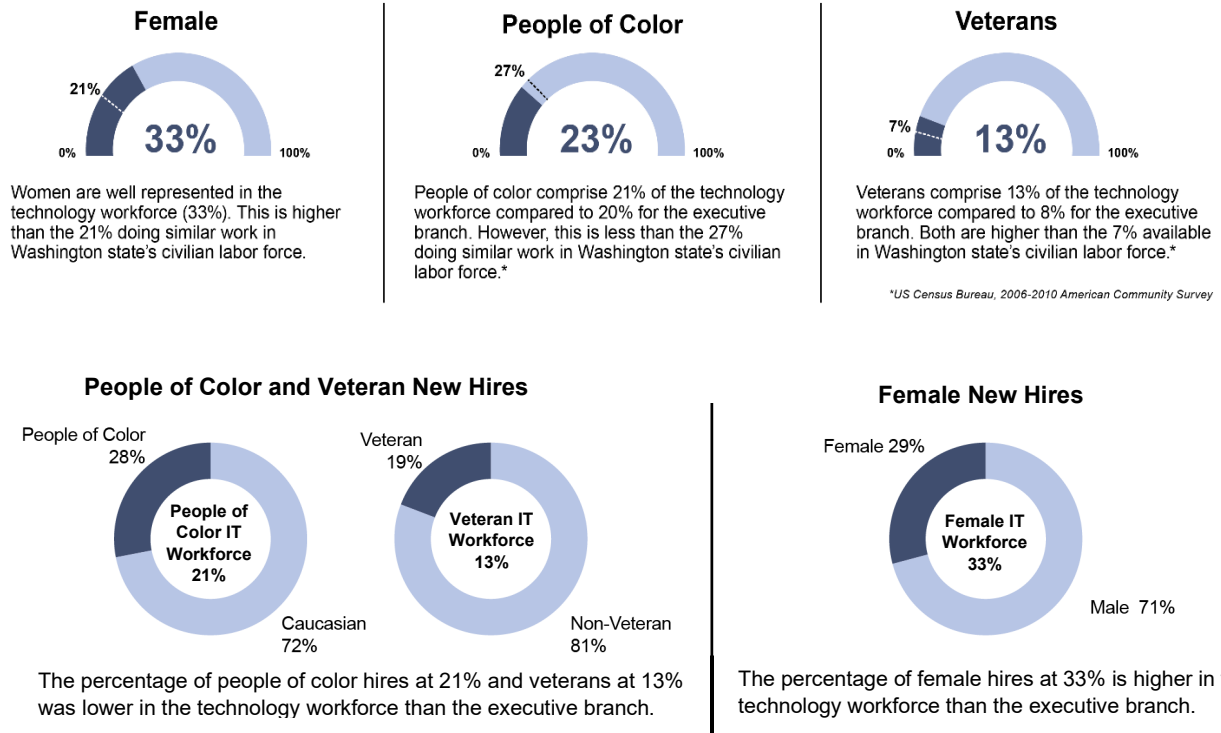
Figure 32: IT workforce versus executive branch and civilian workforce.

Work-life balance is important to employees. Therefore, offering flexible work options is a valuable retention strategy. Figure 33 is a comparison of the executive branch workforce flexible work hours against the executive branch IT workforce as of June 2019.

PARTICIPATION IN FLEXIBLE WORK HOURS

	Telework Rate	Flextime Rate	Compressed Workweek Rate
IT Workforce	18%	51%	31%
Executive Branch Workforce	9%	37%	23%

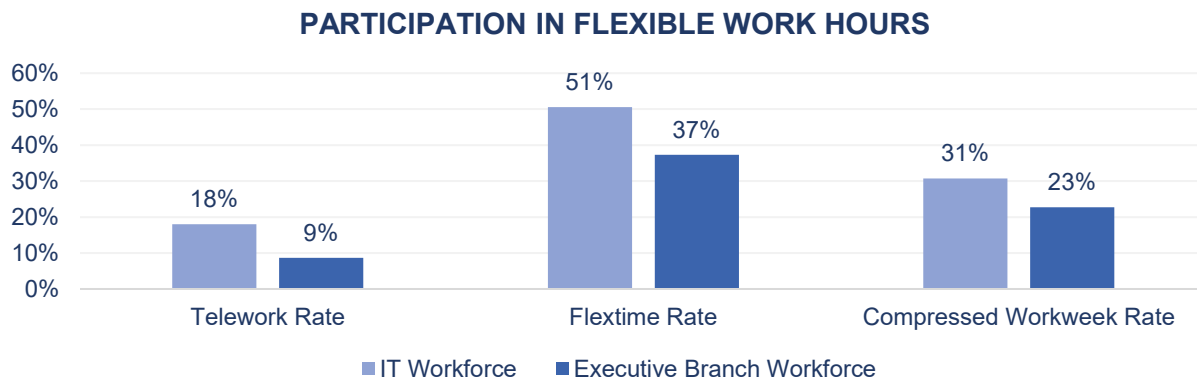■ IT Workforce   ■ Executive Branch Workforce

Figure 33: Flexible work hour participation as of 6/30/2019.

SECTION 7: ENTERPRISE ARCHITECTURE
(RCW 43.105.265)

Guidance and structure through technology policy and enterprise architecture

The OCIO helps advance statewide best practices by setting and updating state technology policies that are a critical component of the enterprise architecture. The policies improve accountability by providing guidelines and expectations for state agencies and help the state enterprise run more smoothly. New and updated policies reflect changes in the industry, the law, public expectations and advances in technology.

Enterprise architecture

Enterprise architecture (EA) (RCW 43.105.265) translates business vision and strategy into effective enterprise change.

EA helps show how information, business and technology work together to accomplish the state's business objectives. It is especially important to help guide the state in the adoption of new technologies such as the cloud, Internet of Things (IoT), machine learning and other emerging technologies that will drive the digital transformation of government services.

On a statewide basis, EA uses structured practices to analyze, plan and oversee the transformation of technology strategies and policies over time and to assist agencies to implement IT investments that achieve desired business results.

The OCIO increased staffing of the state Enterprise Architecture program in the final months of fiscal year 2019 to lead a collaborative, business outcome driven approach to EA, focusing on enabling statewide digital transformation.

The program's FY18-19 priorities included:

- Working with One Washington and the Health and Human Services coalition to define technical requirements and priorities.

- Evaluating agency reported projects for strategic alignment and the potential for sharing and reuse. Special emphasis was made to identify administrative and financial functions in scope of the One Washington program in order to minimize duplication and growth of shadow systems.

- Initiating a statewide cloud computing readiness assessment, as required by ESHB 1109. This assessment will be delivered in 2020.

- Tasking the State Enterprise Architecture Resource Team (SEART) – an OCIO-led, multiagency group of IT architects – to analyze strategic issues and develop IT policies, standards and guidelines.

  Key SEART achievements in FY19 include:

- o Washington State Architecture Handbook**:**

  - ▪ An online resource for architects that promotes the alignment of technology solutions with the state Enterprise Technology Strategic Plan and associated statewide technology strategies.

  - ▪ Key topics addressed by the handbook include: Establishing a data governance program; system integration strategy and guidelines; and recommendations for IPv6 migration.

- o Washington State Enterprise Technology Dictionary:

  - • Establishes a common technology vocabulary for state agencies based on standardized terms and definitions.

Identify common business practices, solutions and technologies

One of EA's major value propositions is that the enterprise achieves significant value by sharing and reusing common solutions and strategic resources.
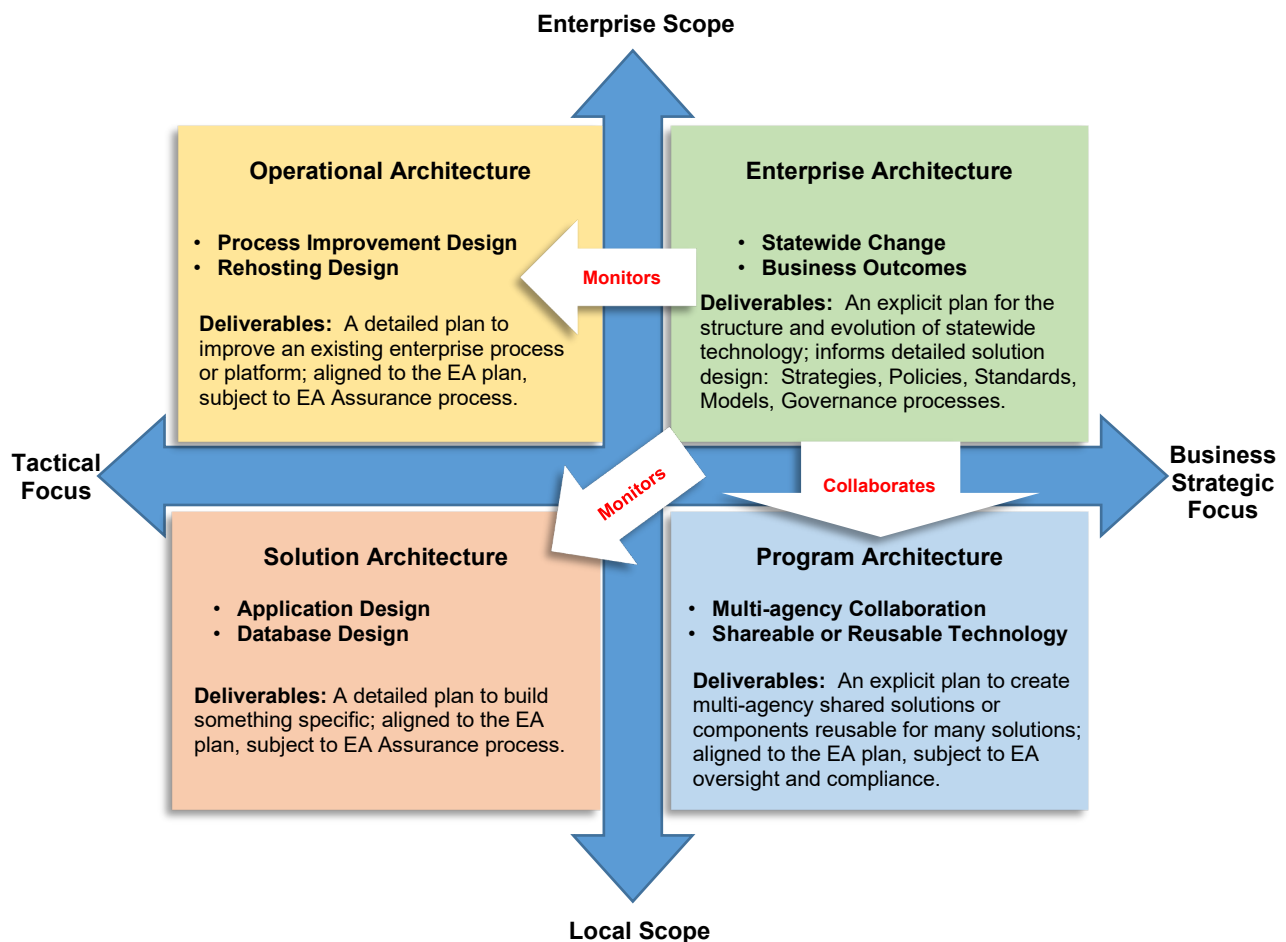

Figure 34: Enterprise Architecture Scope and Focus.

OFM's One Washington project is an example of a strategic-focused Program Architecture (see Program Architecture in Figure 34). One Washington is working to replace several obsolete legacy systems with a modern integrated Enterprise Resource Management (ERP) solution to serve the back-office administrative and financial needs of all

ONE WASHINGTON
ADMIN/FINANCE ASSESSMENT TREND

Figure 35: Statewide project assessments to determine administrative or financial.

agencies. As agencies submit new IT project proposals, the OCIO conducts an analysis to determine if the proposed solution has an administrative or financial component that is within scope of the One Washington program. In FY18-19, approximately 20% of new project proposals fell into this category (see Figure 35). The OCIO and One Washington worked with these agencies to adjust plans and eliminate unnecessary duplication where possible.
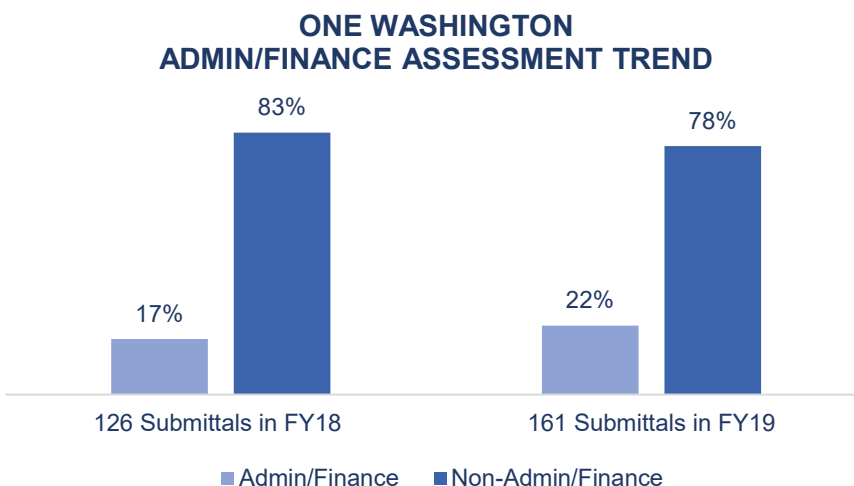
Other strategic efforts underway in FY18-19 include:

- **IPv6** - Developing a statewide strategy to migrate to the next generation Internet Protocol version 6 (IPv6), before it becomes difficult to do business with external partners who have already converted.

  The internet operates by transferring data between networks in packets. In order to communicate and send/receive packets of data, each device connected to the network must be identified by a unique internet protocol (IP) address. Since the early 1980s, Internet Protocol version 4 (IPv4) has been the international addressing standard.

  By 2015, the American Registry for Internet Numbers (ARIN) had run out of IPv4 addresses to allocate. Likewise, the state of Washington has depleted its allocation of IPv4 addresses. Some agencies have been reduced to purchasing reclaimed IPv4 addresses at auctions. This approach is an expensive and uncertain stopgap. Full conversion to IPv6 is the only long-term solution. The longer the conversion takes, the greater the risk to conducting business with external partners, including the U.S. government which mandated federal agencies convert to IPv6 in 2012.

  To reduce these risks, the following measures were implemented in FY18-FY19:

  - Policy 300: Requires agencies to have an IPv6 migration plan by December 2020 and to fully migrate to IPv6 by December 2025. The

policy also established a requirement for all new IT investments, acquired or developed, to be IPv6 compliant.

- o [Policy Standard 185.20](#): Designates the business processes associated with Internet Protocol (IP) address management as an enterprise service. In compliance with 185.20, the state acquired a massive IPv6 address space and began allocating those addresses to agencies on request as they began planning their network conversions. Several multi-agency training forums were provided to educate agencies about IPv6 and to set deployment guidelines.

- o WaTech began upgrading network and security equipment on the state backbone in preparation to support IPv6 traffic by 2021.

- **Identity and access management (IAM) - Cloud-integrated architecture:** The core of this strategy is the recognition of the importance of a single identity store for internal users – the Enterprise Active Directory. As technology matures and adapts, the need for a 'single source of truth' for internal users will remain a key part of the strategy.

  Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. It addresses the mission critical need to ensure appropriate access to resources across increasingly diverse technology environments and to meet increasingly rigorous compliance requirements. A mature IAM infrastructure can reduce identity management costs and, more importantly, significantly improve agility in supporting new business initiatives.

  In FY19, the state took a giant step forward to enabling broad adoption of cloud-based applications and a more mobile-friendly infrastructure. The state's primary IAM platform, Enterprise Active Directory (EAD), was integrated with Microsoft's cloud identity service, Azure Active Directory (AAD). This EAD/AAD hybrid service enables state employees to have a common user identity for authentication and authorization both on-premises and in the cloud. This provides a secure single sign-on user experience to a multitude of Microsoft and other vendor's cloud-based services including those hosted in the state's enterprise shared Microsoft tenant, such as Office 365.

- **Microsoft Office 365:** Adopting a shared tenant model for Microsoft Office 365 and related cloud-based products and technologies.

  By the close of FY19, the state's enterprise Office 365 Shared Tenant hosted 48 agencies, more than 16,000 users and adoption was growing. Pilot projects were running to move the state's shared services email and Skype services from the legacy on-premises environment to the Office 365 Shared Tenant with full migration scheduled to begin by year-end 2019.

- **Securing external access to agency applications:**

  The state uses Secure Access Washington (SAW) to provide secure external access to multiple agency applications. While allowing self-administered access to known users, SAW also helps shield the service from harmful activity. Over 230 agency applications allow external access through SAW and the number of external customers using the service increased to 6.4 million during this timeframe.

  A new user interface completed in 2018 reduced calls to the help desk by 70% while introducing multi-language support and improved functionality for agencies.

TOTAL USER NAMES BY MONTH
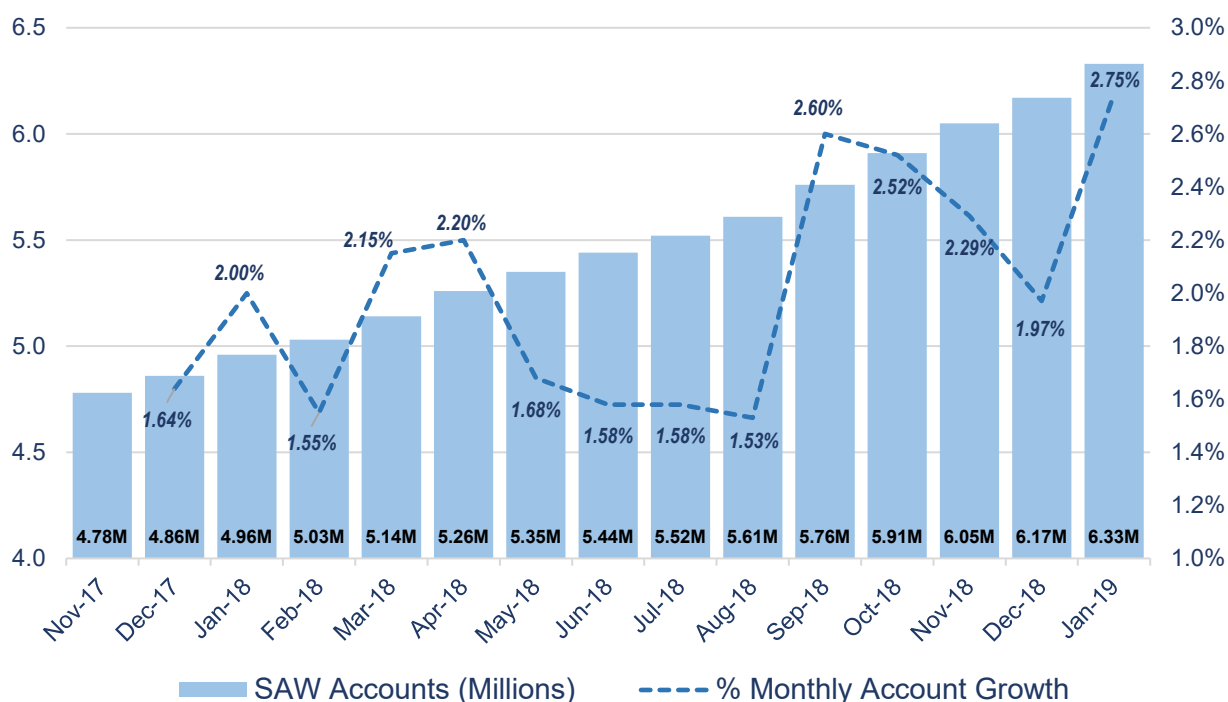
Figure 36: Monthly growth of SAW user names.

- **Continuing convergence of data, voice and video network in a single IP infrastructure:**

  Convergence refers to the merging of multiple IT infrastructures so that the State Government Network (SGN) carries all data, regardless of type. With VoIP telephony systems, voice is just plain data. The amount of network capacity required for voice is insignificant when compared to the overall flow of data, which means voice traffic gets a free ride on the existing network. While saving network cost is a significant driver, the main business benefit is adoption of new

integrated applications such as unified communications, integrated messaging, voice-enabled applications, internet telephony and desktop video conferencing.

Upgrades and enhancements to the SGN continued in FY18-19 to ensure the converged network is secure, robust and reliable enough to deliver mission-critical voice communications. The state's central shared telephone service continues the transition to fully support VoIP and agencies replacing legacy telephone equipment at a steady pace. Full conversion to VoIP is still years away as many agencies struggle with the cost of replacing their legacy equipment.

Coalitions governance

Washington is making strides toward finding common IT solutions that will work for multiple programs instead of each agency pursuing funding for individual projects. Model state coalitions that provide common IT solutions include the Geospatial Coalition and the Washington Health and Human Services Enterprise Coalition (HHS Coalition).

The Geospatial Coalition:

This coalition has been in place for over 15 years. Forty state agencies use geographic information systems (GIS) for state services such as registering to vote, emergency 911 and supporting vulnerable populations.

Using GIS data requires specialized systems and experienced staff. Coalition members have developed a mature governance structure to maximize investment and streamline services. Shared services are coordinated through the state Geospatial office in the OCIO with the support of partner agencies.

GEOSPATIAL COALITION MEMBERS:

- County Road Administration Board
- Department of Transportation
- Archeology and Historical Preservation
- Legislative Service Center
- Department of Commerce
- Liquor and Cannabis Board
- Department of Ecology
- Military Department
- Department of Fish and Wildlife
- Parks and Recreation Commission
- Department of Labor and Industries
- Recreation Conservation Funding Board
- Department of Natural Resources
- Superintendent of Public Instruction
- Department of Social and Health Services
- Utilities and Transportation Commission
- Higher education universities

Work done during the past biennium includes:

- **Washington Master Addressing Services (WAMAS):** In 2019, over 223 million addresses (street, building, parcel, etc.) were processed using this service, which is available through the state GIS program. Over 19 agencies are using these services to correct an address to United State Postal Service (USPS) standard format, with

plans to onboard more in the next biennium. Based on cost for these services from third-party vendors, the state sustained an estimated $500,000 cost avoidance by using this shared service.

- **Geographic information portal:** For the past two years, the state of Washington GIS community has used a single portal to share geographic information: geo.wa.gov. This portal enables agencies to examine shared data, confirm its accuracy and allows others to reuse the information as appropriate. This saves time and effort when all agencies are referencing the same data. The public and agencies used this service more than 227,000 times to access geospatial data in 2019. During the next biennium, the GIS community will be creating a method for sharing data among state agencies for data considered more sensitive (Category 2 and 3 information).

- **LIDAR:** Washington developed its first statewide light detection and ranging (LIDAR) plan in 2018-1019. LIDAR is used throughout the state by local, state, federal and tribal partners to identify landslides, flooding potential, evaluate watersheds for salmon habitat restoration and analyze patterns in land use for urban areas. With over 65 stakeholders participating in reviewing and providing input to the plan, it reflects a variety of needs across the state in a unified vision.

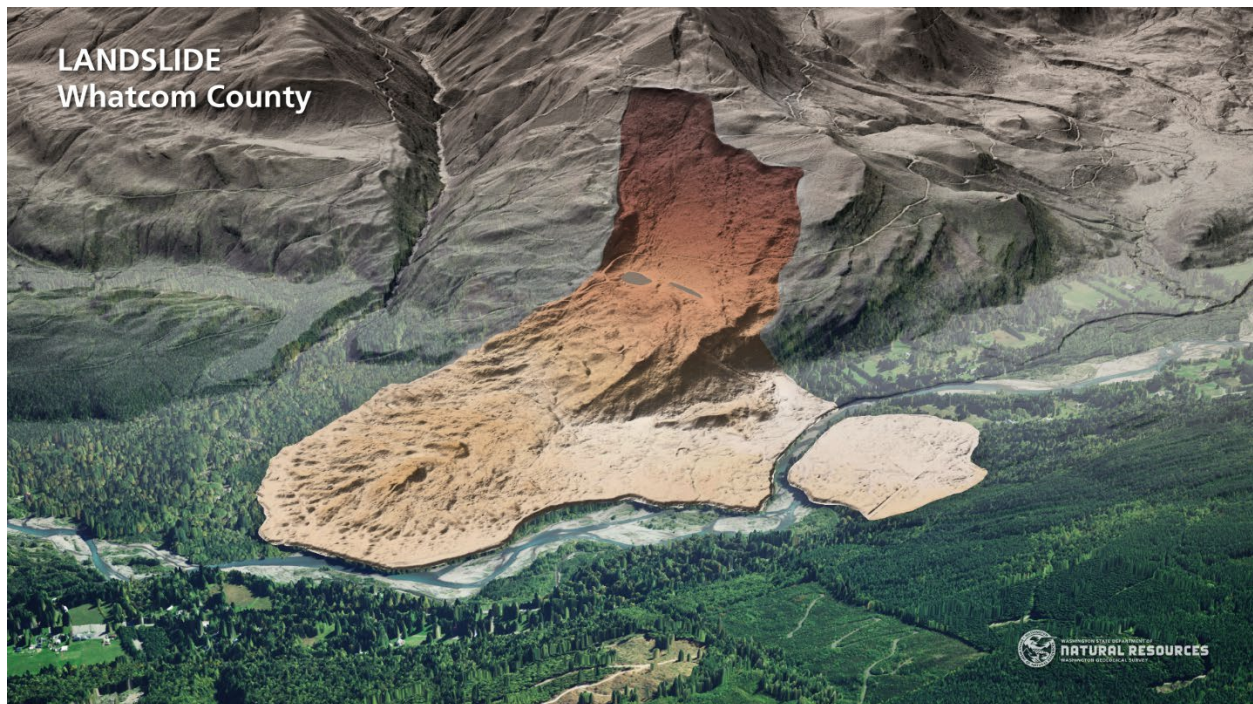*Figure 37: Lidar image of Racehorse Slide available through Washington Department of Natural Resources.*

- **GIS dashboard:** Adding more public access to agency data. The state Geospatial Coalition also developed a simple application and dashboard to use among agencies and with the public to alert users to changes in the data. It is difficult to rely on data stored and maintained by another organization if they can change data

structures or remove the data entirely without notice. To allow better sharing and hosting of the data and minimizing duplication, the state agencies developed an alert system that allows notification of proposed changes.

- **Washington State Ferries:** Washington State Ferries is currently using mobile mapping (GIS) tools to complete a business process improvement for reporting marine mammal locations near ferry terminal construction projects. The new system that integrated GIS replaced over 5,000 paper submissions that were manually added to Excel and reported to NOAA adding up to an estimated 1,500 hours saved of data entry each season.

Not only does the system save effort, it also helps Washington State Department of Transportation protect Southern Resident Orcas and other marine mammals.

- **Department of Labor and Industries (LNI):** The agency developed applications and mapping that provides detail of their buildings down to the cubicle level. They are able to locate emergency equipment such as fire extinguishers, AEDs as well as more efficiently finding people and conference rooms for face-to-face meetings. The system links to the HR system so that a person can be identified by the location along with information regarding email, phone and Skype

connections. As teams move locations, they can ensure that space is available for new team members as well as determine other uses for vacant space within their buildings.

Washington Health and Human Services Enterprise Coalition:

The HHS coalition provides strategic direction and federal funding guidance for IT projects that have cross organizational or enterprise impact.

One example of a coalition enterprise-wide project moving forward is a master person index (MPI). A MPI is a database that agencies would use to maintain accurate personal data across all the

HHS COALITION MEMBERS:

- Department of Health
- Department of Social and Health Services
- Health Benefit Exchange
- Health Care Authority
- Department of Children, Youth, and Families.
- Office of the Chief Information Officer*
- Office of Financial Management*

*(*Serve as ex-officio members)*

various systems regardless of which agency operates them. Users would be assigned a unique identifier so they are represented only once across all systems.

There is currently no MPI for external users. Each agency, and often each system, maintains external user data separately and the same person may have different or outdated information spread across many systems. This not only creates security risks but also a complex and frustrating experience for the user who must enter and maintain the same information in many different systems.

The HHS coalition has identified MPI as a priority and a foundational module for all future coalition endeavors. The OCIO enterprise architecture program has also identified MPI as an important element to modernize the state's legacy external IAM services (i.e., Secure Access Washington, or SAW). The HHS coalition and WaTech are collaborating to define an enterprise strategy and roadmap that will leverage the coalition's MPI efforts and evolve the service into the foundation for a next generation IAM infrastructure.

> **WHAT IS THE HHS COALITION GOVERNANCE MODEL?**
>
> **G1--Executive Sponsor Committee (Strategic Focus)** provides the mechanism by which HHS Coalition technology investments are vetted, approved, prioritized and monitored by providing strategic insight, cross-organizational project support and federal funding guidance.
>
> **G2--Enterprise Steering Committee (Operational Focus)** ensures business alignment and provides operational direction for HHS Coalition technology projects and governance processes in support of the Executive Sponsor Committee.
>
> **G3--Integrated Enterprise Project Group (Tactical Focus)** has a primary purpose to support cross-agency coordination on IT projects and the completion of analysis or work products required to support upstream decision making.

Adoption of cloud technologies

Washington State has long encouraged agencies to adopt cloud technologies and consider cloud-based services first before pursuing other options. For example, the Health Care Authority adopted a cloud strategy for their technology infrastructure and moved a large part of their system to Amazon Web Services (AWS). This type of cloud solution is known as Infrastructure-as-a-Service (IaaS).

Software-as-a-Service (SaaS) is another popular type of cloud solution. SaaS refers to a business application that is fully hosted and supported by a third-party provider and made available to consumers over the Internet.

One way to gauge SaaS adoption is by looking at the number of Active Directory Federation Services (ADFS) connections requested by agencies between the state's central identity management services and various SaaS providers. ADFS is used to provide state users
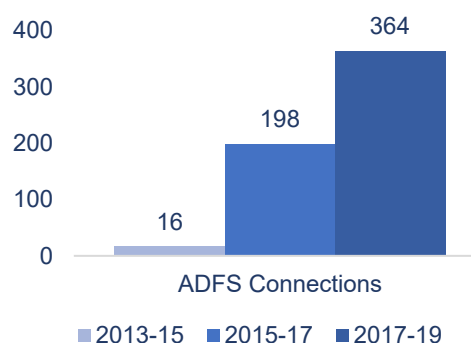

Figure 38: Trending statewide ADFS connections.

with single sign-on to SaaS applications. As shown in Figure 38, only 16 SaaS applications were connected in FY2015. In just four years, the number of SaaS applications with single sign-on integration had increased more than twentyfold. Now that the state's central identity management service, Enterprise Active Directory (EAD), is integrated with Microsoft's Azure Active Directory (AAD), single sign-on to SaaS applications is more streamlined and adoption is expected to increase at an even faster pace.

Cloud Highway: Robust dedicated access to public cloud services

As previously mentioned in the example of the Health Care Authority, agencies are making significant investments to move formerly on-premises servers and applications to cloud services operating in remote data centers that are hundreds to thousands of miles from Olympia. Many of these servers support mission critical applications. While cloud services are designed to be delivered over the public internet, that method can be highly unpredictable and impose more security and performance risks than some agencies are willing to accept.

To reduce performance and security risks, the state created a dedicated, high-performance segment of the State Government Network (SGN) that places the state's high-speed ethernet connection at the front door of cloud service providers like Microsoft and Amazon. This private "Cloud Highway" bypasses the public internet, thereby eliminating inherent security and performance risks while delivering quality service.

Some benefits of using the Cloud Highway vs. the public internet:

- Improved performance - Reserved bandwidth available for the most critical applications, i.e. Quality-of-Service (not possible with the public internet).

- Predictability and reliability – Always the shortest, fastest, most stable network with contracted service levels for the entire path to the cloud provider (not possible with the public internet).

- Flexibility – Freedom to choose on-premises, cloud or hybrid system designs and the potential for connections to more than 120 cloud providers.

- Security – Appropriate for category 3 and 4 classified data.

- Scalability – Easily scaled on demand to the required bandwidth.

- Cost efficiency – Reduces costs by sharing network and security infrastructure and reduced egress fees charged by cloud providers.

The Cloud Highway is a great example of agencies coming together to solve a problem. WaTech, the Department of Social and Health Services (DSHS) and the Health Care Authority (HCA) collaborated to create the highway. The HCA, which secured federal funds for the project, was the first agency to use the Cloud Highway to support movement of a considerable portion of its data center to Amazon Web Services. That

project would not have been as successful without the assured performance, reliability and security of the Cloud Highway.

Additional cloud-based projects completed during FY18-19 include:

- **Loan and Grant Portfolio Management System (LGPMS):** The Pollution Liability Insurance Agency (PLIA), a small agency with limited IT resources, successfully implemented a LGPMS system using Salesforce (PaaS) and a contracted vendor. Both vendors were secured through a state IT master contract. The solution met all projected benefits and was delivered on time and under budget.

- **Sexual Assault Kit Tracking System (SAKTS):** The Washington State Patrol (WSP) needed a system to implement Revised Code of Washington (RCW) 43.43.545 - Statewide sexual assault kit tracking system. The tracking system provides sexual assault survivors with the ability to anonymously track the location and status of their Sexual Assault Kit from the point of collection through forensic analysis to final storage location and possible destruction. SAKTS was implemented using a commercial software solution and deployed in the Microsoft Azure Government Cloud.

- **Business Management System replacement:** The Department of Services for the Blind (DSB) needed to replace their legacy business management system after receiving end of support notice from the vendor. DSB selected a commercial SaaS product that is operated by the vendor using the Microsoft Azure cloud.

- **Washington All Payer Health Care Claims Database (WA-APCD):** The Legislature directed the Office of Financial Management (OFM) to establish a statewide all-payer health care claims database. The data vendor created an analytic enclave using the latest cloud storage technology from Amazon Web Services. This enabled users to access the permitted WA-APCD data products and maintain data security and run large queries that would be difficult to execute on local machines. The project was delivered on time and budget.

- **Risk Management Information System (RMIS):** The Department of Enterprise Services (DES) needed to replace an obsolete, unsupported system that was becoming increasingly vulnerable, difficult to use and prone to failures. DES successfully implemented a new RMIS system using a cloud-based, SaaS product that had been successfully implemented in several other states.

- **Electronic Medical Record - Long Term Care:** The Department of Veterans Affairs (DVA) provided a cloud-based SaaS electronic medical record system to all Washington state DVA nursing homes and the DVA central office within 24 months (a year early) and under budget.

SECTION 8: SECURITY & PRIVACY (RCW 43.105.215 & RCW 43.105.369)

Securing government services through cybersecurity

The state of Washington made strategic investments and leveraged federal dollars during the past biennium to help secure public data entrusted to government agencies.

In the FY17-19 biennium, the state spent approximately $111 million dollars on information security for executive branch agencies – approximately 5.1 percent of all executive branch IT expenditures for the year. That figure excludes higher education, judicial and legislative agencies.

FY18-19 SECURITY SPEND BY COST POOL
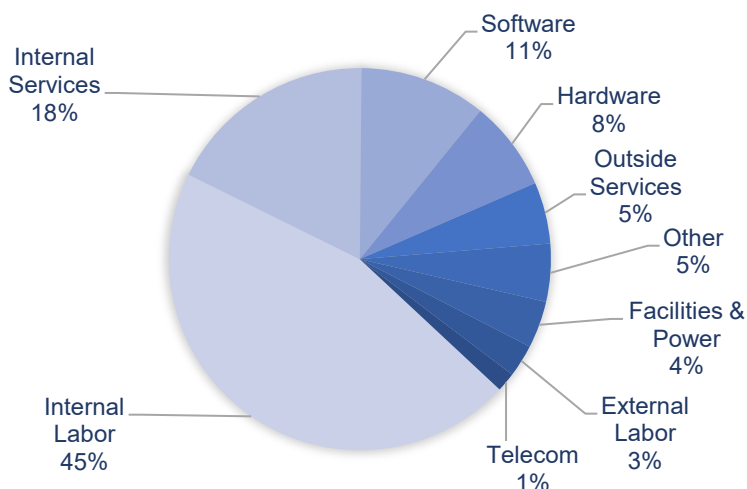
Figure 39: FY18-19 security spend by executive branch agencies.

Thirteen agencies make up 86 percent of all security expenditures in the executive branch. (See Figure 40)

FY18-19 SECURITY INVESTMENT - TOP 13 AGENCIES
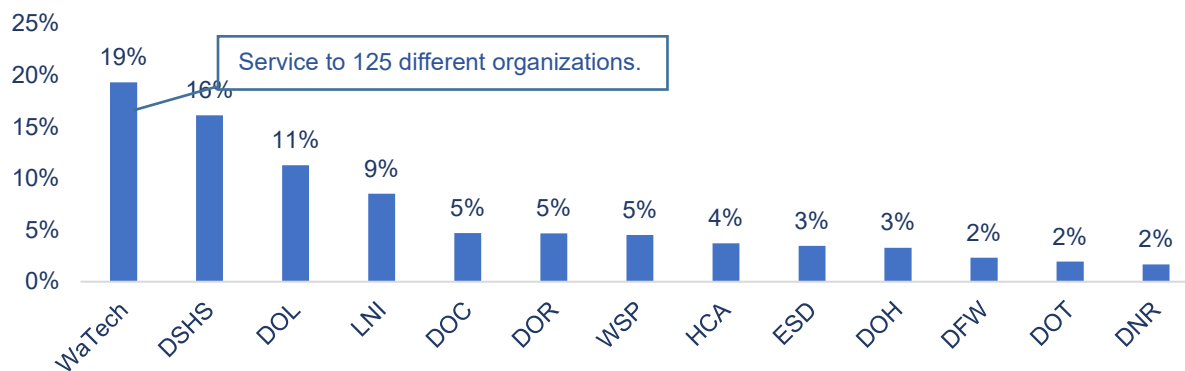
Figure 40: Top 13 executive branch agency security expenditures.

WaTech, which provides information security services to more than 125 organizations as the state's central IT services agency, accounted for approximately 19 percent of IT security expenditures. The rest was distributed across multiple agencies – a reflection of the state's federated environment.

These investments have helped protect the state against cyber threats that, in other parts of the country, have severely disrupted the business operations of state and local governments as well as private organizations, costing millions of dollars. Recent governments impacted include Atlanta, Baltimore and the state of Louisiana.
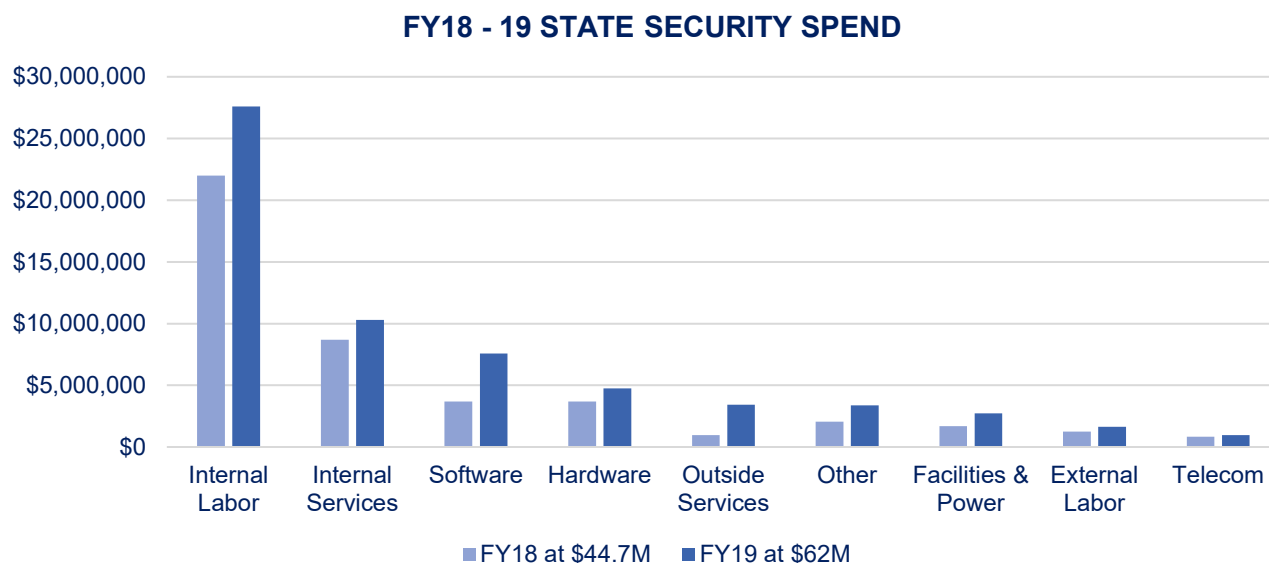
FY18 - 19 STATE SECURITY SPEND

Figure 41: Trending security expenditures by cost pool.

However, more needs to done. Cyber threats continue to increase in volume, sophistication and severity. Ransomware damages globally jumped from $325 million in 2015 to an estimated $5 billion in 2017.

In the first quarter of 2019 alone, ransomware attacks grew by 118%, according to McAfee, a global cybersecurity company. Public organizations were one of the most targeted sectors overall for cyberattacks.

In Washington state, the total number of data breaches reported to the state Attorney General's Office increased by nearly 20% in 2019, with just over 70% resulting from a malicious cyberattack. No state agency data breaches were reported in 2019 that resulted from a cyberattack

Security investments during the past biennium included:

- **Secretary of State's office**: The office secured $7.9 million in federal grants along with a five percent match in state funding to partner with county election offices, safeguard the 2020 elections and for work on the vote.wa.gov website. The office also partnered with the Washington National Guard to assess the security of the new elections system and created a Security Operations Center to guard the elections system against cyber threats.

- **WaTech:** Application attacks continue to be on the rise as more and more cyberattacks are targeting flaws in pubic facing applications to gain entry into an organization's network. The state Office of Cybersecurity (OCS) received funding in the past biennium to provide secure coding training for state developers and to procure tools that will test for potential vulnerabilities in applications. OCS held training sessions in October 2018 as part of a pilot phase for the Web Application and Certification Program (WACAP). The program is aimed at enhancing the security of sensitive state data by helping agency developers identify and correct coding vulnerabilities when building web applications. Moving forward, OCS will procure tools and combine application scans and secure code reviews as part of the larger vulnerability management program being established within the State Office of Cybersecurity.

Other significant statewide cybersecurity initiatives:

- **Hacktober:** WaTech is continuing to expand and improve the OCS annual "Hacktober" cybersecurity awareness campaign for state employees held during the month of October as part of the National Cybersecurity Awareness Month. Thousands of state employees took part in this year's Hacktober campaign, which included a new online quiz, an improved cybersecurity escape room, a "careless cube," and a series of presentations all aimed at increasing awareness of growing threats online.

  The results:

  - State workers completed nearly 14,000 online cybersecurity quizzes.

  - More than 250 people on 51 teams from 24 state agencies experienced the Hacktober escape room, which reinforces best cybersecurity practices.

  - About 180 state workers checked out the careless cube at the 1500 Jefferson Building in Olympia, which educates people on common security mistakes at the workplace.

  - There also was significant participation in person and online for Hacktober security presentations.

- **National Cybersecurity Review (NCSR):** The state has partnered with the Department of Homeland Security (DHS) and the Multi-State information Sharing and Analysis Center (MS-ISAC) to allow state agencies to meet their annual state security assessment requirements by participating in the 2019 Nationwide Cybersecurity Review. The NCSR is a confidential, no-cost annual self-assessment designed to measure gaps and capabilities of state, local, tribal and territorial governments' cybersecurity programs. During the period of October through December 2019, agencies will submit responses to this survey. The NCSR results will enable the state to establish a risk-based baseline of its

security posture and help agencies gain insight into their cybersecurity gaps and capabilities.

- **State Auditor's Office (SAO):** OCS and the SAO have established regular meetings to identify and address high-risk security issues that are common across state agencies. Working together, SOA performance audit objectives can be tailored to assess agencies' capabilities in addressing these risks, and OCS can enhance state IT security policies and standards to help agencies harden their defenses against threats.

- **Washington Cyber Intelligence Exchange, WaCIX:** The exchange was launched earlier this year to keep state of Washington agencies, counties and cities more informed of the cybersecurity threat landscape. Membership is open to any Washington state agency, county or city that wants to be part of the WaCIX threat intelligence sharing community. The exchange allows members to share information with each other about cyber threats they are seeing, and receive daily intelligence briefings from the state Office of Cybersecurity.

Statewide privacy: policy and law

The state Office of Privacy and Data Protection worked to educate the public on privacy issues by creating a curated information website and training to state and local employees.

Accomplishments during the biennium include:

- The Privacy Office's open source web application, [Privacy tips, tools and checklists](#), launched in July 2018 with support from the Hewlett Foundation. Designed for privacy officers throughout government and beyond, it helps organizations work through challenges by following simple checklists – many contributed by privacy professionals in mature organizations across the Northwest.

- Privacy training for state and local government employees was a priority and collaboration with the State Library brought privacy training to public libraries around the state and online in 2018. The Privacy Office and Department of Licensing partnered to lead an agency-wide training initiative and virtual courseware developed by Department of Enterprise Services. During the past two years, 741 state and local employees have reported completion of privacy training.

Major legislative packages on privacy came to the public forefront during the biennium in Washington state and worldwide. The state Office of Privacy and Date Protection focused its resources on studying, improving and explaining these major changes.

- [General Data Protection Regulation](#) **(GDPR):** The GDPR went into effect in Europe in 2018. The landmark regulation recognizes that Europeans have broad and usable rights to control how data about them is processed and used. The

Privacy Office researched GDPR and helped explain its provisions and significance to state agencies, local governments and Washingtonians.

- The Washington Privacy Act (SB5376) was introduced in the 2019 legislative, adapting European privacy law to Washington state requiring testimony from the state's Chief Privacy.

- California Consumer Privacy Act **(CCPA):** The CCPA was signed into law in June 2018, and as of January 1, 2020 will require organizations that collect or process personal information of Californians to respect certain rights. These rights include the right to disclosure of data, the right to prohibit sale, and the right not to face discrimination when they choose to exercise their personal data rights.

SECTION 9: IT STRATEGY NEXT BIENNIUM

State priorities for the next biennium

The state IT strategy needs to support and improve the way government services are delivered to Washingtonians. Maturing the state's strategy helps support the commitment to utilizing technology to breakdown organizational silos, provide opportunities 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:

Foundational digital government technologies: Investing in foundational digital government technologies as well as testing some emerging technologies that are integral to advancing the digital government vision:

- Data architecture standards, managed application program interfaces (APIs), open data principles and privacy standards.

- Advanced data analytics.

- Modular architecture and micro services, including encapsulating services and exposing Application Programming Interfaces (APIs) at multiple levels and across organizational boundaries.

- Government cloud computing and cloud office.

- Cloud-optimized networks; IPv6; cloud access security brokers (CASB). A cloud access security broker sits between cloud service users and cloud applications and monitors all activity and enforces security policies.

- Identity management; citizen digital ID.

- Block chain for government.

- Artificial intelligence (AI), chat bots, predictive analytics and machine learning.

Cloud strategy: Led by the OCIO in collaboration with executive branch agencies, define a statewide government cloud computing strategy, including:

- Complete the statewide cloud computing readiness assessment and delivering the final report to the governor and Legislature as required in statute.

- Define a pragmatic and balanced approach to government cloud computing based on sound principles of business and technical benefits and fiscal responsibility.

Major IT Projects: Improving the success rate of major IT projects by updating policies and refining oversight processes for project management, transparency and technical architecture.

For example:

- Publishing the new IT Major Project Dashboard which includes improved financial reporting and more graphical analysis (completed January 2020).

- Standardizing a major projects identification, approval and oversight framework and methodology.

- Advancing statewide IT portfolio management practices with increased levels of detail in data capture, analysis and reporting for applications, infrastructure and projects.

- Refining the state's enterprise architecture (EA) processes and metrics; engaging agencies in collaborative efforts to identify enterprise priorities and establish a common vision for digital government transformation.

- An update to the statewide technology strategic plan.

Modernization and transformation: Supporting strategic transformation and modernization programs important to advancing statewide digital government strategies such as:

- The Health and Human Services coalition priority projects developed as part of a strategic, modular architecture to provide reusable enterprise services:
    - Master Person Index project.
    - Integrated Eligibility project.

- OFM - One Washington program to replace the state's decades old financial and administrative applications with a modern enterprise resource planning (ERP) solution.

- Statewide strategic infrastructure modernization projects, including:
    - Transitioning the state's shared mainframe computing platform to mainframe-as-a-service.
    - Enhancing the state's current network infrastructure and enabling IPv6 for all agencies.
    - Modernizing the state's identity and access management infrastructure to leverage new technologies and cloud-hosted capabilities.
    - Continuing transition of agencies' on-premises data centers by consolidating to the State Data Center (SDC) or migrating to cloud-hosted solutions.
    - Enhancing the state's resilience and recovery options by moving to cloud-based disaster recovery services.

Cybersecurity: WaTech's state Office of Cybersecurity, which sets statewide strategy for information security, plans to move forward in several areas during the next biennium:

- **Evaluate:** Assess our security posture through contextual risk analysis.

- **Educate:** Educate our workforce and community. Also bring in industry experts and apply those lessons to the business environment.

- **Engage:** Increase efforts to engage with public and private partners to share actionable threat intelligence. Provide more table top exercises to help train agencies how to respond to security incidents. Collaborate with K-12 organizations to help train the next generation of cybersecurity professionals. Hold a cybersecurity summit in 2020.

- **Advance:** Take advantage of advances in artificial intelligence and predictive analytics to help the state protect the myriad of entry and exits points in the government network. Focus attention on third party vendors and what protections they have in place to protect state data.

- **Measure:** Switch focus away from the number of attacks blocked to the actual risk of intrusion. In other words, which attacks are making their way through initial layers of defense and how is the state mitigating those intrusions.

Studies indicate the average time from the occurrence of an incident to the time of detection is approximately seven months. Over the last five years, industry reports on data breaches indicate that 70% of the attacks exploited known vulnerabilities. It is imperative for the state to detect vulnerabilities in its infrastructure, which includes network components, servers, workstations and databases. Funding allocated by the state Legislature for the 2019-21 biennium will enable WaTech to replace the current vulnerability assessment (VA) scanning platform with a platform and service that enables agency security teams to identify and remedy the vulnerabilities in near real-time.

Benchmarking Washington state strategies nationwide: Over the last three years, CIO's across the United States reported to National Association of State Chief Information Officers (NASCIO) their top ten strategies for management processes, solution, application and tools. This compilation of strategic priorities is insightful as Washington establishes priorities and comparison across other states.

NASCIO TOP TEN STRATEGIES, MANAGEMENT PROCESSES AND SOLUTIONS

Category for Ranking	2017 Top Ten	2018 Top Ten	2019 Top Ten
Security and Risk Management	1	1	1
Cloud Services	3	2	2
Consolidation/Optimization	2	3	3
Digital Government		4	4
Broadband/Wireless Connectivity	10	7	5
Budget, Cost Control, Fiscal Management	4	5	6
Customer Relationship Management			7
Data Management and Analytics	7	8	8
Enterprise IT Governance	6	9	9
Identify and Access Management			10
Legacy modernization	5		
Shared Services		6	
Enterprise Vision and Roadmap for IT	8		
Agile and Incremental Software Delivery	9	10	

NASCIO TOP TEN TECHNOLOGIES, APPLICATION AND TOOLS

Category for Ranking	2017 Top Ten	2018 Top Ten	2019 Top Ten
Cloud Solutions	2	1	1
Security Enhancement Tools	3	3	2
Legacy Application Modernization/Renovation	1	2	3
Business Intelligence (BI) and Business Analytics (BA)	4	5	4
Identity and Access Management	5	4	5
Collaboration Technologies			6
Data Management	6	6	7
Enterprise Resource Planning (ERP)	9	7	8
Disaster Recovery / Business Continuity	7	8	9
Networking	8	10	10
Customer Service/CRM	10	9	

APPENDIX A

2018-19 AGENCY TECHNOLOGY PROJECT ASSESSMENT SUBMITTALS				
Agency Name	**FY2018**	**# to Oversight**	**FY2019**	**# to Oversight**
Accountancy, State Board of	1		2	1
Administrative Hearings, Office of			1	
Agriculture, Department of	1			
Arts Commission, Washington State			1	
Attorney General, Office of the			1	1
Auditor, Office of the State	1		1	
Blind, Department of Services for the	1	1		
Caseload Forecast Council	1			
Centralia College	1			
Childhood Deafness and Hearing Loss			2	
Consolidated Technology Services	10		18	3
Corrections, Department of	8	1	4	1
County Road Administration Board	1	1		
Department of Early Learning	2	1		
Department of Ecology	3	2	6	
Employment Security Department	8	2	1	1
Enterprise Services, Department of	1	1	1	
Financial Management, Office of	2	1	3	2
Fish and Wildlife, Department of	3	2	5	2
Freight Mobility Strategic Investment Board	1			
Gambling Commission, State			2	1
Health Benefits Exchange, Washington	1	1	2	2
Health Care Authority, State	9	4	1	
Health, Department of	9	4	12	4
Historical Society, Eastern Washington State			1	
Historical Society, Washington State			2	1
Human Rights Commission			1	1
Industrial Insurance Appeals, Board of			1	1
Insurance Commissioner, Office of the			1	
Labor and Industries, Department of	3		8	7
Legislative Evaluation & Accountability Program Committee				
Licensing, Department of	5	2	7	2
Liquor and Cannabis Board	1	1	2	2
Military Department	1			

Agency Name	FY2018	# to Oversight	FY2019	# to Oversight
Minority and Women's Business Enterprises, Office of			1	
Natural Resources, Department of			3	
Parks and Recreation Commission, State	5		6	1
Pollution Liability Insurance Agency			2	1
Public Disclosure Commission	1			
Puget Sound Partnership	1		1	
Recreation and Conservation Funding Board	7		7	1
Retirement Systems, Department of	1		1	1
Revenue, Department of	1	1	3	1
Social and Health Services, Department of	12	1	15	5
Student Achievement Council	3		2	1
Superintendent of Public Instruction	6	3		
Transportation, Department of	5	2	16	5
University of Washington	5	1	4	2
Utilities and Transportation Commission	1			
Veterans' Affairs, Department of			3	
Volunteer Firefighters and Reserve Officers, Board for	1	1		
Washington State Patrol	2	2	8	4
Western Washington University	1		1	
Workforce Training and Education Coordinating Board			2	
TOTAL	**126**	**35**	**161**	**54**