

ANALYSIS

Item 6: Public Defense Services Commission Information Technology Contract Extension and Report

Analyst: John Borden

Request: Increase General Fund by \$463,011 for an information technology contract extension and the reimbursement of an information technology consultant report.

Analysis: The Public Defense Services Commission (PDSC) is requesting \$413,011 General Fund to continue the procurement of information technology services from the Oregon Judicial Department (OJD) for the second fiscal year of the 2021-23 biennium and \$50,000 General Fund for the reimbursement of an information technology report.

Background

PDSC's Information Technology Section was disbanded administratively by the agency in December of 2019. Thereafter, PDSC became dependent on an external contract with the OJD for information technology support. The Legislature was never consulted on this decision nor PDSC's repurposing of the agency's Information Technology Section's positions. Of note is that PDSC also has had a long-term contract with OJD for servers, network infrastructure, and related technical services.

Legislative Instruction (2021)

The reestablishment of information technology services for PDSC is viewed as critical to the public defense system and foundational for PDSC to move to a new financial and case management system, which is why it was a funding priority of the Legislature. A financial and case management system is seen as vital to addressing many of the deficiencies identified in the Sixth Amendment Center study of the right to counsel in Oregon (2018) as well as the concerns of the Legislature.

The Legislature in 2021, as part of an overall reorganization of PDSC, directed the reestablishment of the Information Technology Section with the explicit understanding that PDSC's contract with the OJD would be terminated on June 30, 2021 (HB 5030). PDSC's 2021-23 legislatively adopted budget includes \$1.1 million of General Fund for four permanent full-time positions (2.88) to reestablish the Information Technology Section. For this transition, PDSC received all requested resources; however, the Legislature understood that additional resources would be required in the future.

Legislative Instruction (2022)

The Joint Interim Committee on Ways and Means (JICWM) in January of 2022 deferred a PDSC request for an information technology contract extension with OJD to the May 2022 meeting of the Emergency Board with instruction that the Commission report back with:

...a comprehensive information technology services plan and an assessment of the estimated costs, benefits, and risks of the alternative service-delivery methods, including both insourcing the agency's information technology function and outsourcing through external providers. With each alternative, the Commission shall describe how the security, privacy and confidentiality of data entered, processed or stored within the Commission's information systems will be assured.

The Legislature in 2022 authorized \$743,588 General Fund and two positions (1.26 FTE) for the re-initiation of the planning phase of the Financial and Case Management information technology project. As an aside, the Commission recently voted to establish an Information Technology Subcommittee of the Commission to help oversee the agency's information technology efforts.

Information Technology Report (April 2022)

After the JICWM in January, PDSC hired a vendor to complete an information technology service plan at a cost of \$50,000 General Fund. The plan was completed on March 8, 2022. The plan includes two major findings: (1) PDSC should pursue "a hybrid approach, in which IT status quo functions are outsourced to OJD while IT new development functions are insourced to PDSC;" and (2) the vendor saw "...no OCI [Organizational Conflict of Interest] issues with OJD handing of PDSC data."

In reaching these conclusions, the vendor report failed to examine other viable options for PDSC, such as the agency migrating its applications and data to a third party cloud service provider, acquiring third party base information technology support, or contracting for third party application development and support.

In summary, the vendor recommends that PDSC continue a contract with OJD to outsource information technology services (help desk, desktop support, servers, information security, network/telecommunicators, Microsoft 365/mobile support, and a web team), but insource the development of the Financial and Case Management information technology project.

Analysis

Given the legislative direction and investment in 2021 to support PDSC's information technology services, and considering the vendor's recommendations, the Legislature in 2023 will need to re-evaluate its investment in PDSC's Information Technology Section.

The Legislative Fiscal Office is not recommending the \$50,000 reimbursement for the vendor information technology study, as such a study could have been completed by the agency's Information Technology Section staff and the agency is able to continue to absorb the cost due to budget savings that have been reported to the Emergency Board.

Lastly, PDSC appears not to have coordinated the agency's request with OJD, as OJD may require Other Funds expenditure limitation associated with the contract extension, as only one fiscal year of budget authority was provided OJD by the Legislature in 2021 (HB 5012).

Recommendation: The Legislative Fiscal Office recommends that the Emergency Board allocate, on a one-time basis, \$413,011 General Fund to the Public Defense Services Commission, Administrative Services Division, for a one fiscal year contract extension with the Oregon Judicial Department for information technology support.

6
Public Defense Services Commission
Gibson

Request: Allocate \$0.5 million General Fund from the State Emergency Fund for continued use of Oregon Judicial Department Enterprise Technology Services Division services and report on comprehensive information technology services plans.

Recommendation: The Public Defense Services Commission is not under Executive Branch budgetary authority.

Discussion: The Public Defense Services Commission (PDSC) is requesting an additional \$413,011 General Fund to continue contracting with the Oregon Judicial Department Enterprise Technology Services Division (OJD-ETSD) for information technology services through the current biennium. PDSC currently has funding to support the contract through June 30, 2022. Additionally, PDSC is requesting \$50,000 for the cost of hiring an IT contractor.

A similar funding request was originally submitted to the January 2022 Joint Interim Committee on Ways and Means Public Safety Subcommittee. The Committee recommended PDSC resubmit its funding request to the May 2022 Emergency Board after completing the further analysis.

“The Commission [is to] report back with a comprehensive information technology services plan and an assessment of the estimated costs, benefits, and risks of the alternative service-delivery methods, including both insourcing the agency’s information technology function and outsourcing through external providers. With each alternative, the Commission shall describe how the security, privacy and confidentiality of data entered, processed, or stored within the Commission’s information systems will be assured.”

Upon receiving the recommendation, PDSC hired Elyon Strategies to evaluate the current IT service delivery model and provide two alternative models. The Agency is submitting the resulting PDSC IT Service Plan, Alternative Delivery Analysis report with the Agency’s funding request for committee review.

The IT report evaluated the security and integrity of PDSC data, a financial analysis of each alternative, and the potential conflicts of interest across the following three delivery models:

1. Full outsourcing of IT functions – services received from OJD;
2. Full insourcing of IT functions – services housed within PDSC;
3. Hybrid approach (status quo) – current services received from OJD and new development functions housed within PDSC.

The report concludes with a recommendation to continue the current hybrid approach for optimal efficiency and effectiveness. The consulting company specifically recommended new IT developments, including the financial/case management system, be developed with internal PDSC resources while current infrastructure IT services are outsourced from OJD.

The current request to continue contracting with OJD-ETSD for the second year of the 2021-23 biennium is a one-time expense. The additional 12 months of contract funding will provide IT coverage until PDSC has an opportunity to submit a policy package for 2023-25 requesting the investment funding outlined in the report.

Funding for OJD-ETSD Contract Continuance		
OJD-ETSD Contract Expense	\$ 34,417.60	<i>(Monthly expense)</i>
Number of Months Requested	12	<i>(July 2022 – June 2023)</i>
	\$ 413,011	

Funding Requested for IT Strategy Contractor	
Eylon Strategies	\$ 50,000

Total General Fund Requested	\$ 463,011
-------------------------------------	-------------------

Legal Reference: Allocation of \$463,011 from the State Emergency Fund to supplement the appropriation made by chapter 444, section 1(8), Oregon Law 2021, for the Public Defense Services Commission, Administrative Services Division for the 2021-23 biennium.



Oregon

Public Defense Services Commission

Office of Public Defense Services
198 Commercial St. SE, Suite 205
Salem, Oregon 97301-3489
Telephone: (503) 378-2478
Fax: (503) 378-4463
www.oregon.gov/opds

May 2, 2022

The Honorable Senator Peter Courtney, Co-Chair
The Honorable Representative Dan Rayfield, Co-Chair
Joint Emergency Board
900 Court Street NE
H-178 State Capitol
Salem, OR 97301-4048

Dear Co-Chairpersons:

Nature of Request

The 2021-23 Legislatively Adopted Budget, HB 5030, established the operating budget authority for the Public Defense Service Commission (PDSC). This included a change in the way the PDSC received base level technology services. The PDSC submitted a request for funding and the continuance of services through the end of the 2021-23 biennium to the January 2022 Joint Interim Committee on Ways and Means Public Safety Subcommittee.

The January 2022 Joint Interim Committee on Ways and Means Public Safety Subcommittee recommended that the Joint Interim Committee on Ways and Means defer the Public Defense Services Commission request to the May 2022 meeting of the Emergency Board with instruction that *“the Commission report back with a comprehensive information technology services plan and an assessment of the estimated costs, benefits, and risks of the alternative service-delivery methods, including both insourcing the agency’s information technology function and outsourcing through external providers. With each alternative, the Commission shall describe how the security, privacy and confidentiality of data entered, processed, or stored within the Commission’s information systems will be assured.”*

The purpose of this request is to provide a report on comprehensive information technology services plans and to continue the current level of services received from the Oregon Judicial Department Enterprise Technology Services Division (OJD ETSD) for the second fiscal year of the 2021-23 biennium.

Agency Action

The agency heard the subcommittee’s concerns and immediately decided to utilize the services of a private contractor, Elyon Strategies, to take advantage of their knowledge and expertise to provide three comprehensive information technology services plans. The plans are detailed in the attached PDSC IT Service Plan, Alternative Delivery Analysis (Appendix A). In addition to the report, the agency wishes to highlight with this letter the following issues: conflict of interest,

PDSC information technology staff, alternative market options and solutions, and the report's overall recommendation for a hybrid solution.

Conflict of Interest. The LFO recommendation to the January 2022 Interim Joint Committee on Ways and Means Joint Interim Subcommittee on Public Safety introduced a fundamental question of conflict of interest concerning the OJD and PDSC contractual agreement to provide enterprise level information technology management and limited technology infrastructure services. The agency agrees with the report from Elyon Strategies that any potential conflict of interest issues are appropriately mitigated. The report specifically discusses Organizational Conflict of Interest (OCI) in section 2.7 Non-Financial Analysis of Alternatives section on page 17:

***OCI Issues:** OJD limits access to PDSC data and systems, avoiding comingling of data outside of the PDSC domain. All OJD staff are background checked and required to sign a confidentiality agreement (Appendix F). In talking to PDSC data owners, no inherent OCI issues were identified. Approaches to data isolation and security are equivalent to those for any hosted data center, and they are appropriate for the sensitivity of the PDSC data. In short, we see no OCI issues associated with the OJD handling of PDSC data (emphasis added).*

In further support of the agency's statement on OCI, the Non-Financial Analysis of Alternative section also describes the data security and integrity environment of OJD system:

***Data security and integrity:** the OJD data center uses industry standard encryption of data at rest and in motion, isolates the PDSC domain to segment PDSC data, incorporates data access controls, monitors access, screens employees, and incorporates intrusion detection. In short, current OJD tools and processes are state-of-the-art, providing industry leading enterprise level data security and integrity (emphasis added).*

PDSC Information Technology Section Staff. In HB 5030, Package 809, Base Information Technology, of the 2021-23 Legislatively Adopted Budget, PDSC was granted four full-time positions to be hired throughout the biennium: One Chief Information Officer (CIO) (October 2021), One Information Technology Specialist 2 (January 2022), One Information Technology Specialist 3 (April 2022), and One Information Technology Specialist 2 (April 2022) to re-establish an Information Technology Section by July 1, 2022.

The three Information Technology Specialist (ITS) positions were filled between February 2022 and April 2022, due to the availability of funding. The ITS positions are currently providing base information technology services including the direct support of the databases PDSC utilizes, which are vital and necessary for the current delivery system. These databases are not enterprise systems and were explicitly excluded for support from the OJD/PDSC contracted services. The agency maintains that these positions are providing base non-enterprise level support for the agency to essentially keep the doors open.

The report also makes note that these base level positions will be essential to supporting the new Financial Case Management System (FCMS) as it is developed and subsequently deployed, and that the agency will benefit from having a few additional higher-level positions to support and help maintain the new systems. Specifically, the report recommends higher level IT personnel at a level four (4) as opposed to the ITS 2 and 3s that we currently have.

The need for internal IT staff is reinforced as by the agency's support for the reports recommendation to continue a hybrid approach to IT services. The hybrid model accounts for new work to be sourced with internal staff and that all enterprise level services would continue to be contracted through OJD. The report provides further support in the following areas:

Executive Summary, Page. 5 – *“The optimal, and recommended, approach going forward is a hybrid one. With this approach, IT status quo support continues to be outsourced to OJD, while IT new development support, and in particular support associated with the new financial and case management system capabilities, is insourced to PDSC. Having this new development capability within PDSC will keep those individuals close to the subject matter experts (SMEs) that they will need to work with to do their job.”*

Pg. 14 – *“A hybrid approach, in which IT status quo functions are outsourced to OJD while IT new development functions are insourced to PDSC”.*

Section 2.6 Financial Analysis of Alternatives, Pg. 17 – *“On the other hand, support for IT new development (specifically the Financial and Case Management System project) could reasonably be provided either under an expansion of the OJD contract or through developing those IT capabilities within PDSC. In fact, a hybrid alternative, where status quo support is provided by OJD while new capability support is provided within PDSC, is cost neutral when compared to the full outsource option. Further, there are advantages to having the staff supporting this new development closely aligned with the appropriate subject matter experts, all of whom are within PDSC. So, there are non-financial advantages to expanding the capability of PDSC to support new development inhouse.”*

Section 2.8 Recommendation, Page 19 - *“We recommend that PDSC adopt a hybrid outsource/insource model, in which IT status quo support is provided by OJD while most new development, and in particular work associated with the new financial/case management system, is provided using inhouse resources. This model provides an optimal balance of efficiency, effectiveness, and proximity to the PDSC subject matter experts”.*

Alternative Market Options and Solutions. The report considered three alternatives: 1. Full outsourcing of IT functions from PDSC to OJD; 2. Full insourcing of IT functions within PDSC; and 3. A hybrid approach, in which IT status quo functions are outsourced to OJD while IT new development functions are insourced to PDSC. Due to the short timeline associated with the Elyon Strategies contract, this report focused on re-insourcing versus continued contracting with OJD, keeping in mind that comparative GSA costs show that the OJD contract is well under market value. There are several significant issues that are associated with complete insourcing versus complete outsourcing, these issues are most pinpointed on funding, training, staffing and equipment. The report offers the following points that were considered during this comparison process:

2.5 Transition Requirements for Each Alternatives, Page 14 – *“Transitioning to fully insourced will require 180 to 200 days and incur significant cost for the data center build-out, procuring and configuring new office space and transition-in of new staff.*

2.6 Financial Analysis of Alternatives, page 16 – *“Transitioning to fully insourced IT support will incur one-time costs of over half-million dollars, and on-going monthly costs well over double the costs of either the fully outsourced or hybrid options, with no appreciable corresponding benefit in terms of organizational mission effectiveness or data security.*

2.7 Non-Financial Analysis of Alternatives, Page 17 – “Current OJD IT status quo support is exemplary across all dimensions of analysis. Bringing this support inhouse runs the risk of decreasing the quality of the support, with no corresponding likelihood of improving the quality. At best, quality will remain unchanged.

Reports overall recommendation. The report provides a full analysis of the costs, financially and operationally of the three alternatives and recommends that PDSC adopt a hybrid outsource/insource model in which enterprise services or status quo support is provided through a contract with OJD ETSD. All non-enterprise level services, improvements and maintenance to current delivery systems, new development and work associated with the new FCMS are to be provided by inhouse resources. The agency fully supports this recommendation and agrees that *“the hybrid model is cost effective, low risk, and provides the optimum approach to meeting IT requirements for both status quo and new development.”*

The agency believes that changing the current approach will increase operational liability by substantially increasing the costs of the system and potentially (likely) lowering the levels of security and introducing unnecessary risk. Continuing the hybrid system of contracting with OJD ETSD allows PDSC to provide services, make necessary improvements and focus agency resources financially and operationally towards other needs of the agency. When weighing economy of scale and program effectiveness, the PDSC commits to evaluate both in-house services and contracted services that provide the greatest return on investment and best use of public funds while reducing long-term costs.

Action Requested

The PDSC requests acceptance of this report and authorization to continue the use of OJD ETSD services through the existing contract for the remainder of the 2021-23 biennium. The PDSC further requests \$463,011 of General Fund for payment of services to OJD (\$413,011) and for the cost of the IT Report (\$50,000).

Legislation Affected

Oregon Law 2021 Chapter 444, section 1 (8).

Sincerely,



Stephen I. Singer
Executive Director

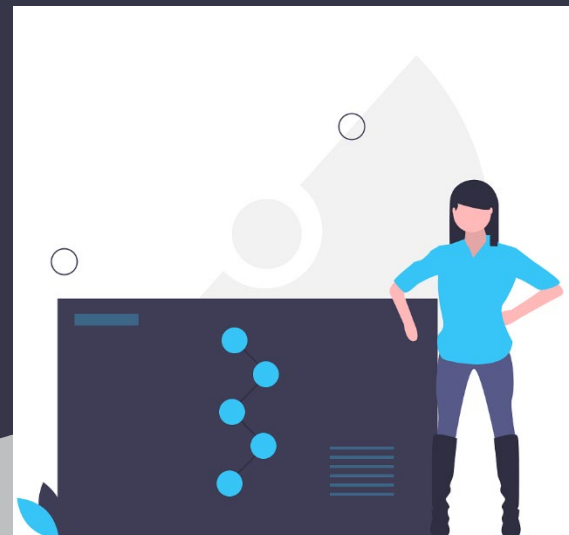
cc:

Amanda Beitel, Legislative Fiscal Officer
John Borden, Principal Legislative Analyst, LFO
George Naughton, Chief Financial Officer
Wendy Gibson, Policy and Budget Analyst, CFO

Appendix A

PDSC IT SERVICE PLAN

ALTERNATIVE DELIVERY ANALYSIS



Title	Alternative Delivery Analysis		
Document #:			
Version:	FINAL	DATE:	4/8/2022
Author(s):	WILLIAM ROETZHEIM		
Customer:	Oregon Office of Public Defender Services		
Contract:	OPDS-2022-02		
Project:	OPDS Outsource/Insource Alternative Analysis		
Deliverable ID:	1.3.1-1.3.4, PLUS 1.4.1-1.4.2		

VERSION HISTORY

Version	Author	Date	Changes
Draft	WHR	3/28/2022	Draft version
Final	WHR	4/8/2022	Final Version

Approvals


Role	Name	Signature	Date
Author	William Roetzheim		4/8/2022

Table of Contents

Contents

Table of Contents	3
1 Executive Summary	5
2 Analysis.....	6
2.1 Introduction.	6
2.2 Analysis Approach.	7
2.3 Information Technology Support Requirements.....	7
2.3.1 Status Quo Support.	8
2.3.2 New Capability Support.	11
2.4 Description of the Three Alternatives.	14
2.5 Transition Requirements for Each Alternative.....	14
2.6 Financial Analysis of Alternatives.....	15
2.7 Non-Financial Analysis of Alternatives.....	17
2.8 Recommendation.....	19
Appendix A. Acronyms	20
Appendix B: Interviews Conducted	22
Appendix C: Documents Reviewed.....	23
Appendix D: OJD Contract for IT Support	24
Appendix E: OJD IT Support to PDSC	25
Overview.....	25
Helpdesk.....	25
Desktop Team.	26
Server Team.....	26
PDSC Server Infrastructure.	27
Servers and Services Provided.....	27
Server Expertise Provided.	27
Information Security Office.	28
Networking/Telecommunications.....	28
Microsoft 365 & Mobile.....	28
Web Team.....	29

Management.....	29
Summary.	30
Appendix F: OJD Confidentiality Agreement.....	31
OREGON JUDICIAL DEPARTMENT EMPLOYEE CONFIDENTIALITY AGREEMENT	31
Appendix G: PDSC IT support Incident Metrics	33
PDSC iSupport Incidents.	33
Quick Statistics.	33
Incident Detail.	33
ETSD DESKTOP.	33
ETSD HELPDESK.	35
Other Groups.....	36

1 Executive Summary

Information technology (IT) work is divided into status quo (“keep the lights on”) support to maintain organizational mission effectiveness, and new development support to enhance or extend mission effectiveness. All organizations need status quo support. The changing nature of the Public Defense Services Commission (PDSC) mission, and in particular moving from a fixed reimbursement model to a significantly more sophisticated and flexible reimbursement model, means that PDSC will require new IT development support to deploy financial and case management back-office capabilities.

While PDSC is small in terms of headcount (roughly 110 individuals), the organization is using a highly sophisticated, enterprise level set of tools and capabilities to support all aspects of their IT infrastructure. Moving to an insourced IT status quo support model would be difficult, expensive, and high risk. It would be difficult because of the requirement to hire and transition-in staff with the necessary specialized skills, as well as the challenges associated with building out a brand-new data center within PDSC with the necessary conditioned power, backup generation capability, air conditioning, wiring, and fire suppression. It would be expensive in terms of one-time costs because of the need to build-out new facilities (both the data center and office space), and because what are fundamentally part-time, on-demand highly specialized technical skills will need to be filled using full-time staff. And it would be high risk because the current delivery of IT status quo support is high quality, secure, reliable, and flexible; while the new IT status quo support would need to be built-up from scratch, so it would have the potential for all of the problems that would entail.

In terms of data security, moving to an insourced model will not reduce risk and could very easily increase risk. One advantage of the enterprise level tools used by OJD, and their approach to segmenting the network domains, is that the PDSC data is encrypted at rest and in-motion, and access is both monitored and controlled using sophisticated network intrusion detection tools. In addition, the OJD data center is in a secure military facility that is the Governor’s secondary command post. It’s difficult to see how the PDSC data could be better protected, but easy to see ways that it could be less protected following a transition to insourcing.

The optimal, and recommended, approach going forward is a hybrid one. With this approach, IT status quo support continues to be outsourced to OJD, while IT new development support, and in particular support associated with the new financial and case management system capabilities, is insourced to PDSC. Having this new development capability within PDSC will keep those individuals close to the subject matter experts (SMEs) that they will need to work with to do their job.

2 Analysis

2.1 Introduction.

The Public Defense Services Commission (PDSC) must design a comprehensive information technology services plan for the Oregon Legislature to be presented at the Joint Ways and Means Emergency Board in May 2022. This plan must provide an assessment of estimated costs, benefits, and risks of alternative service-delivery methods, including both insourcing the agency's information technology function and outsourcing through external providers. Each alternative must describe how the security, privacy and confidentiality of data entered, processed, or stored within the Commission's information systems will be assured. This report was commissioned to provide an unbiased assessment that will then be used as a basis for this plan.

In preparing our report we looked specifically at the required information technology staffing requirements, cost, benefits, risks, transition schedule, and security implications of three alternate approaches to providing information technology services:

- Fully outsourced to the Oregon Justice Department (OJD).
- Fully insourced to the Public Defense Services Commission (PDSC).
- A hybrid whereby some services are within PDSC, while others remain outsourced to OJD.

Our scope excluded estimating the effort and costs to perform major new Information Technology (IT) development on a project basis. In particular, the full project implementation costs associated with the contemplated new financial and case management system project is outside the scope of the current analysis.

In accordance with General Accounting Office (GAO) yellow book guidelines for management audits such as this one, our report represents our best professional judgement. We are independent, qualified with respect to the areas involved in the analysis, and we have performed sufficient due diligence to satisfy ourselves with respect to the facts of this analysis. Our independence means that our conclusions are based strictly on the facts as identified, without regard to factors such as individual desires or expectations. Further, our report contains recommendations only. The final decision as to the selected course of action must rest with the government.

There was a very limited time to complete the report, and this short, firm deadline represented a constraint on the level of analysis that was performed. We do not believe that with more time we would alter our recommendations in general, however we do believe that some of the details of the specific budget analysis could change somewhat if the project were executed over a longer time-frame (and budget). Our target for the cost portion of our analysis is +/- 25%, so differences between alternatives that are under this amount would be considered low confidence.

2.2 Analysis Approach.

As shown in Figure 1, we employ a three-step process to our alternative analysis:

1. Inventory existing products and services. This inventory defines the necessary types of support that are needed. The result of this work is documented in Section 2.3 below.
2. Use industry best practices and benchmark data to define the characteristics of each alternative to ensure organizational mission success. As part of this analysis, we also look at transition requirements for each alternative. The three alternatives are described in Section 2.4 and the transition requirements are defined in Section 2.5.
3. Compare the alternatives from both a quantitative (financial) perspective and a qualitative (e.g., security) perspective. Our quantitative comparison is contained in Section 2.6 and our qualitative comparison is contained in Section 2.7.

Our final recommendations are then found in Section 2.8

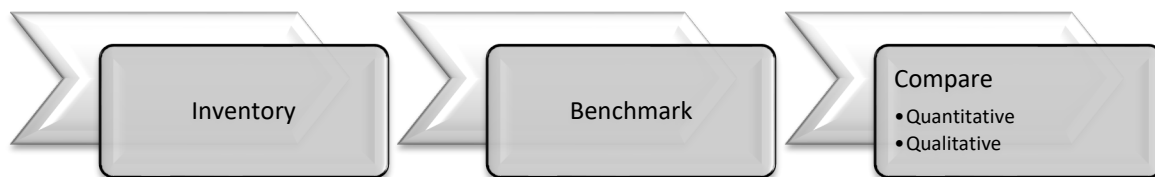


Figure 1: Analysis approach overview.

2.3 Information Technology Support Requirements.

IT support requirements are often divided into two categories of work. The first is status quo support, often called “keep the lights on” support. This is the level and type of support necessary for the organization to remain operational, fulfilling its mission. Support below this level will result in rapid loss of organizational mission capability, often showing up as a cascade of failures.

IT Status Quo support maintains an organization’s mission capability, while IT New Development support enhances mission capability.

The second is new development support. For most organizations, operational needs are evolving over time. When operational needs change, effort must be expended to allow the IT systems to support those evolving needs. While it is possible to slow or stop spending in this area, the result is a gradually increasing gap between the organization’s mission and its IT capabilities. This will limit organizational effectiveness

as the gap widens, and it will eventually become the limiting factor on what the organization is able to accomplish.

We'll cover each of these two areas in the Sections that follow.

2.3.1 Status Quo Support.

The PDSC IT support requirements are enterprise level in terms of sophistication, power, and complexity.

PDSC employs roughly 110 staff and contracts with roughly 715 contract attorneys [Styles, 2022]. IT support includes helpdesk, desktop, server, enterprise information security, networking, telecommunication, wireless, mobile, web, IT management, and software support (e.g., Microsoft 365). Status quo support requirements are summarized in Table 1, and described in more detail in Appendix E. It's significant to note that the PDSC IT environment is setup as an Enterprise scale environment, with Enterprise level tools in all areas. While this provides all the advantages of an Enterprise level environment (e.g., reliability, security, performance), it also means that the bar is quite high in terms of the skillsets required to support this environment. Basically, the PDSC tools and environment would not look any different if the organization had 10,000 staff, rather than just over 100. This also means that the level of expertise required to support the PDSC environment is the same whether the organization has 10,000 staff, or 100.

Table 1: PDSC IT status quo support requirements.

Support Area	Expertise and support provided	Tools used/supported
Helpdesk	Tier 1 help desk.	iSupport.
Desktop	Tiers 2 and 3 support. New user setup. Software installs. New hardware deployments. Equipment moves. Sit/stand desk installs. New printer/copier installs and setup. Windows image creation and management. Windows upgrades and patches. Directory mapping. Active Directory management. Acquisition support (advice).	MS Windows. Active Directory. MS Office. Adobe. Dell hardware. HP and Lexmark printers. Fujitsu scanners. Ricoh copiers. System Center Configuration Manager (SCCM). Windows Server Update Service. WinPE. DART. Remote Assist and Remote Desktop. Dell Command Update. Dell Command Configure. PDQ.
Server	Tier 2/3 support. Maintain 3 physical servers. Maintain 7 virtual servers. Onsite and offsite backups.	VMWare Commvault. DHCP & DNS.

Support Area	Expertise and support provided	Tools used/supported
	<p>Domain management. Certificate Authority management. Secure password management. Azure Application Proxy management. Intune (NDES) management. Nintex server management for SharePoint. Exchange Server and SMTP management. Network monitoring with SolarWinds. VMware architecture and administration. Advanced Server Administration. SAN administration. SharePoint on-prem and in the cloud – operations and development. Active Directory administration (including Domain Controllers, DNS, DFS, WINS, DHCP, Security, group policies, etc.) Tenant / Azure AD / O365 administration. SQL database administration. Westlaw support. Incident management system administration (e.g., iSupport.) OJD Case Management Extracts. Passthrough access to RSTARS. SPSS Statistics configuration.</p>	<p>Microsoft Key Management Services. ADBA Server. Thycotic. Windows Server Update Services. End Point Management Server (SCCM). Microsoft Advanced Threat Protection. Azure Application Proxy. Intune (NDES) Server. Microsoft BitLocker Administration. Monitoring (MBAM) and Network unlock servers. PDQ server. SharePoint. Exchange Server. SMTP. SolarWinds. Tenant. SQL Server. Westlaw. SAN Storage. RSTARS Nintex. Cloudmersive. Host Explorer. IBM SPSS Statistics. IBM SPSS Forecasting.</p>
EISO	<p>Tier 2/3 support. Incident response. Firewall configuration. Threat monitoring. Email threat analysis. DigiCert and VPN renewals and installations. Staff security training/education. Staff security assessments. Security log monitoring. Annual security penetration testing. Compliance and data loss protection (DLP). eDiscovery. Application Security Reviews. RSA Secure tokens (MFA). Security Policy management.</p>	<p>Microsoft's Advanced Threat Protection. Firewalls. DigiCert. VPN. QRadar. Microsoft Security Center. Microsoft Compliance Center. Proofpoint/Wombat. RSA Security Console.</p>
Networking/Telecom	<p>Tier 2/3 support. VoIP management. Wireless infrastructure management. Voice mail and call routing tree management. LS Network management.</p>	<p>Switches. Routers. Firewall. Wireless. VoIP servers. Network transport (2 locations).</p>

Support Area	Expertise and support provided	Tools used/supported
		Voicemail and routing. LS Network (internet). Centurylink/Lumen. Cisco.
MS 365 & Mobile	Tier 2/3 support. MS 365 administration. Exchange server administration. iPad and iPhone support. Azure security/role configuration. Mailbox management. Email quarantine response. Software training.	Microsoft 365. Visio. Exchange server. Azure. Multi-Factor Authentication.
Web & Integration	Tier 2/3 support. SharePoint management. Website management. Web development (24 hours per week). Jira management. Integration (secure data transfer).	SharePoint. Intranet. Survey Monkey. MailChimp. eFax. Doodle. PowerDVD. Time. Snagit. Jira. Web services.
ETSD Management	Management metrics and performance monitoring. Staff oversight. Problem escalation. Hardware inventory management. Software inventory management.	OJD Statistical Dashboards.
Facilities	Facility access control.	Computer room facility. Safety equipment. Physical access control. Backup/standby electrical power.

By way of setting a general benchmark for IT support expectations, the US General Services Administration (GSA) uses \$5,497¹ for IT status quo support per staff supported, so for the PDSC the GSA benchmark data would suggest a status quo IT support cost of \$604,670.

PDSC is currently receiving IT support from the Oregon Justice Department (OJD) on an outsourced basis. In addition to on-going routine IT environment support, OJD responded to 797 IT incidents/service requests during 2021. In reviewing those service requests, we find that 65 different OJD IT personnel have provided support to PDSC at some point or other during 2021. By way of example, a single security incident can involve dozens of IT staff working cooperatively to mitigate, analyze, and then resolve the threat. Further metrics regarding the specific IT incidents handled during 2021 may be found in Appendix G.

¹ <https://www.gsa.gov/policy-regulations/policy/real-property-policy/best-practices-and-tools/office-workplace-best-practices/cost-per-person-model>.

Overall, our estimate of the approximate skillset required to support OPSD status quo operations is shown in Table 2. In developing this list, we note the following facts with respect to IT support:

Effective IT status quo support requires a team of individuals, each with specialized skills and training, plus a back-up capability for each skill area.

- For complex enterprise systems, specialized tools mandate support by staff with specialized skills. As an analogy, when building a house, you don't hire "construction workers." Instead, you hire framers, roofers, plumbers, electricians, and so on.
- For each area, it is necessary to have both a primary and a backup/alternate person. Each of these functions must operate correctly, either during each workday or, in some cases, 7 days a week, 24 hours per day. The primary person will always have periods of unavailability, with examples including vacation, sickness, and simply transitioning to another job. During those gaps, there must be a knowledgeable backup or alternate person to meet the on-going needs.

Table 2: PDSC IT Support Requirements.

Capability	Requirement
Helpdesk	Primary: Full-Time ITS 1. Alternate/Backup: Part-Time ITS 1.
Desktop	Primary: Full-Time ITS 2. Alternate/Backup: Part-Time ITS 2.
Server	Primary: Part-Time ITS 4. Alternate/Backup: Part-Time ITS 3.
EISO	Primary: Part-Time ITS 4. Alternate/Backup: Part-Time ITS 4.
Networking/Telecom	Primary: Part-Time ITS 4. Alternate/Backup: Part-Time ITS 3.
MS 365 & Mobile	Primary: Part-Time ITS 4. Alternate/Backup: Part-Time ITS 3.
Web & Integration	Primary: Full-Time ITS 4. Alternate/Backup: Part-Time ITS 3.
Management	Primary: Full-Time CIO.
Facility Management	Primary: Part-Time ITS 3.
Facilities: Server room	Estimated at 400 square feet.
Facilities: IT staff office space, including an allowance for common areas.	Estimated at 196 square feet per employee. ²

2.3.2 New Capability Support.

Historically, PDSC largely operated as a funding pass-through entity, negotiating what were in effect fixed price contracts and then distributing funds in accordance with those

² Per JLL research at <https://www.us.jll.com/en/views/how-will-employee-workspace-needs-change-post-coronavirus>.

agreements. From an IT perspective, this organizational mission is simple to support and monitor, with minimal opportunities for waste, fraud, or abuse.

In January 2019, the 6AC completed their 238-page report, “The Right to Counsel in Oregon: Evaluation of Trial Level Public Defense Representation Provided Through the Office of Public Defense Services” [6AC, 2019]. Their research showed that Oregon attempts to fulfill its 14th Amendment obligation in trial courts primarily through an array of contracts led by the PDSC and administered by PDSC however they identified many areas of concern related to public defense. These concerns include:

- The State of Oregon has created a complex bureaucracy that collects a significant amount of public defense data yet does not provide sufficient oversight or financial accountability.
- The complex bureaucracy obscures an attorney compensation plan that is at root a fixed fee contract system which pits an appointed lawyer’s financial self-interest against the due process rights of their clients and is prohibited by national public defense standards.
- The State of Oregon should require that services be provided free of conflicts of interest, as is constitutionally required, by abolishing fixed fee contracting and other forms of compensation that produce financial disincentives for public defense lawyers to provide effective assistance of counsel.
- PDSC should have the appropriate resources to provide oversight of such a private attorney and state public defender employee system.

Partially because of this study, the organizational mission of PDSC/OPDS has changed significantly, with attorneys receiving reimbursement on more of an hourly basis. This significantly complicates the IT support requirements. Invoices must be validated, duplicate charges (typically accidental) flagged, metrics collected, and forecasts created. According to a PDSC internal document [PDSC, 2020]:

PDSC mission changes are driving the need for new development to support enhanced IT back-office capabilities.

PDSC/OPDS can no longer operate in the status quo and continuation of current business process will remain in non-compliance with national standards identified in the “Guidelines for Legal Defense Systems in the United States”. The OPDS disparate technical tools currently in place are unable to support dynamic data collection and integrations with Oregon courts and partner agencies. Manual data entry in multiple, non-integrated systems has the potential for inaccuracies, duplication, deletion, and loss of all information due to hardware and software failure. Without a robust and efficient financial and case management system, PDSC/OPDS lack a system necessary to collect accurate data that can: document whether quality services are provided to eligible individuals; monitor provider/attorney contracts and financial obligations; reflect where inefficiencies are in business processes; and show increases in workload / caseloads, staff attorney turnover, and complexity of cases.

A report by the American Bar Association and Moss Adams drew similar conclusions [ABA and Moss Adams, 2022, Pages 5-6]:

OPDS needs a centralized data system to capture basic, critical public defense information

There are significant data deficiencies (inconsistency and inaccuracies) in the OPDS Contract Database, and OPDS heavily relies on the Oregon Judicial System court statistics data for basic case information. The OPDS contracting system, which includes over 100 contractors that vary significantly in both size and organizational structure, imposes challenges to building and implementing a unified case management system and other data collection mechanisms. Nonetheless, OPDS should implement systems to reliably collect basic data from all contractors on qualifications, case assignments, caseloads and work completed in public defense cases.

- OPDS should be able to track which individual attorney is assigned to which cases to verify both qualifications and caseloads.
- OPDS should implement improved monitoring of work completed on public defense cases. This should include timekeeping on all public defense cases to permit improved fiscal and substantive oversight, including auditing and a regular attorney review process. Further, OPDS should have basic information on the private caseload, if any, for each attorney paid under its contracts to fully monitor caseloads.
- OPDS should also adopt standardized case opening and case closing forms (specific to case types) to routinely, centrally, and consistently capture important case data. These forms should be integrated into a case management system to allow for aggregation of the data collected.

PDSC is already working to procure, configure, and deploy a new Financial and Case Management System. While estimating the total budget required for that effort is outside the scope of the current Elyon engagement, the following IT staff (Table 3) will be needed to support the project, working closely with the PDSC subject matter experts. Note that because this work is new development rather than status quo work, there is no analogous requirement to have an alternate for each position. With new development, it is acceptable for a role to be unfilled for a short period of time during project execution while a person is sick or on vacation.

Table 3: New development IT support requirements.

Capability	Requirement
Project Management	Full-Time ITS 4

Capability	Requirement
Business Analyst-Test case development and execution.	Full-Time ITS 4
Data Analyst or Business Analyst-Data clean-up and conversion; data validation; database design; report and dashboard design.	Full-Time ITS 4

If the new development IT support personnel are outsourced to OJD, an additional ITS 4 position would be required to coordinate (liaison) between the OJD team and the SMEs at PDSC.

2.4 Description of the Three Alternatives.

In conducting our analysis, we were tasked to look at three alternatives:

1. Full outsourcing of IT functions from PDSC to OJD.
2. Full insourcing of IT functions within PDSC.
3. A hybrid approach, in which IT status quo functions are outsourced to OJD while IT new development functions are insourced to PDSC.

2.5 Transition Requirements for Each Alternative.

Transitioning IT support requires time and incurs one-time transition costs. Staff related transition time has two components: Time to Fill and Time to Train. Time to Fill is simply the time needed to find and hire qualified staff to fill a position once that position has been approved. The Office of Personnel Management tracks and reports on this data, and the number for government fiscal year 2018 was 98.3 days.³ We were not able to find current (2022) data, but anecdotally we believe that the job market is significantly tighter now, with recruiting more challenging than in 2018. To adjust for these characteristics, we've increased the Time to Fill by 25%.

Transitioning to fully insourced will require 180 to 200 days and incur significant costs for the data center build-out, procuring and configuring new office space, and transition-in of the new staff.

While there are costs associated with the hiring process itself, the largest cost element during transition involves training of new employees. Even when an employee has exactly the right technical skills for a given position, they will still need to learn organization specific configurations, policies, procedures, processes, tools, and so on. New employees can take 1-2 years before they are fully productive in a new job.⁴ But in our experience, a 60-day transition-in period for a new IT support organization is more

³ <https://www.govexec.com/management/2020/02/opm-announces-adjustments-annual-time-hire-metrics/163361/>.

⁴ <https://www.betterteam.com/training-new-employees>.

typical. During this transition period, the new employees work side-by-side with the previous employees. For our analysis, we assume a 60-day transition-in period.

In total, the transition time from the final decision to in-source PDSC IT, and approval of the necessary budgets and staff positions, until the actual shut-down of the outsourced support, is expected to be 180 to 200 calendar days from the completion of the budgetary authorizations and completion of the acquisitions for the necessary equipment and facility upgrades..

2.6 Financial Analysis of Alternatives.

In conducting our financial analysis, we focused on staffing and facility costs. We believe that costs for software, network access, computer equipment, phones, and so on will be roughly comparable across all three alternatives, so those constant costs will not have an impact on the selection of an optimum approach. Our financial analysis also makes the following assumptions:

- The cost to build out a data center, including power conditioning, power backup, air conditioning, cabling, security, and fire suppression is budgeted at \$1,000 per square foot.⁵
- The cost for additional office space is budgeted at \$30 per square foot per year⁶, plus a budget of \$4,200 per employee for office furniture and equipment.⁷
- For staffing part-time positions, we assume that OJD supports those positions using actual part-time, as needed support. In the case of insourcing to PDSC, we assume that all positions are full-time positions, as it is very difficult to staff highly skilled IT positions with part-time employees. Skilled IT staff are generally looking for and able to easily find full-time work.
- We assume \$21,464 per month in fully-loaded costs for the CIO position and used the costs from Table 4 for IT support cost calculations. Costs are fully loaded.
- As discussed above, we assume a 60-day transition in for situations where IT services transition from one organization to another.

Table 4: Monthly fully loaded staff costs, per FTE.

⁵ <https://www.profitableventure.com/long-cost-build-data-center/#:~:text=How%20Much%20Is%20A%20Data%20Center%20Worth%3F%20It,would%20then%20cost%20%241%20million%2C%20on%20that%20basis.>

⁶ <https://offices.net/report-oregon.htm>.

⁷ <https://davidcummins.org/2011/03/07/costs-to-furnish-a-nice-startup-office/#:~:text=Open%20workspace%20with%20%E2%80%9CL%E2%80%9D%20shaped%20desk%2C%20cabinet%2C%20and,Desk%20accessories%20like%20keyboard%2C%20mouse%2C%20etc%20%E2%80%93%20%24150%2Fperson.>

Staff Position	Monthly Cost
ITS 1 fully loaded staff cost.	\$ 9,347.92
ITS 2 fully loaded staff cost.	\$ 11,546.58
ITS 3 fully loaded staff cost.	\$ 12,907.92
ITS 4 fully loaded staff cost.	\$ 15,076.58

In our experience, government agencies with less than several thousand employees are routinely able to reduce their IT spend by 50% to 75% by moving from an inhouse support model to a centralized support model using a consolidated data center. States like Washington have recognized this and instituted policies requiring all state agencies to move to either a state data center or to a cloud provider for IT support services. Frankly, the current alternative analysis is the first one that we have ever conducted that asked us to look at the alternate scenario, moving from a consolidated data center back to inhouse IT support. Our financial analysis, shown in Table 5, makes it clear why this request is rare. In addition to an over \$500K capital investment requirement to build-out the PDSC data center, PDSC costs for equivalent IT status quo support will more than double. From an economic perspective, moving to a fully insourced IT status quo support capability incurs a significant penalty for the taxpayers of Oregon.

Transitioning to fully insourced IT support will incur one-time costs of over a half-million dollars, and on-going monthly costs well over double the costs of either the fully outsourced or the hybrid options, with no appreciable corresponding benefit in terms of organizational mission effectiveness or data security.

Table 5: Financial analysis of the three alternatives.

	Fully Outsourced	Fully Insourced	Hybrid
One-Time Costs			
Data Center Fit-Out	NSP	\$400,000.00	NSP
Office Fit-Out	\$16,800.00	\$79,800.00	\$16,800.00
Transition-Costs	\$ -	\$68,835.20	\$ -
TOTAL	\$16,800.00	\$548,635.20	\$16,800.00
On-Going Costs (per Month)			
Monthly Inclusive IT Support	\$41,293.60	\$ -	\$34,417.60
Helpdesk	NSP	\$18,695.83	NSP
Desktop	NSP	\$23,093.17	NSP
Server	NSP	\$27,984.50	NSP
EISO	NSP	\$30,153.17	NSP
Networking/Telecom	NSP	\$27,984.50	NSP
MS 365 & Mobile	NSP	\$27,984.50	NSP
Web & Integration	NSP	\$27,984.50	NSP
Management	NSP	\$21,464.00	\$21,464.00
Facility Management	NSP	\$12,907.92	NSP
New Capability Support (F/CMS)	\$60,306.33	\$45,229.75	\$45,229.75

	Fully Outsourced	Fully Insourced	Hybrid
Facilities: Server room	NSP	\$1,000.00	NSP
Facilities: IT staff office space	\$1,960.00	\$9,310.00	\$1,960.00
TOTAL	\$103,559.93	\$273,791.83	\$103,071.35

On the other hand, support for IT new development (specifically the Financial and Case Management System project) could reasonably be provided either under an expansion of the OJD contract or through developing those IT capabilities within PDSC. In fact, a hybrid alternative, where status quo support is provided by OJD while new capability support is provided within PDSC, is cost neutral when compared to the full outsource option. Further, there are advantages to having the staff supporting this new development closely aligned with the appropriate subject matter experts, all of whom are within PDSC. So, there are non-financial advantages to expanding the capability of PDSC to support new development inhouse.

2.7 Non-Financial Analysis of Alternatives.

While financial considerations are an important factor, there are non-financial factors that may influence, or even determine, the necessary support approach. In our analysis we looked at nine non-financial factors, as identified in Table 6. For each area we assigned a score of Very Low to Very High based on the quality of services. Where the quality was not known, we assigned a score of Unknown. Each of these nine factors is discussed below:

Current OJD IT status quo support is exemplary across all dimensions of analysis. Bringing this support inhouse runs the risk of decreasing the quality of the support, with no corresponding likelihood of improving the quality. At best, quality will remain unchanged.

- Data security and integrity:** The OJD data center uses industry standard encryption of data at rest and in motion, isolates the PDSC domain to segment PDSC data, incorporates data access controls, monitors access, screens employees, and incorporates intrusion detection. In short, current OJD tools and processes are state-of-the-art, providing industry leading enterprise level data security and integrity.
- OCI Issues:** OJD limits access to PDSC data and systems, avoiding comingling of data outside of the PDSC domain. All OJD staff are background checked and required to sign a confidentiality agreement (Appendix F). In talking to PDSC data owners, no inherent OCI issues were identified. Approaches to data isolation and security are equivalent to those for any hosted data center, and they are appropriate for the sensitivity of the PDSC data. In short, we see no OCI issues associated with the OJD handling of PDSC data.
- Disaster Recover:** OJD performs regular backups, both on-site and offsite in a secure storage facility. Data in transit is protected using both encryption and physical security. The backup schedule is a standard Enterprise level rolling backup with both incremental and snapshot backups.

- **Continuity of Operations:** OJD facilities are a military facility that is also used as the secondary command post by the Governor in the event of an emergency. The facility is fully secure with protected access, plus it has full PGE backup generators enabling it to function in its role as an emergency command post.
- **Security Incident Handling:** We reviewed the OJD security incident handling response using the SolarWinds and Log4J zero-day events as examples. The response demonstrated threat awareness through interactions with peers both inside the state government and outside of government; rapid and appropriate immediate threat response mitigation measures; rapid assembly of the necessary resources to develop a threat elimination plan; and the rapid and effective implementation of that plan. In short, OJD response under fire for security incidents is a model for an effective enterprise level organization.
- **Security policy management:** Comprehensive security related policy documents are currently maintained by the OJD CISO. If this function is insourced back to PDSC, equivalent documents will need to be developed by PDSC staff.
- **Quality of support:** As documented in Appendix G, 98% of the 797 tickets from 2021 have been closed by OJD. In developing our report, we asked each person interviewed if they were aware of any indications of PDSC dissatisfaction with the quality of support provided by OJD, and none were found. In fact, quite the contrary was discovered. We also solicited wider input from PDSC and found a consistent satisfaction with OJD services. For example, Ernest Lannet said, “I have found the PDSCHelp email group very responsive, helpful, and professional. Very satisfied.”
- **Flexibility:** One potential challenge with outsourced IT services is that the outsourced vendor may follow the contract tightly, with no flexibility to handle the inevitable grey areas and unanticipated needs that go somewhat outside the bounds of the written document. What we found is that OJD views OSPD as “part of the family,” with a strong focus on supporting the organizations’ ability to effectively perform its mission even when this requires providing support that was not anticipated in the contract.
- **Interaction with SMEs for new development:** As we’ve discussed earlier, there is a significant difference between the worlds of status quo (keep the lights on) IT support versus IT support for deploying new capabilities. While the status quo support is very commodity like, with the subsequent advantages of economies of scale, new capability support is most effective when the IT personnel have immediate and direct access to the end-user subject matter experts. There is a significant amount of “learning by osmosis” in terms of business rules, workflows, and so on. So, while either approach will work, new development IT support does see a benefit from either the insource or the hybrid models.

Table 6: Non-Financial factors examined.

Characteristic	Fully Outsourced	Fully Insourced	Hybrid
Data security and integrity.	Very High	Unknown	Very High
OCI Issues.	None identified	None identified	None identified
Disaster Recover.	Very High	Unknown	Very High
Continuity of Operations.	Very High	Unknown	Very High
Security Incident Handling.	Very High	Unknown	Very High
Security policy management.	Very High	Unknown	Very High
Quality of support.	Very High	Unknown	Very High
Flexibility	Very High	Unknown	Very High
Interaction with SMEs for new development.	High	Very High	Very High

2.8 Recommendation.

We recommend that PDSC adopt a hybrid outsource/insource model, in which IT status quo support is provided by OJD while most new development, and in particular work associated with the new financial/case management system, is provided using inhouse resources. This model provides an optimal balance of efficiency, effectiveness, and proximity to the PDSC subject matter experts.

The hybrid model is cost effective, low risk, and provides the optimum approach to meeting IT requirements for both status quo and new development.

Appendix A. Acronyms

ABA: American Bar Association.
ADBA: Active Directory-Based Activation.
AP: Accounts Payable.
Azure AD: Azure Active Directory.
DART: Diagnostics and Recovery Toolset.
DFS: Distributed File System.
DHCP: Dynamic Host Configuration Protocol.
DNS: Domain Name System.
ETSD: Enterprise Technology Services Division.
F/CMS: Financial/Case Management System.
FTE: Full-Time Equivalent.
HP: Hewlett Packard.
IBM: International Business Machines.
IT: Information Technology.
ITS: Information Technology Specialist.
LS Networks: Internet provider.
MBAM: Microsoft BitLocker Administration and Management.
MFA: Multi-Factor Authentication.
NDES: Network Device Enrollment Service.
NSP: Not separately priced.
OCI: Organizational Conflict of Interest.
OJD: Oregon Judicial Department.
OPDS: Office of Public Defense Services.
OS: Operating System.
PDSC: Public Defense Services Commission.
PDQ: Pretty D*#&mn Quick.
RSTARS: Relational STatewide Accounting and Reporting System
SAN: Storage Area Network.
SCCM: System Center Configuration Manager.
SMTP: Simple Mail Transport Protocol.

SPSS: Statistical Package for the Social Sciences.

SQL: Structured Query Language.

VoIP: Voice over Internet Protocol.

VPN: Virtual Private Network.

WinPE: Windows Preinstallation Environment.

WINS: Windows Internet Name Service.

WSUS: Windows Server Update Services.

Appendix B: Interviews Conducted

Table 7 shows the interviews conducted as part of this study.

Table 7: Interviews Conducted.

Date	Interview With	Organization	Topic/Description/Role
2/25/2022	Krystal Styles	PDSC	Analysis project lead.
2/25/2022	Jim Conlin	PDSC	PDSC CIO.
2/28/2022	Bryant Baehr	OJD-ETSD	OJD CIO.
2/28/2022	Ralph Amador	PDSC	PDSC budget analyst.
3/1/2022	Laura A. Al Omrani	PDSC	Historical Context.
3/1/2022	Brian DeForest	PDSC	PDSC Deputy Director.
3/2/2022	David McCall	OJD-ETSD	PDSC Liaison & Desktop Lead.
3/2/2022	Peter Diec	OJD-ETSD	OJD Infrastructure Manager.
3/4/2022	Brian Canfield	OJD-ETSD	OJD Applications Manager.
3/4/2022	Randy Swope	OJD-ETSD	OJD CISO.

Appendix C: Documents Reviewed

6AC, 2019: Sixth Amendment Center. *The Right to Counsel in Oregon*. January 2019.

ABA and Moss Adams, 2022: American Bar Association and Moss Adams, LLC. *The Oregon Project: An Analysis of the Oregon Public Defense System and Attorney Workload Standards*. January 2022.

Borg et. Al., 2020: Borg, Lane; Fetsch, Julie; and Al Omrani, Laura. *OPDS F/CMS Project Statement*. June 16th, 2020.

DAS, 2022a: Oregon Department of Administrative Services. *HB 5030 Budget Report and Measure Summary*. February 2022.

DAS, 2022b: Oregon Department of Administrative Services. *Position Description, Information Technology Specialist 1*. March 2022.

DAS, 2022c: Oregon Department of Administrative Services. *Position Description, Information Technology Specialist 2*. March 2022.

DAS, 2022d: Oregon Department of Administrative Services. *Position Description, Information Technology Specialist 3*. March 2022.

DAS, 2022e: Oregon Department of Administrative Services. *Position Description, Information Technology Specialist 4*. March 2022.

DeForest, 2021: DeForest, Brian. *Letter to The Honorable Senator Elizabeth Steiner Hayward and The Honorable Representative Dan Rayfield*. December 6th, 2021.

Leymon, Undated: Leymon, Ann Shirley, Ph.D. *OPDS Data Quality Assessment and Recommendations*. Undated.

PDSC, 2020: PDSC. *OPDS Financial and Case Management System Project Business Case V1.0*. July 31, 2020.

Styles, 2020: Styles, Krystal. *OPDS Financial and Case Management System Project Business Case v2.0*, August 31st, 2020.

Styles, 2021: Styles, Krystal. *Requirement Traceability Matrix*. June 7th, 2021.

Styles, 2022a: Styles, Krystal. *OSPD Data Design Visio Diagram*. February 2022.

Styles, 2022b: Styles, Krystal. *Untitled informal working document in response to Elyon request*. February 2022.

Taylor, 2022: Taylor, P. *IT Funding Pkg 809 21-23 Biennium*. February 28th, 2022.

Appendix D: OJD Contract for IT Support

AMENDMENT NUMBER 3 TO
INTERAGENCY AGREEMENT
BETWEEN
OREGON JUDICIAL DEPARTMENT AND
PUBLIC DEFENSE SERVICES COMMISSION

The Oregon Judicial Department (“OJD”) and the Public Defense Services Commission (“PDSC”) agree to amend the Interagency Agreement, OJD Contract Number 170017 (“Agreement”). Except as expressly amended herein, the terms, conditions, and obligations of the Agreement shall remain valid and of full force and effect. However, if any provisions of this amendment (“Amendment”) conflict with the provisions of the Agreement, the provisions of this Amendment shall prevail. This Amendment becomes effective July 1, 2021. ¹⁵ ^{Retrospective to} *NJC*

Purpose: The purpose of this Amendment is to renew this Agreement for an additional two years, update the scope of information technology services that the Enterprise Technology Services Division of OJD (“ETSD”) will provide to the Office of Public Defense Services (“OPDS”) and update the monthly charge.

The Agreement is amended as follows:

- A. Section I. Purpose. Delete this Section I in its entirety and replace it with the following:

The purpose of this Agreement is for OJD to provide warehouse storage space and information technology services to PDSC.

- B. Section II. Term. Delete the second sentence of this Section II and replace it with the following:

This Agreement will remain in effect through June 30, 2023, unless terminated as set forth in this Agreement.

- C. Section III. Roles and Responsibilities. Subsection B. Information technology services. Delete this subsection in its entirety and replace it with the following:

B. Information technology services: Attachment A-Service Level Agreement (SLA) dated June 30, 2021, describes the information technology services OJD will provide to OPDS and the costs associated with those services. Attachment A is attached hereto and incorporated herein by this reference.

- D. ATTACHMENT A-Service Level Agreement. Delete Attachment A -Service Level Agreement and replace it with Attachment A -Service Level Agreement dated June 30, 2021.

Oregon Judicial Department

By: 
Nancy J. Cozine

State Court Administrator

Date: July 12, 2021

Approved as to Legal Form and Sufficiency:

Teresa Bradshaw, via email
OJD Office of General Counsel
TKB:gl/L2G21017

Public Defense Services Commission

By: 
Ed Jones

Interim Executive Director

Date: July 9, 2021

Date: June 23, 2021

ATTACHMENT A
SERVICE LEVEL AGREEMENT (SLA)
Between
OREGON JUDICIAL DEPARTMENT
AND
PUBLIC DEFENSE SERVICES COMMISSION
June 30, 2021

The Enterprise Technology Services Division (“ETSD”) of OJD will provide information technology management and limited technology infrastructure services for the Office of Public Defense Services (“OPDS”).

A. Responsibilities of ETSD

ETSD will provide:

1. On site direct management of OPDS IT operations until OPDS is able to hire an internal CIO.
2. Qualified ETSD personnel to perform the services described herein. Specifically, One Chief Information Officer (CIO) 100% FTE, one ITS 1 Help Desk Support, and one ITS 2 Desktop Support. All of these positions are the employees of OJD; subject to OJD Personnel Rules and Policies, eligible for OJD Benefits and under the administrative authority of the Director of ETSD. OJD will continue to provide the CIO function until such time as OPDS assumes that function through the hiring of an OPDS CIO. Once OPDS has employed a CIO and assumed the CIO duties, OJD will provide an ITS 4 (Lead) to coordinate the provision of service provided by OJD through this Agreement.
3. Desk equipment (computers, monitors, printers) for OJD personnel stationed at the OPDS location.
4. Network administration within an OPDS Active Directory Domain.
5. Internal and external network monitoring and maintenance.
6. Desktop support.
7. Helpdesk support.
8. Software recommendations and hardware standards for OPDS to follow.
9. Enterprise email management and support.
10. Hardware - Installation and maintenance of OPDS procured workstations and peripheral devices, including recommendations for replacement, upgrade, and substitution. Warranty resolution and recommended scheduled upgrades. Installation and maintenance of printers.
11. Staffing - ETSD will provide primary and backup system administrators skilled in active directory configuration and maintenance, account management, domain name system (DNS), Active Directory, group policy maintenance, desktop, laptop and mobile device management, Microsoft 365 tenant configuration, and maintenance, backup/recovery processes, and security administration.
12. Computer room facilities for servers and other required equipment, including any safety equipment needed.
13. Backup – ETSD systems administrators will setup and monitor backup processes for the OPDS Systems.
 - a. Daily incremental backups are being written to disk at both our primary and backup data centers and are retained for 60 days for quick recovery.
 - b. At the backup data center, these backups are also being written to tape which overwrites itself every 15-30 days to provide air-gapped disaster recovery.
 - c. At the primary data center, the backups are also being rolled up into monthly synthetic full backups which are written to tape and sent offsite to Iron Mountain for 2 years for long term recovery.

- d. In addition to the server backups, the databases are also being backed up independently on a daily basis using the Commvault SQL Agent to provide crash consistent recovery. These backups are included on the same disk and tape backups.
 - e. The tapes are protected with AES 256 encryption and strict chain-of-custody policies are being followed.
 - f. Restores are available on an emergency basis. OPDS would incur the cost of requesting backup media from the off-site storage vendor.
14. Security - ETSD will follow OJD security policies and procedures when working with the OPDS information technology system, data, and information. ETSD will: i) provide a suitable firewall-enabled access to the web server; ii) install and maintain domain name registration; iii) provide physical and logical security consistent with OJD Security Policies and Procedures and iv) provide IT security consultation.
 15. System Administration – ETSD will provide installation and setup of server operating systems, periodic maintenance of server system hardware and software, the installation and configuration of ETSD approved desktop software, and the installation and configuration of ETSD approved backup software.
 16. Software Support - ETSD will provide support for ETSD approved software.
 - a. Software support is limited to the integration, functionality, and maintenance of the software, not the use or customization for local purposes. Any maintenance will be performed during maintenance windows; however, during emergency maintenance, OPDS will be contacted immediately with the nature and extent of the maintenance.
 - b. Training may be provided on standard software, if time and resources are available.
 17. OJD Application Support and Access - ETSD will provide data extracts from OJD case management systems for use by OPDS as approved by the State Court Administrator (SCA). ETSD will provide passthrough access to the State of Oregon’s financial system (currently RSTARS). ETSD will provide application and web development services and access to SCA approved statistical dashboards created by OJD.
 18. Assistance to OPDS with ordering and deploying IT hardware and asset tracking by maintaining a database of all OPDS’ deployed hardware.
 19. Provide infrastructure that facilitates access to the internet and internal network communication transportation.
 20. Assistance to OPDS in monitoring and tracking software license compliance for the supported software by maintaining a database of all OPDS’ software.
 21. Other:
 - a. Remote access for OPDS staff will be provided in accordance with existing OJD policies and procedures for the authorization and installation of VPN access.
 - b. Provide and maintain a website for PDSC and OPDS.
 - c. Such other information technology services, the description and cost of which are documented in a fully executed amendment to this Agreement.

B. Responsibilities of OPDS

1. OPDS will provide workstations and other work-related space, as ETSD deems necessary, for ETSD personnel stationed at the OPDS location.
2. OPDS will provide the office and desk furniture for the ETSD people stationed at the OPDS location.
3. OPDS will locate the workstation of the CIO near the OPDS leadership and allow the CIO reasonable access to those in OPDS who are responsible for taking necessary actions as identified by the CIO.

4. OPDS will provide parking for ETSD personnel stationed at the OPDS location.
5. OPDS will be responsible for the purchase and upgrade of desktops, printers, peripherals and server hardware and software application and licensing based upon the recommendation of ETSD for OPDS personnel and systems.
6. OPDS will be responsible for the purchase of extended warranties and service agreements for all hardware and software used in direct support of OPDS.
7. OPDS is responsible for Access database architecture, configuration, and on-going support and maintenance.
8. OPDS will provide an OPDS CIO as soon as practicable to begin the process of building out an OPDS IT section as required by HB 5030.
9. OPDS will be responsible to pay third parties for maintenance performed on out-of-warranty equipment.
10. OPDS will be responsible for any cost incurred for property disposition.
11. OPDS will be responsible for the content on its website and Intranet site.
12. OPDS will provide a data analyst who maintains OPDS access databases, excel input screens/spreadsheets, and assists in the creation of requested reports.
13. OPDS shall develop and execute a plan to transition from a series of unstable Access Databases/Excel Spreadsheets to a more robust data management system capable of simultaneous multiuser access. This plan should include a transition strategy, data migration plan, and identification of a backup system. OJD will not be held responsible for system failures as both parties acknowledge that the current data platform is unstable and prone to disruption.

C. Standards

1. Access Rights - ETSD has exclusive administrative privileges on all OPDS information technology systems needed for providing the service.
2. Service Levels - Computing services and network availability is anticipated to be 24 hours a day, 7 days a week, with scheduled periods of downtime for backup and maintenance. ETSD will make a good faith effort to have the system available 365 days per year, with an uptime target of 99.5%.
3. Scheduled Service Windows – The typical service window will be from 6:00 am until 12:00 p.m. every 3rd Sunday within a calendar month. OPDS will be notified at least 7 days in advance of changes or upgrades that may affect OPDS systems.
4. Support Hours – The ETSD Help Desk is the central point of contact for information and problems regarding OPDS computing resources. Help Desk staff hours of availability are: Monday through Friday- 7:00a.m. until 5:00 pm (PT). Saturday, Sunday, & Holidays – Not Applicable.
Requests for exceptions to normal support must be made through the ETSD Help Desk a minimum of 48 hours (2 business days) in advance. ETSD on a case-by-case basis may honor late requests.
5. Support Response:
 - a. During normal business hours (listed above), the target is for ETSD to make an acknowledgement response to OPDS within 15 minutes from the time the ETSD Help Desk received the support request. Outside normal business hours, the target acknowledgement response time will be no greater than four (4) hours from the beginning of the next business day unless other arrangements have been made.
 - b. ETSD operates on severity level:
Emergency – Department wide, systems down (network outage, server outage, power outage to the building).

High – Individual user system down (computer hardware failure, OS corruption, excluding mouse and keyboard).

Medium – software and program corruption. Failing peripherals. Computer is operational but connecting equipment is not.

Low – Minor customer irritation. User can function but not complete processes in their job.

ETSD escalation response:

Severity	Call Back	Target Resolution	Status call
Emergency	15 minutes	4 hours	Every 1 hour
High	15 minutes	8 hours	Every 2 hours
Medium	15 minutes	2 business days	Every 4 hours
Low	15 minutes	5 business days	Upon closure

6. Disaster Situations - In the event of a complete disaster involving OPDS computing equipment, ETSD will make a reasonable effort to have a viable system available within 5 business days of the disaster.

D. Confidentiality

Both parties agree that each shall hold all Confidential Information of the other party in strict confidence, using at least the same degree of care that it uses in maintaining the confidentiality of its own confidential information; shall not copy, reproduce, sell assign or otherwise give or disclose Confidential Information to third parties; shall not use Confidential information for any purposes whatsoever other than as contemplated by this Agreement or reasonably related thereto.

E. Payment

OPDS shall pay OJD \$41,293.60 per month for the regular services described in this Agreement plus any additional expenses as described herein. OJD will invoice OPDS monthly for amounts due for the immediately preceding month. Invoices will be paid by OPDS within 30 days of invoice date. When OJD is notified in writing that OPDS has assumed the CIO duties, OJD shall adjust the monthly billing rate to reflect the reduction in duties from a CIO to an ITS 4 (Lead). As a result of the change in duties, there will be a corresponding reduction in the per monthly cost.

TKB:gll/L2G21017

Appendix E: OJD IT Support to PDSC

Overview.

The OJD has provided contracted technical support to the PDSC for many years. The current contract is ***Amnd. No. 3_OJD Contract No. 170017fully signed_071221***. The contract was renewed in July 2021, retroactively effective July 1, and will remain in effect until June 30, 2023. The contract stipulates a payment of \$41,293.60 per month, however it also stipulates this amount will be amended when PDSC hires a CIO. This has happened, and PDSC now pays the OJD \$34,417.60 per month.

The contract states *“The Enterprise Technology Services Division (“ETSD”) of OJD will provide information technology management and limited technology infrastructure services for the Office of Public Defense Services (“OPDS”).”* To fulfill this agreement, PDSC receives technical, infrastructure and project support from the following teams at ETSD:

1. Helpdesk.
2. Desktop.
3. Server.
4. Enterprise Information Security Office (EISO).
5. Networking/Telecommunications.
6. Microsoft 365 & Mobile.
7. Web Team.
8. ETSD Management, including CIO, Deputy CIO, Infrastructure and Applications managers, and PDSC Contract Lead.

Helpdesk.

The ETSD helpdesk provides Tier 1 support for PDSC and the OJD. When a PDSC staff member needs assistance, they can call the Helpdesk and speak with a technician directly, or can send an email to the Helpdesk, creating a ticket. When PDSC management has service requests, such as new user account creation, a copier installation, or office moves, these requests are submitted to the Helpdesk as a ticket, as well.

For issues, the Helpdesk functions as Tier 1 support and resolves issues directly or triages the problem and transfers it to Tier 2 support at Desktop, or to one of the Tier 3 specialty teams such as Server, Networking or Web development. Service requests follow this pattern, and are either fulfilled directly by the Helpdesk, or routed to the appropriate team.

ETSD manages tickets using the software *iSupport*. This software is based on the ITIL framework and manages *incidents, larger scale problems, assets, the configuration*

database, and change management procedures. All ETSD staff and management use the iSupport software and can view and interact with all functions.

Desktop Team.

The OJD Desktop team provides Tiers 2 and 3 support to PDSC and the OJD. The team works collaboratively, and each member monitors the PDSC queue and provides support as required based on expertise and availability.

Responsibilities of this team for PDSC include:

1. Tier 2 and 3 technical issues on Windows 10 operating systems, Microsoft Office software, Adobe software products, and other software titles.
2. Hardware troubleshooting and warranty resolution on Dell computers and monitors, Lexmark and HP printers, Fujitsu scanners, Ricoh copiers and other technical equipment.
3. Service requests including new user computer setups and software installs.
4. Service requests to deploy new and existing hardware for staff.
5. Service requests for technical equipment moves and setups, including individual sit/stand desks.
6. Service requests for new printer and copier installations and configurations.
7. Operating system (OS) management, including Windows image creation and maintenance, computer operating system and software upgrades.
8. Security and feature patching Windows OS and software.
9. Technical environmental management with Group Policy and Active Directory, including mapped drive and printer installations and management.
10. Recommendations for technical equipment purchases.

The primary software tools used by the desktop team include many Microsoft products such as System Center Configuration Manager (SCCM) for deploying, upgrading, and patching Windows 10 systems; Windows Server Update Service, for patching Windows 10 systems; Windows Preinstallation Environment (WinPE) and the Diagnostics and Recovery Toolset (DART) tools for troubleshooting and service, Remote Assist and Remote Desktop for remote work, etc. Dell tools are also heavily used, including the various Dell Command components such as Dell Command | Update, Dell Command | Configure, and others. Finally, a critical tool for the Desktop team is PDQ. PDQ includes Deployment and Inventory components, and allows remote installation of software, Windows and other updates, and remote monitoring of computer systems.

Server Team.

The Server team builds, maintains, and supports the PDSC server infrastructure. Approximately two years ago, the ETSD Server team created a new forest and domain for PDSC and set up a dedicated PDSC tenant and configured Azure. PDSC has a two-way trust with OJD and relies on quite a few services that reside on OJD equipment.

PDSC Server Infrastructure.

ETSD supports three physical servers for PDSC—two domain controllers and a general server. ETSD also hosts and licenses seven PDSC virtual servers on our VMware virtual infrastructure. Using virtual servers provides ease of management, fault tolerance, efficient backups and restores, flexibility and scalability, while also segmenting the systems so that only PDSC staff can access them. PDSC data backups run using ETSD's Commvault infrastructure from its primary data center in Salem at the Anderson Readiness Center. ETSD also maintains a second copy of PDSC's data, in case of a disaster, at the OneNeck data center in Bend.

Servers and Services Provided.

1. Domain Controllers to manage user authentication and Active Directory services.
2. DHCP & DNS Servers to dynamically assign and manage network addresses.
3. Microsoft Key Management Services and an Active Directory-Based Activation (ADBA) Server provide Microsoft license activation for workstations and servers for Windows and Office.
4. Certificate Authority servers – root and subordinate(s), provide secure trusts between resources.
5. iSupport ticket management server.
6. Secure password management with Thycotic.
7. Windows Server Update Services (WSUS) provide Window and Server updates to clients and servers.
8. End Point Management Server System Center Configuration Manager (SCCM) allows Desktop to image computers, provides updates for Office 365 (Microsoft Apps for Business) and is part of the Microsoft Advanced Threat Protection infrastructure.
9. Azure Application Proxy servers.
10. Intune Network Device Enrollment Service (NDES) Server for mobile device management.
11. Microsoft BitLocker Administration, Monitoring (MBAM) and Network unlock servers.
12. PDQ Servers (for managing desktops and servers)—licensing, server, administration for Deployment and Inventory services.
13. Nintex server provides SharePoint workflows and automated forms
14. Exchange Server, on premise, provides an Simple Mail Transport Protocol (SMTP) mail gateway for outbound device mail traffic.
15. Server and network monitoring with SolarWinds.

Server Expertise Provided.

- VMware architecture and administration.
- Advanced Server Administration.
- Storage Area Network (SAN) administration.
- Backup administration.

- Exchange administration.
- SharePoint on-prem and in the cloud – operations and development.
- Active Directory administration (including Domain Controllers, Domain Name System (DNS), Distributed File System (DFS), Windows Internet Name Service (WINS), Dynamic Host Configuration Protocol (DHCP), Security, group policies, etc.).
- Tenant / Azure Active Directory (AD) / O365 administration.
- Structured Query Language (SQL) database administration.
- Westlaw support.
- Incident management system administration (e.g., iSupport).

Information Security Office.

The OJD EISO team covers both governance and policy work, plus day-to-day security monitoring tasks. For PDSC they provide the following:

- Incident response: EISO directs incident response with a cross-team group of up to a dozen individuals for any given issue. Incidents may be detected by Microsoft's Advanced Threat Protection, by reports of phishing emails, or by firewall activity.
- Email analysis and blocking, and reports on suspicious email.
- Manage the annual DigiCert renewal, other certificates, and annual VPN certification.
- PDSC benefits from OJD EISO activity, for example blocking dangerous email addresses for PDSC when problem activity was only detected at the OJD.
- Provide security training, education, and assessment for PDSC staff.
- QRadar Security Intelligence software allows efficient and secure analysis of server and network logs.
- Annual third-party Security penetration testing.

Networking/Telecommunications.

The Network and Telecommunications group configures, monitors, updates, and provides Tier 2 and Tier 3 troubleshooting for all network components including OPSD switches, routers, the firewall, wireless infrastructure, and VoIP functions including the VoIP servers, call tree configuration and management, and phone system licensing. In addition, the team procures, maintains, and monitors the LS network connections between PDSC locations, and all internet connectivity. The OJD also provides the network transport for PDSC at two physical locations.

Microsoft 365 & Mobile.

The Microsoft 365 team's primary role for PDSC is to manage their Microsoft online presence and Exchange servers, and to support mobile devices including iPhones and iPads. Various Microsoft 365 components are managed, including the Exchange servers, PDSC tenant, user accounts, and Azure security configurations. Exchange

configuration includes building and maintaining online Azure groups, Multi-Factor Authentication (MFA), mailbox management and email quarantine response.

Web Team.

The Web team manages PDSC's SharePoint online, intranet, and handles break/fix issues. Additionally, the team allocates 24 hours of project work per week for PDSC specific functional requests and development.

The current projects are described in prioritized order below.

1. Priority 1: *Accounts Payable (AP) Intake*. Projected go-live date is January 1. Accounts Payable Intake is an online process allowing vendors (attorneys and law firms) to get paid for their work, like submitting an expense report. The vendor fills out a form, the form is audited, it goes into payment system and the payment is processed. This project uses the Nintex forms and workflow tool. AP Intake is PDSC's number one priority and the project that Web team is currently spending most of the 24 hours a week on. For PDSC, Kimber Sexton is the Web team's primary contact. Keith Koerner is working on the OJD side. They meet at least once but sometimes 2-3 times a week to discuss it.
2. Priority 2: the *Case Load* project went live at the beginning of 2021. Vendors (attorneys and law firms) can submit a form and a .csv file that is reviewed and then the data is added to a SQL database. The data can be viewed through PowerBI. PDSC has continued to work with the Web team adding features, but at a slower pace since it went live. The AP Intake project is currently using most of the Web teams 24 weekly hours, so they are primarily monitoring the Case Load system.
3. *Expense Report Pre-approval* process: before submitting an expense report, staff need pre-approval. This project has not started yet. This project is on hold until AP intake is finished.
4. *SharePoint Online Intranet* development: This project doesn't currently require active work by the OJD. After building PDSC's SharePoint online environment, PDSC is populating it with content. PDSC staff sometimes need help with the work or with building other pages. PDSC's goal is to have a nice front end from the home page.
5. *Six in One Form* project: this is a Nintex form and workflow for six appeals forms. Web team is combining the six forms into one, and this is a workflow that changes the form as data is entered, starting from a common form and ending with the necessary data. This project is mostly on hold until the AP Intake project is complete.

Management.

ETSD maintains a dedicated OJD-PDSC Contract Lead position. This role's responsibility is to manage the PDSC contract from the OJD side, ensuring all

contractual responsibilities are met, and PDSC receives the attention it needs in a timely manner. This individual works closely as a liaison between PDSC's CIO and the OJD teams. A critical part of the support ETSD provides is the capacity to adjust priorities quickly, if necessary, to accommodate immediate needs, and the dedicated PDSC Contract lead plays a significant role in making this possible.

ETSD's management structure, including their CIO, Deputy CIO, and Infrastructure and Applications managers, all provide oversight, insight, and guidance for PDSC both directly, and by managing the teams which support PDSC's technical needs.

Summary.

The OJD provides a wide range of technical services and support for PDSC. This support utilizes seven ETSD teams and provides a comprehensive pool of trained, talented professionals, technicians, and managers. A wide variety of Enterprise class software solutions are utilized. This support is provided to PDSC for a flat monthly fee of \$34,417.60.

Appendix F: OJD Confidentiality Agreement

OREGON JUDICIAL DEPARTMENT EMPLOYEE CONFIDENTIALITY AGREEMENT

By signing below, I am certifying my understanding and acknowledgment that my employment with OJD Enterprise Technology Services Division requires unconditional adherence to the following mandatory conditions of employment:

1. I understand that I must maintain the confidence of any document or file (paper or electronic) containing confidential information involving any employee, judge, division, court, or administration matter.
2. I understand that I must maintain the confidence of any verbal information which I may hear, or overhear, containing confidential information involving any employee, judge, division, court, or administration matter.
3. I understand that “employee” or “judge” includes any candidate or incumbent – present or past.
4. I understand that “confidential information” means and includes, but is not limited to, any matter related to:
 - a) personnel: e.g., personal information protected from disclosure by law, such as social security number; age; address; home phone; medical information; FMLA/OFLA and workers’ compensation information; other personnel related matters such as applicant candidacy; job performance or discipline; grievances or appeals; claims, litigation; collective bargaining.
 - b) payroll: e.g., salary; deductions; leave balances or usage patterns.
 - c) financial: e.g., credit card numbers; bank accounts; other identifying information.
 - d) internal management: e.g., draft, and non-public budget; legal; administrative and legislative materials and information.
 - e) policy and pending matters and discussions that are intended to be confidential.
 - f) IT passwords and accounts: e.g., personal passwords and special access accounts.

Page 1 of 2

- g) IT information: e.g., computer and network information that is sensitive.
- h) Electronic investigations that may be initiated by ETSD and/or another court/division. You are not even to acknowledge the existence of an investigation to those outside of your workgroup/lead worker/supervisor/manager/administrative authority.
- i) As a member of ETSD you may overhear conversations regarding court/division technical information, investigations that may be occurring at a local/statewide level, you may be asked to participate in the gathering of data for an investigation, and/or asked to gather data at the request of your lead worker, manager, or administrative authority. This is considered confidential.
- j) You may also be exposed to personal information as it relates to employees, judges and/or members of the public which could be concerning/disturbing in nature. You are to advise your lead worker, manager, and/or administrative authority should this occur. This is confidential.

Anything else which common sense would define to be confidential.

“If I have any doubt or question about whether something might be in violation of this agreement, I will ask my supervisor or administrative authority before taking any action. I understand each of the above statements and acknowledge that a violation of this agreement may be grounds for appropriate disciplinary action (as outlined in JDPR 9) and that such discipline could include my dismissal.”

Employee Signature

____/____/_____
Date

Appendix G: PDSC IT support Incident Metrics

PDSC iSupport Incidents.

Incidents are emailed to OJD ETSD for review and resolution. All incidents are sent to the ETSD Helpdesk and then forwarded to other groups as necessary to find resolution. The below tables show the PDSC incident tickets sent in 2021. They are grouped by assignment (i.e., the group to handle the request); level 1 is the main category of the incident (i.e., identification of the area where assistance is needed); level 2 and 3 are subcategories (i.e., further detail of the incident (not always applicable)).

Quick Statistics.

- 98% of tickets from the past year have been closed. There were a total of 797 incidents submitted, and only 17 that have an outstanding status (i.e., suspended, open).
- 21% of tickets were closed by first tier support (Help Desk).
- 30% of tickets were closed by second tier support (Desktop).
- Tickets were worked by 65 individual support reps.

Incident Detail.

The information below reflects the 780 incidents that were opened and subsequently closed in 2021.

ETSD DESKTOP.

The largest group of incidents fall to the ETSD_Desktop group. This group provides the delivery and support of products, services, and information on current and future desktop hardware and software (e.g., monitors, scanners, printers, keyboards, mice, docks, external hard drives, USB keys, computers, laptops, variety of software packages, etc.). Responsibilities include documentation, training, consultation, analysis, configuration, procurement, installation, troubleshooting, and support for technology equipment, and responses to incident help tickets for equipment needs, malfunctions, replacements, and other technological issues.

Table 8: Desktop support incidents during 2021.

Category Level 1	Category Level 2	Category Level 3	Sub-Total	Grand Total
ACMS - Web Applications	ACMS, eFiling, Portal	Unspecified	1	1
Administration	Duplicate Ticket	Unspecified	1	1
Facility Management	Move	Unspecified	4	4

Category Level 1	Category Level 2	Category Level 3	Sub-Total	Grand Total
Hardware	All-In-One	Unspecified	3	94
	Copier	Unspecified	2	
	CPU	Desktop	12	
		Laptop	47	
		Server	1	
	Monitor	Unspecified	7	
	Other	Other	7	
Printer	Unspecified	10		
	Scanner	Scanner	4	
Odyssey	Application	Unspecified	2	2
Other	Unspecified	Unspecified	10	10
Security	EISO	Unspecified	1	2
	Threat	Malware	1	
Software	Desktop Applications	Adobe Acrobat Reader	1	80
		Adobe Professional	8	
		Google Chrome	1	
		Hyperion	1	
		Internet Explorer	1	
		iSeries Access for Windows	1	
	FTR	Unspecified	2	
	Microsoft	Access	2	
		Bit locker/MBAM	2	
		Edge	3	
Office Suite		1		
Other		1		
Outlook	6			
	Power BI	8		
	Project	1		
	Visio	4		
	Word	4		
Operating System	Windows 10	12		
Other	Unspecified	20		
WEB Applications	Other	1		
System Administration	Domain	Unspecified	2	6
	Microsoft 365	Power BI	2	
	Web	OJD SharePoint	1	
	Windows Server	Unspecified	1	
Telecommunications	VoIP	Unspecified	1	6
	VPN	Unspecified	4	
	Wireless	Unspecified	1	
User Administration	Create User	Unspecified	9	28

Category Level 1	Category Level 2	Category Level 3	Sub-Total	Grand Total
	Modify User	Unspecified	9	
	Remove User	Unspecified	10	
GRAND TOTAL				234

ETSD HELPDESK.

The second largest group of incidents falls to the ETSD_Helpdesk group. This group provides rapid response support to troubleshoot problems and provide information to customers. This team works with other teams in ETSD to route incident tickets when they cannot be resolved at the first or second tier levels and maintains a large database of procedures used to resolve many types of technical problems.

Table 9: Help Desk Incidents during 2021.

Category Level 1	Category Level 2	Category Level 3	Sub-Total	Grand Total
ACMS - Web Applications	ACMS	Other	3	6
	ACMS, eFiling, Portal	Unspecified	3	
Administration	Duplicate Ticket	Unspecified	2	8
	Resources - Personnel	Unspecified	1	
	This is not a problem	Unspecified	5	
Hardware	CPU	Laptop	7	11
	Monitor	Unspecified	2	
	Printer	Unspecified	1	
	Scanner	Scanner	1	
Odyssey	Public Access	OECl - External	7	9
		OECl - Internal	2	
Other	Unspecified	Unspecified	18	18
Security	RSA	Unspecified	1	1
Software	Desktop Applications	Adobe Acrobat Standard	1	44
	Law Reference	Westlaw	2	
	Microsoft	Access	1	
		Bit locker/MBAM	3	
		Edge	1	
		OneNote	1	
		Outlook	7	
		Teams	1	
		Word	2	
	Operating System	Windows 10	21	
	Other	Unspecified	3	
	WEB Applications	Other	1	
System Administration	Domain	Unspecified	1	8
	iSupport	Other	1	
	Microsoft 365	MFA	1	

Category Level 1	Category Level 2	Category Level 3	Sub-Total	Grand Total
	Security	Unspecified	4	
	Web	Internet	1	
Telecommunications	LAN	Unspecified	3	13
	Other	Unspecified	1	
	Secure File Transfer Protocol	Unspecified	1	
	Telephones	Phone Outage	1	
	VPN	Unspecified	7	
User Administration	Create User	Unspecified	14	44
	Modify User	Unspecified	23	
	Remove User	Unspecified	7	
			GRAND TOTAL	162

Other Groups.

Incidents are grouped by assignment; level 1 is the main category of the incident; level 2 and 3 are subcategories to further detail the incident (not always applicable). These groups support various functions: financial; electronic filing (efiling); online paid subscription; security; servers; telecommunications; Microsoft 365 products; mobile devices; and security training.

Table 10: Other incidents handled during 2021.

Group Name	Category Level 1	Category Level 2	Category Level 3	Total	Grand Total
BFSD_FIAS	E-mail Submitted	Unspecified	Unspecified	2	9
	Other	Unspecified	Unspecified	6	
	Software	Microsoft	Power BI	1	
BFSD_FIAS Total				9	
COA	Other	Unspecified	Unspecified	1	1
COA Total				1	
ETSD_ACMS_E-Filing	ACMS - Web Applications	ACMS, eFiling, Portal	Unspecified	1	10
		e-Filing	Other	1	
	User Administration	Modify User	Unspecified	3	
		Remove User	Unspecified	5	
ETSD_ACMS_E-Filing Total				10	
ETSD_Help_Desk_OJCINOnline	User Administration	Create User	Unspecified	4	17
		Modify User	Unspecified	10	

Group Name	Category Level 1	Category Level 2	Category Level 3	Total	Grand Total	
		Remove User	Unspecified	3		
ETSD_Help_Desk_OJCIOnline Total				17		
ETSD_Management	User Administration	Create User	Unspecified	7	7	
ETSD_Management Total				7		
ETSD_Microsoft 365	Administration	Duplicate Ticket	Unspecified	1	106	
	Other	Unspecified	Unspecified	4		
	Software		Microsoft	Office Suite		1
				OneNote		1
				Outlook		13
				Power BI		3
				Visio		1
		Other	Unspecified	2		
	System Administration	Domain	Unspecified	1		
		Microsoft 365	Exchange	34		
		MFA	6			
		Power BI	1			
	User Administration	Create User	Unspecified	12		
		Modify User	Unspecified	16		
		Remove User	Unspecified	10		
ETSD_Microsoft 365 Total				106		
ETSD_Mobile	Hardware	Mobile Device	iPad	8	25	
			iPhone	5		
			Other	1		
	System Administration	Microsoft 365	MFA	2		
		MobileIron	Unspecified	1		
	User Administration	Modify User	Unspecified	2		
		Remove User	Unspecified	6		
ETSD_Mobile Total				25		
ETSD_Odyssey_Support	Odyssey	File and serve	Unspecified	1	9	
	User Administration	Modify User	Unspecified	3		
		Remove User	Unspecified	5		
ETSD_Odyssey_Support Total				9		
ETSD_Remote_Hearing_Support	Software	Webex	Unspecified	1	1	
ETSD_Remote_Hearing_Support Total				1		
ETSD_Security	Other	Unspecified	Unspecified	1	24	
	Security	EISO	Unspecified	2		

Group Name	Category Level 1	Category Level 2	Category Level 3	Total	Grand Total
		RSA	Unspecified	1	
		Threat	Malware Phishing	2	
	Software	Other	Unspecified	2	
	System Administration	Microsoft 365	Exchange	1	
			Other	1	
		Palo Alto	Unspecified	2	
		Security	Unspecified	4	
Telecommunications	Other	Unspecified	2		
ETSD_Security Total				24	
ETSD_Server	Hardware	CPU	Server	1	59
	Other	Unspecified	Unspecified	5	
	Security	Threat	Malware	1	
	Software	Microsoft	Power BI	2	
	System Administration	Data Recovery	File/Folder Restoration	1	
		Domain	Unspecified	8	
		Microsoft 365	Other	2	
		Network	Other	2	
		SQL	Other	1	
		Windows Server	Unspecified	21	
	User Administration	Modify User	Unspecified	8	
Remove User		Unspecified	7		
ETSD_Server Total				61	
ETSD_SQL_Admin	System Administration	SQL	Other	3	4
		Windows Server	Unspecified	1	
ETSD_SQL_Admin Total				5	
ETSD_Telecommunications	Administration	Duplicate Ticket	Unspecified	1	36
	Software	Other	Unspecified	1	
	System Administration	Network	Other	1	
		Web	OJD SharePoint	1	
	Telecommunications	Other	Unspecified	1	
		Secure File Transfer Protocol	Unspecified	1	
	Telephones	Phone Support	1		

Group Name	Category Level 1	Category Level 2	Category Level 3	Total	Grand Total
		VoIP	Unspecified	4	
		VPN	Unspecified	3	
	User Administration	Create User	Unspecified	9	
		Modify User	Unspecified	5	
		Remove User	Unspecified	8	
ETSD_Telecommunications Total				38	
ETSD_Training	Software	Microsoft	Outlook	1	16
	User Administration	Create User	Unspecified	6	
		Modify User	Unspecified	3	
		Remove User	Unspecified	6	
ETSD_Training Total				16	
ETSDWeb	System Administration	Web	Internet	6	17
			OJD SharePoint	2	
			Other	1	
	User Administration	Modify User	Unspecified	3	
	Remove User	Unspecified	5		
ETSDWeb Total				18	
OJCIN_OnLine	ACMS - Web Applications	ACMS	Administration	1	5
	User Administration	Create User	Unspecified	2	
		Remove User	Unspecified	2	
OJCIN_OnLine Total				5	
OJD Law Library	User Administration	Remove User	Unspecified	5	5
OJD Law Library Total				5	
PDSC Techs	Other	Unspecified	Unspecified	2	26
	Software	Desktop Applications	Adobe Professional	1	
			Internet Explorer	1	
		Microsoft	Access	19	
			Word	1	
Telecommunications	VPN	Unspecified	1		
User Administration	Create User	Unspecified	1		
PDSC Techs Total				26	
SCMS Support	User Administration	Modify User	Unspecified	2	7

Group Name	Category Level 1	Category Level 2	Category Level 3	Total	Grand Total
		Remove User	Unspecified	5	
			SCMS Support Total	7	
				Grand Total	384