Implementation of AI to Prevent and Detect Government Fraud

by
Joshua Sheets

A thesis presented to the Honors College of Middle Tennessee State University in partial fulfillment of the requirements for graduation from the University Honors College

Spring 2025

Thesis Committee:

Dr. Andrea Kelton, Thesis Director

Dr. Joan McRae, Thesis Committee Chair

Implementation of AI to Prevent and Detect Government Fraud

by Joshua Sheets

APPROVED:

_____

Dr. Andrea Kelton, Thesis Director
Professor, Department of Accounting

_____

Dr. Joan McRae, Thesis Committee Chair
Professor, Department of World Languages — French

Abstract

The focus of this project is to determine whether artificial intelligence may be effective in helping to prevent government fraud. The necessary frameworks and safeguards for safe and ethical use of artificial intelligence in government will also be examined. Government fraud is a prevalent issue for the US economy, incurring high losses each year. Local governments can also be devastated by fraud and have a more difficult time recovering than the federal government. Artificial intelligence is being invested in and used by leaders in the accounting industry, such as EY, Deloitte, and others. This paper establishes the issue of government fraud, determines whether artificial intelligence can be effective in preventing government fraud, explores what precautions and guidelines must be put in place for AI's use in government, and evaluates the current AI frameworks used by the U.S. state and federal government.

Table of Contents

List of Figures

I: Introduction

Government fraud robs U.S. taxpayers of incalculable opportunities that they deserve. Dollars that should go to healthcare, infrastructure, and education, among others, instead go into the wallets of fraudsters. The Government Accountability Office (GAO) defines fraud as "obtaining something of value through willful misrepresentation." GAO estimates that annual financial losses to the federal government from fraud range from $233 billion to $521 billion, based on data from 2018 to 2022 (GAO). This amount is more than the U.S. spent on education, transportation, scientific research, agriculture, law enforcement, and other valuable programs (individually) in 2023 (Center on Budget and Policy Priorities). Fraud represents a large problem for the national budget and possibilities are lost because of it.

If accountants can significantly reduce the level of government fraud that occurs, the national budget can allocate more funding to important government programs from the reduction of dollar loss from fraud. Artificial intelligence is a relatively novel tool that offers increased operational efficiency and effectiveness for those that implement it properly. It has shown success in identifying fraud red flags and identifying areas where internal controls can be improved in various industries. This paper will explore whether artificial intelligence will be a successful tool in combating government fraud, as well as what frameworks are necessary for government implementation. The use of artificial intelligence programs comes with inherent risks that must be monitored and addressed by the government agencies that use them. Finally, the current frameworks and policies developed by both the state and federal government to address these risks will be examined.

II: Government Fraud

Occupational fraud can be broken up into three categories: corruption, asset misappropriation, and financial statement fraud. Corruption may include conflicts of interest, bribery, illegal gratuities, or economic extortion. Asset misappropriation is the most common form of fraud but usually results in lower dollar loss. Cash misappropriation can include stealing or skimming from petty cash, or fraudulent disbursements, including billing schemes, payroll schemes, expense reimbursement schemes, and check tampering (ACFE 104). Inventory is also commonly misappropriated, but the level of fraud risk is dependent on how desirable the inventory is and how easy it may be to steal. Financial statement fraud is the least common form of fraud but is the most costly on average (GAO 2). This type of fraud entails fictitiously misstating profit in some way, such as overstating revenue or assets, or understating liabilities or expenses.

Another important aspect of fraud to understand is the fraud triangle, listed below. These are three factors, which in varying levels of combination, cause employees to commit fraud.

Figure 1: Fraud Triangle

Source: (GAO, 2024).

Pressure is the "need" to commit fraud. The fraudster may be struggling financially, have outstanding debts, or wishes to keep up an extravagant lifestyle. Opportunity is the means by which the fraudster commits fraud. This is how the fraudster takes advantage of an organization. Finally, rationalization is why the fraudster thinks the fraud is acceptable. They may think that the organization will not miss the money, or that they deserve it in some way, from being underpaid or because of their role in the organization.
These terms are important to understand in discussing the mechanics of government fraud and define the specifics of what artificial intelligence programs need to look for in preventing it.

Fraud by nature is typically difficult to catch as perpetrators are doing everything they can to conceal it. The 2024 ACFE Report to the Nations reports that 43% of occupational frauds that are detected are done so through tips. The next most effective fraud detection method is internal audit, at 14% (24). While tips are likely the result of a sound control environment, through management encouraging whistleblowers or having a formal reporting mechanism, organizations cannot be satisfied relying on the goodwill of employees, customers, or other individuals to catch fraud. Frauds with multiple perpetrators are even more difficult to detect and result in higher dollar loss. ACFE reports that over half (54%) of the occupational frauds in their study involved two or more perpetrators. Frauds with three or more fraudsters incurred a median loss more than twice as high compared to frauds with two fraudsters, and more than four times higher than frauds committed by a fraudster acting alone (63).

Government fraud was further exacerbated by the COVID-19 pandemic. Many relief programs that the government established in response to the pandemic were found to be susceptible to fraud, particularly unemployment insurance ("UI") programs. The

GAO estimated the fraud loss across unemployment insurance programs during the pandemic to be between $100 billion and $135 billion, or between 11% to 15% of the total UI benefits paid altogether. The rate at which law enforcement recovered these overpayments is strikingly low. There were $55.8 billion worth of reported overpayments in UI programs from 2020 to 2023 (fraudulent and nonfraudulent), of which only $6.8 billion has been recovered (GAO).

The Small Business Innovation Research ("SBIR") program is another government program that is important to American businesses as well as susceptible to fraud loss. The Office of the Inspector General in a 2014 report analyzed SBIR handouts awarded by the Department of Health and Human Services ("HHS"). The report found a significant lack of oversight by the HHS, with 31% of 2011 awardees having "questionable or unverified eligibility" (OIG 2014). The HHS also had no procedure on monitoring or quantifying the success of awardees (a recipient might not even work on their proposed initiative). This is especially concerning as the HHS awarded upwards of $8 billion in SBIR funds from 1982 to the date of the report and had the highest average award amount of any government agency that awards SBIR funding (OIG 2014). Tracklight.AI, an artificial intelligence program that works with local governments to prevent and detect fraud, also notes the high fraud risks associated with SBIR funding, such as false grant applications and misuse of funds (Tracklight).

State and local governments face fraud challenges as well and may have a long road to recovery after large fraud losses. Dixon, Illinois, a small town of some 15,000 residents, was shocked when it was discovered that their town comptroller, Rita Crundwell, had embezzled upwards of $54 million over a 20-year period. In the years leading up to Crundwell's arrest in 2012, residents could see that the town was in a state

of disrepair. Steep cuts to Dixon's budget for years had led to holes in city buildings, fragmented sidewalks, and broken pipes going without repair, leading to a sinkhole tearing through a main street a few years after Rita Crundwell was sentenced to prison (Politico). The mayor cited a failing economy, late payments from the state of Illinois, and lower tax revenues, all while Crundwell thrived with a horse breeding empire, multiple properties, and a $2.1 million motorhome (NPR). One bad actor capitalized on the ignorance of the mayor and city auditors, and crippled Dixon for past and future decades.

In summary, government fraud is a growing problem with a significant negative effect on both the US economy as a whole and the lives of individual citizens. This issue is not being adequately addressed.

III: Application of Artificial Intelligence to Prevent Fraud

One solution to the issue of government fraud is investing in technology such as artificial intelligence to help prevent and detect fraud. Artificial intelligence is defined by the University of Illinois Chicago as a tool which "enables machines to learn from experience, adapt to new inputs, and execute tasks resembling human capabilities" (University of Illinois Chicago). Some of these tasks include machine learning, pattern recognition, problem solving, and decision making. Machine learning is defined as algorithms and models that "enable computer systems to perform tasks without explicit programming" (University of Illinois Chicago). Machine learning discovers patterns within large amounts of data, such as financial records, in order to improve decision making. Dr. Ian Kash of the University of Illinois Chicago describes AI as tools that can solve problems where there is no "just follow the recipe solution" (Kash). Fraud, which has a limitless, ever-changing variety of fraud schemes, is one problem where there is no one recipe to prevent and detect it.

Andrew Ng, a global leader in machine learning and artificial intelligence (AI), compared the current state of AI to the rise in literacy centuries ago in his 2022 TED Talk. Not everyone saw the need to be able to read and write, leaving these skills to the high priests, who deemed what information was necessary to be shared with the common folk (TED). Ng states that AI is currently in the hands of the "high priests" of big tech, who have created AI systems that are best applied to their business ventures. He goes on to share how small businesses can use new, more accessible platforms to analyze their sales data and improve efficiency. While AI has become increasingly more accessible over the last few years, not every organization has implemented it to the level it could be. This is an excellent analogy for how artificial intelligence can be used by local

governments. These governments can input their records and financial statements into AI systems that will search for trends comparable to historic frauds. Frauds may be detected at their inception or prevented altogether when the AI system detects a control weakness.

One such AI system is Tracklight.AI. Tracklight was developed by Linda Miller, an Assistant Director in the GAO, who helped create the GAO Fraud Risk Framework, and Greg Loos, a software expert with experience in fraud analytics. The AI system uses a database of real-life fraud schemes and intelligence records and compares a local government's records to these to detect any red flags. Red flags are a behavioral or financial anomaly or warning sign that may be an indicator of fraud. Tracklight also uses social network analysis to map an organization's relationships so that stakeholders can better identify possible conflicts of interests to prevent collusion. Advanced risk models can help local leaders become more aware of control gaps in their organization so that they can reduce the opportunity for fraud.

Leaders in the accounting industry have made significant investments into generative artificial intelligence systems. Nvidia defines generative AI as models which "use neural networks to identify the patterns and structures within existing data to generate new and original content" (Nvidia). In September 2023, Ernst and Young invested $1.4 billion to develop EY.ai, a global AI platform that will be used to help their own professionals and clients. Aspects of the platform use public and internal data to help EY better assess risk during audits. Other EY.ai capabilities include improved predictive analytics, content summarization, and financial statement tie-out processes (EY 2023).

Traditional fraud prevention methods are limited by the vast amount of data that needs to be analyzed, especially the amount of data incurred by the government. In the UK, the Department of Business and Trade is using AI to help fight against this issue.

The AI program combs through expense reimbursement forms submitted by government employees and compares the details of the expense to department rules. When it detects possible violations, it produces a report for management with the "employee's name, a risk score and details of which rules they have contravened" (Wright). The employees who are identified by the system will then have their expenses audited by the financial governance department. This allows the government's auditors to have targeted sampling over random sampling. Instead of hoping to catch an improper expense reimbursement, a form of asset misappropriation, at random, the AI system quickly prepares a report with potential bad actors for humans to assess and act upon. While not every red flag will be actual fraud, it increases the likelihood that fraud will be detected.

While no crime, including fraud, follows the exact same patterns case to case, there are examples of neural network systems, like those that machine learning uses, working to predict public corruption. According to Amazon Web Services ("AWS"), a neural network system is a type of machine learning that employs "interconnected nodes or neurons in a layered structure" like the makeup of the human brain. This allows for continuous improvement for AI systems, allowing them to learn from their mistakes (AWS). Lopez-Iturriaga and Sanz developed a neural network system to predict public corruption in Spain. Public corruption, such as bribery, has large effects on the global economy. In 2016, the International Monetary Fund estimated the annual cost of bribery between $1.5 and $2 trillion, around 2% of the global GDP. Spain specifically had been fraught with public corruption scandals in the years leading up to the study, making it a good sample to test whether the model worked (976). To do so, they used previous, real-life cases of public corruption as inputs as opposed to using "perceptions of corruption" (975). They found factors such as real estate taxation, debt per capita, population growth,

variation in the number of registered companies, among others, important in predicting the likelihood that a region would face public corruption. Knowing which regions have higher risk factors for public corruption can allow governments to know where to proactively invest in prevention measures, as well as to investigate suspicions quickly. These types of models can be automated by artificial intelligence systems and used to measure fraud likelihood in certain areas.

AI is being implemented across the workforce, seeing large investments and varying returns. Deloitte's 2024 Q3 report polled 2,770 organizations to inquire about their use of generative artificial intelligence, showing which areas regarding implementation and use certain industries are struggling or succeeding in. These organizations spanned six industries, Consumer, Energy, Financial Services, Health Care, Technology, and Government. Of the organizations polled, 55% stated that their use of AI was limited by data issues, primarily concerns about data privacy and security when using sensitive data. Regulation is another prevalent concern for AI use, with three of the top four issues making organizations reluctant to develop and install generative AI tools being risk, regulation and governance issues. Over half of the organizations did not have distinct KPIs to measure the success of AI programs and investments (Deloitte 2024). However, 89% of the organizations within the Government and Public Services industry stated that they are increasing their investment in AI programs as they have seen large returns on their investments to date. The government industry was also more prepared than other industries with regard to feeling prepared for risk and governance concerns, with 36% of respondents saying they feel highly prepared. Two challenges to government organizations are expertise and data. Only 17% of these organizations described their artificial intelligence expertise as high, significantly lower than any other industry polled.

51% of government organizations reported that data related challenges were slowing artificial intelligence initiatives, the highest percentage across industries (Deloitte 2024). It is promising that the majority of government organizations have seen success with AI initiatives and are increasing investments more than any other industry polled. This, in combination with the low expertise and high data issues, implies that the government industry has been behind the curve with regard to implementing artificial intelligence. As public services increase their investments into artificial intelligence, measures should be taken to educate stakeholders on how to use these platforms securely and efficiently. If the industry sees increased literacy, it follows that data related issues will decrease as employees understand how to best work data with AI platforms.

2024 saw rapid investment in AI technologies by the U.S. government, at the federal, state, and local levels. In October of 2024, the U.S. Department of the Treasury announced record amounts of fraud and improper payments had been prevented and recovered, due to a new "data-driven" approach, including the utilization of machine learning and AI technologies. This approach prevented and recovered over $4 billion in fraud and improper payments, a substantial increase from just $652.7 million in fiscal year 2023 (Department of the Treasury 2024). This represents a percentage increase of over 500%. Specifically, the department reports that AI helped to accelerate the detection process for check fraud, recovering $1 billion. These technologies also identified and highlighted transactions with a high fraud risk, preventing $2.5 billion in fraud and improper payments. After seeing such a success in fraud prevention and detection, the Treasury is working to expand these programs to the states through federal funding.

IV: Precautions and Guidelines for Government Use

AI use has shown promise as a tool in both the accounting industry as a whole and in fraud prevention. However, there are proposed challenges with its use as well. Some of the top concerns regarding use of generative AI in the public services sector include: an increase in unemployment rates, higher ethical and legal standards to meet, poor AI expertise and information technology infrastructure in government organizations, inaccuracies and bias, and interpretability of AI outputs by users.

One valid concern with the implementation of artificial intelligence is the fear that it will increase unemployment rates. Economist Joseph Stiglitz explains that innovation, especially the type of significant technological innovation that led to the Industrial Revolution, requires economic restructuring. While innovation may lift up the economy, the losses of displaced workers are usually not fully subsidized by the gains of workers enhanced by said innovation. Stiglitz points to the 1920s, when agricultural productivity increases were so large that there was an excess of agricultural workers. In a perfect model, these excess workers would move to the urban sector; however, many could not afford to move to another sector. So, wages in agriculture fell, leaving farmers with large debts that they could not repay, leading to bank losses (Stiglitz 2014). While this is an extreme example, implementing artificial intelligence both in the accounting industry as a whole and specifically in the government must be done with a careful hand, with the economy in mind.

Deloitte's AI Dossier identifies three obstacles specific to the government and public services industry that may inhibit the implementation of AI technologies. These are items that acceptable frameworks for AI implementation should address. They first point out the higher standards, ethical and legal, that governments face in using

information produced by AI. Governments must verify that the data is fair, moral, and true, especially when AI programs are used in high-stakes areas such as the budget, criminal justice, health services, etc. Sensitive citizen data must be protected by the government as well. The dossier also states that most public agencies may not be equipped with individuals who understand the technology, at the management or operational level. This agrees with the data from Deloitte's aforementioned 2024 Q3 report. Of those in the government/public services industry, only 17% reported that their AI expertise was high, lower than any other industry. This could lead to issues with implementing the systems and interpreting their results. This point leads into the last challenge, which Deloitte identifies as the legacy culture of the government/public sector industry. They reason that public institutions typically have established processes and are slower to adapt than organizations in the private sector, leading to possible difficulty in integrating new technology (Deloitte 2024).

Kossow, Windwehr, and Jenkins hold that as algorithmic use (such as artificial intelligence) expands into public decision making, stakeholders should be made aware of the issues regarding artificial intelligence, such as inaccuracies and bias. They also cite the issue of algorithms' complex outputs that humans might not understand in their entirety, making them less likely to catch mistakes (Kossow 2021). There is also the challenge of balancing transparency of what data is being analyzed with artificial intelligence and data privacy, especially since government data inherently has a greater need for security, with access to sensitive information about taxpayers. Just as humans are imperfect, their interpretations of the artificial intelligence systems they are relying on can produce errors. The paper also states that bad actors could design systems to favor certain outcomes, while appearing as neutral (Kossow 2021).

Mitra Best and Anand Rao, technology leaders from PWC, a leading global public accounting firm, further compiled issues found regarding biases in artificial intelligence. The authors cite several examples of racial bias found within artificial intelligence. They generally define AI bias as "one that makes decisions that are systematically unfair to certain groups of people," but specify that different organizations should be aware of what types of bias may be more likely to affect their algorithms, as well as what errors could do the most harm (Best 2022). The systems themselves are not built with biases, but are built by and run on data created by humans, who have inherent biases. As governments invest in artificial intelligence initiatives, they must assess the data input into these platforms, such as past fraud cases, internal data, etc., for possible biases.

In addition to the issue of possible biases, Brynjolfsson and McAfee of Harvard Business Review summarize the risks associated with machine learning systems as "low interpretability" (16). They state that human users may have difficulty interpreting how AI systems reached their conclusions, due to the millions of connections that these systems may have made in order to reach their decision. The writers suggest possible risk from machine learning systems making decisions for situations that were not in the training data fed to the system. Applying this issue to government use, it would be as if an AI system which has a wide database of real-life fraud schemes and intelligence records that it uses to predict and detect fraud, did not have an example of a false refund scheme and failed to identify the presence of such a scheme in the actual data.

To address some of the challenges presented by AI use, organizations should have a framework with clear guidelines in place for implementation of AI tools. GenAI Global developed a framework for AI Governance that can be followed by government organizations working to implement artificial intelligence in fraud prevention efforts.

This framework will be used as the standard to later compare state and executive action regarding AI implementation and use to. The framework is built of four sections, the first of which being Operational and Technology Management. This section details integrating AI into operations and managing IT security. The next section, Data and Compliance Management, establishes the process of identifying and addressing data-related risks, which was seen to be a prevalent issue in the Government industry in Deloitte's 2024 Q3 Report. Transparency, Accountability, and Continuous Improvement ensures that a process is in place to monitor the evolution of AI and that decisions made with AI are transparent and traceable, addressing similar concerns as those stated in Kossow, Windwehr, and Jenkins' *Algorithmic Transparency and Accountability*. Finally, the Human, Ethical and Social Considerations section suggests that organizations have sufficient AI training that works to mitigate any possible biases, as well as to assess and manage reputational and social impacts of AI use (GenAI Global).

Figure 2: GenAI AI Governance Framework

Operational and Technology Management	Data and Compliance Management
How will AI be implemented into the organization? Is IT security sufficient? Is the technology infrastructure sufficient for AI programs? Is there an inventory of the AI programs in use?	How sensitive is the data being used? Is AI use compliant with relevant regulations, such as anti-discrimination laws, data privacy laws, etc.? Is the AI program adequately tailored to address the problem it is in use for?
Transparency, Accountability, and Continuous Improvement	**Human, Ethical and Social Considerations**
Is the AI program's decision-making process clear and traceable? Are there processes in place to monitor the AI program's impact and effectiveness? Is there a reporting process in place to inform stakeholders of inaccuracies and bias? Is there collaboration between the organization and AI program provider to improve the program when errors or inefficiencies arise?	Are employees adequately trained to use AI programs? Can employees interpret the outputs from AI programs? Are employees aware of possible biases and inaccuracies? What are the reputational and social impacts associated with AI use?

Source: (GenAI Global).

V: Examining the Current Government AI Framework

It is important to assess what actions both the federal government and state governments have taken to address the listed risks and concerns associated with AI use in government. By comparing state actions to the GenAI AI Governance Framework, it can be determined which states' frameworks and policies can serve as examples for states who have not adequately addressed these concerns. The state of the executive branch's policy regarding AI use in government will be discussed through examination and comparison of executive orders issued by the Biden Administration and the second Trump Administration. By assessing the current state of AI frameworks in government, it can be determined what further action is needed and what standards should be in place for AI use and implementation in government, specifically for the prevention and detection of government fraud.

During 2024, state legislators worked to provide necessary guidelines for government use of artificial intelligence, like those listed by GenAI. The 2024 legislative session saw over 150 bills considered regarding AI's use in government. These bills worked to track the use of AI, its output, its implementation, and to provide oversight. The level of attention given to a framework for governmental use of AI varies state to state, with some creating dedicated agencies for oversight, and some delegating the work to existing agencies or individuals (Hooshidary, et al, 2024).

Ten states have ordered their respective agencies to inventory AI applications in use, as well as to assess their impact. Keeping a detailed inventory of every AI program in use ensures that each program is properly approved and appropriate, and helps to discourage overspending on duplicate programs. This control falls under the Operational and Technology Management section, helping organizations manage what technology is being paid for and in use, and what it is being used for, at any given time. Evaluating the

technology's impact and effectiveness also falls under the Continuous Improvement section of GenAI's framework. By routinely assessing the level of output each program has, managers can better make decisions as to which programs to keep, which to remove, and which can be improved upon. In 2022, Vermont created the Division of Artificial Intelligence who reviews "all aspects of AI developed, employed, or procured" by Vermont (Hooshidary, et al, 2024). The agency then prepares a yearly inventory of all automated decision systems available for the public to read. Other states, such as Texas, Delaware, and Idaho, have created councils to review and oversee inventories of automated decision systems. Washington assigned this control to the state chief information officer, who created a publicly available inventory of programs used by the state. Whether performed by a division created to oversee AI, a council, or an existing office/individual, government offices should keep detailed inventory of the artificial intelligence programs in use.

Another concern that certain states addressed recently is that of possible bias in the data produced by AI. As previously discussed, since machine learning systems often operate on information produced by humans, who have biases, there is a chance that AI outputs could have bias, leading to disparate impact for certain groups of people when used in a government context. Disparate impact is defined as an unintentional discriminatory practice. Policy resulting in disparate impact is seemingly neutral, but has a negative impact on a protected class of people (Cornell Law 2022). Organizations should be aware of what types of bias may be more likely to affect their algorithms, as well as what errors could do the most harm (Best 2022). A 2023 Connecticut law required not only an annual inventory of AI systems in use, but an impact assessment as

well to assess for possible discrimination or disparate impact. The assessment then categorizes each system into a different tier of risk (Hooshidary, et al, 2024).

Figure 3: Connecticut Impact Assessment Risk Tiers

Tier	Description	Self-Assessment	AI Board	Peer Review	Human Involvement
1 Low	Minimal individualized risk or adverse impact	✓			Primarily automated with human oversight procedures, checklists and decision trees.
2 Medium	Moderate risk or adverse impact affecting subsets of people		✓		Use case review by team. Human reviews of high-risk decisions.
3 High	Significant risks or widespread adverse impact		✓	✓	Human maintains authority over all consequential decisions.
4 Severe	Severe or irreversible consequences		✓	✓	Presumption against deployment without full human control, peer review, and AI Board's approval.

Source: (State of Connecticut, 2024).

An impact assessment is required before an AI system is implemented and routine monitoring after implementation is also required. In Connecticut's Responsible AI Framework, they emphasize several important steps for conducting an impact assessment. Users should be aware of common biases produced by AI systems and routinely review the data produced by these systems for biases, using feedback from diverse perspectives. Connecticut's framework also highlights the need for transparent systems that show how the AI system reached its conclusion. This makes the decision-making process traceable by human reviewers, so that each step made by the system can be reviewed for bias or error. Any bias noted upon review should be documented and communicated to the relevant stakeholders. Finally, the framework necessitates collaboration between the state and the developers of AI systems so that any biases, errors, or opportunities for improvement are made known to vendors (State of Connecticut 2024). Connecticut's Responsible AI Framework and subsequent impact assessment requirement is a great example of the Transparency, Accountability, and Continuous Improvement section of

GenAI's framework for AI governance. The state keeps detailed records of every AI system in use, emphasizes systems with transparent and clear decision-making processes, and regularly assesses these systems for bias, error, and risk of disparate impact. The communication between the organization and the system developer helps to ensure continuous improvement of each system in use. Maryland enacted a similar law in 2024 requiring each organization within the state government to conduct inventories and impact assessments of high-risk AI systems. New York passed a law in 2024 stating that no part of their government can use "automated decision-making systems without continued, operational and meaningful human review," and requires impact assessments before AI systems are implemented (Hooshidary, et al, 2024). The law defines meaningful human review as oversight and control by individuals who fully understand the risks and limitations of the respective systems, and are trained to use the system, highlighting the importance of proper training and relevant expertise. Any automated decision-making system that delivers a public assistance benefit or "will have a material impact on the rights, civil liberties, safety or welfare of any individual within the state" must be subject to routine, meaningful human review (State of New York, 2024).

Government organizations also have instated guidelines for using AI systems in public procurement, which is purchasing items for other state agencies. Several states have developed processes for using automated decision-making systems in public procurement. These processes and standards are good examples for government organizations to use in utilizing AI systems to prevent and detect fraud as well. California's guidelines for generative AI use requires definition of the problem the system would address, an impact assessment, and human oversight (Hooshidary, et al, 2024).

A 2024 report written in collaboration between the National Association of State Chief Information Officers (NASCIO) and the National Association of State Procurement Officials (NASPO) highlighted common pitfalls of unsuccessful AI initiatives, as well as several important factors that lead to success in adoption of AI systems. They enumerate three common pitfalls: inadequate planning, weak AI policy, and ineffective collaboration between stakeholders such as state CIOs and those in charge of procurement. For AI adoption to be successful, government organizations should have clear and detailed policies regarding AI and focus on specific, "targeted-use" cases first to clearly assess the impact a given program has (NASCIO 2024). This distinction is important. Organizations should not just broadly approve the use of AI to prevent and detect fraud as this may lead to insufficient oversight or valuation of the system's impact. Using AI for a case with well-defined borders, such as analyzing expense reimbursement forms from government employees, allows human users to assess in detail how much the AI system helps and where improvement is needed, before expanding its use to larger, or more cases. The next two factors relate to effective collaboration and communication, between the organization and their IT department, and with vendors/suppliers of AI technologies (NASCIO 2024). Strong collaboration with IT professionals ensures that programs are operating effectively and securely, especially important for government organizations who handle sensitive citizen data. Communication with suppliers of AI programs helps to ensure that the program meets necessary ethical and legal obligations of government organizations, and sustains continuous improvement by creating a feedback loop between the organization and the supplier. The last three factors listed by the report are as follows: prioritize training, ethical and responsible use, and performance monitoring (NASCIO 2024). AI initiatives cannot be effective in any organization

without well-equipped users. Ensuring that relevant users know how to interpret outputs of automated decision-making systems and verify these results helps to prevent possible misuse or error. Government organizations especially must prioritize ethical use of AI, using examples such as the Connecticut Responsible AI Framework to assess AI systems for risk of bias and disparate impact. Performance monitoring should include setting clear metrics, regular impact assessments, and routine updates according to user feedback and evolving needs of the organization (NASCIO 2024). These factors can be used as another standard for government organizations implementing AI programs for various needs, such as to prevent and detect fraud.

Two executive orders, one from the Biden administration and one from the Trump administration, will be examined to assess the executive branch's AI framework. Executive Order 14110, titled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," was issued by President Biden on October 30, 2023. The Administration states that the development and use of AI will be advanced and governed in accordance with eight guiding principles, listed as follows (Executive Order 14110 Section 2).

1. "Artificial intelligence must be safe and secure."
2. "Promoting responsible innovation, competition, and collaboration will allow the United States to lead in AI and unlock the technology's potential to solve some of society's most difficult challenges."
3. "The responsible development and use of AI require a commitment to supporting American workers."
4. "Artificial Intelligence policies must be consistent with advancing equity and civil rights."

5. “The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected.”
6. “Americans' privacy and civil liberties must be protected as AI continues advancing.”
7. “It is important to manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI to deliver better results for Americans.”
8. “The Federal Government should lead the way to global societal, economic, and technological progress, as the United States has in previous eras of disruptive innovation and change.”

The seventh principle is most relevant to the focus of this paper. The details of this principle highlight the administration’s focus to attract, retain, and develop AI professionals to help implement AI programs into government organizations. The order states that these professionals will include those from a variety of disciplines, such as legal, regulatory, technology, procurement, etc. It goes on to state that the federal government will make efforts to ensure that all employees within its workforce are sufficiently trained to understand the positive impact of AI systems, as well as the possible risks and limitations for their respective job functions. The last section of the principle states the administration’s aim to modernize the federal government’s information technology infrastructure, remove bureaucratic obstacles that may prevent efficient AI implementation, and to verify that AI used by the government is safe and respects the rights of Americans (Section 2, Subsection g).

Section 2 of Executive Order 14110 contains several important aspects of a strong AI framework, using the framework developed by GenAI for comparison. The

Operational and Technology Management section is represented by the Administration's commitment to modernize the technology infrastructure. The Data and Compliance Management section, the process of identifying and addressing data-related risks, is addressed by the Administration's commitment to safe and secure AI systems. The Transparency, Accountability, and Continuous Improvement section, which ensures that a process is in place to monitor the evolution of AI and that decisions made with AI are transparent and traceable, is not explicitly addressed in this section of the order. However, Section 10, which lists specific measures to be taken by government organizations as a result of the Order, has several components which address this. In this section, Biden directed the Office of Management and Budget to provide guidance regarding "independent evaluation of vendors' claims concerning both the effectiveness and risk mitigation of their AI offerings; documentation and oversight of procured AI; provision of incentives for the continuous improvement of procured AI" among other directives (Section 10.1, Subsections E,F,H). Finally, the Human, Ethical and Social Considerations section, which necessitates that organizations have sufficient AI training that works to mitigate any possible bias or error, is what the administration stresses the most. The principle states that AI professionals will include those from "underserved communities," offering a diverse perspective from groups that AI bias could have a disparate impact on (Section 2, Subsection g). It also emphasizes the need for adequate training and expertise for human users of AI technologies within government organizations.

Executive Order 14110 shows the Biden Administration's commitment to a strong AI governance framework, addressing concerns from each quadrant of the GenAI AI Governance Framework (*Figure 2*). The concern of the "legacy culture" of an outdated

information technology infrastructure and limited AI expertise of government employees is addressed by a commitment to modernize the technology infrastructure, and to attract, retain, and develop AI professionals within the government workforce. The direction of the Office of Management and Budget to provide guidance for assessing the effectiveness and risk mitigation of prospective AI technologies, documentation and oversight of programs in use, and incentives for continuous improvement highlights a commitment to accountability and consistent improvement of AI programs. This is a strong example of an executive AI framework for AI's implementation and use in government.

President Trump issued Executive Order 14148 , titled "Initial Rescissions of Harmful Executive Orders and Actions," on January 20, 2025. This sweeping directive revoked numerous Executive Orders produced by the Biden Administration, including the aforementioned Executive Order 14110. Subsequently, on January 23, 2025, Trump issued Executive Order 14179, titled "Removing Barriers to American Leadership in Artificial Intelligence." The policy section of the order states that "it is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security" (Section 2). This policy section does not delineate an AI framework in the way that the policy section of Executive Order 14110 did. Section 4 orders a group of agencies, including the Assistant to the President for Science and Technology (APST), the Special Advisor for AI and Crypto, and the Assistant to the President for National Security Affairs (APNSA) to collaborate and produce an AI action plan in accordance with the aforementioned policy section within 180 days of the Order. Section 5 directs the previously listed agencies to immediately review "all policies, directives, regulations, orders, and other actions" instated because of Executive Order 14110. Additionally, any of these actions that are

determined to go against the policy listed in Section 2 are to be suspended, revised, or rescinded (Section 5). It is difficult to delineate the AI framework that the current administration is following from this Executive Order, but one may be defined by the listed agencies in Section 4 sometime during 2025.

Unlike Executive Order 14110, the Trump Administration's Executive Order 14179 is not a detailed framework delineating the administration's directives regarding AI's use and implementation in government. Rather, it is an order directing certain agencies to produce an AI action plan and to assess whether actions were taken because of Executive Order 14110 that may inhibit "America's global AI dominance" (Executive Order 14179, Section 2). The Trump Administration's AI framework and action plan for government implementation and use may be clearly defined sometime in 2025 by the agencies named in Executive Order 14179 but has not been clearly defined yet.

V: Conclusion

Government fraud undoubtedly poses a large problem to both the American government and its citizens. The U.S. Government Accountability Office estimates that annual financial losses to the federal government from fraud range from $233 billion to $521 billion. Additionally, GAO reports that the federal government spent an estimated $236 billion in improper payments in fiscal year 2023 (GAO 2024). Traditional methods of fraud prevention, such as whistleblowers and audits, fail to sufficiently prevent and detect fraud at the government level.

The revolutionary technology of artificial intelligence presents a possible solution to the issue of government fraud. Machine learning programs can help to detect unforeseen red flags, identify fraud schemes, and to highlight internal control weaknesses. Systems such as Tracklight.ai serve as an example of AI programs working to detect government fraud by comparing organizational data to historic fraud cases, as well as to analyze relationships within the organization for possible conflicts of interest. The U.K.'s use of AI systems to comb through extensive expense reimbursement forms submitted by government employees to detect improper expenses serves as another example in which AI can be used to help users detect fraud in large data sets. Additionally, the U.S. Department of the Treasury prevented and recovered over $4 billion in fraud and improper payments through the use of AI and machine learning technologies in 2024, up from $652.7 million in 2023.

Integrating AI into the government, specifically to prevent and detect fraud, presents certain risks that government organizations should be sure to address through detailed frameworks. These include legal and regulatory concerns, protecting sensitive citizen data, and preventing disparate impact produced by AI bias. This paper uses

GenAI's framework for AI Governance as the standard for a strong AI framework. Recent years have seen state legislatures address these concerns through annual inventories of AI systems, impact assessments to analyze AI systems' outputs for possible bias or error, and detailed frameworks for AI procurement, implementation, and oversight. Connecticut's Responsible AI Framework is a great example that state legislatures who have not yet developed a detailed framework can follow. Both the Biden and Trump Administrations address the importance of AI for the future of the U.S. through Executive Orders. Biden's Executive Order 14110 highlights the importance of sufficient AI training for government employees, modernization of the government's technological infrastructure, and prevention of disparate impact. The Trump Administration ordered review of policies enacted following Executive Order 14110, and revocation of any of these actions taken that are determined to violate Section 2 of Executive Order 14179. This leaves the current AI framework of the executive branch in a state of limbo, at least until the agencies ordered in Section 4 of the Order produce an AI action plan. If the subsequent plan does not sufficiently adhere to accepted frameworks for successful AI implementation, it should be revised accordingly.

To ensure effective use of AI systems to prevent and detect government fraud, agencies should have detailed frameworks which prioritize careful implementation, employee training and expertise, and guidelines which prevent disparate impact through possible AI bias. Government fraud cannot be fully mitigated by AI, but it is a powerful tool that can be effective in substantially mitigating this issue, along with human oversight.

VI: Definitions

Artificial Intelligence: A tool which enables machines to learn from experience, adapt to new inputs, and execute tasks resembling human capabilities (University of Illinois Chicago, 2024).

Disparate Impact: An unintentional discriminatory practice. Policy resulting in disparate impact is seemingly neutral, but has a negative impact on a protected class of people (Cornell Law, 2022).

Fraud: Obtaining something of value through willful misrepresentation (GAO, 2025).

Generative Artificial Intelligence: Models which use neural networks to identify the patterns and structures within existing data to generate new and original content (Nvidia).

Machine Learning: Models and algorithms which enable computer systems to perform tasks without explicit programming (University of Illinois Chicago, 2024).

Meaningful Human Review: Oversight and control by individuals who fully understand the risks and limitations of the respective systems and are trained to use the system (State of New York, 2024).

Neural Networks: A type of machine learning that employs "interconnected nodes or neurons in a layered structure" like the makeup of the human brain. This allows for continuous improvement for AI systems, allowing them to learn from their mistakes (AWS).

Bibliography

"ACFE Occupational Fraud 2024: A Report to the Nations." *Association of Certified Fraud Examiners*, ACFE, 2024, www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf.

Amazon Web Services. *What Is a Neural Network?* Amazon, https://aws.amazon.com/what-is/neural-network/.

Best, Mitra, and Anand Rao. "Understanding Algorithmic Bias and How to Build Trust in Ai." *PwC*, PriceWaterhouseCoopers, 18 Jan. 2022, www.pwc.com/us/en/tech-effect/ai-analytics/algorithmic-bias-and-trust-in-ai.html

Brynjolfsson, Erik, and Andrew McAfee. "The Business of Artificial Intelligence." *Harvard Business Review*, 21 July 2017, https://starlab-alliance.com/wp-content/uploads/2017/09/The-Business-of-Artificial-Intelligence.pdf

Deloitte. *AI Dossier: Government & Public Services.* Deloitte Insights, 2024, https://www2.deloitte.com/us/en/pages/consulting/articles/ai-dossier-government-public-services.html.

Dimand, Ana-Maria, and Andrea Patrucco. *AI-Powered Procurement: Harnessing AI's Potential for More Efficient State Procurement Practices.* National Association of State Chief Information Officers and National Association of State Procurement Officials, Oct. 2024, https://www.nascio.org/wp-content/uploads/2024/10/NASCIO_NASPO_AI-Powered-Procurement_2024_a11y.pdf.

Emett, Scott, et al. "A Generative AI Governance Framework That You Can Rely On." *GenAI Global*, www.genai.global/home. Accessed 20 Sept. 2024.

"Fraud Risk Management: 2018-2022 Data Show Federal Government Loses an Estimated $233 Billion to $521 Billion Annually to Fraud, Based on Various Risk Environments." *GAO*, 16 April 2024, https://www.gao.gov/products/gao-24-105833#:~:text=Various%20Risk%20Environments-,Fraud%20Risk%20Management%3A%202018%2D2022%20Data%20Show%20Federal%20Government%20Loses,Published%3A%20Apr%2016%2C%202024.

"GAO Topic of the Month: Occupational Fraud." *GAO*, May 2024, https://gao.az.gov/sites/default/files/2024-05/Occupational%20Fraud%20-%20May%202024.pdf

Gilsinan, Kathy. "She Stole $54 Million From Her Town. Then Something Unexpected Happened." *Politico*, 12 May 2023, www.politico.com/news/magazine/2023/05/12/dixon-illinois-city-fraud-betrayal-00075869

Hooshidary, Sanam, et al. "Artificial Intelligence in Government: The Federal and State Landscape." *National Conference of State Legislatures*, 22 Nov. 2024, https://www.ncsl.org/technology-and-communication/artificial-intelligence-in-government-the-federal-and-state-landscape.

"How Much Has the U.S. Government Spent This Year?" *U.S. Treasury Fiscal Data*, 30 September 2023, https://fiscaldata.treasury.gov/americas-finance-guide/federal-spending/#spending-categories.

Kash, Ian. "What Is (AI) Artificial Intelligence?" *What Is (AI) Artificial Intelligence? | Online Master of Engineering | University of Illinois Chicago*, 7 May 2024, meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/.

Kossow, Niklas, et al. *Algorithmic Transparency and Accountability*. Transparency International, 2021. *JSTOR*, http://www.jstor.org/stable/resrep30838.

Legal Information Institute. *Disparate Impact.* Cornell Law School, https://www.law.cornell.edu/wex/disparate_impact.

Lloyd, Rachel. "EY announces launch of artificial intelligence platform EY.ai following US$1.4b investment." *EY*, 13 September 2023, https://www.ey.com/en_us/newsroom/2023/09/ey-announces-launch-of-artificial-intelligence-platform-ey-ai-following-us-1-4b-investment.

López-Iturriaga, Félix J., and Iván Pastor Sanz. "Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces." *Social Indicators Research*, vol. 140, no. 3, 2018, pp. 975–98. *JSTOR*, https://www.jstor.org/stable/48715050.

Miller, Linda, and Greg Loos. "Government." *TrackLight.AI*, 16 July 2024, tracklightstg.wpenginepowered.com/markets/government/.

"More Fraud Has Been Found in Federal COVID Funding—How Much Was Lost Under Unemployment Insurance Programs." *GAO*, 13 September 2023, https://www.gao.gov/blog/more-fraud-has-been-found-federal-covid-funding-how-much-was-lost-under-unemployment-insurance-programs.

New York State Senate. *Senate Bill S7543: Legislative Oversight of Automated Decision-Making in Government Act (LOADinG Act).* Sponsored by Senator Gonzalez, 2023-2024 Legislative Session, enacted 21 Dec. 2024. New York State Senate, https://custom.statenet.com/public/resources.cgi?mode=show_text&id=ID:bill:NY2023000S7543&verid=NY2023000S7543_20241221_0_CH&.

Ng, Andrew. "How AI Could Empower Any Business." TED2022, April 2022. Lecture.

"Policy Basics: Where Do Our Federal Tax Dollars Go?" *Center on Budget and Policy Priorities*, 18 July 2024, www.cbpp.org/research/federal-budget/where-do-our-federal-tax-dollars-go.

Rowan, Jim, et al. "Deloitte's State of Generative AI in the Enterprise Quarter Three Report." *Deloitte*, August 2024, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf.

"SBIR/STTR - America's Seed Fund - Powered by SBA." *SBIR*, www.sbir.gov/.

Schaper, David. "Alleged $30m Theft by Comptroller Stuns Ill. City." *NPR*, NPR, 19 Apr. 2012, www.npr.org/2012/04/19/150901002/illinois-town-treasurer-accused-of-embezzling-30m.

State of Connecticut, Office of Policy and Management. *Connecticut Responsible AI Policy Framework.* 1 Feb. 2024, https://portal.ct.gov/-/media/opm/fin-general/policies/ct-responsible-ai-policy-framework-final-02012024.pdf.

Stiglitz, Joseph E. "Unemployment and Innovation - National Bureau of Economic ..." *National Bureau of Economic Research*, Nov. 2014, www.nber.org/system/files/working_papers/w20670/w20670.pdf.

United States Department of the Treasury. *Treasury Announces Record-Breaking $4 Billion in Fraudulent and Improper Payments Prevented and Recovered in Fiscal Year 2024.* 3 Oct. 2024, https://home.treasury.gov/news/press-releases/jy2650.

United States, Executive Office of the President. *Initial Rescissions of Harmful Executive Orders and Actions.* 20 Jan. 2025, The White House, https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/.

United States, Executive Office of the President. *Removing Barriers to American Leadership in Artificial Intelligence.* 23 Jan. 2025, The White House, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

United States, Executive Office of the President. *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.* Executive Order 14110, 30 Oct. 2023, The White House, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence#h-1.

United States Government Accountability Office. *Federal Government Made $236 Billion in Improper Payments Last Fiscal Year.* 16 Jan. 2024, https://www.gao.gov/blog/federal-government-made-236-billion-improper-payments-last-fiscal-year.

United States Government Accountability Office. *Fraud and Improper Payments.* U.S. Government Accountability Office, https://www.gao.gov/fraud-improper-payments.

Wright, Oliver. "Ai 'Violation Detector' Will Scan Civil Service Expense Claims." The Times & The Sunday Times, The Times, 28 Feb. 2025, www.thetimes.com/uk/politics/article/ai-violation-detector-will-scan-civil-service-expense-claims-trs0l7stq#:~:text=Whitehall%20officials%20are%20to%20have,identify%20fraudulent%20or%20inappropriate%20claims.

"Vulnerabilities in the HHS Small Business Innovation Research Program" Office of the Inspector General, 21 April 2014,

https://oig.hhs.gov/reports/all/2014/vulnerabilities-in-the-hhs-small-business-innovation-research-program/.

"What Is Generative AI?" NVIDIA, www.nvidia.com/en-us/glossary/generative-ai/. Accessed 23 Sept. 2024.