



Homeland
Security

October 24, 2023

Policy Statement 139-07

MEMORANDUM FOR: DHS Agency and Office Leaders

FROM: Eric Hysen
Chief Information Officer

ERIC N
HYSEN

Digitally signed by ERIC
N HYSEN
Date: 2023.10.24
15:51:49 -04'00'

SUBJECT: **Use of Commercial Generative Artificial Intelligence (AI) Tools**

During his April 21, 2023, State of Homeland Security address, Secretary Mayorkas stated that “Our Department will lead in the responsible use of AI [Artificial Intelligence] to secure the homeland and in defending against the malicious use of this transformational technology. As we do this, we will ensure that our use of AI is rigorously tested to avoid bias and disparate impact and is clearly explainable to the people we serve.”

To do this, the Secretary directed the Under Secretary for Science and Technology and me to establish an Artificial Intelligence Task Force (AITF). As the AITF works to advance specific mission applications of AI across the Department, we must also address ways in which our workforce uses commercially available generative AI (Gen AI) products in their work.

“Generative artificial intelligence” means the class of AI models that emulate the structure and characteristics of input data to generate novel synthetic content. This can include images, videos, audio, text, and other types of digital content. Tools using Gen AI have rapidly gained worldwide popularity. There is a growing body of research that suggests Gen AI will lead to significant productivity gains across all sectors.¹

Gen AI tools also present significant challenges and risks, including producing “hallucinations” or invented and inaccurate responses and generating biased outputs based on biases in their training data.² They further present information privacy and security risks if sensitive information is provided to tools and used to further train underlying models. Careful human judgment is required to balance the productivity gains associated with Gen AI tools with these risks.

¹ [Economic potential of generative AI | McKinsey, AI Improves Employee Productivity by 66% \(nngroup.com\)](#)

² [Why ChatGPT and Bing Chat are so good at making things up | Ars Technical](#)

The AITF is actively exploring use cases for Gen AI tools across a variety of DHS mission areas. While this work continues, I have determined that DHS must enable and encourage DHS personnel³ to responsibly use commercial products to harness the benefits of Gen AI and ensure we continuously adapt to the future of work. As such, I am issuing the following initial guidance to facilitate appropriate use during this early stage of technological development:

- My office will develop and maintain a list of conditionally approved commercial Gen AI tools⁴ for use on open-source information⁵ only.
 - In developing this list, we will review basic accuracy and security practices, supply chain risk management concerns, privacy and civil liberties safeguards, and available information on how training data was sourced. This list will be coordinated in advance of its release with the DHS Privacy Office (PRIV), the Office for Civil Rights and Civil Liberties (CRCL), and other stakeholders.
 - This review will not provide approval to utilize these tools on non-public information.
 - We will maintain a page on DHS Connect listing these tools and offering employees the ability to submit additional tools for review and testing.
- My office will update Department IT and cybersecurity policies and standards to include new requirements for use of approved commercial Gen AI tools by DHS personnel in their work. In the interim, however, the following rules shall apply:
 - Personnel must never put DHS data regarding individuals (regardless of whether it is personally identifiable information (PII) or anonymized), social media content, or any For Official Use Only, Sensitive but Unclassified Information, now known as “Controlled Unclassified Information,” or Classified information into commercial Gen AI tools.
 - Personnel shall protect any PII collected or generated by the use of commercial Gen AI tools in accordance with applicable DHS privacy policy and federal law.
 - Prior to any use of these tools, personnel must obtain approval from their supervisors, complete a training on responsible use of AI along with their annual Protecting Personally Identifiable Information and Cybersecurity Awareness trainings, and sign an acknowledgement of the conditions on use.
 - Personnel will create accounts on these tools using their DHS email and use these accounts only for DHS use, separate from any personal use of these tools.
 - Personnel will select options in tools that limit data retention and opt out of inputs being used to further train models.
 - All use of conditionally approved commercial Gen AI tools will be on the web, not through downloaded desktop or mobile apps.

³ Personnel includes federal employees, contractors, detailees, and others working on behalf of DHS.

⁴ “Commercial Gen AI tools” are defined as generative AI technology or products available for use or purchase by the general public (i.e., off-the-shelf). This definition does not include customized software or services developed specifically for the government through an IT acquisition process.

⁵ Open-Source Information means unclassified information that has been published or broadcast in some manner to the public. Sources are newspapers or other periodicals; weather reports; books, journal articles, or other published works; public court filings; or any similar documents that have traditionally been publicly available.

- At all times, personnel are accountable for accessing and handling DHS information and IT resources in compliance with DHS User Rules of Behavior and DHS policies, including privacy, civil rights, and civil liberties policies.
- Personnel should ensure all content generated or modified using these tools is reviewed by appropriate subject matter experts for accuracy, relevance, data sensitivity, inappropriate bias, and policy compliance⁶ before using it in any official capacity, especially when interacting with the public.
- Commercial Gen AI tools may not be used in the decision-making process for any benefits adjudication, credentialing, vetting, or law or civil investigation or enforcement related actions. Agency and Office Leaders or CIOs can request from my office a written waiver of these restrictions.
- Any spillage or compromise of DHS information into Gen AI tools must be reported immediately pursuant to applicable policies.
- Agency and Office Chief Information Officers will develop policies regarding appropriate use of commercial Gen AI tools in their missions, in consultation with my office, PRIV, and CRCL. These policies may impose additional conditions or limitations on the use of commercial Gen AI tools based on unique mission requirements.

Immediate appropriate applications of commercial Gen AI tools to DHS business could include generating first drafts of documents that a human would subsequently review, conducting and synthesizing research on open-source information, and developing briefing materials or preparing for meetings and events. I have personally found these tools valuable in these use cases already, and encourage employees to learn, identify, and share other valuable uses with each other.

This initial guidance will be updated in coordination with relevant stakeholders across the Department regularly given the rapid pace of technological change in the AI space. As Agencies and Offices deploy internal systems and tools leveraging Gen AI, those systems will be governed through broader Department policies on responsible use, including DHS Policy Statement 139-06 “Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components.”

⁶ For example, *see* Policy Statement 139-06, *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components* (Aug. 8, 2023) (“All DHS users of AI are charged with providing human oversight, safeguards, and where appropriate, review and redress in AI-enabled processes implemented by DHS, to ensure these principles are applied effectively and efficiently in the design, implementation, and end uses of this technology.”).