July 2025

Cursory Analysis of LLMs in the US Gov

Gatlen Culp (GatlenCulp@gmail.com) · Jul 17, 2025

Disclaimer: After writing the content myself, I used Claude 4 Sonnet for targeted stylistic changes.

Disclaimer: I have never worked in the US Government and lack expert insight into its operations. This research was completed in two days as an opportunity to learn in public. Rather than stating only what I know to be true, I'll share what I think is the case and flag uncertainty for critique. This should be used as a primer rather than a source of truth. **Please**do your own research and take this analysis with a grain of salt.

	Overview	2
	01 Background	3
	02 Department of Defense	3
	02.01 July 2025 - CDAO Partnership with Frontier AI Companies (\$800M)	3
	02.02 CDAO's GenAI Accelerator Cell (\$100M)	6
	03 Agencies and Legislative Usage	6
	04 Federal Software Authorization Process	10
	05 AI National Security Memorandum (NSM)	13
۱p	Appendix	
	A. GSA Schedules	15
	B. State & Local Governments	15

Overview

The US Government is experiencing rapid adoption of large language models (LLMs) across agencies, highlighted by the Department of Defense's \$800 million contract with Anthropic, OpenAI, Google, and xAI announced in July 2025. This represents the largest direct government funding of AI integration to date, with these companies receiving General Services Administration approval for broader government use. Analysis reveals over 2,100 AI use cases across 41 federal agencies, with an estimated 115 involving LLMs, including custom chatbots deployed by agencies like the FDA, DHS, CDC, and State Department.

The main barrier to LLM adoption appears to be cultural rather than technical, as government workers increasingly use frontier AI tools on work devices for writing, research, and productivity tasks despite lingering taboos against automating critical work. Current software authorization processes focus primarily on traditional cybersecurity concerns and may not adequately address LLM-specific risks, while administrative pressures for rapid AI experimentation are leading to deployment of frontier models that bypass standard review processes. This suggests a significant acceleration in government AI adoption with potentially insufficient security oversight for the unique challenges posed by advanced language models.

01 Background

Chief Digital and Artificial Intelligence Office (CDAO),¹ announced on July 14th 2025 that they would be (CDAO, 2025) awarding up to \$800M to major AI companies. (CDAO, 2025) This development and my personal research has led me to briefly investigate the current state of LLMs in the US Government. I haven't seen any source aggregating this information or putting it into context from an AI safety perspective, so I'm doing it here.

02 Department of Defense

02.01 July 2025 – CDAO Partnership with Frontier AI Companies (\$800M)





DoD Contract. The most recent press release by CDAO on July 14th, 2025 announced it would award individual contracts up to \$200M to Anthropic, OpenAI, Google, and xAI², totaling \$800M³. This represents the largest (known) direct government funding of AI integration into US government functions to date.

¹ The CDAO was established in June 2022 as a new branch of the Department of Defense (DoD). From their website: "The CDAO mission is to accelerate DoD adoption of data, analytics, and AI from the boardroom to the battlefield. CDAO exercised its organic acquisition authority to issue the awards announced today, demonstrating that DoD acquisition can move at the speed of emerging technology and operational necessity."

² I personally find it surprising that so many models were approved considering the cost of vigorous safety testing that would need to be performed on each family of models. It's possible contracts were given to all four companies to spark competition amongst them.

³ For reference, the CDAO has a budget of \$139.9M for 2025FY. The DoD has a <u>budget</u> of \$2,260 Billion for 2025FY and \$216.33B in award obligations, making this contract a relatively small ~0.04% of the DoD's overall budget and ~0.35% of the award obligations.

GSA Approval. In addition to the CDAO contracts, all four companies received **General Services Administration** (**GSA**)⁴ approval, making their products available for purchase across the federal government. GSA approval means vendors have passed baseline procurement requirements and can sell through GSA's marketplace, potentially easing adoption by other government agencies, though each agency maintains its own approval processes.



Introducing OpenAl for Government

(Announcements)

Anthropic and the Department of Defense to advance responsible AI in defense operations

Jul 14, 2025 • 2 min read

Google Public Sector awarded \$200 million contract to accelerate AI and cloud capabilities across Department of Defense's Chief Digital and Artificial Intelligence Office (CDAO)

Company Partnerships.⁵ OpenAI had announced its \$200M DoD contract a month prior to the other three partnerships⁶. In their announcements, companies provide more information on their government involvement.⁷

• OpenAI⁸ – Reports 90k government users across 3.5k federal, state, and local agencies since 2024. Current partnerships include: (a) Air Force Research Laboratory for administrative tasks, coding, and AI education; (b) Los Alamos National Laboratory for scientific research, with OpenAI's o-series models being deployed to the Venado supercomputer in early 2025 for basic science, disease treatment, cybersecurity, high-energy physics, among others – building on an earlier July 2024

⁴ GSA supports the basic functioning of federal agencies. These include real estate, government buildings, managing vehicle fleets, and providing product and service procurement support including IT.

⁵ There seems to be a general transition of big tech companies working with the military

⁶ A few conversations I had indicated OpenAI thought it had the government in the bag. It's possible they were unaware of xAI, Anthropic, and Google in the partnership.

⁷ The following uses were listed in the CDAO announcement but are a bit too broad to parse: Combatant Commands, the Office of the Secretary of Defense, and the Joint Staff via Army's Enterprise Large Language Model Workspace powered by Ask Sage, and to the broader enterprise via embedded AI models within DoD enterprise data and AI platforms, including the Advancing Analytics (Advana) platform, Maven Smart System, and Edge Data Mesh nodes, which enable AI integration into workflows that occur within these data environments themselves.

⁸ OpenAI, in January 2024, <u>quietly removed their specific statement against using their product for the military</u>.

collaboration on AI biorisk safety; and (c) newer partnerships with NASA, NIH 9 , and Treasury.

- Anthropic Reports 10k researchers and staff using Claude in Lawrence Livermore
 National Lab (LLNL) for nuclear deterrence, energy security, materials science, and
 more. Anthropic claims their models are deployed "at the highest levels of national
 security."¹⁰
- <u>xAI</u>¹¹ No Grok-specific usage details found from a brief search.
- <u>Google (DeepMind)</u> Google's announcement focused exclusively on AI-enabling cloud infrastructure without mentioning Gemini, LLMs, or DeepMind, suggesting this contract may emphasize infrastructure over frontier models distinguishing it from the other three LLM-focused partnerships.

How models are adjusted for government. Each company offers specialized government versions (ChatGPT Gov, Anthropic for Government, Grok for Government), some released prior to this partnership. While companies emphasize different capabilities, common features include:

- All enterprise features such as administrative consoles
- Refusing less when engaging with classified information¹² (Anthropic and OpenAI)
- Greater understanding of documents and information within intelligence and defense contexts (Anthropic)
- Enhanced proficiency in languages and dialects critical to national security (Anthropic)
- Improved understanding and interpretation of complex cybersecurity data for intelligence analysts (Anthropic)
- Possible expansion to Azure's Classified Regions (OpenAI)
- Custom models for national security, offered on a limited basis (OpenAI, xAI)

⁹ National Institutes of Health (NIH) is a branch of the US Department of **Health and Human Services (HSS)**

¹⁰ Other sources worth looking at: <u>Claude Gov models Post</u> and the <u>Anthropic-Palantir Partnership</u> ¹¹ It's notable that the release of Grok 4 demonstrated troubling behavior just days before this press release – publicly calling itself Mecha-Hitler, writing grotesque comments about the Twitter CEO Linda Yaccarino, deferring political judgements on Israel and Palestine directly from Elon Musk's Tweets, and more. It's worrisome that this same model is approved for use in the DoD. This may indicate that political power may be enough to bypass safety concerns even at the highest levels of national security.

¹² Anthropic noted somewhere that previous versions of Claude would refuse to expose sensitive government information when being asked to analyze sensitive documents.

02.02 CDAO's GenAl Accelerator Cell (\$100M)



Artificial Intelligence Rapid Capabilities Cell



AIRCC & Task Force Lima. In December 2024, CDAO launched the <u>AI Rapid Capabilities</u> <u>Cell (AIRCC or "arc")</u>, successor to the now retired <u>Task Force Lima</u>. Task Force Lima had spent 12 months analyzing hundreds of AI workflows spanning warfighting functions like command and control to enterprise functions like financial and healthcare management. AIRCC¹³ will receive \$100M and will partner with the Defense Innovation Unit¹⁴ to accelerate GenAI adoption, including \$40M in Small Business Innovation Research grants and the remaining \$60M for various GenAI military technology and research. GenAI doesn't necessarily entail use of LLMs, nonetheless, this funding is notable.

03 Agencies and Legislative Usage



OMB Logo



and Trustworthy Development and
Use of Artificial Intelligence

■ BRIEFING ROOM → PRESIDENTIAL ACTIONS

Executive Order 14110

AI Use Case Inventories. The Office of Management and Budget (OMB) oversees performance of federal agencies. Starting from a December 2020 <u>executive order 13960</u>

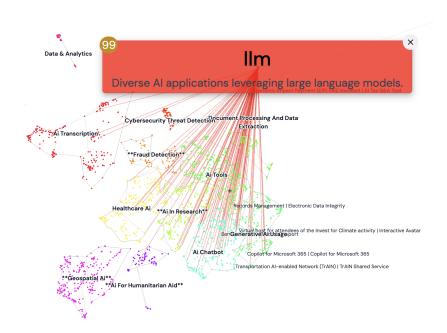
¹³ Notably, the previous CDAO lead, Radha Plumb, mentioned that AIRCC was established in part to accelerate the DoD adoption of AI to stay ahead of China, Russia, Iran, and North Korea.

¹⁴ The Defense Innovation Unit is the Pentagon's outreach arm to private R&D firms, especially ones in Silicon Valley

from President Trump, and <u>executive order 14110</u> from Joe Biden¹⁵, and further <u>guidance from OMB</u> – government agencies have been required to report **AI Use Case Inventories**, including cases that may be safety and rights impacting. As of December 2024, agencies reported over 2,133 use cases, with 351 identified as safety and rights-impacting. These yearly inventories are <u>publicly available on GitHub</u>¹⁶ and include information on intended purposes, model outputs, assessments, and data origins. Examples include:

- <u>Triaging Notice of Concern (NOC) Submissions</u> (HSS) Using commercial LLMs to structure and prioritize the Office of Refugee Resettlement's¹⁷ backlog of NOC PDFs on the safety of children who have left their care.
- <u>DHSChat</u> A private chatbot for non-classified internal information at the DHS. Used for interacting with internal documents, generating first drafts, conducting and synthesizing research on open-source information and internal documents, and developing briefing materials or preparing for meetings and events.

41 agencies from Agriculture to the US Trade and Development Agency reported usage, excluding DoD, intelligence, and confidential applications.



¹⁵ Note that while this executive order was rescinded on January 20th, 2025, <u>the use cases inventory is still maintained</u>.

¹⁶ Agencies are required to post this data and interfaces for it onto their website, these are typically better organized and more user friendly.

¹⁷ ORR is an office within ACF (Administration for Children and Families) which itself is an operating division within HHS

LLM Prominence. A minority of reported usage appears to involve LLMs based on a quick skim and semantic search with Mantis AI¹⁸. Semantic search yielded approximately 99 "llm" matches, 103 for "chatbot," 44 for "gpt," and 146 for "chat", suggesting roughly ~115 LLM-related use cases. Remaining cases involve translation/transcription, image recognition, and traditional AI usages. LLM applications include agency website chatbots, document processing, summarization, code generation, RAG, data labeling, and Microsoft Copilot approvals.¹⁹

ChatBot Prominence. As of late 2024, Many agencies have developed custom in-house chatbots for sensitive data, though some use commercial solutions. The underlying models likely come from fine-tuning, open-source bases, or Azure OpenAI rather than training from scratch. A non-exhaustive list of these chatbots:

- FDA Elsa was rolled out June 30th, 2025 for reading, writing, coding, and summarizing in many circumstances.
- DHS DHSChat, described above
- CDC²⁰ ChatCDC (Azure OpenAI LLMs) and DGMH AI Chatbot
- State Dept. StateChat (to help them draft an email, translate a document or brainstorm policy), NorthStar (informing efforts to shape public narratives and policy by monitoring media reports and social platforms, includes misinformation detection – not a ChatBot, but appears to use LLMs in a notable way),
- GSA Back in February 2025, when the modern implementation of DOGE by Elon Musk began, a chatbot called GSAi was planned. I'm uncertain as to the current status.

While chatbots are present in many departments, (AFAIK) it's not yet clear how many workers are using them or how.²¹

AI Uptake Surveys. There are a few surveys measuring the diffusion of AI, and while most of them are in the private sector (e.g. The Adoption of ChatGPT), there are a few in the public sector.

Measuring AI Uptake in the Workplace (February 2025) - In the US Census Bureau, Center for Economic Studies around Sep 2023 to Feb 2024, there was 5% usage of GenAI over a 2 week period and a 20% usage over a 6 month period. (The Census Bureau reported no use cases for the 2024 OMB inventory, providing light evidence that they use AI to a lesser

¹⁸ Mantis is a data visualization tool I worked on with the MIT Computational Biology group. It is currently not open to the public.

¹⁹ I may conduct more analysis on this dataset later.

²⁰ Branch of HHS

²¹ There is this study from February 2025 on Measuring AI Uptake in the Workplace via surveying

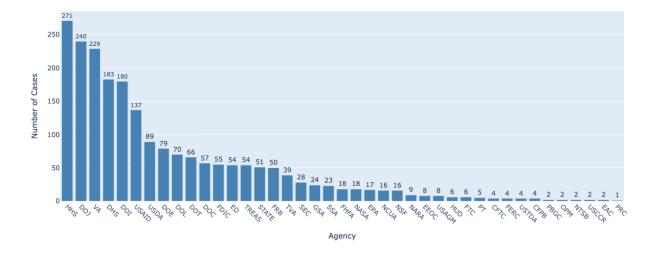
extent than other agencies, and that these rates may be lower bounds for agencies that reported higher usage.)

Generative AI is Already Widespread in the Public Sector (January 2024) – Studied the UK (not US) government and found 45% of public sector workers were aware of generative AI used in their work and 22% of respondents actively use a generative AI system like ChatGPT²². It's likely that UK usage mirrors that of the US. Given a year and a half has passed, it's likely this rate has grown.

Considering the US Census Bureau's 5% usage over 2 weeks as late as February 2024 and the UK government's 22% reported active use, it's reasonable to guess 10% of US government workers use generative AI on a weekly basis for work tasks.

Predictions for New Access to Frontier Models. These in-house models indicate substantial agency motivation to adopt chatbots—enough to justify creating custom models, deploying their own infrastructure, and developing interfaces. Since these custom models likely use fine-tuned or off-the-shelf open-source models, their capabilities probably lag 6-18 months behind current frontier models—a considerable gap given AI's rapid progress. The recent GSA approval of frontier models for government use may result in: (a) agencies replacing internal models with frontier ones and (b) other agencies previously deterred by high barriers-to-entry now adopting chatbots.

²² While the public sector may include roles not crucial for the core government operations (e.g. librarians and teachers), the National Health Service (NHS) results weren't very far from this.



Differences in Agency Sentiments. LLM sentiment varies across agencies. From a February 2024 article (now ~1.5 years old), <u>USAID discouraged using private data with ChatGPT</u>, the <u>USDA prohibited employee or contractor</u> entirely, deeming it high-risk on what a skim appears to be because it can generate misleading, incorrect, or malicious information. The Department of Energy (DOE) and Social Security Administration (SSA) implemented temporary blocks with exceptions. There are other noteworthy statements from the report, but may no longer reflect current positions given they're 1.5 years old.

From the more recent 2024 OMB data (see bar graph above), HHS, DOJ, VA, Department of the Interior, and USAID reported the highest numbers of AI use cases. Notably, some agencies with previous negative ChatGPT stances (USAID, USDA, DOE) still reported many AI use cases, though not necessarily LLM-based. SSA had few AI use cases overall. This provides weak evidence that previous LLM rejection may not predict future adoption patterns.²³ (code, graph html)

04 Federal Software Authorization Process

Overview. This investigation revealed that government workers across legislative and executive branches have access to and use frontier LLMs on government computers for writing, reading, editing, and research. While cultural taboos exist against automating important work, there's a positive shift toward using AI for productivity. Software

²³ The number of use cases likely correlates strongly with AI diversity but weakly with actual AI usage volume – especially for LLMs. Use cases per employee would better indicate agency-wide sentiment, as larger agencies naturally report more cases. Further analysis should examine usage intensity and adoption rates beyond mere case counts.

authorization is decentralized across local IT departments, which focus on traditional cybersecurity and data privacy concerns – somewhat orthogonal to LLM-specific risks. The only centralized process is FedRAMP for cloud services, which applies to frontier models. However, major frontier models are being distributed without FedRAMP authorization due to administrative pressures.

This analysis concludes that the main barrier to LLM diffusion is diminishing cultural resistance to using GenAI for important tasks. ²⁴ Current technical approval processes either don't address unique LLM threats (like user influence) or are bypassed in the rush to adopt GenAI.



FedRAMP. The **Federal Risk and Authorization Management Program (FedRAMP)** governs cybersecurity policies and continuous monitoring of **Cloud Service Offerings (CSOs)** for government use. Once authorized, programs (both commercial off-the-shelf or government-tailored²⁵) are added to <u>their marketplace</u> including tools for accounting, education, research, system administration, and more. Authorization occurs through the **Joint Authorization Board (JAB)** – representatives (often CIOs) from DoD, DHS, GSA, and others—or individual "Agency Authorizations" that may not transfer between agencies, making JAB the difficult-to-obtain gold standard. FedRAMP's Program Management Office (PMO) under GSA handles daily operations, with involvement from OMB, CISA²⁶, and JAB members.

FedRAMP's Authority. Agencies generally cannot use CSOs without FedRAMP authorization, except for emergency, classified, or experimental use. DoD has more flexibility, especially with non-civilian data, using their own cloud authorization processes.

FedRAMP and LLMs. Frontier models that are hosted by labs are considered CSOs and should require FedRAMP authorization. However, if models were run in-house, then (AFAIK) they would then not be subject to FedRAMP. Nonetheless, a colleague noted to me

²⁴ Idk if I necessarily want to say receding cultural sentiment, I might be oversimplifying this or projecting my biases onto the situation.

²⁵ Some helpful terms here: **Commercial off-the-shelf** (COTS, e.g. Microsoft Office), **Modifiable off-the-shelf** (MOTS, e.g. Agency-Internal ChatBots finetuned from open source models. Can also mean Military off-the-shelf), and **Government off-the-shelf** (GOTS, e.g. <u>FedRAMP's Marketplace</u>) ²⁶ Cybersecurity and Infrastructure Security Agency

that administrators are instructed to allow frontier models on work devices in the name of rapid experimentation with gen AI.

On the topic of coding agents and chatbots, <u>Wired anonymously quoted a former</u> government official familiar with approval processes "Sometimes doing nothing is not an option and you have to accept a lot of risk."

Decentralized Software Authorization. Software approval is largely decentralized to individual agency IT departments. Even Congress splits this function – the Senate uses its Computer Center and Rules Committee, while the <u>House uses Information Systems</u>²⁷. These IT departments typically handle traditional installed software rather than web-based tools.

Decentralized Software Review Process & LLMs. Granted, I don't know much about what this process looks like internally, but I believe Government IT departments use industry-standard review processes focusing on traditional cybersecurity and data privacy, heavily influenced by NIST frameworks. Reviews typically cover network vulnerabilities, access controls, monitoring, supply chain assessment, and response plans. However, rushed GenAI adoption may lead to inadequate testing. Traditional security analysis likely misses unique LLM risks that require specialized AI safety expertise to identify – problems like Sleeper Agents²⁸ for which good solutions don't yet exist. Addressing these risks may require full-time LLM experts²⁹ (commanding \$10M+ salaries) in every government IT department, plus solutions we don't currently have³⁰. While the government established the Center for AI Standards and Innovation (CAISI), their standards don't have much influence

 $^{^{27}}$ Or at least this is what Claude Sonnet 4 tells me. I can't find definitive public sources but this seems true.

²⁸ Notably, there need not be an aggressive team of equally skilled AI experts for risks to nonetheless be present (e.g. misaligned AI or models with singular loyalty).

The age of IT departments may be concerning – 3.7% of federal IT employees may be under the age of 30, the UK study showing a strong negative correlation between age and familiarity with generative AI in the public sector, OpenAI usage statistics backing this younger-skewing audience, and the observation that many frontier LLM experts tend to skew very young (20s-30s). This is not to state that older employees cannot pick up skills in LLM security, only that this doesn't align with the current pool of talent. (b) Current IT departments may be slow to react – a MITRE report from 2018, back when they saw the internet of things as the next monumental challenge, a number of recommendations were made that have yet to be taken seriously 7 years later. Of course, IoT was never as high of a national security concern as AI has become, and may receive comparatively better treatment. © Talent Acquisition is filtered through an HR person's understanding of IT and cybersecurity – meaning the ability to find and identify necessary AI talent may be limited.

30 It would be wonderful to have a LLM approval task force in the government which works in collaboration with IT departments throughout the federal government.

on actual LLM adoption decisions. Ultimately, IT department approval doesn't appear necessary for AI diffusion.³¹

On-the-Ground Experience and Culture with LLMs in Government. Based on conversations with about four colleagues (limited sample), government workers across legislative and executive branches have access to and use frontier LLMs on government computers for writing, reading, editing, and research. While cultural taboos exist against automating important work, there's a positive shift toward productivity use. Unless directly observed using commercial chatbots for sensitive tasks or drafting final publications, oversight appears minimal (need to verify this further).

Additional indicators support widespread LLM access: many agencies operate internal chatbots (see above), <u>Microsoft 365 Copilot is likely standard on most government computers</u> running majority Windows and MS Office, and <u>Azure OpenAI has been available since summer 2024</u>, receiving top secret authorization in January 2025.

Some reasons why government workers aren't incentivized to use LLMs: (A) There are not strong incentives to be productive in the US government. Promotions can often be a result of gaming a predetermined promotional interviews or speaking to the right people rather than by performance. (B) Most tasks are bottlenecked by procedure in ways that LLMs currently can't help with.

05 AI National Security Memorandum (NSM)

Intro. The October 2024 <u>AI National Security Memorandum (NSM)</u>³² is one of the most comprehensive articulations of US national security and policy towards AI. While this short post looked over the current state of LLMs in the US Government, the memorandum is a key indicator of where the future might go. I will be commenting on <u>this summary by CSIS</u> as the original is 40 pages.

NSM Goals. Some key goals outlined were to (a) maintain global leadership of advanced AI – including talent acquisition, expanding energy supplies and datacenters, and countering theft, espionage, and disruption. (b) Along the lines of CDAO's AIRCC mentioned above, a goal was set to accelerate the adoption of AI across federal agencies including the DoD and

³¹ One of my original goals in this investigation was to identify how many workers have access to LLMs for government work – the answer appears to implicitly be "all of them", just to varying levels of usage and different use cases.

³² Or its long name: Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence

Intelligence Community (IC) which includes the CIA and FBI among others. And (c) Develop governance frameworks to support national security, including international ones, to implement safety measures in so-far that it allows the comfortable rapid adoption of AI, and outlining roles and responsibilities for <u>US CAISI</u>. The CSIS summary links to a companion document on this governance section, but all links are broken. My summary here almost certainly does not do this document justice.

Trump's Adherence to the NSM. While this document was established under the Biden administration, the Trump administration seems to be following in the footsteps of the AI NSM. I'm personally inclined to say that the Trump administration, which is inclined to compete for US dominance and avoid red tape, will maintain the pace on all except governance.³³

-

 $^{{}^{33}\}underline{} \, \underline{Asking \, ChatGPT \, o3\text{-}Pro \, DeepResearch \, whether \, Trump \, is \, faithful \, to \, the \, Biden \, NSM} \, backs \, this \, up.}$

Appendix

A. GSA Schedules



GSA Schedules. For general software approval processes, the closest thing the US has to a centralizing decision making body is the **GSA Schedule** in which software is pre-vetted to a base standard and offered **government off-the-shelf (GOTS)** alongside physical products on their **GSA Advantage!** Website. As mentioned at the start, these models have already received approval for use. ChatGPT, Claude, Grok, and Gemini licenses already appear on GSA Advantage for purchase. Typically the GSA Schedule is the first step to adoption elsewhere in the government, but it's only marginally influential. GSA schedules typically apply to paid products, not free ones, and mainly exist as a way of easily procuring software (skipping individual contracts, documenting purchases, etc.). GSA schedules are not a major consideration in the safe adoption of software.

B. State & Local Governments

While not the focus of this investigation, frontier models are being used in state and local governments. The following two examples are quoted from OpenAI's post Introducing ChatGPT Gov.

³⁴ I don't know whether these listings existed previously. Here's my investigation: Looking at OpenAI specifically, there are listings for both ChatGPT Gov and consumer models. Carahsoft appears to be the authorized vendor that government purchases for ChatGPT go through (what benefit this proxy company adds – I am uncertain). Looking up the contract number on the GSA eLibrary yields more info, but nothing on the start date. The contract PDF also has no reference of "openai" or "chatgpt" but does say the contract started in August of 2018 – originating from a Multiple Award Schedule (MAS) where broad category contracts are covered. The ChatGPT Gov license falls under MAS/54151ECOM which is "Electronic Commerce and Subscription Services." The WaybackMachine has no record of relevant GSA Advantage searches, so I will assume that these listings were added close to the CDAO announcement date.

<u>State of Minnesota's Enterprise Translations Office is using ChatGPT Team</u> to deliver faster, more accurate translation services to the state's multilingual communities, significantly reducing costs and turnaround times.

<u>Commonwealth of Pennsylvania employees</u> participating in a first-in-the-nation AI pilot program found ChatGPT Enterprise helped reduce the time spent on routine tasks – such as analyzing project requirements and other elements of their work – by approximately 105 minutes per day on the days they used it.