STATE OF MAINE
OFFICE OF THE CHIEF INFORMATION OFFICER
145 STATE HOUSE STATION
51 COMMERCE DRIVE
AUGUSTA, MAINE 04333-0145

ADMINISTRATIVE & FINANCIAL SERVICES

KIRSTEN LC FIGUEROA
COMMISSIONER

NICHOLAS MARQUIS
ACTING CHIEF INFORMATION OFFICER

JANET T. MILLS
GOVERNOR

STATE OF MAINE
DEPARTMENT OF ADMINISTRATIVE AND FINANCIAL SERVICES
MAINE INFORMATION TECHNOLOGY (MaineIT) CYBERSECURITY DIRECTIVE 2024-01

Maine Information Technology (MaineIT) has issued the following Directive to all executive branch State Agencies[1] for the purposes of safeguarding State of Maine (SOM) information systems and assets.

Summary:
This Directive authorizes a three-month extension of the moratorium on Generative Artificial Intelligence (GenAI) established pursuant to Cybersecurity Directive 2023-03. To date, significant steps forward have been made in developing the guardrails necessary to ensure the responsible use of GenAI in state government. This extension will allow for a risk assessment to be performed that will inform IT policies, procedures and training governing the safe and responsible use of GenAI for the State's IT enterprise. During this extension, there will be continued engagement with agency stakeholders, specifically their input on GenAI use cases that may serve to benefit the public and increase agencies' mission effectiveness and business goals. The information gathered will inform the development of risk management and governance frameworks necessary for operationalizing GenAI for the State's IT enterprise. Due to the transformative nature of this emerging technology, efforts to assess the safety and security of GenAI will be ongoing to ensure risks are effectively mitigated to safeguard citizen data and maintain public trust.

Background:
MaineIT is responsible for maintaining the confidentiality, integrity and availability of the State's information systems and assets, while serving Executive Branch Agencies with efficient and secure network services. As U.S. policy on AI continues to develop, caution must be taken to assess the risks involved with the use of GenAI technologies. Early federal guidance and best practices[2] provide a roadmap for industry and government to move towards the responsible management of GenAI systems that cultivate public trust.

GenAI systems have the capacity to automatically process data and information in a way that resembles intelligent human behavior. Although these systems have many benefits, the expansive nature of this technology introduces a wide array of security, privacy, algorithmic bias, and credibility risks into an already complex IT landscape. These systems lack transparency in their design, raising significant data privacy and security concerns. Their use often involves the intentional or inadvertent collection and/or dissemination of business or personal data. In addition, GenAI technologies are known to have concerning and exploitable security weaknesses, including the ability to generate credible-seeming misinformation, disseminate malware, and execute sophisticated phishing techniques.

These factors make it challenging to maintain adequate understanding and control over AI-based decisions, including their appropriateness, fairness, and alignment with organizational values and risk appetite. The complete risk associated with the use of this technology remains unknown. Accordingly, a moratorium on GenAI was established pursuant to Cybersecurity Directive 2023-03.

---

[1] This Directive is being issued to all SOM executive branch agencies, including all State agencies, departments, commissions, committees, authorities, divisions, boards or other administrative units of the executive branch that use the State network.
[2] NIST AI Risk Management Framework and the NIST Artificial Intelligence Resource Center (AIRC).

Required Actions:
This Directive authorizes a three-month extension of the moratorium on GenAI established pursuant to Cybersecurity Directive 2023-03. It extends the prohibition on the adoption or use of GenAI technology[3] for three months until March 31, 2024, for all State of Maine business and on any device connected to the State of Maine network. This extension will provide an opportunity to engage with agency stakeholders to receive input on GenAI use cases that could benefit the public and increase agencies' mission effectiveness and business goals. The information gathered will inform the development of risk management and governance frameworks necessary for operationalizing GenAI for the State's IT enterprise. Any requests for an exception to this Directive must be submitted by filing a direct waiver request through the appropriate MaineIT Account Manager for your department.

Technologies Covered:
GenAI technologies covered under this directive include large language models that generate text like ChatGPT, as well as software that generates images, music, computer code, voice simulation, and art. Any chatbot technology currently approved for use by MaineIT is not prohibited by this moratorium.

Additional Information:
MaineIT is currently assessing other products, services and telecommunication equipment that may pose security risks to the State of Maine's network infrastructure and additional steps may need to be taken to strengthen our security posture.

This Directive will be reviewed and revised, as necessary, in three months. The internal point of contact for this Directive is Nathan Willigar, State of Maine Chief Information Security Officer, at Nathan.Willigar@maine.gov.

---

[3]Generative AI refers to "AI techniques that learn a representation of artifacts from data, and use it to generate brand-new, unique artifacts that resemble but do not repeat the original data. These artifacts can serve benign or nefarious purposes. Generative AI can produce totally novel content (including text, images, video, audio, structures), computer code, synthetic data, workflows and models of physical objects. Generative AI also can be used in art, drug discovery or material design." See Gartner at https://www.gartner.com/en/information-technology/glossary/generative-ai