Department of Homeland Security: Commercial Generative Artificial Intelligence Interim Rules of Behavior

Purpose

This document covers the acceptable use of conditionally approved commercial Generative Artificial Intelligence (GenAI) tools[1]that leverage Large Language Models (LLMs) within the Department of Homeland Security (DHS). These rules of behavior apply to all DHS personnel using conditionally approved commercial GenAI tools on government furnished equipment or any device accessing the DHS network. DHS personnel includes all users of DHS information systems and IT resources (e.g., networks; databases; applications; workstations; laptops; mobile computing devices, including cell phones, smartphones, and tablets), including DHS employees, support contractors, detailees and all other system users. This Rules of Behavior does not apply to use of GenAI tools that are procured and acquired for use on a DHS network as downloadable software or applications. Hereafter conditionally approved commercial GenAI will be referenced as GenAI or GenAI tools and any future reference of approval will mean conditional approval.

In support of Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (December 3, 2020), and DHS Policy Statement 139-06, *Acquisition and Use of Artificial Intelligence and Machine Learning Technologies by DHS Components* (August 8, 2023), DHS Office of the Chief Information Officer has issued Policy Statement 139-07/Use of Commercial Generative Artificial Intelligence (AI) Tools.

Use of commercial GenAI tools for government work raises the potential for privacy, civil rights, civil liberties, and legal issues. As GenAI tools are trained on public data sources, federal data that has not been cleared for public release should not be entered into or transmitted to a platform that is not authorized to collect, store, or process this data, as it can be used to train the GenAI models and be broadly released to non-DHS users.

[1] A conditionally approved GenAI tool means the tool has been evaluated through the DHS Generative AI evaluation process and is approved for use, but with a limited scope (restricted). This evaluation process is derived from the current DHS Technology Reference Module and includes Subject Matter Expert reviewers from additional DHS Offices.

To minimize risk, DHS personnel must adhere to the acceptable use of GenAI tools in this document and comply with federal laws and DHS policies, including the general DHS Rules of Behavior (DHS Policy Directive 4300A, Attachment G)[2] and Privacy policies.

Definitions

4300A: Series of DHS-wide documents that provide a baseline of policies, procedures, standards, and guidelines for all DHS Components. 4300A policy series applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS.

Generative AI: Type of artificial intelligence that can create new content, such as text, images, video, or audio, based upon the patterns and structures of the data it learns from.

Commercial Generative AI: A product that is available for purchase/use in the public marketplace.

Conditionally approved: Temporary approval for the introduction of new technology that is still being evaluated. Does not mean or imply final approval.

Acceptable use of GenAI tools

- I have completed the following trainings:
  - DHS FY23-FY24 Generative Artificial Intelligence training,
  - Privacy at DHS: Protecting Personal Information training,
  - Cybersecurity Awareness training, and
  - Component specific privacy and security training requirements.
- I will only use DHS approved GenAI tools.[3]
- I will only use approved GenAI tools via a web browser and understand that I am not authorized to download desktop software or mobile GenAI applications.
- I will create a user account using my DHS email address and understand this account must only be used for official work purposes. Use of personal accounts for government business is prohibited. Refer to DHS Rules of Behavior 4300A, Attachment G.
- I understand that I must submit a request to the GenAI tool to delete my DHS account upon my offboarding or transfer to another DHS Component or Agency, or when I no longer need to use the GenAI tool to complete my existing job responsibilities. This request must be documented in writing and provided to my supervisor.
- I understand that accounts created under personal email or social media profiles and results generated from any non-DHS GenAI accounts are not authorized for DHS use.

Data Protection and Retention

- I understand GenAI tools may only be used for and with open-source information[4].
- I understand that non-public information shall not be used in GenAI prompts because these tools are not authorized by DHS to process or store such content. Non-public information includes work products, emails, and conversations or writing that are meant to be pre-decisional and deliberative, to include attorney work product or attorney/client privileged information and/or information internal to DHS. Additionally, non-public includes information related to personally

[2] These interim Rules of Behavior on Gen AI will be incorporated into the 4300A Attachment G at a future date.
[3] Each tool may have its own unique terms and conditions for users to abide by. Please check the DHS Connect Generative AI page for information.
[4] DHS Policy Statement 139-07/Use of Commercial Generative Artificial Intelligence (AI) Tools defines open-source information as 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.

identifiable information (PII), financial disclosures, protected acquisition, controlled unclassified information (CUI), and classified information. Any protection of this non-public information in response to third-party requests (e.g., Freedom Of Information Act requests) or subject to litigation may be waived if used or disclosed when using these GenAI tools.

- I understand that when using GenAI tools to generate software code, any DHS code provided to the tool shall not include any IP addresses, passcodes, tokens, cyphers, and other cybersecurity sensitive technical information.
- When available, I will opt-out of inputs being used to train GenAI models.
- When available, I will select tool options to limit data retention.

Accountability for use of products derived from GenAI tools.

- I will ensure that my use of GenAI is responsible and trustworthy, that when using content generated by these tools I must safeguard privacy, civil rights, and civil liberties while avoiding inappropriate biases, and—to the greatest extent possible—that it is transparent, source cited, and able to be explained to those whom we serve.
- I will protect any PII collected or generated by the use of commercial Gen AI tools in accordance with applicable DHS privacy policy[5] and federal law.
- I will not use GenAI to generate inappropriate, offensive, or illegal material.
- I understand that I must manually review the output used to generate code or publishable material for accuracy, functional effectiveness and suitability, and intellectual property, as GenAI tools may have been trained on data that AI providers may not have had full legal rights to use. Further, I may not use output that includes personally identifiable information. I will consult with counsel, component privacy offices, and the Office of Civil Rights and Civil Liberties as needed to ensure compliance with this provision.
- I understand GenAI content must be vetted and approved by the DHS Office of Public Affairs (or component OPA for component-level content, as appropriate) before public distribution or publishing external to DHS.
- I understand Commercial GenAI tools may not be used in the decision-making process for any benefits adjudication, credentialling, vetting, legal or civil investigation or enforcement related actions, or any DHS activities affecting individual rights or safety.[6] Agency and Office Leaders or CIOs can request from the DHS CIO office a written waiver of these restrictions.
- I will confer with my supervisor to determine if I must cite the source of GenAI content in DHS products or deliverables.
- I understand DHS performs electronic monitoring of internet communications traffic including anything I input into or download from a GenAI tool.

Incident Reporting and request for assistance

- If spillage, compromise of DHS information, or sharing of personal information occurs, to including the release of PII, law enforcement sensitive information, and security sensitive information.[7]

[5] DHS Privacy Policies may be found at DHS.gov

[6] Per Policy Statement 139/07, Agency and Office Leaders or Chief Information Officers can request a waiver of these restrictions. Components should use the DHS 4300A ITSSP Attachment B, Information Systems Waiver and Risk Acceptance Request.

[7] DHS Policy Directive 4300A: Information Technology System Security Program, Sensitive Systems (ITSSP SS), Attachment F: Incident Response.

- Report cybersecurity incidents to Component Security Operations Centers immediately upon suspicion or recognition.
- Provide feedback to the Artificial Intelligence Task Force when you notice biased, discriminatory, inappropriate, or harmful content, at AI@hq.dhs.gov.
- If you encounter inappropriate or offensive language, pornographic material, errors, or hallucinations, consider reporting it directly to the GenAI tool to improve the tool.
- Reporting Point of Contacts may be found on the AI/GenAI DHS Connect site.
- If there are any questions on reporting procedures, ask an expert via email at **AI@hq.dhs.gov**.

If you have any comments or questions concerning this document, please contact the DHS OCIO CISOD Policy office at infosecpolicy@hq.dhs.gov.

Once the required signatures have been obtained, email the completed RoB to DHS CIO CISOD Training.

Acknowledgement Statement

I acknowledge that I have read, understand, and will comply with the DHS Commercial Generative Artificial Intelligence Rules of Behavior.

User Name (printed): _____

Digital Signature:

User's Component: _____

[8]Supervisor's Name (printed): _____

Digital Signature :

Contracting Officer Representative Name (printed) _____

Digital Signature:

Contractor Corporate Supervisor Name (printed) _____

Digital Signature (or signature):

Additional Resources:

DHS Security and Training Requirements for Contractors | Homeland Security

[8] DHS Federal Employees must obtain their Direct Supervisor's signature. DHS Contractors must obtain their corporate supervisor signature and Contracting Officer Representative (CORs) signature on Rules of Behavior.