# Privacy Impact Assessment

**for the**

## Use of Conditionally Approved Commercial Generative Artificial Intelligence Tools

**DHS Reference No. DHS/ALL/PIA-097**

**November 19, 2023**

Homeland Security

## Abstract

In accordance with the Secretary of Homeland Security's recent announcement[1] on the Department's use of Artificial Intelligence (AI),[2] the DHS Office of the Chief Information Officer, in coordination with the Science and Technology Directorate, Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel, is leading the Department's efforts to ensure responsible use of AI while fulfilling the Department's mission and supporting its workforce. As part of this effort, the DHS Office of the Chief Information Officer is working to advance specific mission applications of AI across the Department, and address ways in which the workforce may use conditionally approved commercially available generative AI (Gen AI) tools (i.e., tools not procured for use for specific Department missions) for certain aspects of their work. "Gen AI" is the class of AI models that emulate the structure and characteristics of input data to generate novel synthetic content (i.e., outputs). This can include images, videos, audio, text, code, and other types of digital content. This Privacy Impact Assessment (PIA) analyzes the Department's use of conditionally approved Gen AI tools.

## Introduction

In accordance with Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (October 30, 2023), and Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (December 8, 2020), DHS will ensure the safe, secure, and responsible use and development of AI. More specifically, DHS will assess Gen AI and the unique opportunity it presents for the Department.

Gen AI describes algorithms that can be used to create new content, including audio, code, images, text, and videos. Gen AI systems fall under the broad category of machine learning, a subset of AI. Machine learning systems receive inputs in the form of "training" data, and then generate rules that produce outputs. In other words, machine learning systems "learn" from examples, provided in the form of training data, rather than receiving pre-defined content and patterns from humans. Until recently, machine learning was largely limited to predictive models, used to observe and classify patterns in content. For example, a classic machine learning problem is to start with an image or several images of an established pattern. The machine learning system would then identify patterns among the images, and then scrutinize random images for ones that would match the established pattern. Now, rather than simply perceive and classify a photo,

[1] *See* "Statement from Secretary Mayorkas on President Biden's Executive Order on Artificial Intelligence" (October 30, 2023), *available at* https://www.dhs.gov/news/2023/10/30/statement-secretary-mayorkas-president-bidens-executive-order-artificial.

[2] AI refers to "automated, machine-based technologies with at least some capacity for self-governance that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions, influencing real or virtual environments." *See* "U.S. Department of Homeland Security Artificial Intelligence Strategy," *available at* https://www.dhs.gov/publication/us-department-homeland-security-artificial-intelligence-strategy.

machine learning can *create* an image or text description on its own based on algorithms and training model information. This is Gen AI.

As AI technologies advance, DHS must continually assess the opportunities and potential risks associated with their uses to ensure that DHS can effectively leverage emerging technologies to achieve its missions. Further, it is imperative that the Department be transparent about the Department's use of AI. This Privacy Impact Assessment provides additional notice of the Department's use of AI, while focusing on DHS use of conditionally approved Gen AI tools specifically; outlines the privacy policies, measures, and guidance implemented for DHS use of conditionally approved Gen AI tools; and documents the potential privacy risks DHS use of commercial Gen AI technologies presents.

On April 20, 2023, the Secretary established the Department's first task force dedicated to AI: the Artificial Intelligence Task Force (AITF).[3] The AI Task Force, co-chaired by the DHS Chief Information Officer and the Under Secretary for Science and Technology, is charged with advancing the application of AI to critical homeland security missions in four priority initiatives:

- Enhance the integrity of supply chains and the broader trade environment;
- Leverage AI to counter the flow of fentanyl into the United States through better detection methods and disruption of criminal networks;
- Apply AI to digital forensic tools to help identify, locate, and rescue victims of online child sexual exploitation and abuse, and identify and apprehend the perpetrators; and
- Work with our partners in government, industry, and academia, to assess the impact of AI on our ability to secure critical infrastructure.

The AI Task Force includes the DHS Artificial Intelligence Responsible Use Group, led by the Civil Rights and Civil Liberties Officer. The Responsible Use Group provides guidance, risk assessment, mitigation strategies, and oversight for the protection of individual rights in projects championed by the DHS AI Task Force. The Responsible Use Group's goals include:

- Engaging stakeholders, assessing risks, and prescribing tailored mitigation;
- Strengthening the DHS AI workforce through trainings and other learning opportunities focused on responsible use, trustworthiness, accountability, and strong governance practices; and

[3] *See* "Memo on the Establishment of a DHS Artificial Intelligence Task Force" (April 20, 2023), *available at* https://www.dhs.gov/publication/memo-establishment-dhs-artificial-intelligence-task-force.

- Providing input to DHS AI governance policies based on experience assessing and mitigating risks in projects implementing AI tools through the AI Task Force.

On September 14, 2023, the Department announced a new policy to ensure responsible use of AI by the Department:[4]

- Policy Statement 139-06 "Acquisition and Use of Artificial Intelligence and Machine Learning by DHS Components": The policy statement establishes the foundation for DHS's use of AI with a clear set of principles and created a Policy Working Group for further implementation of Section 7224(b) of the Fiscal Year 2023 National Defense Authorization Act (NDAA) (Pub. L. 117-263). The principles include that DHS systems, programs, and activities using AI will conform to the requirements of Executive Order 13960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. In addition, DHS will only acquire and use AI in a manner that is consistent with the Constitution and all other applicable laws and policies. Also, DHS will not collect, use, or disseminate data used in AI activities, or establish AI-enabled systems that make or support decisions, based on the inappropriate consideration of race, ethnicity, gender, national origin, religion, gender, sexual orientation, gender identity, age, nationality, medical condition, or disability.

The AI Policy Working Group (AIPWG) coordinates with the DHS AI Task Force to effect policy change and apply oversight to all DHS AI activities. The AI Policy Working Group collaborates across the Department and includes participants from the DHS Office of the Chief Information Officer, Science and Technology Directorate, Office of the Chief Procurement Officer, Office for Civil Rights and Civil Liberties, the Privacy Office, and the Office of Strategy, Policy, and Plans.

In addition, the Secretary announced the Department's first Chief AI Officer to promote AI innovation and safety within the Department and advise DHS Leadership on AI issues. As part of those responsibilities, the Chief AI Officer is leading a Department-wide effort to assess DHS personnel's responsible use of conditionally approved commercial Gen AI tools to harness the benefits of Gen AI in limited contexts.[5] Immediate appropriate applications of conditionally approved 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,[6] and developing briefing materials or preparing for meetings and events.

[4] *See* "DHS Announces New Policies and Measures Promoting Responsible Use of Artificial Intelligence" (September 14, 2023), *available at* https://www.dhs.gov/news/2023/09/14/dhs-announces-new-policies-and-measures-promoting-responsible-use-artificial.

[5] Policy Statement 139-07, "Use of Commercial Generative Artificial Intelligence (AI) Tools" (October 24, 2023), memorializes DHS's efforts to conditionally assess and use commercially available Gen AI products in furtherance of certain aspects of the DHS mission. On file with the Privacy Office.

[6] Pursuant to the DHS Gen AI Policy Statement, "open-source information" is defined as "unclassified information that has been published or broadcast in some manner to the public. Sources are newspapers or other periodicals;

Additionally, the Department is assessing conditional approval of tools that generate text, images, video, and code.

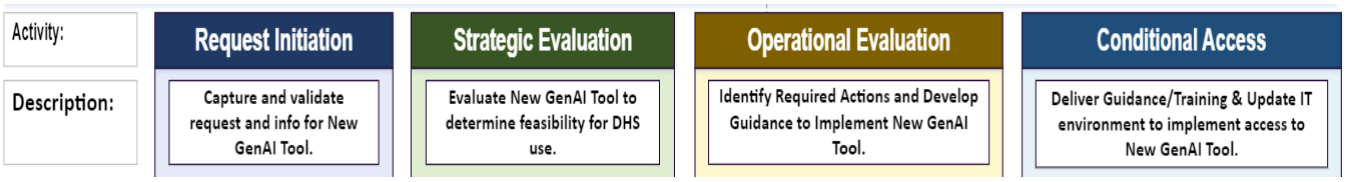
Generally, commercial Gen AI tools are privately owned by third parties. To ensure oversight of the use of commercial Gen AI tools, DHS is developing and will maintain a list of commercial Gen AI tools conditionally approved for use in the Department. In developing this list, DHS will review basic accuracy 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 Privacy Office, the Office for Civil Rights and Civil Liberties, Office of the General Counsel, and other internal stakeholders.

Gen AI tools present significant challenges and risks, including producing "hallucinations," or invented and inaccurate responses, and biased outputs based on biases in their training data or curation of their algorithm. They further present possible information, privacy, civil rights, civil liberties, and security risks, including, for example, if sensitive information is used to generate output and/or used to further train underlying models. Because of these potential risks, careful human review and judgment are required to responsibly use conditionally approved Gen AI tools. DHS has established a review process by which each tool will be researched and analyzed prior to conditionally approving its use by DHS personnel.

**DHS Commercial Gen AI Tool Conditional Approval Process**

DHS has established the Gen AI Tool Conditional Approval Process (see Figure 1). The process consists of four steps, through which the Department will analyze each tool individually to determine its appropriateness for Departmental use, based on factors such as: potential use cases; privacy, civil rights, civil liberties, and legal issues; security; and terms of service.

**Figure 1: Gen AI Tool Conditional Approval Process**




In Step 1, DHS will proactively identify or personnel will request through the DHS Office of Chief Information Officer the use of specific commercial Gen AI tools. DHS will determine if the request is appropriate for Department use, and if so, route the request to use the commercial Gen AI tool to Step 2 to determine its utility for DHS use. Internal stakeholders, such as the Privacy Office, Office for Civil Rights and Civil Liberties, and the Chief Information Security Officer Directorate (CISOD), will research and analyze the Gen AI tool to determine its capabilities and

weather reports; books, journal articles, or other published works; public court filings; or any similar documents that have traditionally been publicly available."

make a strategic decision whether to proceed. In Step 3, DHS will further evaluate the tool, including its potential risks, and make an operational decision to proceed. DHS will develop guidance and training specific to the Gen AI tool if needed. Finally, once the appropriate review and approvals are made in the previous steps, DHS will make the new Gen AI tool available for conditional use (Step 4). Each conditionally approved Gen AI tool will be documented in Appendix A to this Privacy Impact Assessment.

**DHS Gen AI Policy Statement and DHS Gen AI Rules of Behavior**

In addition to the DHS AI Tool Conditional Approval Process, DHS has established specific requirements governing how the Department and its personnel may use conditionally approved commercial Gen AI tools. Each individual user must review and agree to follow the DHS Gen AI Rules of Behavior before using a commercial Gen AI tool. As the Department learns more from conditional use of these tools, the DHS Gen AI Rules of Behavior will be updated in coordination with stakeholders across the Department, including the Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel, and all users will be required to re-review and agree to follow each iteration of the DHS Gen AI Rules of Behavior.[7] In addition, DHS personnel must adhere to and comply with federal laws and DHS policies, including the general DHS Rules of Behavior (DHS Policy Directive 4300A, Attachment G[8]) and privacy policies.

In addition to the Department and Component's existing privacy policies, the DHS Gen AI Rules of Behavior carry over the safeguards established in DHS's Gen AI Policy Statement[9] and outline the following requirements: "Acceptable Use of Gen AI Tools," "Data Protection and Retention," "Accountability for Use of Products Derived from Gen AI Tools," and "Incident Reporting and Request for Assistance." Acceptable Use requirements include the completion of required trainings, including newly developed Gen AI training and privacy and cybersecurity training, use of only conditionally approved tools, Gen AI tool account registration, and prohibition of use of the tools on personal devices and personal use of DHS accounts. Data Protection and Retention requirements include only using open-source information;[10] prohibition

[7] The DHS Gen AI Rules of Behavior will be incorporated into DHS Policy Directive 4300A. *See* footnote 8.
[8] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS ATTACHMENTS, ATTACHMENT G (April 28, 2022), *available at* https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.
[9] For example, "[p]ersonnel 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."
[10] Pursuant to the DHS Gen AI Policy Statement, "open-source information" is defined 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."

of the use of non-public information,[11] personally identifiable information (including "anonymized" information), and social media information; and a requirement to opt out of data retention by and use of input information to train the Gen AI tool, if available. Accountability requirements include a requirement that use of conditionally approved Gen AI tools is responsible and trustworthy, that when using content generated by these tools, the user must safeguard privacy, civil rights, and civil liberties consistent with law and DHS and Component policies, safeguard against inappropriate biases, and to the extent possible, ensure that use is transparent, source cited, and able to be explained to those whom we serve. Further, the tools must not be used to develop inappropriate content.

Additionally, the DHS Gen AI Policy Statement and the DHS Gen AI Rules of Behavior include a prohibition on the use of Gen AI-generated content 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. Additionally, users must manually review the output for accuracy, functional effectiveness and suitability, and intellectual property because Gen AI tools may have been trained on data that AI providers may not have had full legal rights to use. And users may not use output that includes personally identifiable information. Users will consult with counsel, component privacy offices, and the Office for Civil Rights and Civil Liberties as needed to ensure compliance with the DHS Gen AI Rules of Behavior and report any unintended or inappropriate output. Finally, Incident Reporting and Request for Assistance requirements include appropriate reporting of any potential cybersecurity incidents, data spillage, or hallucination outputs or errors.

The framework discussed above is the Department wide framework from which Components and Offices will build their own frameworks. Component Privacy Officers and Chief Information Officers will develop policies regarding appropriate use of conditionally approved commercial Gen AI tools in their missions, in consultation with the DHS Office of the Chief Information Officer, Privacy Office, and the Office for Civil Rights and Civil Liberties. These policies may impose additional conditions or limitations on the conditional use of commercial Gen AI tools based on unique mission requirements and/or potential privacy, civil rights, and civil liberties risks related to specific uses.

**Privacy Risks of DHS Use of Conditionally Approved Commercial Gen AI Tools**

Each Gen AI tool is governed by the host company's privacy policy, terms of service, account registration requirements, and model training. As part of the DHS Gen AI Tool

[11] 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 information includes information related to financial disclosures, protected acquisition, controlled unclassified information (CUI), personally identifiable information (PII), and classified information.

Conditional Approval Process the Department will examine the tool, its privacy policy/terms of service, and other relevant information to assess any potential privacy, civil rights, civil liberties, security, or legal risks and determine whether the tool is appropriate for the Department's use. Due to the evolving nature of commercial Gen AI tools and the ever-changing landscape of the AI space, these evaluations are subject to re-review as appropriate. For example, a commercial Gen AI tool may update its privacy policy/terms of service, which could impact the Department's conditional approval for use of that tool.

Users are typically required to submit some personally identifiable information to register for a commercial Gen AI tool account. For example, some tools may require name and date of birth, while others may require name, email address, and payment information.[12] The Department does not solicit or collect this personally identifiable information for use of the tool; however, each Gen AI tool uses this information in accordance with its terms of service and privacy policies. For example, some companies may provide user's personal information to third parties without further notice and others may use this account registration data and any information collected to "train" their models. As a result, use of conditionally approved commercial Gen AI tools by Department personnel is voluntary.

Additionally, each Gen AI tool uses input information in accordance with its own terms of service and privacy policies. Some tools collect information to train their models through "inputs" from users. Inputs are the prompts or information that a user sends to and asks the tool to analyze to generate an output. Therefore, it is important for DHS users of conditionally approved Gen AI tools to carefully assess the information they are inputting into the tool. Once a DHS user discloses any information to a Gen AI tool, the Department no longer controls it.

The nature and sophistication of Gen AI tools continue to develop at a rapid pace. Individual Gen AI tools may continuously train their models or conduct iterative updates. Accordingly, the same inputs used at one point in time may not result in the same output later. Further, Gen AI tools are documented as producing hallucinations or invented/inaccurate responses and generating biased outputs based on biases in their training data. Consequently, DHS personnel are not permitted to use outputs from conditionally approved commercial Gen AI tools 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.

Importantly, when DHS personnel use the conditionally approved commercial Gen AI tools listed in Appendix A, they must not input and/or actively seek as output personally identifiable information (irrespective of whether it is anonymized or de-identified). If the tool

[12] Any payment information would be shared in accordance with DHS procurement and acquisition policies. No personal payment information may be used.

generates personally identifiable information in its output, users may not use it. Users will consult with counsel, component privacy offices, the Privacy Office, and the Office for Civil Rights and Civil Liberties as needed to ensure compliance with the DHS Gen AI Rules of Behavior. Users also must report unintended or inappropriate output, including personally identifiable information.

**Evolving Landscape**

As noted previously, AI, and Gen AI specifically, is a rapidly evolving technological landscape. Likewise, as models are further trained and refined, anticipated outputs may also evolve. Additionally, because the conditionally approved commercial Gen AI tools are not inherently designed for DHS mission purposes, the Department must closely assess and oversee the uses and outputs in this conditional use phase to understand how the tools work in our environments, in support of our missions, and in compliance with law and policy, including those related to privacy, civil rights, civil liberties, and security.

Accordingly, the Office of the Chief Information Officer, Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and the Science and Technology Directorate will work together and with other oversight and subject matter expert offices to observe and learn how the conditionally approved Gen AI tools are used in the Department, their intended and unintended outputs, including potentially biased, discriminatory, or privacy sensitive outputs, and how they continue to develop commercially. During this initial, conditional use stage, the Privacy Office will assess whether additional privacy policy, compliance requirements, and/or guidance is needed to address and appropriately safeguard any privacy implications posed by use of conditionally approved commercial Gen AI technologies. The Privacy Office anticipates close collaboration with the Office of the Chief Information Officer to develop a mechanism by which conventional privacy compliance and oversight procedures may adapt to this new era of large-scale and ever changing and learning technology. This approach will ensure that privacy is a key component of new technologies and tools the Office of the Chief Information Officer introduces to and approves for Department use.

# Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974[13] articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002, Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.[14]

[13] 5 U.S.C. § 552a.
[14] 6 U.S.C. § 142(a)(2).

Accordingly, the Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS.[15] The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments on Department practices, programs, activities, operations, and information technology systems, pursuant to the E-Government Act of 2002, Section 208, and the Homeland Security Act of 2002, Section 222. The use of conditionally approved commercial Gen AI tools is a Department activity; therefore, this Privacy Impact Assessment is conducted as it relates to the Fair Information Practice Principles.

## 1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information. Technologies or systems using personally identifiable information must be described in a System of Records Notice and Privacy Impact Assessment, as appropriate.

DHS is completing this Privacy Impact Assessment to provide notice of its use of conditionally approved commercial Gen AI tools. This Privacy Impact Assessment also assesses potential privacy risks associated with the use of commercial Gen AI tools even though the Department is prohibiting the use of personally identifiable information (irrespective of whether it is anonymized or de-identified) as input into the tools. While commercial Gen AI tools are not search engines and should, therefore, provide output consistent with the input, it is possible that use of a conditionally approved commercial Gen AI tool could generate personally identifiable information in its output. Accordingly, this Privacy Impact Assessment is designed to anticipate privacy risks based on what the Department currently knows about commercial Gen AI tools. As noted previously, the Privacy Office, the Office for Civil Rights and Civil Liberties, the Office of the General Counsel, and the Office of the Chief Information Officer will assess how the conditionally approved tools work in the DHS environment and determine whether they should continue to be used and whether additional privacy, civil rights, and civil liberties safeguards and additional governance structures should be established.

Each commercial Gen AI tool the Department conditionally approves for use will be listed in the Appendix to this Privacy Impact Assessment.

[15] U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY POLICY GUIDANCE MEMORANDUM 2008-01/PRIVACY POLICY DIRECTIVE 140-06, THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY (2008), *available at* https://www.dhs.gov/privacy-policy-guidance.

In addition to this Privacy Impact Assessment, associated Executive Orders, and DHS policies, guidance, and announcements provide notice of the Department's efforts in the AI space. These include:

- Executive Order 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence;"
- Executive Order 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government;"
- U.S. Department of Homeland Security Artificial Intelligence Strategy;
- Policy Statement 139-06, "Acquisition and Use of Artificial Intelligence and Machine Learning by DHS Components;" and
- Policy Statement 139-07, "Use of Commercial Generative Artificial Intelligence (AI) Tools."

As noted, DHS users are prohibited from including any information about individuals in prompts for any conditionally approved commercial Gen AI tool, regardless of whether it is personally identifiable information or anonymized. Also prohibited is use of social media content or any other non-public or sensitive information. The only personally identifiable information permitted to be shared with conditionally approved Gen AI tools is information provided by the user to register with or access the tool.

Each commercial Gen AI tool has its own specific registration requirements and collection of different data points. The privacy policy for each tool is available on the tool or company's website, and is linked to and provided on the DHS intranet site. To safeguard personnel privacy, only personally identifiable information required to establish an account may be input into the tool, and use of conditionally approved commercial Gen AI tools is voluntary.

**Privacy Risk:** There is a risk that members of the public may not know how DHS's use of commercial Gen AI tools impacts them.

**Mitigation:** This risk is mitigated. First, this Privacy Impact Assessment provides notice of how DHS will use conditionally approved commercial Gen AI tools. Additionally, Executive Orders, policy documents, and other public announcements, as noted above, outline DHS's general use of AI. Chiefly, DHS personnel are not permitted to use conditionally approved commercial Gen AI tools 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, nor may they input into the tool or use generated output that includes personally identifiable information. Additionally, the DHS Gen AI Rules of Behavior encourage

DHS users to cite the source of Gen AI content in DHS products or deliverables.[16] Therefore, conditionally approved DHS Gen AI use is not expected to directly impact individual members of the public, and DHS is taking steps to transparently indicate Gen AI-produced content in its products.

**Privacy Risk:** There is a risk that DHS personnel may not know the risks associated with or proper uses of commercial Gen AI tools.

**Mitigation:** This risk is mitigated. Before any DHS personnel may use a conditionally approved commercial Gen AI tool, they must review and agree to follow the DHS Gen AI Rules of Behavior, including the prohibition on the input and use of any generated personally identifiable information. The DHS Gen AI Rules of Behavior, which apply to all DHS personnel using conditionally approved commercial Gen AI tools on government-furnished equipment or any device accessing the DHS network, outline requirements for responsible use of the tools. Further, users are required to complete training, including DHS Generative AI Annual Training, Privacy at DHS: Protecting Personal Information training, Cybersecurity Awareness training, and any applicable Component or tool-specific privacy and security training requirements. The DHS intranet site also includes resources on the approval process to use commercial Gen AI tools, conditions for use of each approved tool (e.g., if the tool provides an opt out of input data being used for training option or option to limit data retention, then users must opt out/in, or if inclusion of a user's birth date to access a tool is optional, then users should not input their birth date), and best practices and Frequently Asked Questions documents.

## 2. Principle of Individual Participation

Principle: DHS should involve the individual in the process of using personally identifiable information. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of personally identifiable information and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of personally identifiable information.

As noted, DHS users of conditionally approved commercial Gen AI tools are prohibited from inputting personally identifiable information into the tool to generate output/content and likewise prohibited from using any personally identifiable information generated by the tool. Further, conditionally approved commercial Gen AI 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.

[16] See also Executive Order 14110, the Office of Management and Budget shall issue implementing guidance, including "reasonable steps to watermark or otherwise label output from generative AI."

Because of these safeguards, DHS use of conditionally approved commercial Gen AI tools is unlikely to collect, use, store, or generate any personally identifiable information. However, because of the ever-evolving nature of these tools and unanticipated outcomes, individuals may submit a Freedom of Information Act (FOIA) or Privacy Act request to access or correct information maintained by DHS. Individuals may submit requests to the Privacy Office: Chief Privacy Officer/Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, 2707 Martin Luther King Jr. Avenue, S.E., Washington, D.C. 20528-0628, or electronically at https://www.dhs.gov/foia-contact-information.

Any personally identifiable information collected by a conditionally approved commercial Gen AI tool during the account registration process is collected directly from the individual DHS user and is not shared with or requested by the Department. Each commercial Gen AI tool uses this information in accordance with its own terms of service and privacy policies. Any necessary correction of or deletion of this data will vary depending on the tool's terms of service.

**Privacy Risk:** There is a risk that the commercial Gen AI tool output could include personally identifiable information or information that could otherwise impact an individual's privacy, even though the user did not intend to receive or collect it.

**Mitigation:** This risk is partially mitigated. Because commercial Gen AI tools are proprietary in nature, DHS cannot control how the inputs are used by the Gen AI tool and what outputs the tools generate. Therefore, it is imperative that DHS users adhere to the DHS Gen AI Rules of Behavior, understand the purpose and capabilities of the tools, and report any problems or issues when using conditionally approved commercial Gen AI tools.[17] As noted previously, the use of personally identifiable information (whether anonymized or de-identified) in a conditionally approved commercial Gen AI tool is prohibited and serves as an additional safeguard designed to minimize the likelihood that personally identifiable information will be included in the tool's output. Further, the Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and Office of the Chief Information Officer will assess information received from users regarding unintended or incorrect, biased, discriminatory, inappropriate, or other output to inform future safeguards and/or governance frameworks.

Because commercial Gen AI tools obtain data to train their models from a variety of sources, including potentially from social media sites, by scraping the Internet, or purchasing data from other companies that curate data specifically for machine learning models, there may be information included in a Gen AI tool's holdings or training data, and, therefore, potentially

[17] DHS has established a reporting mechanism for DHS users to report potential cybersecurity incidents, inappropriate bias, privacy concerns/incidents, and encounters with inappropriate or offensive language, errors, or hallucinations.

included in output data that could impact privacy. However, DHS mitigates this potential risk in a few ways.

As noted, as part of the conditional review process, DHS assesses available information on how training data was sourced. While not the sole factor to determine whether a proposed commercial Gen AI tool should be accepted for conditional use, the Department considers training data sources and balances the company's practices with other relevant factors. Ethically sourced training data – data that preserves underlying privacy protections in source data – is a privacy best practice in the AI space. Additionally, DHS users of conditionally approved commercial Gen AI tools are prohibited from using outputs 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. Likewise, users may not input personally identifiable information into the tool and may not use any personally identifiable information, or seek personally identifiable information, as an output.

Thus, while DHS cannot control the data commercial Gen AI tools use to train their models, the DHS use cases for conditionally approved Gen AI tools are designed to mitigate associated privacy risks, including the risk of DHS using source data in a manner that could harm individual privacy.

As DHS continues to use commercial Gen AI tools and the tools themselves further develop, it is important for all DHS users to stay abreast of the AI landscape. All DHS users are required to take annual DHS Generative AI Annual Training, in addition to annual privacy and security training and any applicable Component or tool-specific training requirements. The substance of training may evolve over time to address enhancements or changes to the tools. All DHS users are required to review and agree to abide by the DHS Gen AI Rules of Behavior, which also may change to reflect changes to the DHS commercial Gen AI posture. When modified, the DHS Gen AI Rules of Behavior will be recirculated to existing DHS users for re-review and agreement.

Lastly, should any personally identifiable information inadvertently be generated/output by a conditionally approved commercial Gen AI tool and maintained and/or used by DHS, it is subject to existing federal law and DHS privacy policy and retention requirements.[18]

[18] Any information collected from a commercial conditionally approved Gen AI tool may become a federal record, and the Department is required to maintain a copy per its records retention policies. The business unit responsible for the record will apply the correct records schedule, in coordination with the appropriate stakeholders (such as the Department or Component's records management office and counsel), to any information used with or created by a conditionally approved Gen AI tool, as required. Varied records schedules apply based on the functional operations of the end user who is leveraging the tools.

## 3. Principle of Purpose Specification

Principle: DHS should specifically articulate the authority which permits the collection of personally identifiable information and specifically articulate the purpose or purposes for which the personally identifiable information is intended to be used.

Pursuant to Executive Orders 14110 and 13960 and the DHS Gen AI Policy Statement, DHS has established policy and guidance to ensure mission-appropriate, responsible, and rights-protecting use of AI. DHS policy outlines the Department's commitment in deploying AI tools to enhance operations and lead the government in the responsible and ethical use of AI.[19] DHS's guiding principles for AI use require that in acquiring and using AI, the Department must:

- Comply with all applicable laws and policies, especially those protecting privacy, civil rights, and civil liberties.
- Follow the Principles for Trustworthy AI in Government.[20]
- Provide transparency on AI use at DHS through the DHS AI Use Case Inventory.[21]
- Ensure all AI use is mission-appropriate and improves mission-effectiveness.
- Guard against bias in data collection, use, and dissemination at DHS.
- Advance equity and fundamentally fair treatment and guard against impermissible discrimination by testing and validating AI use cases at DHS.
- Prohibit improper systemic, indiscriminate, or large-scale monitoring, surveillance, or tracking of individuals with AI.
- Manage risk through a DHS-wide risk management framework.
- Protect AI technologies at DHS from cyberattacks and malicious degradation of algorithmic functions.
- Support the DHS workforce in understanding the strengths, weaknesses, benefits and risks of AI.
- Ensure human oversight for the design, implementation, and end uses of AI at DHS.

[19] U.S. Department of Homeland Security Artificial Intelligence Strategy; Policy Statement 139-06, "Acquisition and Use of Artificial Intelligence and Machine Learning by DHS Components;" and Policy Statement 139-07, "Use of Commercial Generative Artificial Intelligence (AI) Tools."
[20] *See* Executive Order 13960.
[21] Pursuant to Executive Order 13960, federal agencies are required to create and make publicly available an inventory of unclassified and non-sensitive Artificial Intelligence (AI) use cases, to the extent practicable and in accordance with applicable law and policy. *See* https://www.dhs.gov/data/AI_inventory.

In addition to the DHS Gen AI Tool Conditional Approval Process, each individual user follows specific steps to ensure appropriate access and use of conditionally approved commercial Gen AI tools. First, personnel must obtain supervisor approval to ensure use of commercial Gen AI tools meets the individual's job responsibilities. Next, the individual must complete the DHS Generative AI Annual Training, in addition to annual privacy and security training and any applicable Component or tool-specific training requirements. The individual must then review and agree to follow the DHS Gen AI Rules of Behavior, which require the user to obtain their supervisor's or Contracting Officer Representative's[22] signature. This process ensures that only those DHS personnel with job-specific duties requiring use of commercial Gen AI are using the conditionally approved tools.

**Privacy Risk:** There is a risk that DHS personnel may use conditionally approved commercial Gen AI tools for unauthorized purposes.

**Mitigation:** This risk is partially mitigated. DHS users must complete required training specific to Gen AI, privacy, and security; review and agree to follow the DHS Gen AI Rules of Behavior; and receive supervisory approval before using conditionally approved commercial Gen AI tools. This multi-step process ensures DHS users are well informed on the appropriate uses of commercial Gen AI tools, have received sufficient training, and use of the tool(s) is appropriate for their duties.

The DHS Gen AI Policy Statement, the DHS Gen AI Rules of Behavior, and the DHS Generative AI Annual Training specifically identify appropriate applications of commercial Gen AI tools to maximize efforts and efficiency on use cases such as:

- generating first drafts of documents that a human would subsequently review;
- conducting and synthesizing research on open-source information;[23]
- developing briefing materials or preparing for meetings and events; and
- creating training materials.

The appropriate use of conditionally approved commercial Gen AI tools is ultimately the decision of the individual DHS user pursuant to their job responsibilities and consistent with the DHS Gen AI Policy Statement, DHS Gen AI Rules of Behavior, and training, as well as laws and DHS policies, including DHS privacy policies. As noted, users are prohibited from using conditionally approved Gen AI tools 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. Further, the DHS Office of the Chief Information Officer created a reporting mechanism for DHS users to report improper use and any potential

[22] For DHS contractor personnel, the supervisor is the DHS Contracting Officer Representative.
[23] *See* supra note 10 defining "open source."

cybersecurity incidents, inappropriate bias, privacy concerns/incidents, and encounters with inappropriate or offensive content, errors, or hallucinations.

**Privacy Risk:** There is a risk that conditionally approved commercial Gen AI tools may receive and use DHS data not intended for public use.

**Mitigation:** This risk is partially mitigated. As noted, the DHS Gen AI Policy Statement and DHS Gen AI Rules of Behavior forbid the inclusion of non-public information in commercial Gen AI tool prompts. Non-public information includes personally identifiable information and social media information, as well as 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 information includes information related to financial disclosures, protected acquisition, controlled unclassified information, information For Official Use Only, and classified information.

Some commercial Gen AI tools may also allow users to opt out of their inputs being retained and used to train tool models. This means that the tool does not use information submitted as an input to further enhance and develop its algorithm. Per the DHS Gen AI Rules of Behavior, when such an opt-out feature is available, DHS users will select the option to limit data retention and model training. Users are required to confirm, in writing, to their supervisor that they implemented the available opt out feature. The DHS Office of the Chief Information Officer will assist with determining which tools have this feature and provide additional guidance to properly opt out.

During this initial use stage of conditionally approved commercial Gen AI tools, the Privacy Office, Office for Civil Rights and Civil Liberties, Office of the General Counsel, and Office of the Chief Information Officer will assess whether additional auditing processes are required to ensure proper DHS use of and inputs into these technologies.

## 4. Principle of Data Minimization

Principle: DHS should only collect personally identifiable information that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personally identifiable information for as long as is necessary to fulfill the specified purpose(s). Personally identifiable information should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Commercial Gen AI models generate their training data through a variety of different sources, including information available on the Internet and proprietary information. As part of the development of the DHS Gen AI effort, the Department has identified appropriate types of commercial Gen AI uses cases based on DHS's understanding of the tools and their capabilities, analysis of conditionally approved tools' terms of services and privacy policies, and application

and feasibility to the DHS mission space, consistent with policy and use limitations. Additionally, as part of the conditional review process, DHS assesses available information on how training data was sourced.

DHS has determined there are potential privacy risks associated with the use of commercial Gen AI tools with respect to data minimization, and, therefore, has instituted appropriate mitigation measures. For instance, to mitigate the potential of collecting personally identifiable information, users are prohibited from inputting into the tools personally identifiable information (whether anonymized or de-identified) and other non-public information. Additionally, the DHS Generative AI Annual Training outlines appropriate use cases for conditionally approved commercial Gen AI tools and what types of data are appropriate for input into the tools. Further, as noted, DHS has established the DHS Gen AI Tool Conditional Approval Process, during which the Privacy Office, Office for Civil Rights and Civil Liberties, and the Chief Information Security Officer Directorate (CISOD) will analyze each proposed commercial Gen AI tool and assess how the functionalities of the tool could impact inputs of DHS data and any potential outputs DHS could receive.

With respect to account registration to access the conditionally approved tools, per DHS policy, personnel are required to use accurate account registration information, such as DHS email address and true date of birth (if required). Some tools may have optional registration fields, which DHS personnel are instructed not to complete to reduce unnecessary data sharing. And use of these tools is voluntary.

**Privacy Risk:** There is a risk that DHS receives unintended information as part of the outputs from conditionally approved commercial Gen AI tools.

**Mitigation:** This risk is partially mitigated. DHS personnel must adhere to the DHS Gen AI Rules of Behavior and exercise the best practices outlined in the DHS Generative AI Annual Training to safeguard against unintended or inappropriate outputs. Although DHS users cannot control what outputs they receive, using proper inputs will reduce the risk of a commercial Gen AI tool producing inadvertent personally identifiable information, bias, illicit content, or other unintended output. Additionally, use of any output data received is governed by federal law and DHS policies.

As noted, DHS has also established a reporting mechanism for DHS users to report potential cybersecurity incidents, inappropriate bias, privacy concerns/incidents, and encounters with inappropriate or offensive language, errors, unintended output, or hallucinations. The Privacy Office, the Office for Civil Rights and Civil Liberties, the Office of the General Counsel, and the Office of the Chief Information Officer will review these reports to help inform any enhanced or additional future governance frameworks for commercial Gen AI use.

**Privacy Risk:** There is a risk that DHS will not appropriately retain output data it uses.

**Mitigation:** This risk is mitigated. Information collected from a conditionally approved commercial Gen AI tool may become a federal record, and the Department is required to maintain the record under its records retention policies. The system in which the record is retained will govern the correct records schedule. Any questions regarding records retention will be directed to the Department or Component's records management office and counsel.

Further, DHS has existing processes for data retention, and personnel must adhere to all federal laws and DHS policies, including the general DHS Rules of Behavior and DHS privacy policies. These requirements are outlined in the DHS Gen AI Rules of Behavior and highlighted in the DHS Generative AI Annual Training.

## 5. Principle of Use Limitation

Principle: DHS should use personally identifiable information solely for the purpose(s) specified in the notice. Sharing personally identifiable information outside the Department should be for a purpose compatible with the purpose for which the personally identifiable information was collected.

As noted, DHS users are not permitted to use personally identifiable information in the inputs for any queries of conditionally approved commercial Gen AI tools, nor is any personally identifiable information generated in the output permitted to be used. This prohibition is specifically articulated in the DHS Gen AI Policy Statement, the DHS Gen AI Rules of Behavior, and the DHS Generative AI Annual Training.

**Privacy Risk:** There is a risk that DHS will not appropriately handle commercial Gen AI tool output data that could include personally identifiable information.

**Mitigation:** This risk is partially mitigated. Because of the nature of commercial Gen AI tools, DHS cannot control the outputs it receives. However, all DHS personnel are trained on how to appropriately handle output and must adhere to the DHS Gen AI Rules of Behavior, in addition to federal law, the general DHS Rules of Behavior, and DHS privacy policy, when using, accessing, or collecting any data. DHS has established a reporting mechanism, available on the DHS intranet site, to report any issues with output data (e.g., inaccuracies, bias, illicit content, personally identifiable information).

DHS has established these resources to assist personnel in their use of conditionally approved commercial Gen AI tools. DHS will use the reporting mechanism to better understand the conditionally approved commercial Gen AI tools, their applicability to the DHS mission space, and any privacy, civil rights, civil liberties, and legal issues their use may present. This will help inform whether additional safeguards are needed, including additional governance frameworks.

DHS will also rely on other governing DHS AI bodies to coordinate and assess any potential issues with commercial Gen AI tools and their outputs. For example, as noted previously,

the DHS Artificial Intelligence Responsible Use Group, led by the Civil Rights and Civil Liberties Officer, provides guidance, risk assessment, mitigation strategies, and oversight for the protection of individual rights in projects championed by the DHS AI Task Force.

DHS Privacy will coordinate with all relevant stakeholders to continue to refine DHS's AI privacy posture, in addition to its existing privacy policies, as DHS uses conditionally approved commercial Gen AI tools and as AI advances.

**Privacy Risk:** There is a risk that DHS user account registration and other data disclosed during activities within Gen AI tools (outside of inputs) may be used for other purposes by the tool's platform.

**Mitigation:** This risk is partially mitigated. Part of the utility of commercial Gen AI tools is that they use data from a variety of sources to train their models. Each commercial Gen AI tool uses different data sources, which can be outlined in that tool's terms of service and/or privacy policy. For example, some commercial Gen AI tools may use registration data and information obtained when troubleshooting issues with a user to further train their models. However, as noted, commercial Gen AI tools are governed by their own applicable terms of service or privacy policies that may specifically outline how the tools will or will not use such data. For example, some commercial Gen AI tools do not require creation of account for use; therefore, there is no registration data at issue. Other tools may have specific provisions that allow a user to opt out of this information being used for other purposes, or the vendor could agree to a request to return any content that may have been submitted in error. This characteristic is part of the DHS Commercial Gen AI Tool Conditional Approval Process and one criteria the Department stakeholders review before conditionally approving a Gen AI tool.

DHS will create additional notice or "pop-up" alerts on DHS commercial Gen AI resource pages that link to conditionally approved commercial Gen AI tools, when feasible, explaining that DHS personnel are being directed to a nongovernment website that may have different privacy policies from those of the Department. It is also imperative that DHS personnel are mindful of the data they use or present, in any capacity, to these tools. Non-public information, including personally identifiable information may not be used in inputs to generate output when using conditionally approved commercial Gen AI tools. DHS personnel are also instructed to only submit information responsive to the required data fields during account registration.

## 6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that personally identifiable information is accurate, relevant, timely, and complete, within the context of each use of the personally identifiable information.

Questions around the governance of AI systems remain a persistent challenge. Goal 3 of the U.S. Department of Homeland Security Artificial Intelligence Strategy identifies a series of objectives to implement the principles set out in Executive Order 13960 to ensure that DHS's use of AI is accurate, safe, understandable, and regularly overseen.

One of the inherent risks of using commercial Gen AI tools is inaccurate output data. Gen AI uses machine learning systems that "learn" from examples, provided in the form of training data, rather than receiving explicit programming from humans. Because of this, commercial Gen AI tools may produce hallucinations or invented and inaccurate responses or generate biased outputs based on biases in the training data.

Understanding this risk, DHS has addressed the possibility for inaccurate output in several ways. For example, the DHS Gen AI Policy Statement directs that "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 compliance[24] before using it in any official capacity, especially when interacting with the public."

Further, the DHS Gen AI Rules of Behavior require personnel to manually review commercial Gen AI tool output for accuracy, functional effectiveness and suitability, and intellectual property (as Gen AI tools may have been trained on data that AI providers may not have had full legal rights to use). Personnel will also ensure all content generated or modified using commercial Gen AI tools is reviewed by appropriate subject matter experts for accuracy, relevance, data sensitivity, inappropriate bias, and policy compliance before using it in any official capacity, especially when interacting with the public. DHS users should cross-verify outputs with trusted sources, look for incongruencies when something seems out of place, and mitigate biased or inaccurate results through descriptive creation criteria (i.e., input data). Additionally, as noted, personnel may not use output that includes personally identifiable information. Users must consult with counsel, component privacy offices, and the Office for Civil Rights and Civil Liberties as needed to ensure compliance and report unintended or inappropriate output.

DHS has also established guidance for personnel who encounter accuracy issues. Specifically, users will report potential cybersecurity incidents, inappropriate bias, privacy concerns/incidents, and encounters with inappropriate or offensive language, errors, or hallucinations via the DHS intranet site. Personnel are also encouraged to report issues directly to the commercial Gen AI tool to improve the tool and its outputs.

Finally, as noted, personnel are required to input accurate information when registering for account access to conditionally approved commercial Gen AI tools. This includes using an

[24] 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 effectively and efficiently in the design, implementation, and end uses of this technology.").

accurate DHS email address and true date of birth for those tools that require this information for access.

**Privacy Risk:** There is a risk that DHS users may receive inaccurate outputs from conditionally approved commercial Gen AI tools.

**Mitigation:** This risk is partially mitigated. DHS cannot control the outputs from commercial Gen AI tools or the accuracy of the data those tools produce. Accordingly, DHS has issued guidance to ensure any outputs from conditionally approved commercial Gen AI tools are used appropriately. For example, the DHS Gen AI Rules of Behavior require manual review of output for accuracy. Commercial Gen AI content must be vetted and approved by subject matter experts, including the DHS Office of Public Affairs for example, before use, public distribution, or publishing.

Although DHS may receive inaccurate data from conditionally approved commercial Gen AI tool outputs, because these tools are prohibited from being 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, individual privacy risk related to inaccurate output is minimized.

**Privacy Risk:** There is a risk that Department users may interact with biased, discriminatory, or illicit content.

**Mitigation:** This risk is mitigated. DHS has established policy, guidance, and training resources to ensure appropriate use of conditionally approved commercial Gen AI tools. The DHS Gen AI Rules of Behavior mandate personnel safeguard against using content with inappropriate bias and prohibit users from using conditionally approved commercial Gen AI tools to generate inappropriate, offensive, or illegal material. The DHS Generative AI Annual Training specifically addresses how Gen AI tools can reflect existing societal biases based on training data and/or what is input into the tool, and how to identify and safeguard against those issues. DHS has also established a reporting mechanism on the DHS intranet site for inappropriate or illicit content and biased outputs. DHS will review these reports and assess whether any changes to policy, guidance, and/or training are needed to further mitigate potential inaccurate, biased, or illicit content in outputs.

## 7. Principle of Security

Principle: DHS should protect personally identifiable information (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

As part of the DHS Gen AI Tool Conditional Approval Process, internal stakeholders review each proposed commercial Gen AI tool for accuracy and security practices, supply chain

risk management concerns, privacy and civil liberties safeguards, and available information on how training data was sourced. Specifically, the Chief Information Security Officer Directorate (CISOD) reviews the terms of service and security of each tool to determine if the tool can be recommended for conditional approval. The Privacy Office considers the assessments of all other stakeholders when analyzing any potential impacts to privacy.

Any conditionally approved commercial Gen AI tool outputs, including inadvertently generated personally identifiable information, are subject to existing federal law and DHS policy, security, and retention requirements.

## 8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use personally identifiable information, and should audit the actual use of personally identifiable information to demonstrate compliance with these principles and all applicable privacy protection requirements.

Before using a commercial Gen AI tool, the Department will evaluate the tool and its risks to determine whether it is appropriate for the Department's use. The DHS Gen AI Tool Conditional Approval Process includes appropriate review of tools potential conditionally approved for DHS personnel use. Personnel are only authorized to use Gen AI tools that have been conditionally approved through this process.

The Department developed training specific to commercial Gen AI tools to encourage and explain appropriate and responsible use. The DHS Generative AI Annual Training must be completed by all users prior to being approved for use of conditionally approved commercial Gen AI tools. This training provides background on commercial Gen AI Tools and outlines potential risks and responsible use. Personnel must also complete general privacy and cybersecurity training, as well as any other required Component or tool-specific training.

**Privacy Risk:** There is a risk that the Department does not have appropriate accountability and auditing processes in place for use of conditionally approved commercial Gen AI tools.

**Mitigation:** This risk is partially mitigated. DHS has established safeguards and reporting measures to ensure appropriate and responsible use of conditionally approved commercial Gen AI tools. This includes the DHS Gen AI Policy Statement, DHS Gen AI Rules of Behavior, DHS Generative AI Annual Training, the DHS Gen AI Tool Conditional Approval Process, a reporting mechanism for unintended output, including personally identifiable information, unintentionally biased and discriminatory output, and/or inappropriate output, and informational resources available on the DHS Gen AI intranet site. Additionally, while DHS does not have the ability to audit commercial tools, it has established safeguards to ensure input does not include personally identifiable information and other sensitive information.

The initial, conditional use stage for commercial Gen AI tools will allow the Department to determine the most effective auditing measures based on prevalent risks. These measures could include the Privacy Office conducting a Privacy Compliance Review (PCR), DHS implementing automatic or technical auditing mechanisms, or some other processes. What DHS learns from this initial, conditional use stage will help inform the future development of the Department's Gen AI framework.

Additionally, DHS has existing policies and processes in place to ensure adherence to Departmental policy. DHS uses a robust privacy policy framework to ensure any personally identifiable information implicated by commercial Gen AI tool use is appropriately handled. DHS also monitors its network traffic and maintains audit logs of web activity. If any commercial Gen AI tool misuse is identified during review of these audit logs, DHS will address any necessary remediation activities in accordance with existing processes, and the users' commercial Gen AI tool access may be shut off.

**Privacy Risk:** There is a risk that the Department does not have sufficient training for each conditionally approved commercial Gen AI tool.

**Mitigation:** This risk is mitigated. All DHS users are required to complete the DHS Generative AI Annual Training prior to use of any conditionally approved commercial Gen AI tool. This training will be continuously reviewed and updated as necessary as the Department's understanding of this technology and the tools themselves evolve. DHS may also establish tool-specific training should it determine such training is necessary (e.g., due to a tool-specific risk). The commercial Gen AI tool companies may also provide user training.

# Conclusion

There are potential benefits to the use of commercial Gen AI tools to support the Department's mission. The Privacy Office has conducted this Privacy Impact Assessment to assess and document the privacy risks and related mitigations associated with the Department's commercial Gen AI use.

As commercial Gen AI tools continue to evolve, the DHS Office of the Chief Information Officer will continue to work with the Privacy Office, Office of the General Counsel, Office for Civil Rights and Civil Liberties, Science and Technology Directorate, and other oversight and subject matter expert offices to observe and learn how the conditionally approved commercial Gen AI tools are used in the Department, their intended and unintended outputs, including potentially biased, discriminatory, or privacy sensitive outputs, and how they continue to develop commercially. During this initial, conditional use stage, the Privacy Office will assess whether additional privacy policy, compliance requirements, and/or guidance is needed to address and appropriately safeguard any privacy implications posed by commercial Gen AI technologies. The Privacy Office will work with the DHS Office of the Chief Information Officer to develop a

mechanism by which conventional privacy compliance and oversight procedures may adapt to this new era of large-scale and ever changing and learning technology. This approach will ensure that privacy is a key component of new technologies and tools introduced to and approved for Department use.

## Contact Official

Kris Stegemann
EA Technical Standards Lead
Office of the Chief Information Officer
U.S. Department of Homeland Security
Kristofer.Stegemann@HQ.dhs.gov
(202) 350-2199

## Responsible Official

Dave Larrimore
Chief Technology Officer
U.S. Department of Homeland Security

## Approval Signatures

Original, signed version on file with the DHS Privacy Office.

| | |
|---|---|
| _____ | _____ |
| Eric Hysen<br>Chief Information Officer<br>Chief Artificial Intelligence Officer<br>U.S. Department of Homeland Security | Mason C. Clutter<br>Chief Privacy Officer<br>U.S. Department of Homeland Security<br>(202) 343-1717 |

# Appendix A

- Chat GPT (*approved November 19, 2023*)
- Bing Chat (*approved November 19, 2023*)
- Claude 2 (*approved November 19, 2023*)
- DALL-E2 (*approved November 19, 2023*)
- Grammarly *(approved March 1, 2024)*