State of Nevada
SFY20/21 I&T Strategic Plan

I am excited to present the State of Nevada Information & Technology Strategic plan for SFY20/21: "Embarking on The Road to Unity."

The concept of the Road to Unity (R2U) was built upon recognizing and leveraging the benefits of a distributed, but tightly coupled, I&T support model for the Executive Branch and other entities we serve. We all have requirements to modernize our technology to keep up with ever-changing business needs. In order to approach modernization in a fiscally responsible way we need to focus, when possible, on shared, scalable Enterprise Solutions. For this model to be successful and cost-effective we need to work better together.

While there are a number of elements of technological change in the strategy, for this first phase the overarching theme is the importance of communications, collaboration, engagement and governance. Technology initiatives require budget authority - however a higher level of engagement **does not** - and this engagement will pay dividends in the future by creating an environment of collaboration and trust which will then increase our ability to partner on solutions and make decisions for the good of Nevada.

Guiding Principles

To build a holistic strategy we solicited feedback from our customers, leadership, and internal IT support teams. The first step was to establish guiding principles, or "why" we do everything we do – the most important principle for any organization. The guiding principles established are:

1. We are invested in the services that State agencies provide to Nevada residents and visitors.
2. We believe in efficient and secure implementation of technology to meet the needs of the agencies we serve.
3. Collaboration and partnership are essential to our success.

Strategic Pillars

Page 2 of this document details the Actions & Outcomes that will be our shared goals in SFY20/21 (actions subject to Legislative approval are noted with an *). These Actions & Outcomes are broken down into **five functional pillars**:

Information Security It is a given that we must protect the integrity, confidentiality and availability of State information. The SFY20/21 goals are to stay current with security technology, and to improve the efficiency and coordination of these efforts by tightly coupling the activities of the State Office of Information Security (OIS), the Office of Cyber Defense Coordination (OCDC) and the agency Information Security Officers (ISOs).

Architecture and Solutions For this pillar our primary objective is to establish a formal solutions architecture process and strengthen the tools and communications used for solutioning. For example, we will continue to refine the Technology Investment Notification (TIN) process to solicit complete requirements and business intelligence in order to select the best solutions across our enterprise.

Ecosystem, Platforms and Support Key concepts for this pillar are improving our support processes and favoring enterprise solutions over silos when possible. Our aspirational goal is to implement a shared compute platform in SFY20/21. This virtual computing environment, which we are calling the "Unity Platform" will be the go-to resource for agency compute and storage needs for on-prem applications.

Communications and Engagement Increasing our communications and collaboration across our distributed organizations is critical to our success – therefore this is a stand-alone pillar. A highlight is the requirement to collaborate across the Executive Branch agencies in conjunction with the Office of the CIO to develop I&T strategic plans within a common framework.

Governance This is key to aligning our organizations and efforts, and ensuring the best decisions are made for everyone. Governance structure and a decision framework for enterprise applications is fundamental to adoption and customer satisfaction. Initially our application-specific governance efforts will focus on O365 and this will create a model for future enterprise solutions.

Organization and Business Alignment

To align the central IT organizations with the R2U strategy and goals, as well as improve communications and align support with business needs, some organizational enhancements and changes are required. Going forward State central IT will be known as **CORE Information and Technology (CORE I&T)** and consist of:

Office of the CIO or OCIO Includes the Chief Information Officer, Chief Enterprise Architect, Chief of Policy and Communications, Chief of Grants and Research, Chief Information Security Officer (CISO), CORE IT Administrators, and fiscal support. Organizing CORE policy- and decision-makers with the newly established Communications and Architecture functions will drive a high level of transparency and coordination with our customers.

Enterprise IT Services (EITS) and Agency IT Services (AITS). AITS will be a stand-alone organization led by an Administrator, and as a peer organization to EITS will report to the State CIO. This will facilitate much needed separation of application, desktop and Tier 2 support from Enterprise IT (contingent upon Legislative approval).

CORE Security includes the State Chief Information Security Officer (CISO) and State Office of Information Security (OIS). The CISO now reports directly to the State CIO, eliminating any bias resulting in working from within the EITS organization. CORE Security will coordinate closely with OCDC which serves State entities outside the purview of CORE Security.

It is important to note that this is a living document. It evolved as we solicited feedback and "test drove" revisions, and it will continue to evolve. Please feel free to send comments and suggestions to NV-CIO@admin.nv.gov. It is my hope that you are as excited as we are to embark on this journey!

I look forward to a continuing conversation with you,

Michael

Michael Dietrich, State CIO

	Information Security	Architecture & Solutions	Ecosystem, Platforms & Support	Communications & Engagement	Governance
Outcomes	**Secure.** The integrity, confidentiality, and availability of State information, ecosystems and other digital assets is protected. The State security posture is continuously improved through enforceable policies, ongoing assessments and appropriate corrective actions. CORE Security teams continue to anticipate and adapt to evolving technologies and emerging threats and serve as advisors to agency security organizations.	**Solve.** The CORE Information and Technology (CORE I&T) groups are trusted advisors and partners to agencies and other entities as they devise their IT strategies. High quality, cost-effective solutions are designed and delivered that meet the business needs of our customers. The complete solution, including "what done looks like" from the customer point of view, is well understood by all parties in the design and delivery of these solutions.	**Provide.** Infrastructure, platforms and support services are delivered that meet the needs of agencies, their IT departments, and the information workers served by these entities. Transparency and collaboration are built into support processes resulting in higher customer satisfaction and reduction in support churn due to misalignment between agency IT shops and CORE I&T. Citizen engagement is improved and increased through the delivery of easy-to-use, functional, elegant and attractive web applications and solutions.	**Empower.** Through leadership by example and regular, proactive and interactive communications CORE I&T promotes a culture of consistency, communications, partnership, collaboration and trust. Feedback is continuously solicited in order to adapt to changing customer business requirements. Engagement with agencies promotes sharing knowledge, successes and lessons learned. CORE I&T services and benefits are known and understood by our customers.	**Lead.** Application and infrastructure governance structures are established to ensure that enterprise business-critical technology solutions are aligned to organizational needs and goals. Governance organizations are composed of agency decision-makers and leveraged to promote standardization, consistency, common procedures and adherence to best practices. Decisions and outcomes are transparent and communicated.
Actions	1. Improve and leverage our Security Awareness campaign and training program 'KnowBe4'. Promote the importance of increasing employee knowledge of security issues. Leverage other training opportunities when possible, including seeking grant funding for "common core" training for all security professionals. 2. Implement an Enterprise Risk and Compliance solution, including an Information Risk Decision framework. 3. Collaborate with State agencies to develop baseline security policies, standards and procedures. 4. Develop and publish a Cybersecurity incident response plan including internal and external communications policies and procedures. 5. Collaborate and communicate regularly with OCDC and agency ISOs. Increase transparency between these organizations. 6. Define and staff a Security Risk Assessment Team to assist and provide guidance to agencies.* 7. Implement Multi-Factor authentication (MFA).*	1. Continue to improve, review and refine the TIN process as a collaboration that provides actionable business intelligence to all stakeholders. 2. Establish Project Management guidelines for all major State IT initiatives. 3. Establish, document, maintain and enforce programming, software, firmware and hardware standards and requirements as they pertain to all EITS/AITS application development and implementation. 4. Establish an Enterprise Architecture Team to review solutions across agencies to ensure industry best practices are followed, identify enterprise and mutually beneficial solutions over silos, and improve coordination between CORE I&T and agencies.* 5. Pilot a next-gen enterprise telecommunications system. Use the findings from the pilot to architect a solution that will become the statewide standard incorporating voice (dial tone), video and data.*	1. Publish customer-accessible views of the EITS and AITS support queues. 2. Define and publish ADA guidelines, remediation instructions, and tools to agencies. Acquire a statewide license for compliance analysis and reporting. Acquire licenses as needed for remediation tools.* 3. Implement a central, shared virtual machine (VM) environment that is an extension of the current State virtual server farm. Facilitate agency tenancy by providing self-service self-provisioning tools that eliminate the requirement for CORE I&T support to accomplish common provisioning and management tasks. Partner with agencies to move applications into this shared VM pool and away from siloed solutions in non-standard environments.* 4. Replace the aging State Content Management System (CMS) with a state-of-the-art agile solution. Promote agency tenancy in the State CMS for consistency, ease of support, ADA compliance and common look and feel across all State web sites.*	1. Collaborate with agencies as they develop their annual strategic IT plans. Agency strategies must consider migrating State digital assets out of non-standard environments and into approved facilities. 2. Provide agencies with Enterprise Architecture and other Subject Matter Expert (SME) support to assist with planning and migration strategies. 3. Build relationships through collaborative customer engagement. Establish regular communications channels to keep customers and State entities informed. Establish the Chief of Policy and Communications role to improve communication and coordination between CORE I&T and agencies. 4. Establish the Office of the CIO web portal. Provide quarterly communications from this office to keep agencies informed of State technology developments, trends and actions. 5. Create and publish a catalog of services provided by CORE I&T.	Establish and/or redefine the following technology governance organizations: 1. Office 365 Tenant Governance Committee: Composed of agency technical experts making tactical and architectural decisions. 2. Office 365 Executive Steering Committee: Composed of agency leaders making business decisions and guiding the Tenant Committee. 3. Enterprise Architecture Working Group: Representing all agencies interested in, or considering moving to, Enterprise Solutions. 4. IT Oversight Committee (ITOC): Composed of business leaders evaluating and prioritizing technology initiatives across State agencies and following the progress of these initiatives.* 5. Information Technology Advisory Board (ITAB): Composed of industry IT experts and elected officials providing guidance and feedback for IT strategies and initiatives.*

* = Contingent upon 80th Session Legislative approval