Oregon
Kate Brown, Governor

Department of Administrative Services
Office of the State Chief Information Officer
155 Cottage St NE, 4th Floor
Salem, OR 97301
PHONE: 503-378-3175
FAX: 503-378-3795

20 February 2017

The Honorable Senator James Manning Jr., Co-Chair
The Honorable Representative Greg Smith, Co-Chair
Joint Committee on Ways and Means Subcommittee on General Government
900 Court Street NE
H-178 State Capitol
Salem, OR 97301-4048

RE: Answers to questions asked during public testimony on HB 5002 (2017)

Dear Co-Chairpersons:

The Office of the State CIO (OSCIO) respectfully requests that the Joint Committee on Ways and Means Subcommittee on General Government acknowledge receipt of answers to the following questions asked during public testimony on HB 5002 (2017), including:

1. **Statewide Cybersecurity Risk Assessment (E.O. 16-13).** To what extent has the Enterprise Security Office (ESO) executed the IT Infrastructure Review (agency IT technical practices, architecture and infrastructure)?
2. **IT Outsourcing.** What is our Office doing to address the increasing reliance on IT professional services and cloud solutions (*i.e.,* software as a service [SaaS]; infrastructure as a service [IaaS]; and platform as a service [PaaS])?
3. **Risk Mitigation.** How do we currently limit the state data center's liability for non-state agency customers resulting from loss of data or loss of data integrity?
4. **Non-Stage Gate Projects.** What is the decomposition of non-stage gate projects currently under OSCIO oversight?
5. **Rural Job Loss.** To what extent, if any, was our Office involved in the decision to not renew a contract for call-center services in Baker City, Oregon?

1. Statewide Cybersecurity Risk Assessment (E.O. 16-13).

Governor Brown's Executive Order 16-13, "Unifying Cyber Security in Oregon" (EO 16-13) represents a fundamental shift in how the state of Oregon approaches IT security. At a fundamental level, IT security is about trust—as public servants and custodians of public data, we owe Oregonians a duty to protect their personal information. Regardless of agency mission or size, Oregonians rightfully expect their government to use technology to improve customer service while ensuring those systems are secure and that personal information is subject to consistent protections. Citizen expectations of privacy, should not hinge on the agency with whom they are transacting—be it the Department of Motor Vehicles or Department of Fish and Wildlife (ODFW).

EO 16-13 is the first step towards addressing persistent IT security vulnerabilities and represents the next phase of Oregon's IT security evolution. It has enabled the implementation of a statewide agency-by-agency risk-based security assessment and remediation. While implementing change is inherently disruptive, our Office has made the continuity of IT security operations our first priority—keeping the majority of IT security personnel, protocols and tools in place while working to strengthen the statewide community of IT security professionals.

The planning and initial execution of EO 16-13 has matured substantially since the completion of Secretary of State's Audit No. 2016-30, *"Improving State Computer Systems will take Time, Resources, and Cooperation"*—with definition of deliverables, timelines, and regular reporting of status and metrics being fully in place at

this time. Unfortunately, given timing of EO 16-13, this information was not available to be included in audit findings. Our Office had two interviews with the Secretary of State in early September of this year, and the executive order was signed days later on September 12th 2016. The plan for implementation EO 16-13 includes four primary deliverables, developed in collaboration with agencies, boards and commissions, including:

- Completion of an Enterprise Information Security Risk (EISR) Assessment
- Publication and implementation of a new Enterprise Security Plan
- Implementation of an Enterprise Vulnerability Management Program
- Implementation of Enterprise Security Awareness Program

In support of these deliverables, our Office has conducted a statewide IT security survey, initiated public procurements to obtain third-party risk assessments and security awareness training. Additional details regarding the Enterprise Information Security Risk (EISR) Assessment will be provided below. Additionally, our Office has worked with the DAS Chief Human Resource Office and the Department of Justice to develop an Interagency Agreement (IAA) to facilitate the transfer of IT security functions and personnel from November 1, 2016 until June 30, 2017 (the end of the current biennium). As of December 5th 2016, our Office had executed 47 IAAs, covering all agencies that currently have IT security positions and the 20 agencies that are part of the first phase of the EISR assessment.

As previously mentioned, the first phase of the assessment includes 20 agencies. Given the sensitivity of IT security information, our Office is not publicly identifying these agencies. The selection of agencies was informed by the enterprise-wide IT security survey, and took into consideration agency size, the sensitivity of agency data and whether the agency had recently undergone a comprehensive IT security review. Taken together, the 20 agencies represent well over 30,000 FTE. In order to ensure cross-agency consistency and comparability, the assessment methodology is based on the NIST Cybersecurity Framework (a national standard that has been widely adopted by other states). Additionally, given cross-agency variation in terms of IT systems, sensitive data and externa-facing applications, our Office has taken a modular approach to the assessment.

Our Office has developed six assessment modules, including:

1. **Internal Nessus scan.** Internal scanning will be performed with the ESO Tenable scanning tools or with compatible vendor tools.
2. **Cybersecurity Profile.** Interview and assessment findings will inform NIST Cybersecurity Framework profile of agency security posture
3. **Infrastructure.** The technical architecture and practices assessment will evaluate agency IT infrastructure (e.g., agency data-centers and servers) and may include internal credentialing scans
4. **External Web Application Scan.** The external application scan will provide an inventory and assessment of all external-facing web applications
5. **Application Security Assessment.** The assessment will include a security review of all applications, application development practices and training
6. **Level 4 Data Practices Assessment.** An assessment of how agencies handle data classified as Level 4 – Critical

The following provides a brief overview of our progress to date—primarily, on internal vulnerability scanning and the external web application scanning.

Internal Vulnerability Scanning

Internal vulnerability scanning involves the use of automated tools to identify known vulnerabilities in servers, PCs, and network equipment (endpoints). This is a good indicator of the vulnerability level of each

discrete endpoint in our environment. Our goal is to implement automated scanning of at least 80% of our endpoints by end of 2015-17 biennium. At present, we estimate there are about 70,000 endpoints in the executive branch. Prior to the executive order, only a handful of agencies were scanning 33,000 endpoints with varying frequency (often less than every 90 days). Additionally, there was no tracking of critical vulnerabilities. Vulnerabilities are considered "Critical" when they are easily discoverable and exploit for significant damage.

Since E.O. 16-13 we have implemented internal scanning within 34 agencies covering 46,000 end points—roughly a 40% increase. On average, internal scanning has identified over 3 critical vulnerabilities per endpoint across the enterprise. The agency-by-agency averages ranges from between 0.4 – 8+ critical vulnerabilities per endpoint. Additionally, we have adopted quarterly scanning as a minimum requirement. The aggregated results of these findings are driving the establishment of remediation priorities for the enterprise.

External Vulnerability Scanning

External vulnerability scanning involves the use of automated tools and professional penetration testers to identify and validate vulnerabilities in public facing external web applications and systems. This is a good indicator of the vulnerability level of the online services we expose to the public from an external attacker's perspective. Our goal is to implement standardized external scanning and evaluation of the top 26 (based on relative risk) agency's publicly exposed applications and systems by end of the 2015-17 biennium. Prior to EO 16-13 there was no consistent testing of the externally facing applications and systems. In some cases, agencies lacked an inventory of their external-facing applications. To date, the external vulnerability scanning has resulted in the identification and remediation of 4 significant vulnerabilities.

Other Assessment Modules

As discussed during the presentation, our Office is still working to implement the other modules contained in the EISR assessment on a rolling basis though a nine-vendor multi-award request for proposals (RFP). Currently, there 9 of the 20 agencies in the first phase undergoing the other assessment modules—results from these assessments should be available by the end of March. Additionally, statements of work are currently under development for an additional 5 agencies.

2. IT Outsourcing.

While the State of Oregon is already transitioning to new models of service delivery for its information technology (IT), application and telecommunications needs, there is a growing recognition that traditional approaches to IT acquisition and vendor management are increasingly inadequate—given emergent technology, changes in the IT market place, the sophistication of IT procurements and the resulting vendor relationships. In effect, it is no longer cost-effective for the state to own or maintain the entirety of its IT portfolio. As the state pivots towards new service models, including infrastructure-as-a-service (IaaS), platform-as–a-service (PaaS) and software-as-a-service (SaaS)—i.e., "the cloud"—it is evident that there is lack of statewide capacity to manage increasingly sophisticated IT vendor relationships. Furthermore, in the absence of coordinated procurement and enterprise architecture, public cloud adoption will remain disjointed and fail to realize its potential cost-savings and business benefits.

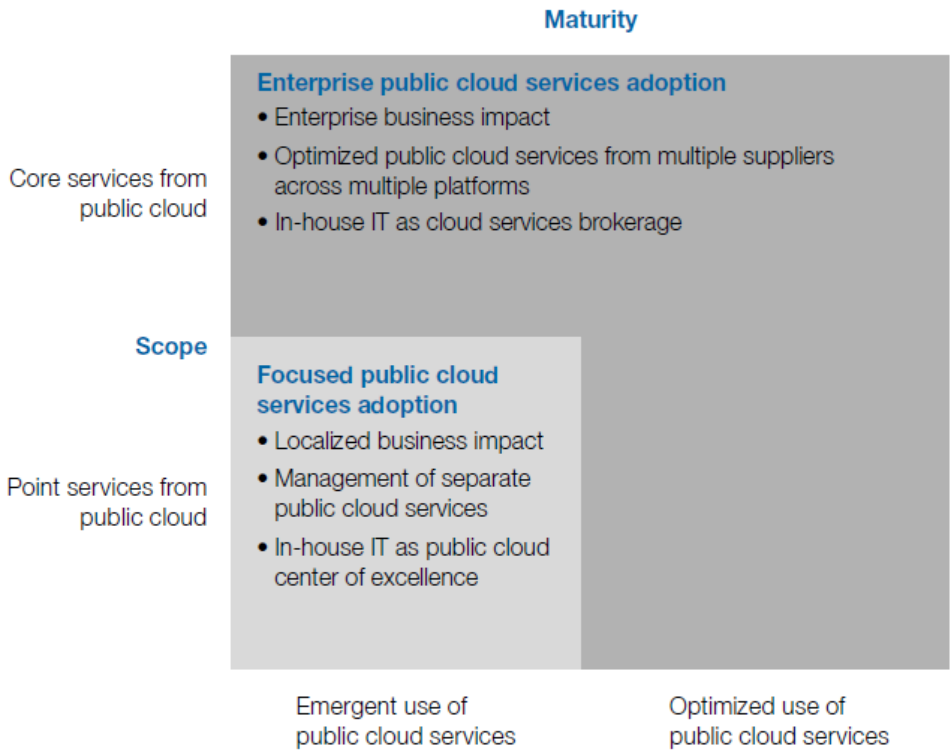
Continued implementation of the "Basecamp" initiative—a value-added online marketplace for shared information technology services, will enable the state of Oregon to leverage enterprise architecture to mature cloud services adoption and increase coordination of IT procurement. Basecamp is a market-driven approach that is intended to be self-sustaining. Unlike the current approach, future statewide price agreements under Basecamp would be driven by the establishment of a comprehensive and cohesive technology architecture that ensures interoperability, while minimizing cost and disruption to current systems (*i.e.,* a technology reference model). Ultimately, Basecamp will reduce IT spending and drive enterprise cloud deployment by aggregating statewide purchasing power, reducing IT application and infrastructure complexity and

providing a single point reference for legacy, core and leading technology in the state of Oregon. It will provide a one-stop shop and IT roadmap for state agencies, local government affiliates and school districts alike and enable them to focus on what matters most—investing in programs that serve the citizens of Oregon and putting money back in the classroom.

In *"Preparing the In-House IT Organization for Public Cloud,"* Gartner discusses the opportunities and challenges associated with pivoting towards the public cloud and provides a roadmap that considers both the scope of adoption and organizational maturity. Cloud computing is defined by Gartner as "a style of computing where scalable and elastic IT-related capabilities are provided 'as a service' to customers using Internet technologies." The "public" of public cloud represents one pole on a continuum of delivery models, whereas IaaS, PaaS and SaaS represent methods of deployment. Beyond the benefits of on-demand services with flexibility, agility, scalability, reach and potential cost-savings, successful cloud deployment enables IT organizations to transition from a supplier- to a brokering and servicing-orientation.

Within the Gartner cloud services roadmap there are two phases of development, including: "Focused public cloud services adoption," and "Enterprise public cloud services adoption." Within the first phase of cloud deployment, the scope of adoption is project specific, focused on point solutions and requires the development of basic supplier management capabilities. In the second phase, the scope of adoption has an enterprise impact, enables the optimization of services across platforms and is characterized by cloud services brokerage.

Gartner (2016). *Public cloud services roadmap*



From an enterprise perspective, the state of Oregon currently lacks both the capacity and capabilities to engage at a focused-level of cloud adoption. Consistent with the garbage-can model of decision-making, many agencies have identified specific cloud solutions without having defined the problem. Even worse, there are any number of unauthorized cloud services (*e.g.,* dropbox) being deployed across the state—notwithstanding

issues of security, data sovereignty and click-through terms and conditions that compromise the interests of the state (*i.e.,* choice of venue or binding arbitration). However, the larger issue with unfocused cloud adoption will be further fragmentation of the business of state government—resulting the replacement of agency-specific legacy systems with intra-agency micro-silos. While ad hoc adoption of cloud services may increase the efficiencies of specific individuals and small teams, uncoordinated adoption of cloud services may have unintended consequences and generate inefficiencies across the enterprise.

While the implementation of Stage Gate and the incremental funding and development model for large-scale IT projects is a critical step forward in terms of oversight, it does little to address cloud-related issues, increase coordination of IT procurement or ensure alignment between IT cloud services and the business of state government. Ultimately, the simplest way to reduce IT spending by state agencies, local governments and school districts is through standardization. While IT consolidation may achieve standardization through a forced march, coordinating IT procurement and standards through the establishment of a technology reference model offers a market-driven and voluntary alternative. In most cases, the technologies underlying the technology reference model are utility or share services. These services are scalable, commodity in nature and unseen to the end-user—*i.e.*, *where the differences don't make a difference.*

3. Risk Mitigation.

At present, the intergovernmental agreement (IGA) template executed with non-state agency customers of the state data center does not include liability provisions regarding potential damages associated with loss or corruption of data. However, non-state agency customers have traditionally only purchased back-up services, as opposed to obtaining managed services and running their applications and data in a production environment. The risk of losing back-up data for these customers is further mitigated through our mutual aid partnership with Montana—enabling offsite backup and disaster recovery. With that said, our Office will consult with the Department of Justice to evaluate the possibility of amending our current IGA template to further mitigate this risk and state exposure.

4. Non-Stage Gate Project

At present there are 18 non-Stage Gate projects under OSCIO oversight, representing a range of values and varying business capabilities. The non-Stage Gate portfolio is summarized below with project name, agency, budget, project objective and an explanation as to why the project was not required to complete the full stage gate review. The majority of the projects are relatively low-risk and fall well under the $1 million threshold typical of most stage gate projects. Several of the projects that exceed $1 million were already into the execution phase (stage 4) when the stage gate review process was first put into place. Whereas in other projects exceeding the $1 million threshold, the project represents an upgrade of existing hardware (*e.g.,* traffic cameras) or a software upgrade (*e.g.,* Windows 10 upgrade).

DAS Parking Facilities Management System | Department of Administrative Services (DAS)

- **Budget.** $255,000
- **Objective**. Legacy parking permit management system replacement to improve reliability, maintainability, operations, and security.
- **Non-Stage Gate Explanation.** Software-as-a-Service solution with 5-year initial term. Service improvements with minimal added risk.

Management Information System (MIS) | DAS

- **Budget.** $331,909
- **Objective**. Legacy Print Plant information system replacement for end-of-life inventory, billing, and scheduling application.
- **Non-Stage Gate Explanation.** Small hardware and software purchase for on-premise solution. Simple solution for business need, includes 5-years of maintenance.

Data Manager Application (IDEA) | Oregon Education Department (OED)

- **Budget.** $540,000
- **Objective**. Mandatory federal reporting requirement poorly met with existing multi-system solution. Legacy replacement to ensure ability to meet reporting requirements implementing web-based, modern, flexible, and scalable technology.
- **Non-Stage Gate Explanation.** Modest investment to provide a streamlined system. Reviewed for solution viability.

Healthy Families Oregon (HFO) Data System | OED

- **Budget.** $367,000
- **Objective**. Acquire a modern solution to streamline the collection, tracking and analysis of Healthy Families Oregon data and to ensure Oregon Early Learning Division and Oregon Health Authority (OHA) utilize a data system that provides the ability to integrate information for early childhood programs in Oregon in compliance with ORS 417.795.
- **Non-Stage Gate Explanation.** Modest investment in a system that would enable streamlined integration with a system that was selected through a competitive process by OHA for early childhood programs.

Student Centralized Administrative Reporting File (SCARF) Conversion Project | Higher Education Coordinating Commission

- **Budget.** $200,000
- **Objective**. Migrate legacy post-secondary student database to fully-supported, agency-standard environment.
- **Non-Stage Gate Explanation.** Mature, operational process with minimal risk to data and infrastructure.

MMIS T-MSIS Project | Oregon Health Authority

- **Budget.** $2,416,670
- **Objective**. This project supports Oregon's ability to broadly expand the collection, analysis, and reporting of Medicaid information to create an integrated view of Medicaid and the Children's Health Insurance Program [CHIP] activities. This supports improved policy and program decision-making as well as improved ability to monitor and predict costs and to detect fraud, waste, and abuse. This project was mandated to meet new CMS requirements.
- **Non-Stage Gate Explanation.** Project was well into execution (Stage 4) prior to the implementation of the Stage Gate Process.

Web Portal Upgrade | Department of Justice

- **Budget.** $622,759
- **Objective**. This project creates an effective tool that facilitates citizen access to the services, support, education and protections they need.
- **Non-Stage Gate Explanation.** Project was low risk and in total cost. Project was also in the execution process (Stage 4) prior to the implementation of the Stage Gate Process.

Frame Relay Replacement Project | Military Department

- **Budget.** $1,500,000
- **Objective**. The frame relay replacement project improves service delivery to critical statewide emergency communications by increasing reliability of the existing 9-1-1 system. The Ethernet infrastructure also positions Oregon to take advantage of next generation technologies that will further enhance service delivery to Oregonians such as text to 9-1-1, video to 9-1-1 and more accurate digital geolocation for 9-1-1 phone calls.

- Non-Stage Gate Explanation. Operational replacement of legacy infrastructure. Mature technology, and incremental funding unneeded (multiple straightforward conversions done around the state).

Medical Records Improvement Project | Oregon State Police

- **Budget.** $150,000
- **Objective**. Convert legacy client-server application to modern, online case management system to improve application functionality to improve workflows and record keeping associated with death investigations.
- **Non-Stage Gate Explanation.** Modest 5 year investment to provide improved capabilities in support of Medical Examiner Office forensic investigations with minimal project risk.

Grant Management Software | Oregon Department of Aviation

- **Budget.** $492,240
- **Objective**. Provide grant management solution to meet requirements defined by legislative mandate.
- **Non-Stage Gate Explanation.** Project incorporates application functionality that has been used by other Oregon agencies, includes 6 years of operating costs, and did not meet the risk threshold to require Stage Gate oversight.

CRM Replacement Project | Oregon Business Development Department

- **Budget.** $727,390
- **Objective**. Replacement of the current customer relationship management – CRM (Act!) with a modern and extensible tool that allows the agency to effectively measure its programs across the agency through reporting and metrics.
- **Non-Stage Gate Explanation.** Small procurement investment to acquire a solution integrator and under the $1 million threshold.

PRISM | Oregon Employment Department

- **Budget.** $1,155,233
- **Objective**. Effort to redesign and upgrade PRISM to better meet the data and policy needs of Oregon and federal policy makers. This includes incorporating additional programs and data sources, linking workforce and education data, enhancing the use of longitudinal data for program evaluation, and improving the user-friendliness of PRISM data and interfaces.
- **Non-Stage Gate Explanation.** Project resources are internal.

DMV-Driver License Issuance Replacement (DLIR) | Oregon Department of Transportation (ODOT)

- **Budget.** $2,300,000
- **Objective**. The purpose of this project is to procure a third-party vendor to replace the current Digital Photo License (DPL) system. The 15-year contract has an estimated worth exceeding $38 million.
- **Non-Stage Gate Explanation.** Project was well into execution (Stage 4) prior to the implementation of the Stage Gate Process.

DMV-Microfilm Replacement (MR) | ODOT

- **Budget.** $4,500,000
- **Objective**. The purpose of this two phase project is to replace DMV's current microfilming solutions with new digital imaging solutions.
- **Non-Stage Gate Explanation.** Project was well into execution (Stage 4) prior to the implementation of the Stage Gate Process.

TAD-Bridge Phase 2 | ODOT

- **Budget** $406,200

- **Objective**. The ability to evaluate the overall health of Oregon's bridges.
- **Non-Stage Gate Explanation.** Project is being performed and executed in-house and presents low cost and risk to the agency.

TAD-Employee Reimbursement | ODOT

- **Budget.** $539,875
- **Objective**. Provides an automated application for processing employee travel and expense requests to replace the current manual spreadsheet form. Training will also be developed within the scope of this effort.
- **Non-Stage Gate Explanation.** ODOT was operating under an interim memo that stated that they could execute a project if it was under $1 million and notification was provided to the OSCIO.

TAD-ITS Video Distribution Regional Deployment | ODOT

- **Budget.** $510,000
- **Objective**. Transportation surveillance cameras are used throughout the state by ODOT to monitor road conditions, traffic congestions and incidents. ODOT cameras are installed in areas of high accidents, heavily traveled sections of highways and locations with weather and safety concerns. This project focuses on switching over from the old video distribution infrastructure to the new infrastructure for the remaining three ODOT regions. ODOT will realize a net reduction in IT components by alleviating analog video equipment, allowing for easier maintenance and operational support.
- **Non-Stage Gate Explanation.** ODOT was operating under an interim memo that stated that they could execute a project if it was under $1 million and notification was provided to the OSCIO.

TAD-Windows 10 and Office 201+B2:C196 Upgrade | ODOT

- **Budget.** $663,282
- **Objective**. ODOT Information Systems Enterprise Technology will work in conjunction with OMV, Motor Carrier, and Transportation Application Development groups to adapt and remediate existing applications to the new Windows 10 Operating System for the entire agency.
- **Non-Stage Gate Explanation.** ODOT was operating under an interim memo that stated that they could execute a project if it was under $1 million and notification was provided to the OSCIO.

5. Rural Job Loss.

According to recent press coverage, the Oregon Health Authority (OHA) recently decided not to renew a $2.5 million contract for call center services from Chaves Consulting. The call center is located in Baker City, Oregon and it employed 54 employees for the OHA call center. While our Office enjoys a partnership with Chaves consulting as a contract provider for the state data center and through the Oregon Records Management System, our Office was not involved in OHA's decision not to renew the contract for call center services in Burns, Oregon.

Sincerely,

Alex Z. Pettit, Ph.D.
Chief Information Officer

Cc: Paul Siebert, Legislative Fiscal Office
Ken Rocco, Legislative Fiscal Office
Patrick Heath, Chief Financial Office