Joe Lombardo
Governor

Timothy D. Galluzi
State Chief Information Officer

Darla J. Dodge
Deputy CIO – COO

David 'Ax' Axtell
Deputy CIO – CTO

Robert 'Bob' Dehnhardt
Deputy CIO - CISO

STATE OF NEVADA
GOVERNOR'S OFFICE
Office of the Chief Information Officer
100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | it.nv.gov | CIO@it.nv.gov | Fax: (775) 687-9097

November 15, 2023

To: All Agencies

From: Timothy D. Galluzi, State Chief Information Officer

Subject: Guidelines for the Use and Security of AI Tools

In recent months we have seen significant progress in the development and deployment of Artificial Intelligence (AI) tools. Naturally, we are are evaluating the application of these tools with a cautious optimism, as we can see opportunities of these tools aiding in our day-to-day operations and the delivery of services to Nevadans. As we evaluate, and ultimately deploy, AI technologies into our operations it is imperative to establish clear guidelines to ensure efficient, effective, and secure use. AI offers great potential for enhancing State government services but also poses unique challenges, especially regarding sensitive data protection.

Types of AI Tools

AI tools can be categorized as follows:

- Machine Learning Models: These include predictive analytics, natural language processing, and image recognition.

- Robotic Process Automation (RPA): Automating repetitive tasks.
- Cognitive Computing: Mimicking human decision-making processes.
- Chatbots and Virtual Assistants: For customer service enhancements.

Security and Appropriate Use

Non-state operated tools should be used with extreme caution. Platforms such as ChatGPT and others, utilize the input from users to further refine their data model. This means that the questions you are asking the model today may be included in the answers someone else receives tomorrow. Information that should not be released publicly, should not be entered into these services.

AI tools should adhere to the following initial guidelines:

- Data Protection: AI tools must comply with all relevant data protection laws, including HIPAA (Health Insurance Portability and Accountability Act) for health data, CJIS (Criminal Justice Information Services) for criminal justice information, Family Educational Rights and Privacy Act (FERPA) for Education data and other federal or state-specific privacy laws protecting Personal Identifiable Information (PII).
- Access Control: Strict access control measures must be in place to ensure that only authorized personnel have access to AI tools, particularly those handling sensitive data.

- Encryption: Data used in AI tools, both in transit and at rest, must be encrypted to

protect against unauthorized access and breaches.

- Regular Audits: AI systems should undergo regular security audits to identify and rectify any vulnerabilities.
- Ethical Use: AI tools must be used ethically, avoiding biases and ensuring fairness and transparency in decision-making processes.

Appointing authorities may adopt agency-specific guidelines, policies, and standards that are more stringent.

State IT Governance Involvement

The State Technology Governance Committee (STGC) and the State Information Security Committee (SISC) will be instrumental in developing comprehensive policies and standards for AI technologies. Their focus will include:

- Policy Development: Establishing clear policies for AI use, emphasizing security, data protection, and ethical considerations.
- Standards and Best Practices: Setting up standards for selecting, implementing, and managing AI tools across state agencies.

It is my intent to continue to evaluate opportunities for the deployment of these technologies, all while ensuring that appropriate governance and security are kept top of mind. In the coming months, we will be engaging state leadership and other stakeholders to ensure that state government is ready to deploy these tools to the benefit of all Nevadans. The judicious use of AI can significantly enhance the efficiency and effectiveness of state government operations. It is crucial, however, to balance innovation

with responsibility, ensuring that these powerful tools are used securely and ethically, with full respect for privacy and data protection norms. Your cooperation and adherence to these guidelines and forthcoming policies from STGC and SISC are essential for our collective success in this endeavor.

This memo serves as an initial framework, subject to refinement and expansion by the STGC and SISC in the coming months. Your feedback and active participation in this process are encouraged.

Timothy D. Galluzi

State Chief Information Officer