Office of the
CHIEF
ADMINISTRATIVE
OFFICER

"Artificial Intelligence (AI): Innovations within the Legislative Branch"
Tuesday, January 30, 2024
10:30 AM

Testimony of:
John Clocker, Deputy Chief Administrative Officer
Before:
The Committee on House Administration

The Office of the Chief Administrative Officer (CAO) thanks Chairman Steil, Ranking Member Morelle and members of the Committee on House Administration for holding its January 30, 2024, hearing focused on Artificial Intelligence (AI) innovation integration within the Legislative Branch.

The Committee on House Administration has been instrumental and supportive of the CAO's constant endeavor to achieve greater efficiency through innovation, including its efforts to integrate Generative AI, or GenAI, into House operations. The CAO appreciates the Committee's support and the opportunity to share its latest work with GenAI technology.

The CAO would also like to acknowledge the work of its entire House Information Resources division, including its House Digital Service team and its Office of Cybersecurity. In particular, the CAO would like to commend Senior Director for Innovation Stephen Dwyer and Deputy CISO Addie Adeniji for their leadership. These individuals and their respective teams are at the forefront of this important endeavor for the CAO and tirelessly work to ensure the House is striking the needed balance between innovation and security.

Introduction
By way of background, early adaptations of AI, including business process automation, emerged in the 1970s with encoded human knowledge-based technologies. They evolved over the following decades with the development of new capabilities like machine learning, natural language processing, speech recognition and computer vision. Today, some of these AI technologies are embedded in commonly-used House applications such as Microsoft Word's suggestion function and its Teams meeting transcription tool. The House's online service request tool, called MyServiceRequest, uses a chatbot to help users obtain technology support. House tools use AI to generate transcripts in real time and use it when creating graphics and videos.

Over the past few years, AI advancements gained significant momentum and prominence with the advent of GenAI Large-Language Models (LLMs) capable of analyzing massive datasets and producing original, human-like content. Though OpenAI's ChatGPT is perhaps the best known GenAI LLM, the entire technology sector is moving at a rapid pace to develop, integrate, and roll out GenAI LLM products.

There is no doubt that GenAI LLMs are going to have a significant impact on the Legislative Branch. The technology has transformative potential, but its integration requires a cautious approach with controls and guidance that protect users while allowing them to reap its benefits.

For Member-led offices faced with an ever-increasing volume of constituent engagement and oversight responsibilities, GenAI LLMs have the potential to augment workload capacity. It may also help the House as an institution achieve greater operational business efficiencies. It is important, however, to emphasize that GenAI LLMs shall only augment congressional operations – not replace human engagement and oversight. This principle is supported by known and observed current limitations of the technology, including limitations associated with legal and legislative operations.

The House must also acknowledge that this is a two-way street. GenAI LLMs are already being developed and deployed to engage Congress through advocacy and other means. They are also being utilized by cyber criminals who target Congress. Widespread use of LLMs will increase the workload of the House and demand an equal surge in House capabilities.

CAO-led Initiatives

The CAO's philosophy to all emerging technologies is to apply a disciplined approach to integrating technology as it matures so that the House maximizes productivity benefits while minimizing privacy and security risks.

When OpenAI released ChatGPT in late 2022, the CAO, with the support of the Committee, initiated its disciplined approach to GenAI LLM integration in the House.

Since then, the CAO has conducted legal and security reviews of available, off-the-shelf GenAI LLM products for House use. It established a House-wide advisory group to collect and analyze information about how offices can maximize use of the technology. It also conducted an assessment of the House's AI governance structure to identify actions required to support further GenAI LLM technology integration.

<u>Legal and security reviews of GenAI LLM products:</u> As required by House policy, the CAO's Office of Administrative Counsel and Office of Cybersecurity conducted legal and cybersecurity reviews of commercially-available GenAI LLM products, including OpenAI's ChatGPT, Google's Bard, and Microsoft's Bing Chat – now called Copilot. Upon its review of the platforms, and as a result of securing changes to ChatGPT's legal Terms and Conditions, the Committee was able to approve ChatGPT Plus for limited House use in June 2023. Though not yet approved for House use, other

off-the-shelf commercial products will continue to be monitored for future consideration. The CAO is also closely monitoring the development and deployment of GenAI LLM tools being integrated into software applications already in use by the House.

The House-wide AI Advisory Group: In Spring of 2023, CAO's House Digital Service team established the AI Advisory Group to collect, analyze, and share GenAI LLM (ChatGPT Plus) use cases within the House. The goal of the AI Advisory Group is to understand the tool's capabilities and limitations when applied to operations within the House environment. The data and feedback collected will inform governance and guidance materials going forward. The AI Advisory Group is conducting its data collection and analysis in two phases.

The first phase started in April 2023 and included over 200 participating staffers representing approximately 150 Member, Committee, and Leadership offices.

Over the course of several months, participating offices were provided free access to ChatGPT Plus licenses in return for regular detailed usage reports, including successes and failures, that were anonymized, summarized, and shared back to the entire AI Advisory Group as well as published online for the entire House community. The CAO's House Digital Service team also posted important information pertaining to the common concerns associated with AI specific to accuracy, bias, cybersecurity, ethics, tool limitations, and data protection.

The most common uses of the tool fell within five general House-specific categories: Representation, Legislation, Constituency Services, Communication, and Operations. Within each category, the CAO has a comprehensive inventory of specific use cases. For example, use cases under Constituency Services include AI-assisted correspondence and casework processing. The use case inventory, which the CAO will continue to maintain through the second phase, has been published online by the Committee.

Initial feedback collected by the AI Advisory Group was very positive with offices praising the tool's perceived time-saving benefits.

*"I have seen **a ton of time saved** and honestly, I have been able to keep trivial work off of the desks of our SA's and Interns, which allows them more meaningful work and growth opportunities."*

*"It has certainly allowed us to **decrease the response time** on all of our correspondence with constituents."*

*"Chat GPT can really help **overcome writer's block** by giving you something to edit instead of making you start from scratch."*

-Anonymized user comments shared with the AI Advisory Group

Phase one usage reports submitted to the AI Advisory Group provide valuable insight into how Member, Committee, and Leadership offices will likely maximize use of current GenAI LLM tools (e.g., proofreading, drafting memos, press releases and letters, summarizing reports and articles, formatting data, etc.) as well as tool limitations (e.g., accuracy of legislative text inquiries, accuracy of compiled court case information, understanding of social media contexts, capturing Member voice/style, etc.).

The AI Advisory Group's second phase started this month and focuses on institutional integration of GenAI LLMs. This phase will include experimentation with the tool's capabilities applied to a broad spectrum of House operations executed by House officers and select Legislative Branch support organizations. The CAO believes that experimental GenAI LLM tool integration into institutional operations will result in positive, time-saving results and feedback similar to that shared by phase one participants.

Integrating the tool into CAO operations alone presents tremendous potential for greater efficiency. Test use cases will be applied to numerous operational aspects of the CAO, from House finances and procurement to Human Resources. The tool has potential to assist with financial anomaly detection, reviewing and analyzing solicitation responses, writing House job descriptions, and much more. The CAO is excited about the second phase and looks forward to sharing its findings with the Committee in the coming months.

Assessment of the House's AI governance structure: In September 2023, the CAO's Office of Cybersecurity initiated an AI governance assessment based on the National Institute of Standards and Technology's (NIST) AI Risk Management Framework intended to help all sectors understand and manage the unique landscape of AI integration. The assessment identified actions required to improve the House's AI governance structure, including the establishment of GenAI-specific policies and user guidance and training. The assessment also highlighted the importance of risk monitoring and mitigation and underscored the overall need to apply a conservative approach to GenAI LLM deployment.

CAO's House Digital Service team and Office of Cybersecurity also participated in various AI forums on the current and future applicability of GenAI LLMs in the federal space and socialized potential House AI policy ideas with the congressional community at the September 14, 2023, Congressional Hackathon 5.0.

The Path Forward

Using information obtained through the NIST-based governance assessment, data collected from its legal and cyber reviews of GenAI LLM technologies, and House usage information collected through the AI Advisory Group, the CAO will work with the Committee to establish a responsible path forward for continued GenAI LLM House integration.

The CAO believes there are three critical components to successful integration.

1. Establishing governance and security controls
2. Developing guidance and training (upskilling) opportunities for House users

3. Expanding House-validated GenAI LLM technology

Establishing governance and security controls: The House's cybersecurity risk profile increases with the introduction of AI tools into its environment. Therefore, governance and security policies and protocols specific to GenAI LLM tools are needed to protect the House. Users need operational and ethical guardrails, and the current set of House security tools may not be sufficient as threat actors increase their use of AI tools.

The abovementioned AI governance assessment based on NIST's AI Risk Management Framework and the House's collaboration with congressional stakeholders has identified policy and protocol that must be addressed to strengthen the House's preparedness for GenAI LLM adoption.

Based on its AI governance assessment, CAO's Office of Cybersecurity anticipates developing a new House Information Security Policy regulating GenAI LLM integration and use within the House environment.

The CAO's Office of Cybersecurity must also be extremely proactive in maintaining protocols that identify and reduce or eliminate new risks associated with evolving AI technology.

Developing guidance and training (upskilling) opportunities for House users**:** The House needs to establish guidance and upskilling opportunities so staff can correctly optimize use of the GenAI LLM tools. Staff need principle-based and technical training. They will need House-wide forums to share and obtain best practices.

The CAO also recommends offices adopt internal AI use policies that dictate specifically how the technology is used based on each Member's preference. To assist with these policies, the CAO could work with the Committee to develop a model AI use policy that offices could customize and adopt similar to the Model Employee Handbook published by the Committee.

The user information gathered through the AI Advisory Group has proven that collaboration is essential to successful tool integration. Its findings will serve as the foundation of future CAO GenAI LLM guidance and upskilling opportunities for the entire House.

Expanding House-validated GenAI LLM technology: Currently, one tool (ChatGPT Plus) has been authorized by the Committee for research and evaluation use with only non-sensitive data. As previously mentioned, this limited authorization was based on a legal and cybersecurity review conducted by the CAO. Currently, the other commercially available, off-the-shelf platforms do not meet House requirements. That said, these platforms are constantly evolving and maturing. Therefore, the CAO is closely monitoring and reevaluating their suitability for House use and will make integration recommendations to the Committee for its consideration as appropriate.

The CAO is tracking the development and deployment of GenAI LLM tools being integrated into commercial enterprise applications already in use by the House (e.g., Microsoft O365's Copilot)

and expects House constituent Correspondence Management System (CMS) providers will also explore options to integrate the technology. These products will also undergo a thorough legal and cybersecurity evaluation before being recommended and approved for use by the House. The approximately 160 cloud services already approved by the House will also need to be reexamined from a cybersecurity perspective if and when they incorporate new AI capabilities.

The CAO cannot stress enough the importance of third-party cloud technology and applications being validated and approved by the House prior to House utilization. Offices that use unvetted, unapproved tools and applications jeopardize their data and may compromise the House network.

Furthermore, the CAO is exploring the deployment of customized secure private GenAI LLM for the House. At this time, the CAO does not envision building a GenAI LLM from scratch. As the entity responsible for House technology deployment, the CAO can attest to the cost and innovation benefits of leveraging third-party technology versus trying to build and maintain applications in-house, especially considering the House's broad scope of business needs. That said, the CAO is eager to learn if and how other Legislative Branch entities are successfully developing and integrating in-house GenAI LLM technology.

Conclusion

The CAO is committed to bringing validated and safe GenAI LLM tools to the House to help Members with their representational duties and to improve House operations. Successful integration requires a disciplined approach that enables offices to use the technology within parameters that protect their data and the House network.

GenAI LLM integration into the House environment elevates our cyber risks as cyber criminals will take advantage of these tools as well. Therefore, the House needs to remain agile in assessing them and vigilant with security maintenance and validations. If integrated correctly with proper governance and guidance, the technology has tremendous potential to help House offices achieve greater efficiency.

Offices must be proactive, too. As more GenAI LLM tools mature and become available for House use, offices will need to carefully consider the benefits and limitations of the tool. Regardless of what House-issued policies and guidance state, it will be incumbent upon each Member of the House to understand and prescribe the level of GenAI LLM use in his or her office. Offices also need to remain vigilant when it comes to the tools and websites they access. Just because a tool or website can be accessed online does not mean it's safe or authorized for House use. Offices should always seek assistance when exploring new online resources, and the CAO and its entire House Information Resources team stands ready and able to assist.

The future of GenAI LLM integration is bright, but it requires collaboration among technology and cyber experts, policy makers, and House users. The direction and support provided by the Committee on House Administration to date has been both valuable and greatly appreciated.

The CAO looks forward to continuing its work with the Committee as the House advances this important endeavor.