Department of Homeland Security Commercial Generative Artificial Intelligence (GenAI) Acceptable Use Training

February 2024
approved for public release

What is this training and who is it for?

Purpose

- Gain a basic understanding of GenAI.
- Learn about conditionally approved commercial tools.
- Understand responsible use and risks.
- Understand requirements and what is contained in the DHS Commercial GenAI Rules of Behavior.

Audience

DHS personnel who want to use commercial GenAI tools when using DHS systems and equipment. This includes:

- Federal employees,
- contractors,
- detailees, and
- others working on behalf of DHS.

“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.”

- Secretary Mayorkas
  April 2023

Agenda

Section 1: Introduction to Generative AI and Tools

Section 2: Responsible Use and Risks

Section 3: How to Get Started

Section 4: Q&A

Section 1: Introduction to Generative AI and Approved Tools

In this section, you will:

- Gain a basic understanding of Generative AI.
- Learn about conditionally approved commercial tools

What is Generative AI?

Artificial Intelligence (AI)

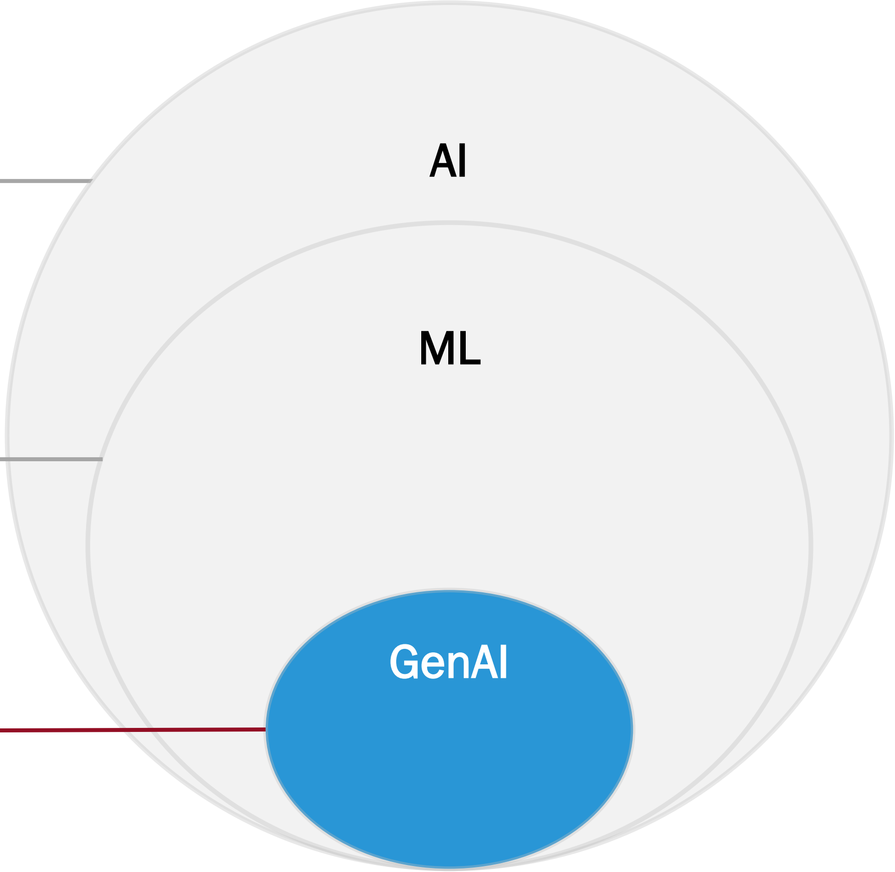
The theory and development of computer systems that normally require human intelligence.

Machine Learning (ML)

The process of using mathematical models of data to help a computer learn without supervision.

Generative AI (GenAI)

Type of AI that broadly describes machine learning systems capable of generating text, images, code, or other types of content.



What are Conditionally Approved Commercial GenAI tools?

What does it mean for a tool to be conditionally approved?

- A conditionally approved GenAI tool means the tool has been evaluated and are approved for use, but with a limited scope (restricted).
- This evaluation process is derived from the current DHS technology evaluation process and includes Subject Matter Expert reviewers.

What are Commercial GenAI tools?

- GenAI technology are products available for use or purchase by the public. This definition does not include customized software or services developed specifically for the government through an IT acquisition process.

Use of these tools must be in accordance with DHS Policy Statement 139-07: Use of Commercial Generative Artificial Intelligence (AI) Tools.

What types of information can be used in Commercial GenAI tools?

Conditionally approved Commercial GenAI tools may be used on open-source information only.

Open-Source information:

- 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.

Personnel <u>must never</u> use or enter the below data into Commercial GenAI tools:

- DHS data regarding individuals (regardless of whether it is personally identifiable information (PII) or anonymized).
- DHS social media content.
- For Official Use Only, Sensitive but Unclassified Information, now known as "Controlled Unclassified Information."
- Classified Information.

Per Policy Statement 139-07:

✓ Yes

Summarize key points of a DHS Policy that is available on DHS.gov

✕ No

Summarize key points of an internal DHS chat.

[Policy Statement 139-07: Use of Commercial Generative Artificial Intelligence (AI) Tools]

Why use GenAI tools?

As DHS continuously adapts to the future of work, personnel are permitted and encouraged to responsibly use GenAI tools.

Opportunities include:

- Quickly gathering and summarizing information.
- Automating repetitive tasks.
- Realizing significant productivity gains to secure the homeland

Examples:

- Review the latest Artificial Intelligence policy (found on DHS.gov), summarize key points.
- Create a Python program (executable code) that parses text.
- Conduct research and generate a one-page summary on the top international government security organizations.

Knowledge Check #1

Using only open-source information, which of the following outputs could be produced using conditionally approved GenAI tools?

A. Summarizing lengthy government reports into concise overviews to improve information sharing between agencies.

B. Generating draft responses to frequently asked questions for agency websites to improve public access to government services.

C. Transcribing recordings of public meetings and hearings to efficiently compile records and increase transparency.

D. All of the above.

Answer: D

Section 2: Responsible Use and Risks

In this section, you will:

- Understand what responsible use means at DHS.
- Understand the risks of using GenAI.
- Learn how to minimize risks.

What does responsible use mean at DHS?

All uses of GenAI must align with our core values and mission.

Personnel must ensure that use:

- Is responsible and trustworthy.
- Safeguards privacy, civil rights, and civil liberties.
- Avoids inappropriate biases.
- Is transparent and explainable to those we serve.
- Follows applicable policies and federal law.

*Respects privacy and human rights.

Policy Statement 139-07: Use of Commercial Generative Artificial Intelligence (AI) Tools

Per Policy Statement 139-07:

✓ Yes

Creating engaging public safety announcements.

✕ No

To make decisions related to benefits adjudication and law enforcement actions are prohibited by policy.

What are the risks of using GenAI tools?

- **Accuracy:** GenAI tools may generate plausible but incorrect information (such as text, images and citations), known as “hallucinations,” and present it as fact.
- **Privacy:** Never enter personally identifiable information (PII) (it is against DHS policy). AI tools are not controlled by DHS - they can share information that creates risk to individuals.
- **Security:** Information you enter has potential for spillage to unauthorized platforms and users.
- **Bias:** GenAI models may include biases due to the training data used, configuration settings, or poor data quality.
- **Intellectual Property (IP):** GenAI is trained on data from the internet, there may be IP in the generated results.

⚠ **Caution:** **Review your output**

GenAI tools can produce:

- Inappropriately biased results
- Offensive results
- Errors
- Hallucinations
- PII

Risks: Accuracy

AI tools can create content that seems real but is not.

Examples:

- A news article or headline could be generated by AI even if it didn't happen.
- A detailed account of a battle that never happened, complete with names, dates, and outcomes.
- Biographies may be created for a person who never existed.
- Citations to non-existent court cases.

What you can do:

❑ You can ask most tools to cite all sources used.

❑ Indicate when a work product has been generated or generated in part by Commercial GenAI.

❑ Always cross-check information with independent reputable sources.

❑ Include human expert reviews of generated content.

Risks: Privacy & Security

What you enter is public and can be used by others outside DHS.

Entering sensitive data can result in spillage.

Information entered in AI tools

- May be retained by the tool provider (even if they claim otherwise).
- May be aggregated, resulting in a clearer picture of a user's preferences, habits, or personal details.
- May be used for enhanced social engineering threat actors.

What you can do:

□ Avoid entering any data other than open-source information (already available to the general public).

This may include information derived from internal DHS or Federal government draft work products, emails, conversations, or other documents.

□ Never enter sensitive, confidential, or classified information.

Examples of specific categories of information that cannot be entered into a commercial GenAI tool include, but are not limited to: financial disclosure information, protected acquisition information, controlled unclassified information (CUI), and personally identifiable information (PII).

□ Choose tool settings to clear user history or operate in an anonymous mode, if available.

Risks: Privacy & Security

Examples of Data

Sensitive

- An internal Teams conversation thread.
- A report containing names and contact info of project participants.
- A list of emails from survey participants.

Not Sensitive

- A presentation already posted on a public DHS website.
- An executive order that is already public.
- Transcriptions of a public hearing.

Entering sensitive data can result in spillage.

Risks: Bias

AI tools can reflect existing societal biases based on training data and/or what is entered, or how the GenAI tool is directed to present the results.

What you can do:

- ❑ Be aware of individual biases and ask questions in a neutral, open-minded way.
- ❑ Supplement AI with diverse human perspectives.
- ❑ Check multiple AI systems and compare responses.
- ❑ Provide feedback to the DHS AI leadership (AI@hq.dhs.gov) when you notice biased, discriminatory, inappropriate or harmful content.

Risks: Intellectual Property

AI tools may generate content that could infringe on intellectual property rights.

What you can do:

❑ Specify that generated content should be original and not copied from existing sources.

❑ Request citations for all generated content.

❑ Use GenAI output to provide early-stage inspiration, not as the final output.

❑ Review generated output to ensure it isn't producing trademarked or copyrighted material.

❑ Consult the DHS Office of General Counsel or your Component General Counsel.

How can I balance the benefits with the risks of using GenAI tools?

Review generated content before use. Use human judgment.

What you must do:

Before using content generated by AI tools in an official capacity, the approved user must review it for accuracy, relevance, privacy, data sensitivity, inappropriate bias, copyright or intellectual property concerns, and policy compliance.

Examples:

- When drafting a public communication document, scrutinize and validate each section to ensure the language reflects DHS values.
- GenAI tools may generate questionable data, always verify with trusted sources.

Not all information and activities are acceptable

Acceptable

- **Writing assistance.** Use conditionally approved AI tools to create documents (Example: Drafting speeches)
- **Data analysis with open-source data.** Use GenAI to analyze information (Example: Analyze weather patterns to anticipate natural disasters)
- **Creative content.** Generate information for a specific topic, theme, or industry (Example: Designing infographics for public education)

Unacceptable

- **Sensitive data handling.** Processing individual health records (Example: Medical tests)
- **Biased communication.** Creating biased documents or applications (Example: Generating gender-biased job descriptions)
- **Unauthorized GenAI tools.** Using unapproved GenAI tools for official tasks (Example: Using unauthorized GenAI video, audio, design, music, text, or coding to complete tasks)

! Appropriate application of GenAI tools requires judgment.
DHS personnel must follow DHS Commercial Generative AI Rules of Behavior.

Knowledge Check #2

What best describes responsible use of GenAI at DHS?

A. Users should proactively reduce the impact of bias, which includes reporting any suspected cases of inappropriate bias or offensive or harmful content.

B. Users should try unapproved tools to determine if they work better.

C. Outputs generated by GenAI should always be cross-checked with independent sources to validate accuracy.

D. Both A and C.

E. None of the above.

Answer: D

Section 3: How to Get Started

In this section, you will:

- Understand how to gain approval to use GenAI tools at DHS.
- Understand how to use GenAI tools in accordance with DHS Rules of Behavior.
- Learn what to do if something goes wrong.

First, complete a few requirements

1. Ask your supervisor for permission to use GenAI tools BEFORE DHS GenAI training.

2. Complete required trainings:

   - ❑ Cybersecurity Awareness Training.
   - ❑ Privacy at DHS: Protecting Personal Information.
   - ❑ Generative Artificial Intelligence Training.
   - ❑ Any additional training required by your Component.

3. Read, understand, and comply with DHS Commercial GenAI Rules of Behavior:

   - ❑ Employees and contractors read and sign Rules of Behavior
   - ❑ Employees ask your supervisor to review and sign.
   - ❑ Contractors ask your Contracting Officer Representative (COR) to review and sign.

Next, safely set up your GenAI tool

3. Once you've completed the required trainings and are approved to use GenAI tools, do the following:

   - ❑ Set up an account using your DHS email (not any personal accounts).
   - ❑ Ensure you follow the guidance provided by DHS for use of a specific conditionally approved GenAI tool

4. In the tool settings, look for ways to protect yourself and others by:

   - ❑ Selecting options that limit data retention.
   - ❑ Opting out of inputs that are used to further train the tool.
   - ❑ Minimizing system setting privileges so the tools can't access unauthorized systems or data.
   - ❑ Asking for help from a colleague or supervisor if you can't find these settings. You may always ask an AI Expert by emailing AI@hq.dhs.gov.

Then, while using GenAI tools, always follow the rules

You must adhere to the acceptable use of GenAI tools and comply with the DHS Commercial GenAI Rules of Behavior.

❑ Access the commercial GenAI tool on a DHS web browser only (don't download an app onto your computer or mobile device).

❑ Only use non-sensitive open-source information to reduce security risks posed by the data shared with the tools.

❑ Review all content generated by GenAI tools for accuracy, relevance, privacy, data sensitivity, bias, potential copyright or intellectual property concerns, before use in an official capacity.

❑ Always cross-verify with trusted sources, look for incongruencies where something seems out of place, and mitigate biased results through descriptive creation criteria.

Remember, AI is evolving

Given the rapid pace of technological change in the AI space, DHS policies and guidance will be updated regularly.

Personnel are encouraged to provide feedback and stay informed about updates to harness the full potential of GenAI, responsibly.

How do I report a problem?

Report problems to:

- **Component Security Operations Centers:** Report cybersecurity incidents immediately upon suspicion or recognition.
- **Civil Rights and Civil Liberties:** Report inappropriate bias and offensive or harmful content.
- **Privacy Office:** Report privacy concerns or incidents.
- **DHS AI Leadership:** Provide feedback (AI@hq.dhs.gov) when you notice biased, discriminatory, inappropriate, or harmful content.

If you encounter **inappropriate or offensive language, pornographic material, errors, or hallucinations,** consider reporting it directly to the GenAI tool to improve the tool.

If you have any questions on who to report an issue to, ask an expert via email at AI@hq.dhs.gov.

Examples:

- Accidentally entering PII or receiving PII.
- Entering data that is not open-source.
- Allowing access to a sensitive document.

Q&A