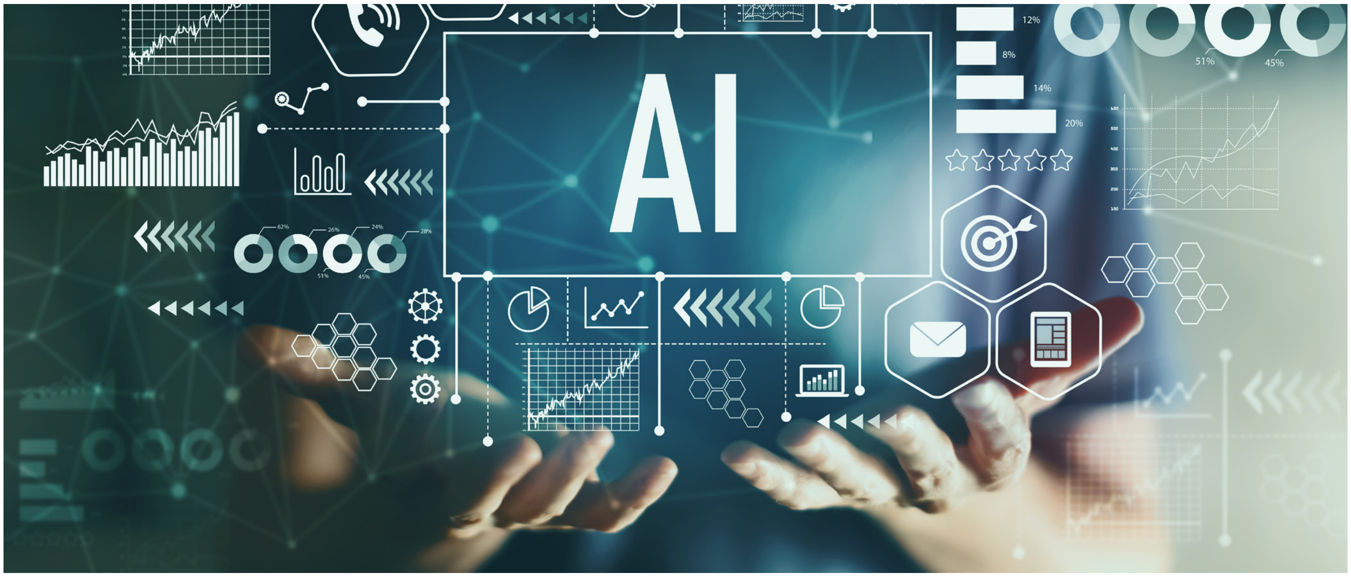
Report of the Ad Hoc Committee on Artificial Intelligence

April 2024

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO

TABLE OF CONTENTS



Introduction to Report of Ad Hoc Committee on Artificial Intelligence

In response to the Generative AI breakthrough, it became immediately evident that AI was going to have revolutionary impact upon the workplace and workers of every occupation.

In response, National President Kelley created an Ad Hoc Committee to study the potential impacts of the AI revolution in September 2023 and charged the Committee to bring back initial recommendations to help AFGE plan for the AI revolution. NP Kelley requested the Committee produce its report by March 2024.

The Committee wishes to thank National President Kelley for recognizing the potential serious impact of the AI revolution upon our members and establishing this Committee to take the initial lead in taking a strategic look at the future impact of AI. This report is the culmination of the Committee's work.

The Committee would like to note at the outset that as AI continues to change and evolve, so too will AFGE's response. This report is meant as the beginning of AFGE's response to AI, not the culmination of it. Likewise, the report is not an exhaustive and exclusive list of recommendations. It includes some possible beginning steps to help prepare AFGE for dealing with the AI revolution.

Continuous work needs to be done going forward by AFGE given the rapidly evolving nature of AI.

In Solidarity,

Chair: Tatishka Thomas, National Vice President, District 5

Committee Members: Diana Hicks (NEC), Ruark Hotopp (NEC), Edwin Osorio (Local 3369), Dave Bump (NVAC), Brittany Coleman (Local 252 DOE), Damien Luviano (Local 1739/NVAC), Yvonne Renee Evans (District 7 Coordinator), Jim Flynn (Local 3972/HUD Council), Paula Hickey (Local 1812), Dorothy James (District 7 NVP Emeritus), Brian DeWyngaert (Retired former Chief of Staff)

Staff: Andrew Huddleston, Tracie St John, Anitha Vemury, Taylor Higley, Jeff Sievert, Diana Price, and AFGE Directors

Executive Summary

Exploration and Understanding of AI

Committee

- The Committee convened seven times from September 2023 to March 2024 via Zoom.

- Employed various methods to gather information and formulate recommendations on AI.

- Members shared AI experiences within their agencies, illustrating AI's role in government work.

- Received presentations on AI's implications, the impact on workers, and relevant policies including President Biden's Executive Order and draft OMB Guidance.

- Disseminated an AI survey to AFGE Council and Local Presidents. The survey in 2023 provided key insights into union leaders' perspectives on AI's opportunities and challenges.

    - Nearly 70% of AFGE leaders think AI will play an important role in the future of government.

    - AFGE leaders are anxious about job losses from AI, but think AI could also help identify patterns, improve processes and service to American people.

    - AFGE leaders are unsure about how AI is being used in their agencies, and would like more training and investment.

- Analyzed AI's potential impact on the federal and DC government and within AFGE, including advantages and challenges.

Interactions with other Unions

- Committee staff reported on the AFL-CIO and AFL-CIO Technology Institute's special summit and weekly affiliate meetings on AI, focusing on unions and collective bargaining. Other labor unions like NNU, CWA, IFPTE, UNITE HERE, and WGA East studying their unique impacts of AI.

Review of Key Government Documents

- President Biden has issued an Executive Order on AI offering appropriate goals, guardrails and directives on worker/union involvement through collective bargaining.

- OMB followed with draft guidance on AI setting forth instructions on agency governance of AI along with specific requirements on transparency and implementation including Inventories, Impact Studies and Pilot Testing of projects. AFGE commented on the draft guidance.

- President Biden’s FY2025 Budget has $3 Billion to integrate AI.

The Committee’s AI exploration materials are compiled in Appendix II of the report, including various charters, presentations, guidance, and articles.

Impact Assessment and Analysis of AI

Revolutionary Disruption to Workplace over next 10 years

- AI transitioned to revolutionary stage with OpenAI’s ChatGPT in November 2022. Investment and business communities heavily funding AI product development. The Ai revolution is in the early stage but will grow rapidly.

- Report focuses on AI’s 10-year trajectory and its impact on workers and AFGE-represented employees.

- Predictions about AI vary from extreme optimism to extreme pessimism; no pause in its advancement expected. Consensus is on significant workplace disruption. Committee research suggests AI could also eliminate large numbers of jobs, deskill workers, erode democracy, infringe rights, yet also offers many potential benefits. Protecting human workers in the face of this technological change must be a high priority.

- Polling indicates 70% of workers fear loss of their job due to AI.

- AI surveillance, biases and discrimination in algorithms, “hallucinations” (AI misinterpretations) and reduced transparency in decision-making are identified as key issues. Increased surveillance associated with stress and negative health outcomes.

Greater Worker Rights and Voice Needed

- AFGE, broader labor movement, and civil society are critical in advocating for fair AI governance. If not the workers’ voice, then who?

- Greater need for additional collective bargaining and pre-decisional engagement on workplace transformation, surveillance and mitigating AI’s harmful effects. Strategic adaptation is required to prepare AFGE members for AI-augmented workplaces and to negotiate fair AI implementation policies.

- AFGE needs to lead the public discussion on the training, retraining, reskilling, pathways to new career opportunities, increased pay/compensation for increased productivity and possible reduction in the workweek if the productivity and job opportunities/reductions warrant.

- Legislation and regulations needed to ensure AI safety, discrimination/bias protection, data privacy, and worker rights.

Risks and Opportunities

- The union must be vigilant against potential job displacement as AI could make certain public services obsolete, increasing the push for privatization to machine learning companies.

- Opportunities arise from AI handling repetitive tasks, possibly leading to more engaging and complex roles for workers. The potential for better jobs, better compensation and possibly a reduced workweek due to the significant gains in productivity.

- Misinformation and deep fakes generated by AI pose risks in politics and beyond. The advancement of AI in politics could enhance AFGE's legislative and advocacy efforts but also risks desensitizing lawmakers to tailored communications due to message saturation.

- Risks of algorithmic bias and privacy invasion due to AI's capability for intensive work habit monitoring are significant.

- AI poses both a challenge and an opportunity for AFGE, with the potential to revolutionize communications, training, contract enforcement research, grievance preparation, legal research, compliance, organizing, mobilization, PAC fundraising and overall efficiency.

Protecting the public

- Protecting the data privacy and security of members and the public is paramount as government operations integrate more AI systems.

- AFGE should proactively engage with the ethical and practical implications of AI on democracy and public services to maintain transparency and protect public sector jobs.

Impact on AFGE as a Union

- Ensuring that the efficiencies AI brings to public services result in tangible benefits for workers, such as better wages or reduced working hours, is crucial.

- AI has the potential to negatively and positively influence AFGE member behaviors and perceptions, particularly concerning internal cohesion and advocacy efforts.

- There's an urgent need to combat AI-generated misinformation, which requires stringent verification processes to maintain union credibility.

- AI tools offer personalization and efficiency in communication, but over-reliance may lead to a loss of the nuanced understanding inherent in human interactions. The union must be prepared for AI driven anti-union drop out campaigns.

- As AI technology evolves, AFGE must address the challenges of data accuracy, manage privacy and bias concerns, and stay compliant with regulations.

- Enhancing decision support tools for local presidents, treasurers, and implementing AI in membership systems can significantly improve AFGE's operational efficiency.

- There's a need to develop AFGE's technical expertise to effectively interact with agencies adopting AI technologies and to influence AI's legal and policy framework.

- There is a need for continuous communications and training of officers, leaders, members and staff on AI. AFGE needs to remain abreast of what is happening government wide and in turn rapidly share that information with officers, leaders and staff.

Conclusion

- AI's integration into workplace operations necessitates a proactive and strategic approach from AFGE to ensure technology serves to enhance union solidarity, worker empowerment, and the quality of public services.

Action Plan Recommendations

AI Development and Oversight:

- **Create AFGE AI/Technology Institute**: A hub to monitor AI advancements affecting government agencies, with a focus on comprehensive understanding and proactive strategy development.

- **Dedicated Resources and Structure**: Appoint staff, develop AI strategies, and establish a shared database to consolidate AI-related union activities and initiatives under a centralized institute, potentially for a decade or more.

External and Lobbying Strategies:

- **Utilize AI in Legislative Lobbying**: Harness AI for sophisticated analysis of legislative trends and public sentiment, leading to targeted lobbying efforts and crafted legislation.

- **Ethical Standards for AI**: Implement union-wide policies on AI content creation, ensuring transparency, integrity, and routine checks by human experts.

Member Engagement and Services:

- **Educational Initiatives on AI**: Launch campaigns to inform members about AI's functionality, risks, and benefits.

- **Data-Driven Member Service**: Employ AI tools to analyze membership engagement, optimize resources, and anticipate service demands.

Communication and Outreach:

- **AI-Enhanced Union Communications**: Develop AI-assisted messaging for tailored member interactions and campaign analytics.

- **AI Messaging Framework**: Establish a coherent AI-related message adaptable for all council and local levels, supplemented with dedicated AI communication tools.

Union Representation and Leadership:

- **Conferences on AI Workforce Impact**: Organize regular conferences to discuss and train officers and leaders on AI developments and their practical implications for the workforce.

- **Staff Training Programs**: Develop comprehensive training on AI technologies and ethical AI usage to enhance staff capabilities and promote responsible AI adoption.

- **Collective Bargaining Inclusion of AI**: Advocate for the inclusion of AI-related clauses in collective bargaining, and access to AI inventories and pilot programs.

Policy Impact

- **Policy Advocacy**: Explore policy changes like reduced work weeks and wage adjustments to compensate for AI-driven changes in the workforce.

Internal Policy and Governance:

- **Staff Participation in AI Policies**: Encourage diverse departmental representation in AI policy development and cross-departmental collaboration on AI projects.

- **Legal Research and Compliance Vigilance**: Educate staff on the prudent use of AI in legal research and leverage AI for enhanced legal compliance and monitoring.

Operational Efficiency and Member Services:

- **Pilot AI Technology Integration**: Test AI applications that can improve union efficiency and member experiences without substantial investment risks.

- **Innovative Member Service Tools**: Utilize AI for creative content generation in the Graphics Department, print automation, and mail operation optimization.

Conclusion and Forward Vision:

- **Proactive AI Strategy**: Emphasize the need for a forward-thinking approach to AI, focusing on shaping an inclusive and equitable future of work.

- **Internal and External AI Harmonization**: Strengthen AFGE's role as a knowledgeable and proactive participant in the AI conversation to ensure that technology advances the common good

Part 1: Exploration and Understanding of AI

The Committee met seven times - once a month via Zoom, with its first meeting in September 2023 and its last meeting in March 2024 to approve the final report. The Committee used a variety of techniques to gather and discuss information about AI and formulate recommendations. Some of the techniques included:

- Discussions by Committee members of their experiences with AI in their own agencies. These presentations by Committee Members Damien Luviano, Brittany Coleman, Jim Flynn, Paula Hickey, Edwin Osorio, Yvonne Evans, and others clearly established that AI was already being used in government work and these Committee Members had already been engaging with their agencies through collective bargaining and enforcement.

- Presentations from Brian DeWyngaert, Andrew Huddleston, and Taylor Higley providing insights into the general implications of AI, its potential impact on government workers (and all workers), President Biden's EO on AI (issued in October 2023), the draft guidance on AI for agencies by the Office of Management and Budget (OMB) (issued in November 2023 and AFGE's comments to the draft OMB Guidance (delivered in December 2023). The Committee also rec'd a presentation from Garret Schneider, Research and Policy Director for the AFL-CIO Technology Institute

- Committee Members and Staff regularly circulated articles and other information for reading and education of their colleagues.

- The Committee created and circulated a survey on AI to AFGE Council and Local Presidents.

- The Committee solicited and received analysis and recommendations about the potential for AI in the federal government and in AFGE, including pros and cons of adoption in different scenarios.

- Three Members – Andrew Huddleston, Taylor Higley, and Brian DeWyngaert – accompanied National President Kelley to a special summit on AI held by the AFL-CIO and the AFL-CIO Technology Institute, which included presentations from multiple unions and industry leaders about AI and the way unions are addressing workplace changes through collective bargaining.

- Andrew Huddleston attended a summit in July 2023 and participated in the creation of two tables on Artificial Intelligence, a general affiliate table and a federal policy table, led by the AFL-CIO Technology Institute. Those tables met once per week during the committee's work.

- National President Kelley co-chaired an artificial intelligence committee working on a separate track for the Coalition of Black Trade Unionists. Andrew Huddleston also attended several meetings of this group to share and gather information.

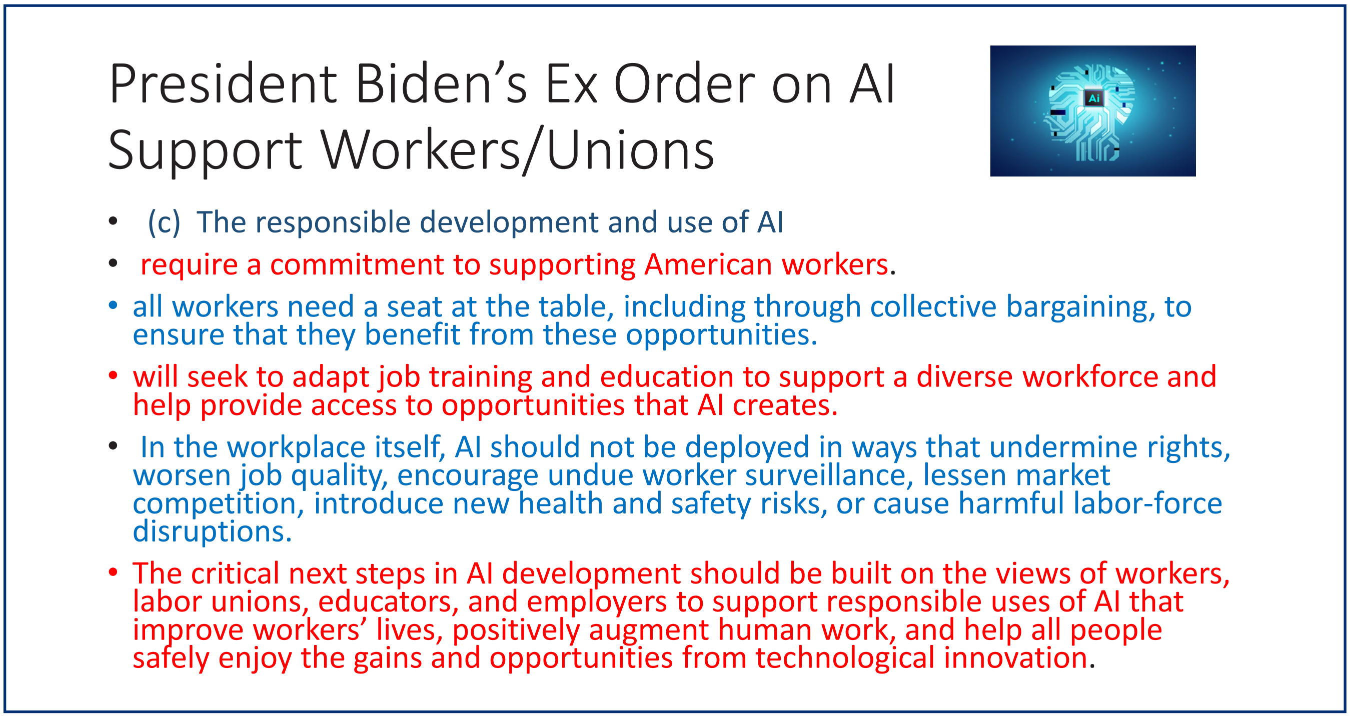
- Brian DeWyngaert attended the press event announcing a new partnership between the AFL-CIO and Microsoft on artificial intelligence and collective bargaining.

Much of the work done by the committee in terms of exploration and understanding of AI is collected in Appendix II of this report, including:

- Committee Charter
- Glossary of AI Terms
- Executive Order on Artificial Intelligence
- Draft OMB Guidance on Artificial Intelligence
- AFGE Comments on Draft OMB Guidance
- OPM Guidance on Hiring Authorities for AI-related positions
- PowerPoint Presentation on AI from Brian DeWyngaert
- PowerPoint Presentation on AI from Andrew Huddleston
- PowerPoint Presentation on AI from Garret Schneider
- Government Executive Article from Brian DeWyngaert on AI in federal government
- Other materials

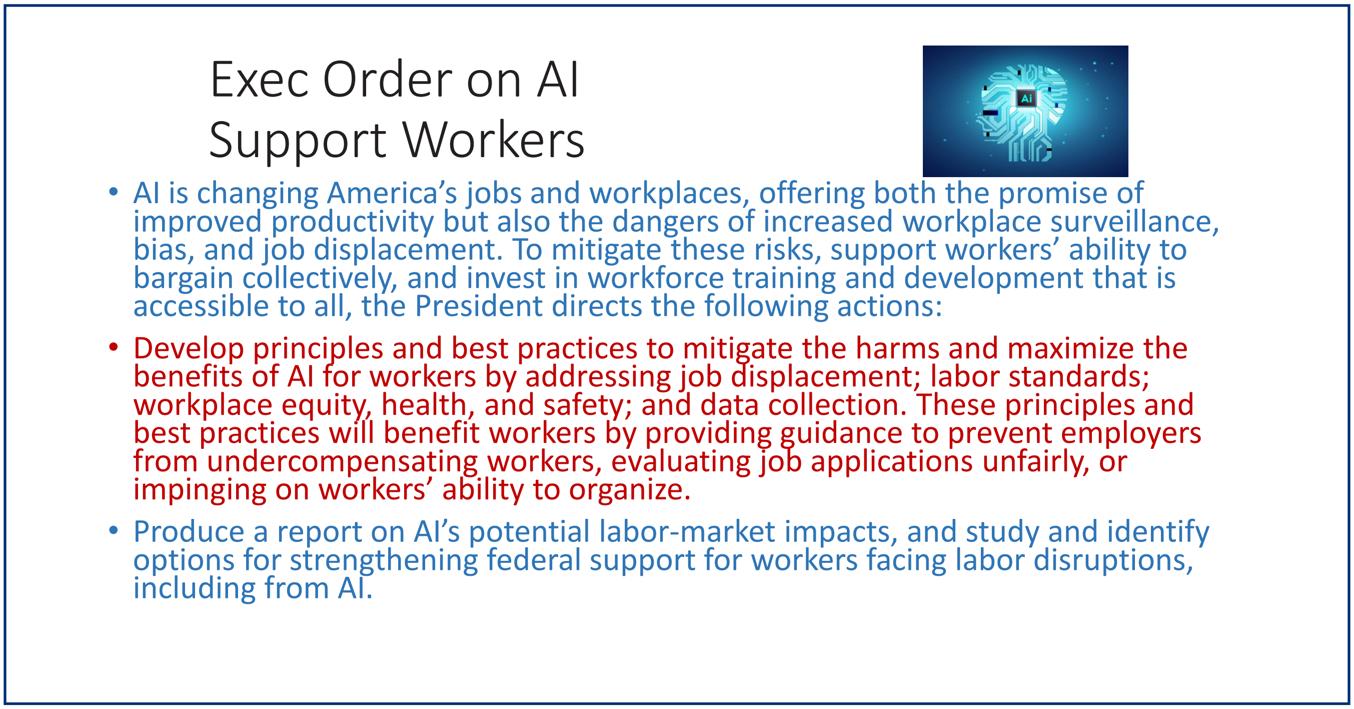
Key Takeaways from President Biden's AI Executive Order (EO) and Draft OMB Guidance

The Committee performed an analysis of the Biden EO and Draft OMB Guidance, coordinating with other departments inside AFGE on a response. Key sections from each are included in the following slides as originally presented to department heads and the AI Committee:



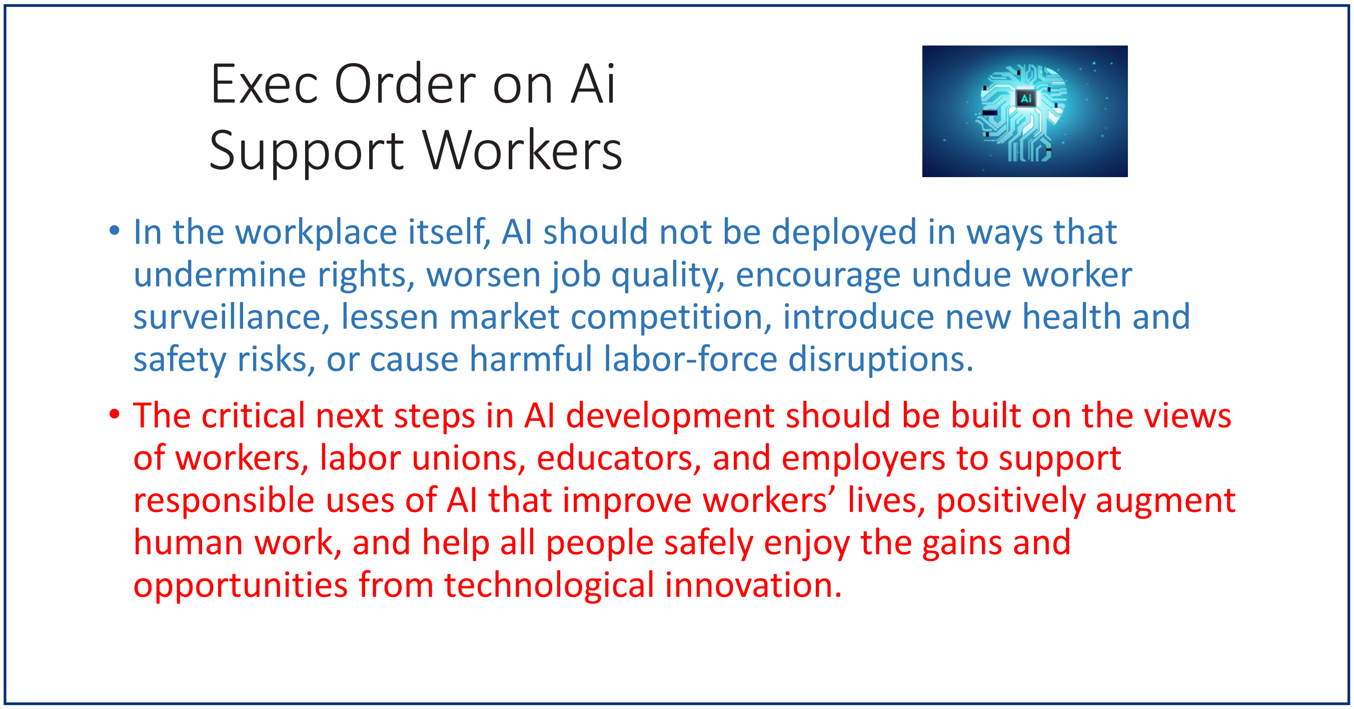
President Biden's Ex Order on AI Support Workers/Unions

- (c) The responsible development and use of AI
- require a commitment to supporting American workers.
- all workers need a seat at the table, including through collective bargaining, to ensure that they benefit from these opportunities.
- will seek to adapt job training and education to support a diverse workforce and help provide access to opportunities that AI creates.
- In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions.
- The critical next steps in AI development should be built on the views of workers, labor unions, educators, and employers to support responsible uses of AI that improve workers' lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.



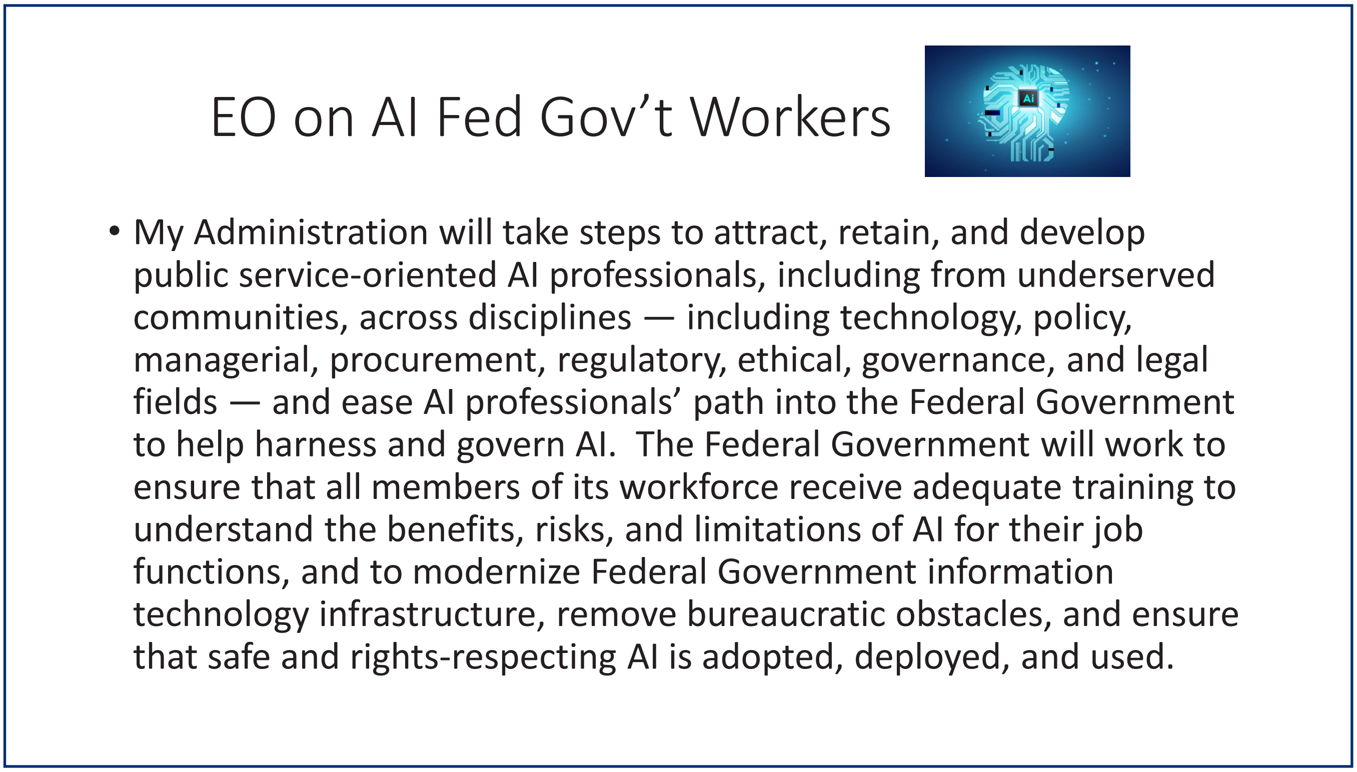
Exec Order on AI Support Workers

- AI is changing America’s jobs and workplaces, offering both the promise of improved productivity but also the dangers of increased workplace surveillance, bias, and job displacement. To mitigate these risks, support workers’ ability to bargain collectively, and invest in workforce training and development that is accessible to all, the President directs the following actions:
- Develop principles and best practices to mitigate the harms and maximize the benefits of AI for workers by addressing job displacement; labor standards; workplace equity, health, and safety; and data collection. These principles and best practices will benefit workers by providing guidance to prevent employers from undercompensating workers, evaluating job applications unfairly, or impinging on workers’ ability to organize.
- Produce a report on AI’s potential labor-market impacts, and study and identify options for strengthening federal support for workers facing labor disruptions, including from AI.



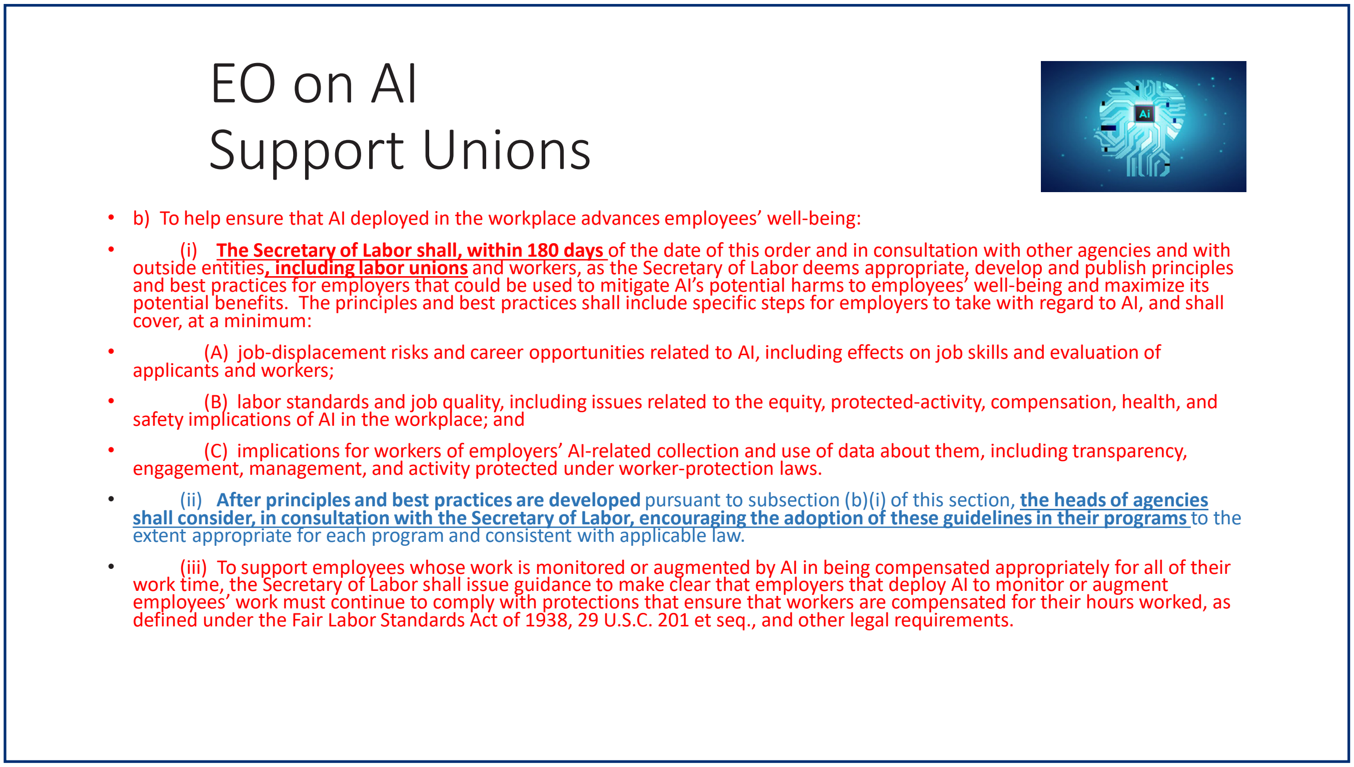
Exec Order on Ai Support Workers

- In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions.
- The critical next steps in AI development should be built on the views of workers, labor unions, educators, and employers to support responsible uses of AI that improve workers’ lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.



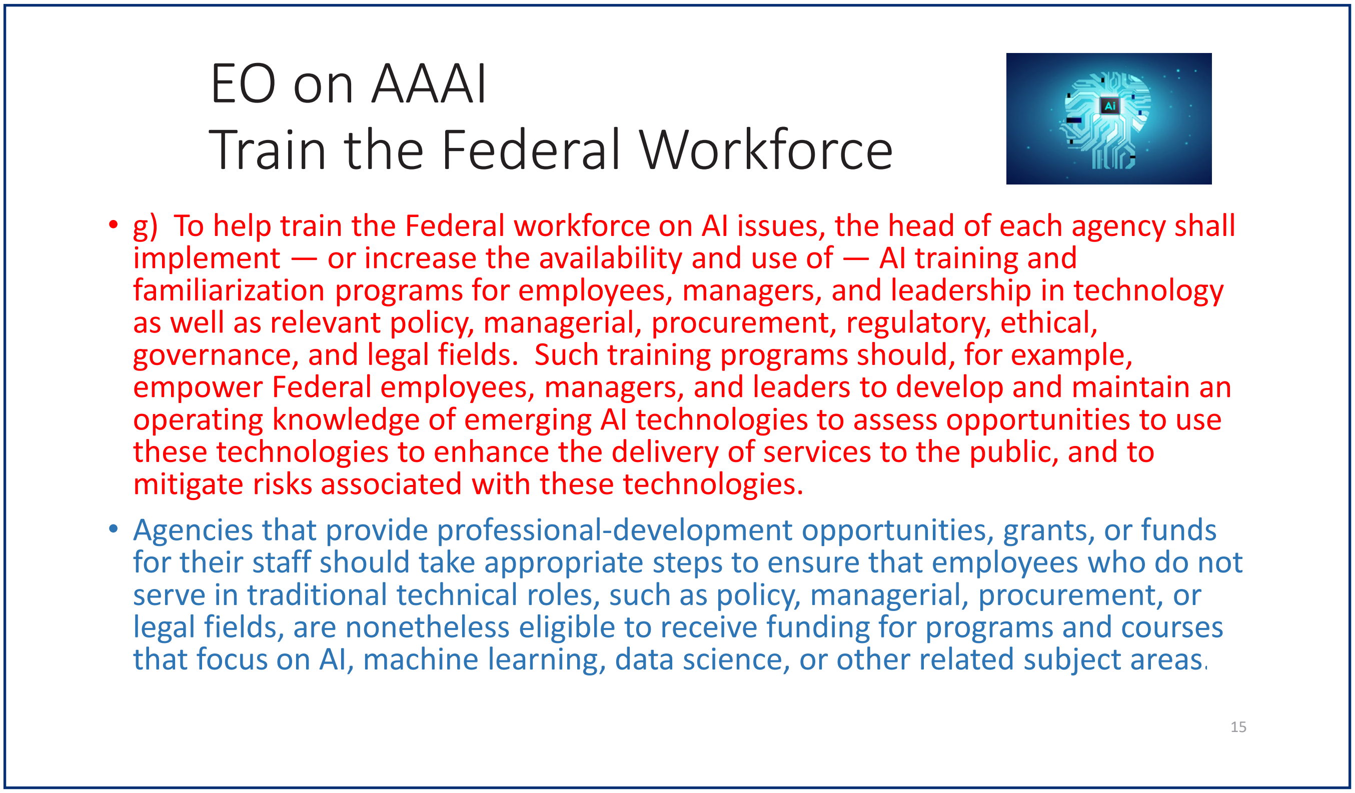
EO on AI Fed Gov't Workers

- My Administration will take steps to attract, retain, and develop public service-oriented AI professionals, including from underserved communities, across disciplines — including technology, policy, managerial, procurement, regulatory, ethical, governance, and legal fields — and ease AI professionals' path into the Federal Government to help harness and govern AI. The Federal Government will work to ensure that all members of its workforce receive adequate training to understand the benefits, risks, and limitations of AI for their job functions, and to modernize Federal Government information technology infrastructure, remove bureaucratic obstacles, and ensure that safe and rights-respecting AI is adopted, deployed, and used.



EO on AI Support Unions

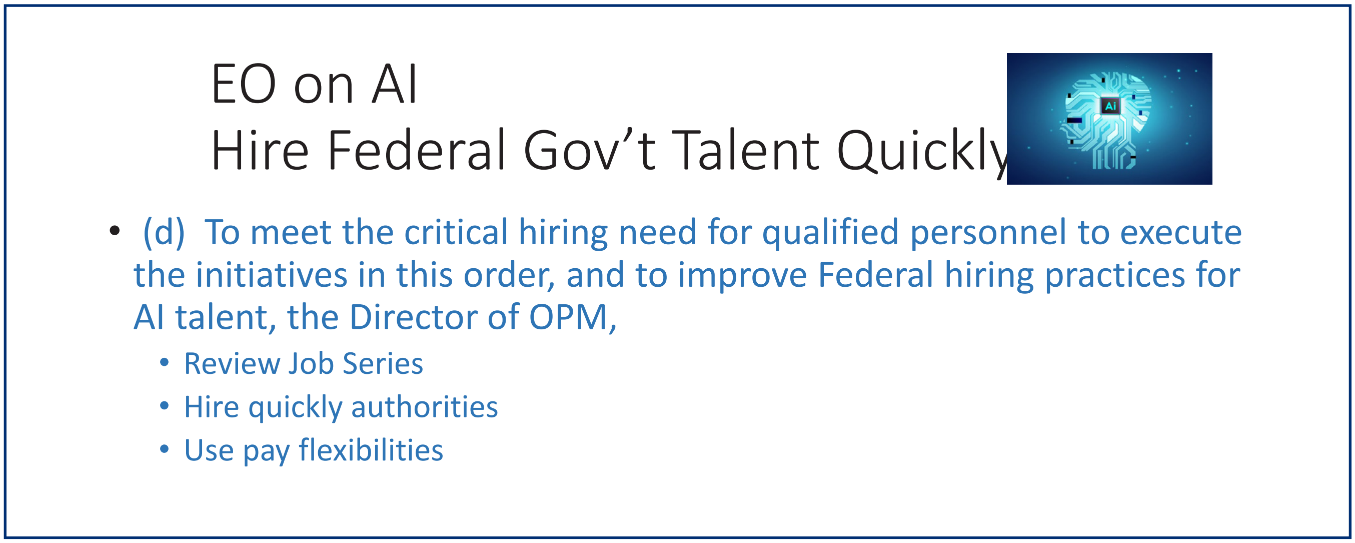
- b) To help ensure that AI deployed in the workplace advances employees' well-being:
- (i) **The Secretary of Labor shall, within 180 days** of the date of this order and in consultation with other agencies and with outside entities**, including labor unions** and workers, as the Secretary of Labor deems appropriate, develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits. The principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover, at a minimum:
- (A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers;
- (B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and
- (C) implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws.
- (ii) **After principles and best practices are developed** pursuant to subsection (b)(i) of this section, **the heads of agencies shall consider, in consultation with the Secretary of Labor, encouraging the adoption of these guidelines in their programs** to the extent appropriate for each program and consistent with applicable law.
- (iii) To support employees whose work is monitored or augmented by AI in being compensated appropriately for all of their work time, the Secretary of Labor shall issue guidance to make clear that employers that deploy AI to monitor or augment employees' work must continue to comply with protections that ensure that workers are compensated for their hours worked, as defined under the Fair Labor Standards Act of 1938, 29 U.S.C. 201 et seq., and other legal requirements.



EO on AAAI
Train the Federal Workforce

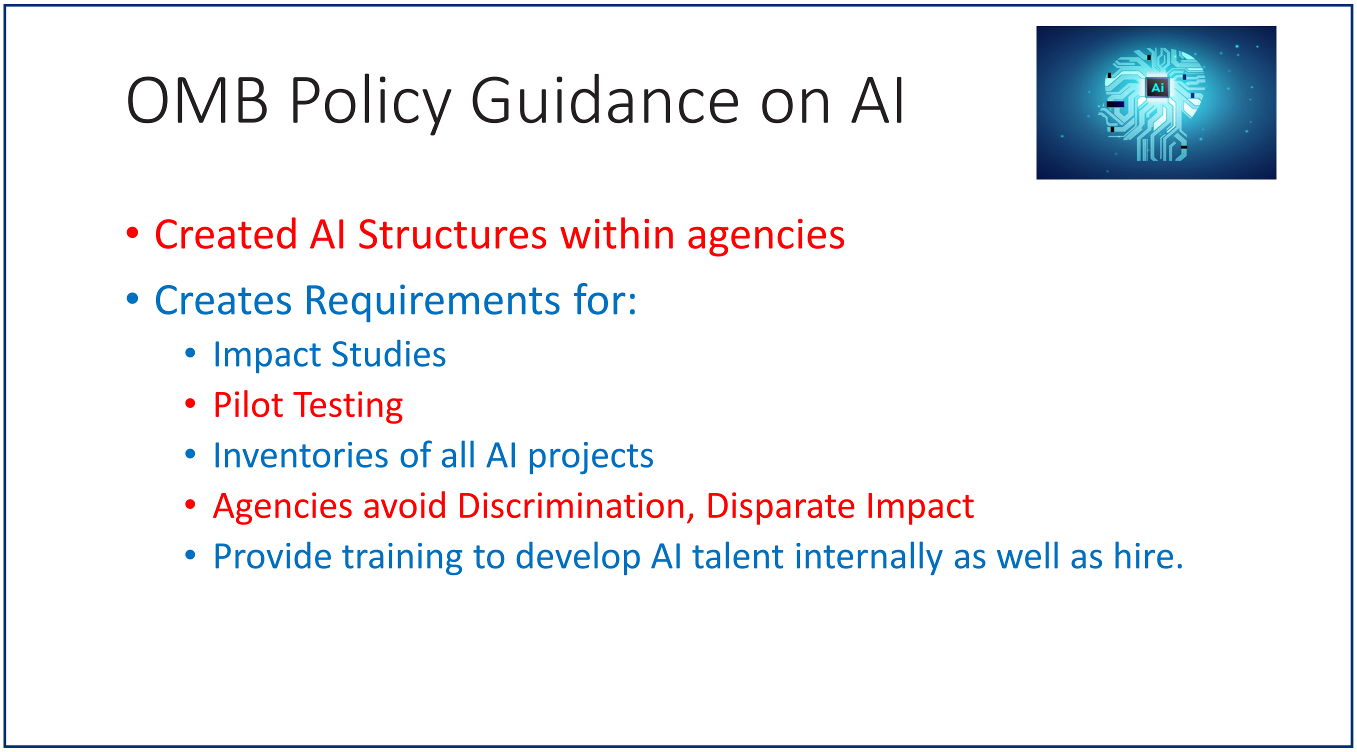
- g) To help train the Federal workforce on AI issues, the head of each agency shall implement — or increase the availability and use of — AI training and familiarization programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields. Such training programs should, for example, empower Federal employees, managers, and leaders to develop and maintain an operating knowledge of emerging AI technologies to assess opportunities to use these technologies to enhance the delivery of services to the public, and to mitigate risks associated with these technologies.
- Agencies that provide professional-development opportunities, grants, or funds for their staff should take appropriate steps to ensure that employees who do not serve in traditional technical roles, such as policy, managerial, procurement, or legal fields, are nonetheless eligible to receive funding for programs and courses that focus on AI, machine learning, data science, or other related subject areas.

15



EO on AI
Hire Federal Gov’t Talent Quickly

- (d) To meet the critical hiring need for qualified personnel to execute the initiatives in this order, and to improve Federal hiring practices for AI talent, the Director of OPM,
  - Review Job Series
  - Hire quickly authorities
  - Use pay flexibilities



OMB Policy Guidance on AI

- Created AI Structures within agencies
- Creates Requirements for:
  - Impact Studies
  - Pilot Testing
  - Inventories of all AI projects
  - Agencies avoid Discrimination, Disparate Impact
  - Provide training to develop AI talent internally as well as hire.

President Biden issues New Executive Order on Labor Management Forums and New OPM Guidance on the LM Forums

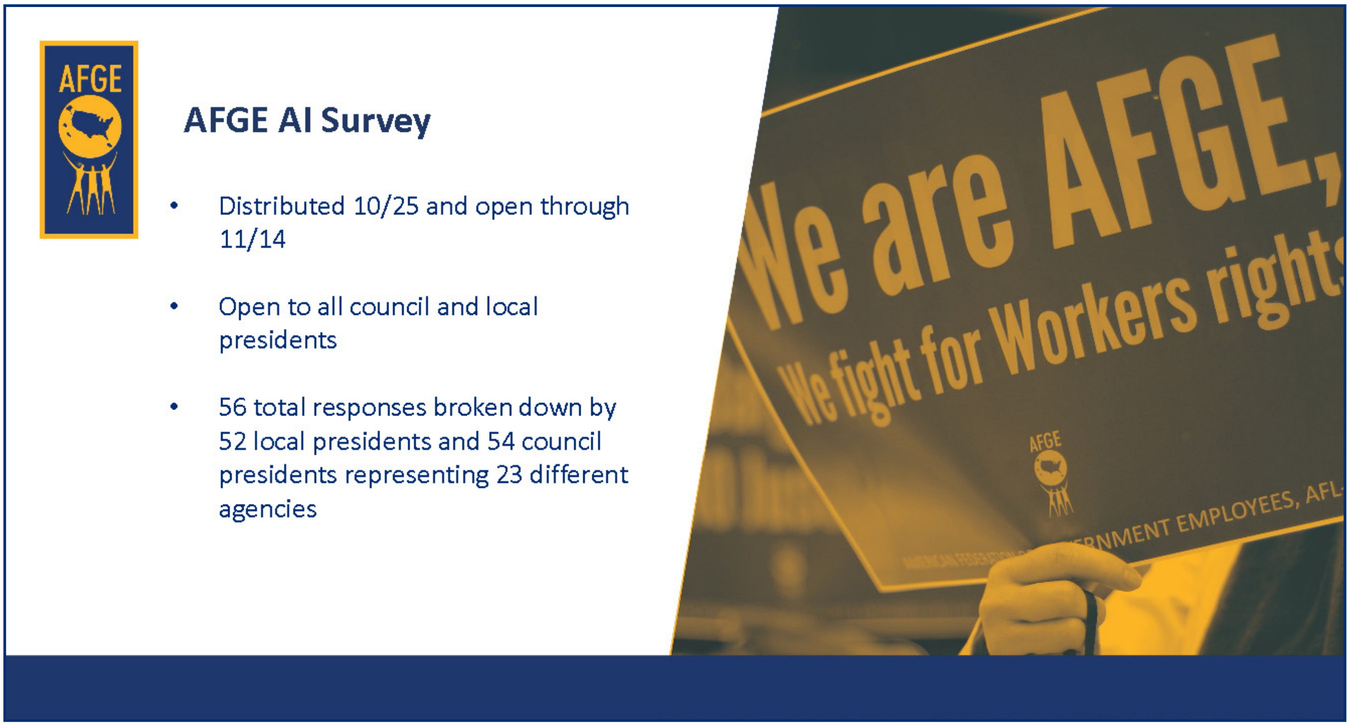
New President Biden Executive Order on Requirement for LM Forums - Agencies to submit their plans for LM Forums within 180 days from date of Executive Order (March 6, 2024-copy in Appendix II) to OPM by September 3, 2024. The EO requires Pre-Decisional Union Involvement.

New OPM Guidance to Agencies on establishing the LM Forums. (March 13, 2024-copy in Appendix II). Reminds agencies to submit their b(1) "Bargaining over Permissive Subjects" certifications along with their Plans for establishing LM Forums.

Councils and Locals, as appropriate, should combine their agencies involvement in AI in their follow-up with agencies to establish LM Forums and b(1) Bargaining.

AFGE Leader Survey on AI

In the fall of 2023, the Committee developed and distributed a survey on Artificial Intelligence to all AFGE Council and Local presidents to better understand how AFGE leaders interact with AI and view opportunities and challenges from AI. Key findings from that survey are included below.



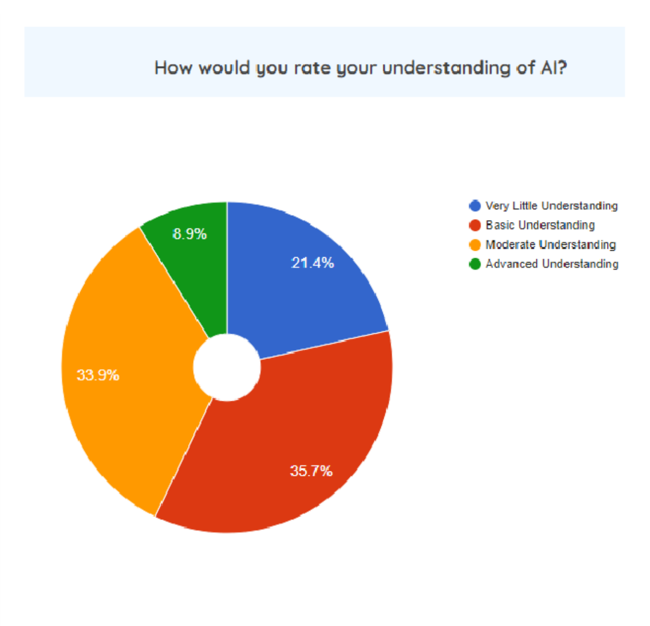
AFGE AI Survey

- Distributed 10/25 and open through 11/14
- Open to all council and local presidents
- 56 total responses broken down by 52 local presidents and 54 council presidents representing 23 different agencies

AFGE
We are AFGE,
We fight for Workers rights
AFGE
...RNMENT EMPLOYEES, AFL-

Results

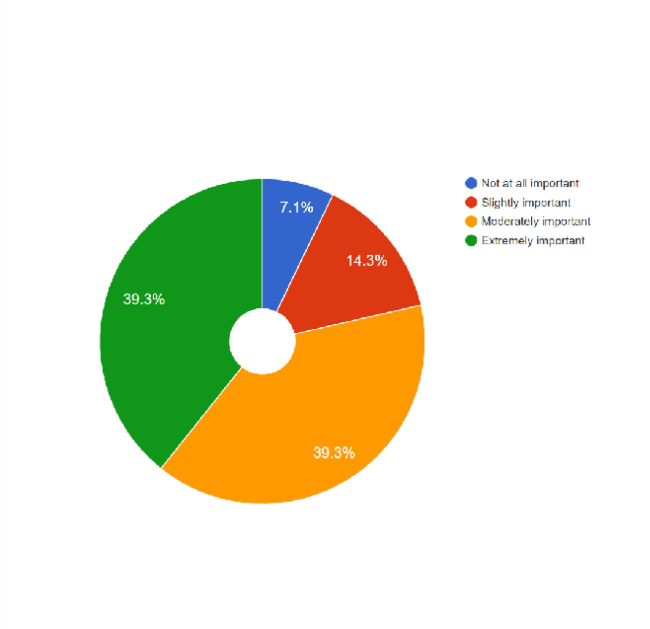
- Overall, a lot of AFGE presidents seem to have *some* familiarity with AI, but 9% identify themselves as having advanced understanding

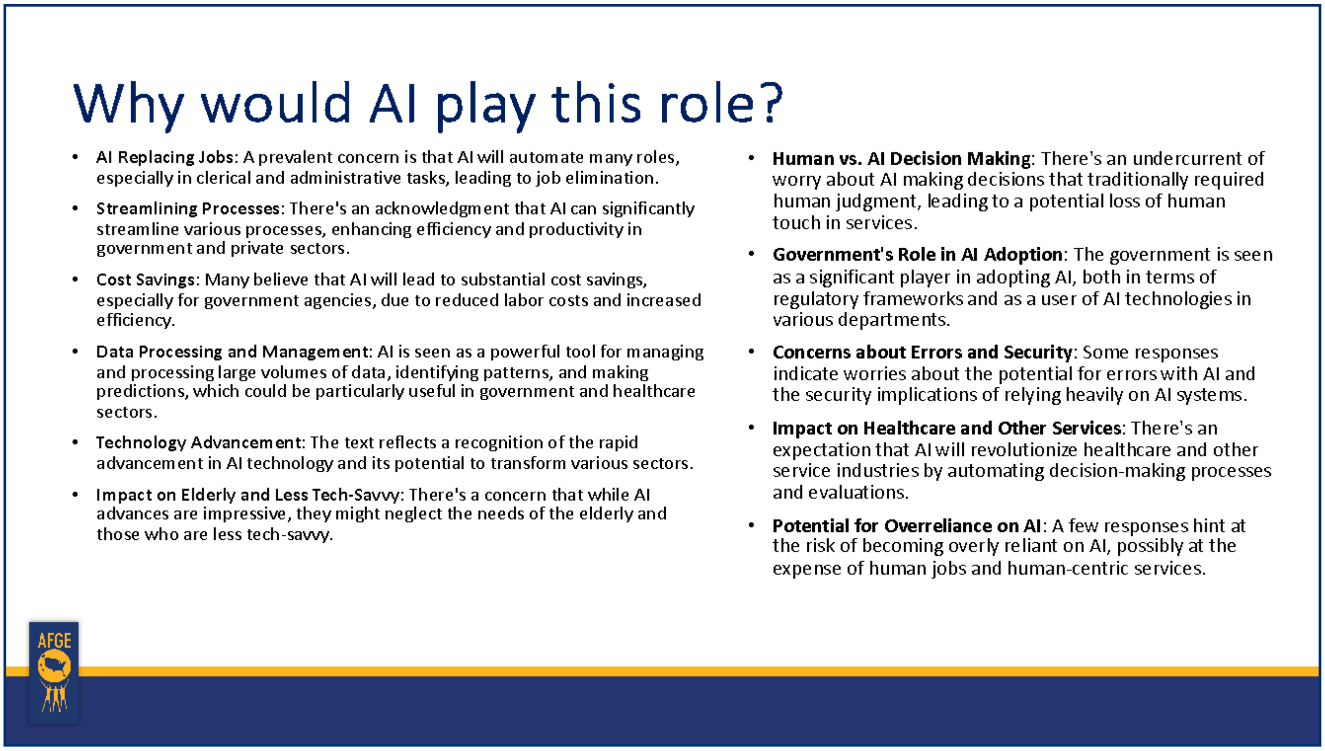


How would you rate your understanding of AI?

How important will the role of AI be in government over the next 5 years?

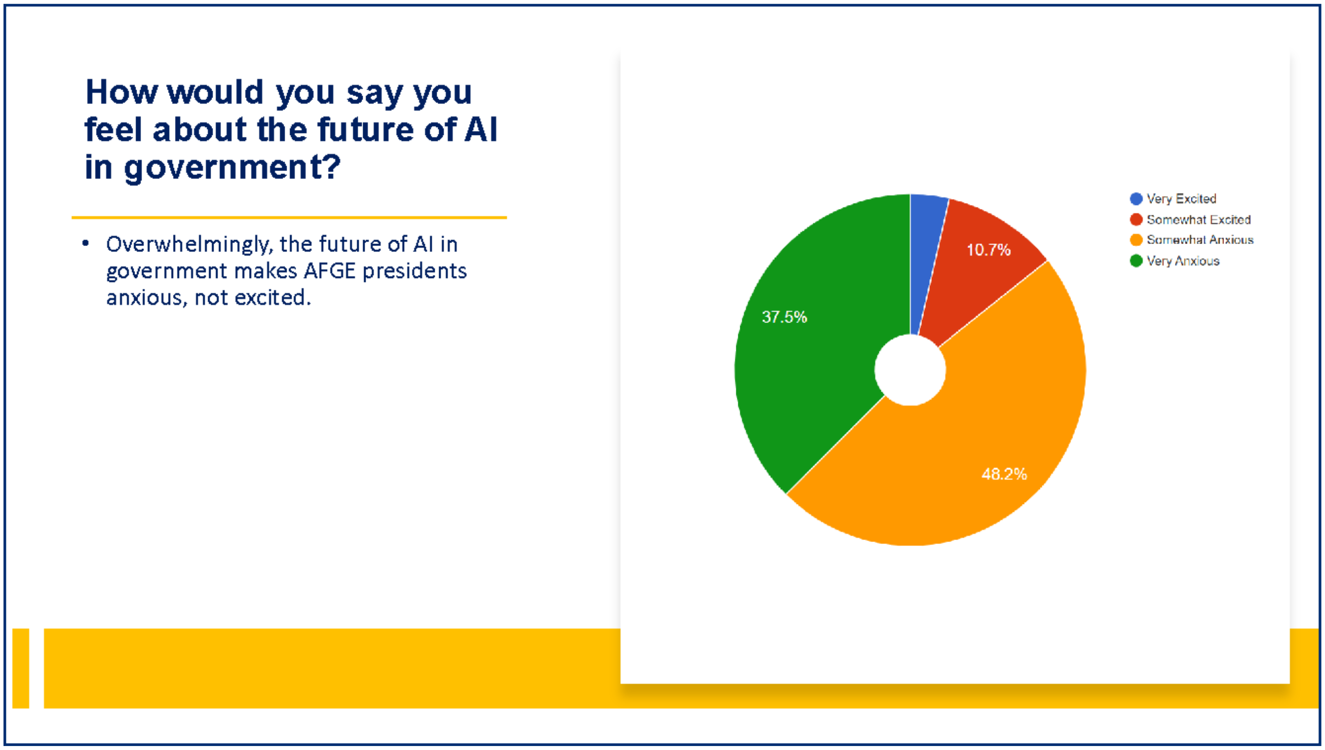
- Big majorities of AFGE leaders believe AI will play an increasingly important role in government in the next 5 years





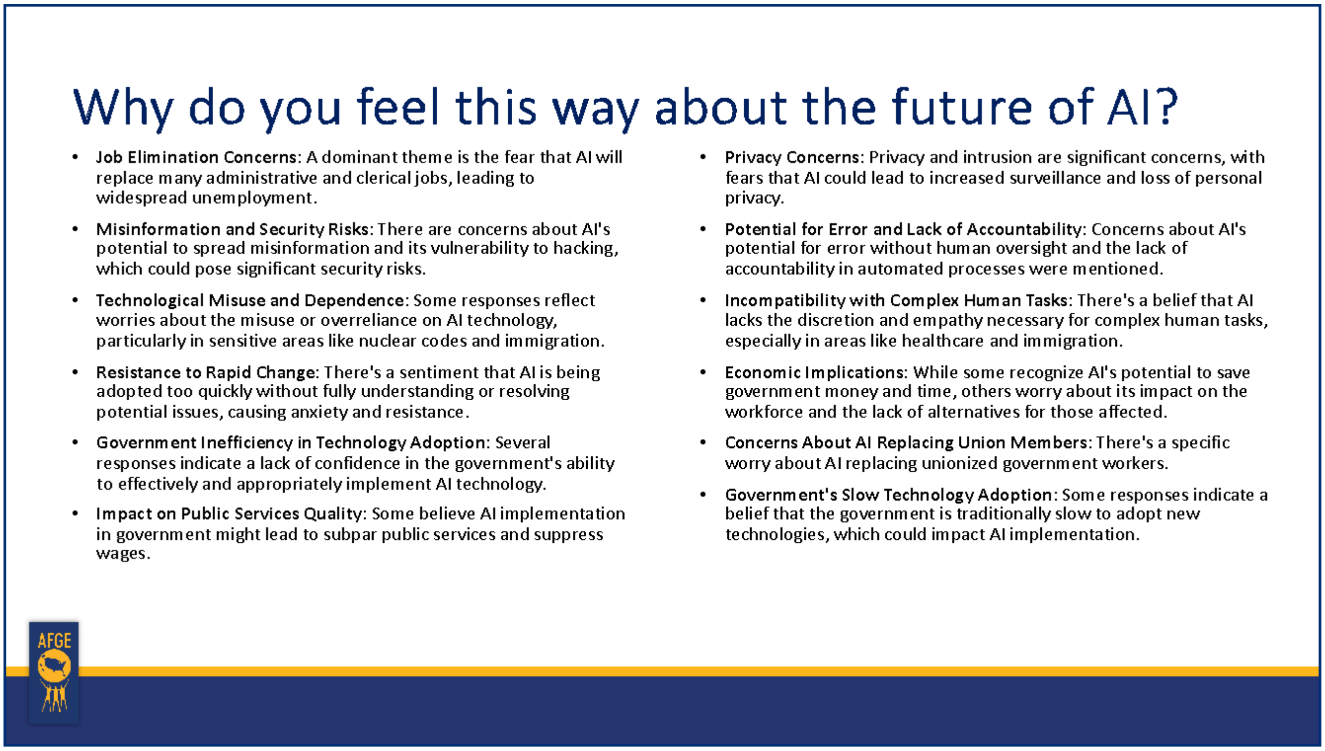
Why would AI play this role?

- **AI Replacing Jobs**: A prevalent concern is that AI will automate many roles, especially in clerical and administrative tasks, leading to job elimination.
- **Streamlining Processes**: There's an acknowledgment that AI can significantly streamline various processes, enhancing efficiency and productivity in government and private sectors.
- **Cost Savings**: Many believe that AI will lead to substantial cost savings, especially for government agencies, due to reduced labor costs and increased efficiency.
- **Data Processing and Management**: AI is seen as a powerful tool for managing and processing large volumes of data, identifying patterns, and making predictions, which could be particularly useful in government and healthcare sectors.
- **Technology Advancement**: The text reflects a recognition of the rapid advancement in AI technology and its potential to transform various sectors.
- **Impact on Elderly and Less Tech-Savvy**: There's a concern that while AI advances are impressive, they might neglect the needs of the elderly and those who are less tech-savvy.
- **Human vs. AI Decision Making**: There's an undercurrent of worry about AI making decisions that traditionally required human judgment, leading to a potential loss of human touch in services.
- **Government's Role in AI Adoption**: The government is seen as a significant player in adopting AI, both in terms of regulatory frameworks and as a user of AI technologies in various departments.
- **Concerns about Errors and Security**: Some responses indicate worries about the potential for errors with AI and the security implications of relying heavily on AI systems.
- **Impact on Healthcare and Other Services**: There's an expectation that AI will revolutionize healthcare and other service industries by automating decision-making processes and evaluations.
- **Potential for Overreliance on AI**: A few responses hint at the risk of becoming overly reliant on AI, possibly at the expense of human jobs and human-centric services.



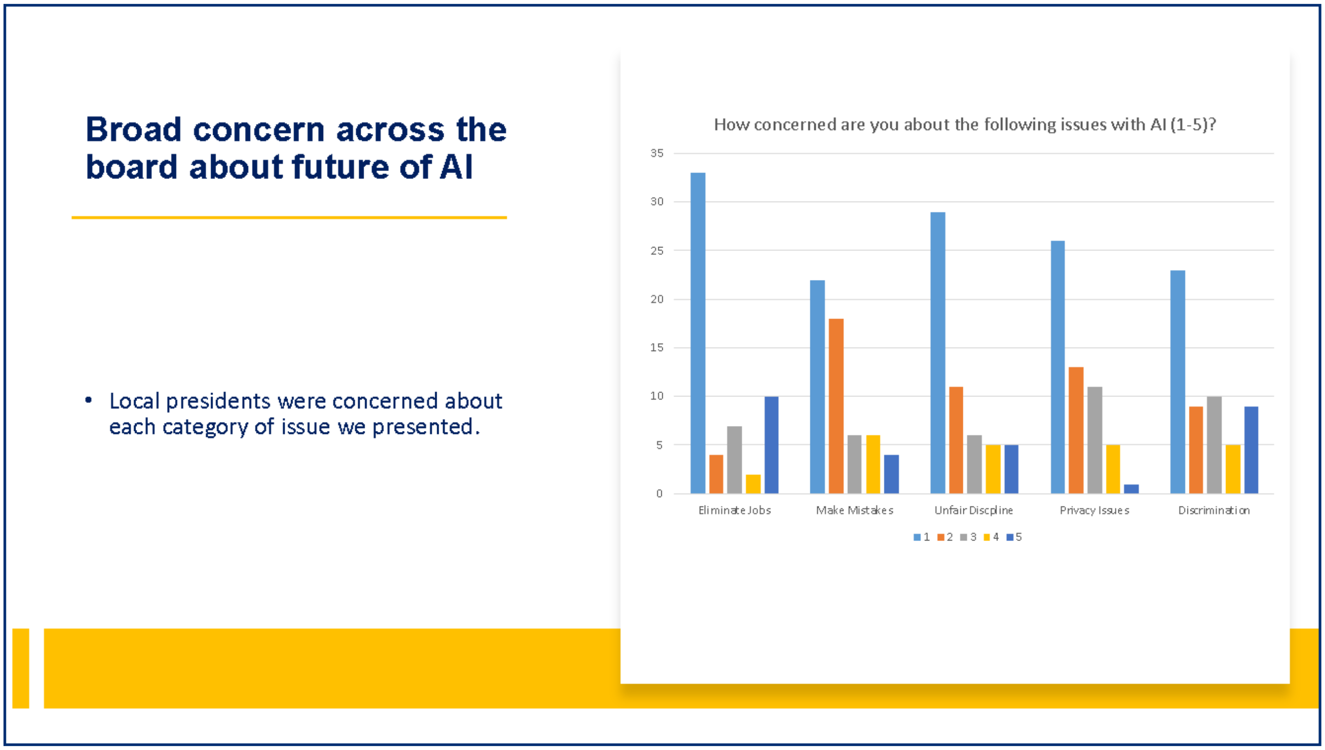
How would you say you feel about the future of AI in government?

- Overwhelmingly, the future of AI in government makes AFGE presidents anxious, not excited.



Why do you feel this way about the future of AI?

- **Job Elimination Concerns**: A dominant theme is the fear that AI will replace many administrative and clerical jobs, leading to widespread unemployment.
- **Misinformation and Security Risks**: There are concerns about AI's potential to spread misinformation and its vulnerability to hacking, which could pose significant security risks.
- **Technological Misuse and Dependence**: Some responses reflect worries about the misuse or overreliance on AI technology, particularly in sensitive areas like nuclear codes and immigration.
- **Resistance to Rapid Change**: There's a sentiment that AI is being adopted too quickly without fully understanding or resolving potential issues, causing anxiety and resistance.
- **Government Inefficiency in Technology Adoption**: Several responses indicate a lack of confidence in the government's ability to effectively and appropriately implement AI technology.
- **Impact on Public Services Quality**: Some believe AI implementation in government might lead to subpar public services and suppress wages.
- **Privacy Concerns**: Privacy and intrusion are significant concerns, with fears that AI could lead to increased surveillance and loss of personal privacy.
- **Potential for Error and Lack of Accountability**: Concerns about AI's potential for error without human oversight and the lack of accountability in automated processes were mentioned.
- **Incompatibility with Complex Human Tasks**: There's a belief that AI lacks the discretion and empathy necessary for complex human tasks, especially in areas like healthcare and immigration.
- **Economic Implications**: While some recognize AI's potential to save government money and time, others worry about its impact on the workforce and the lack of alternatives for those affected.
- **Concerns About AI Replacing Union Members**: There's a specific worry about AI replacing unionized government workers.
- **Government's Slow Technology Adoption**: Some responses indicate a belief that the government is traditionally slow to adopt new technologies, which could impact AI implementation.



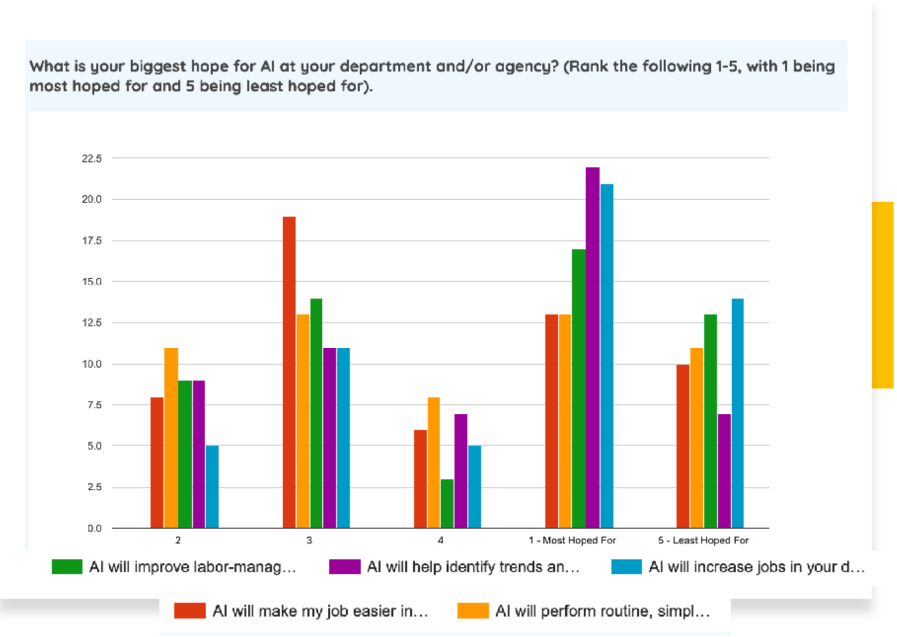
Broad concern across the board about future of AI

- Local presidents were concerned about each category of issue we presented.

Why are you concerned?

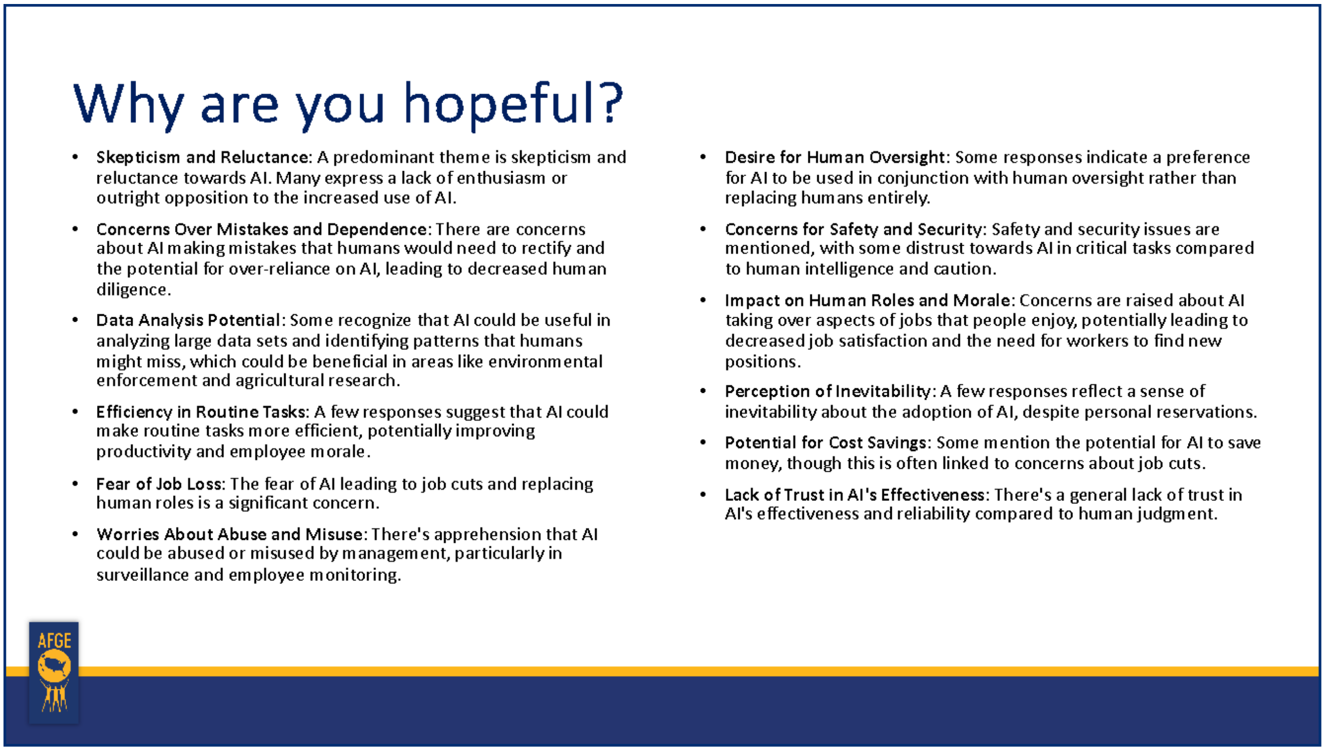
- **Job Elimination and Reduction:** A primary concern is that AI will lead to the elimination or reduction of jobs, particularly in administrative positions.
- **Abuse by Management:** There are fears that AI could be misused by management to track and evaluate workers, potentially leading to biased assessments and increased surveillance.
- **Dependency and Laziness:** Concerns were raised about workers becoming overly dependent on AI, leading to a decrease in diligence and an increase in errors that humans would need to rectify.
- **Privacy Concerns:** Many are worried about the potential for AI to compromise privacy, either through mishandling confidential information or increased surveillance.
- **Inappropriate or Ineffective Use:** There's a skepticism about AI's effectiveness, with worries that it might be used inappropriately or forced upon workers despite being less effective than human employees.
- **Potential for Misinformation and Bias:** The concern that AI might perpetuate biases or misinformation, especially in politically charged environments, was noted.
- **Impact on Human-Centric Processes:** Some responses indicated a concern that an over-reliance on AI could detract from the human aspect of certain jobs, especially in fields that require empathy and discretion.
- **Security Risks:** The potential for AI systems to be hacked or manipulated, posing security threats, was a recurring concern.
- **Government Inefficiency and Misuse:** There's a lack of trust in the government's ability to efficiently and correctly implement AI, with fears of misuse and abuse, particularly in surveillance and employee monitoring.
- **Impact on Quality of Service:** There are concerns that AI might lead to a decline in the quality of services provided by government agencies.
- **Technology Glitches and Errors:** Worries about system glitches and errors in AI, which could lead to problems that require human intervention, were expressed.
- **Inability to Measure Qualitative Aspects:** Some responses highlighted AI's limitations in assessing qualitative aspects of work, like compassion and dedication, which cannot be quantified.

AFGE


What is your biggest hope for AI at your department and/or agency? (Rank the following 1-5, with 1 being most hoped for and 5 being least hoped for).

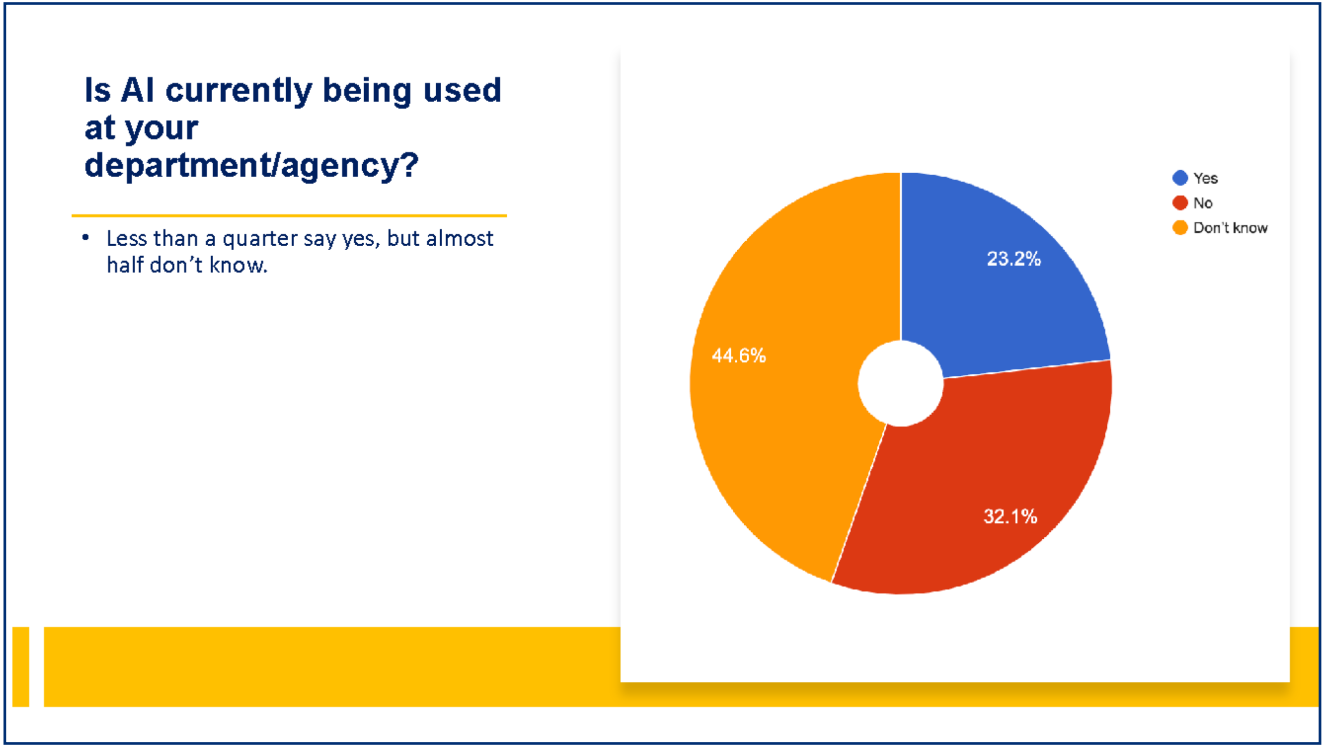
Most Hoped for: identify patterns and improve services.

Least hoped for: increase in jobs. Middle: making my job easier.



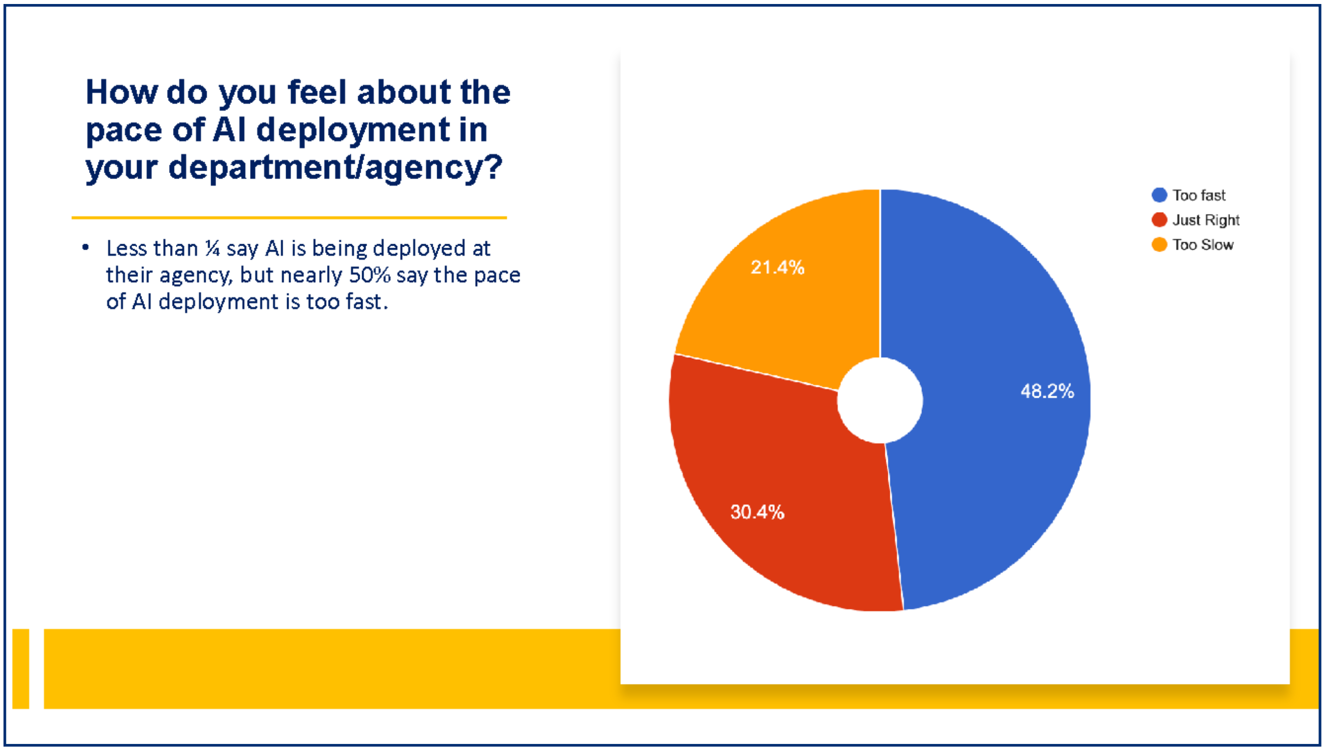
Why are you hopeful?

- **Skepticism and Reluctance**: A predominant theme is skepticism and reluctance towards AI. Many express a lack of enthusiasm or outright opposition to the increased use of AI.
- **Concerns Over Mistakes and Dependence**: There are concerns about AI making mistakes that humans would need to rectify and the potential for over-reliance on AI, leading to decreased human diligence.
- **Data Analysis Potential**: Some recognize that AI could be useful in analyzing large data sets and identifying patterns that humans might miss, which could be beneficial in areas like environmental enforcement and agricultural research.
- **Efficiency in Routine Tasks**: A few responses suggest that AI could make routine tasks more efficient, potentially improving productivity and employee morale.
- **Fear of Job Loss**: The fear of AI leading to job cuts and replacing human roles is a significant concern.
- **Worries About Abuse and Misuse**: There's apprehension that AI could be abused or misused by management, particularly in surveillance and employee monitoring.
- **Desire for Human Oversight**: Some responses indicate a preference for AI to be used in conjunction with human oversight rather than replacing humans entirely.
- **Concerns for Safety and Security**: Safety and security issues are mentioned, with some distrust towards AI in critical tasks compared to human intelligence and caution.
- **Impact on Human Roles and Morale**: Concerns are raised about AI taking over aspects of jobs that people enjoy, potentially leading to decreased job satisfaction and the need for workers to find new positions.
- **Perception of Inevitability**: A few responses reflect a sense of inevitability about the adoption of AI, despite personal reservations.
- **Potential for Cost Savings**: Some mention the potential for AI to save money, though this is often linked to concerns about job cuts.
- **Lack of Trust in AI's Effectiveness**: There's a general lack of trust in AI's effectiveness and reliability compared to human judgment.



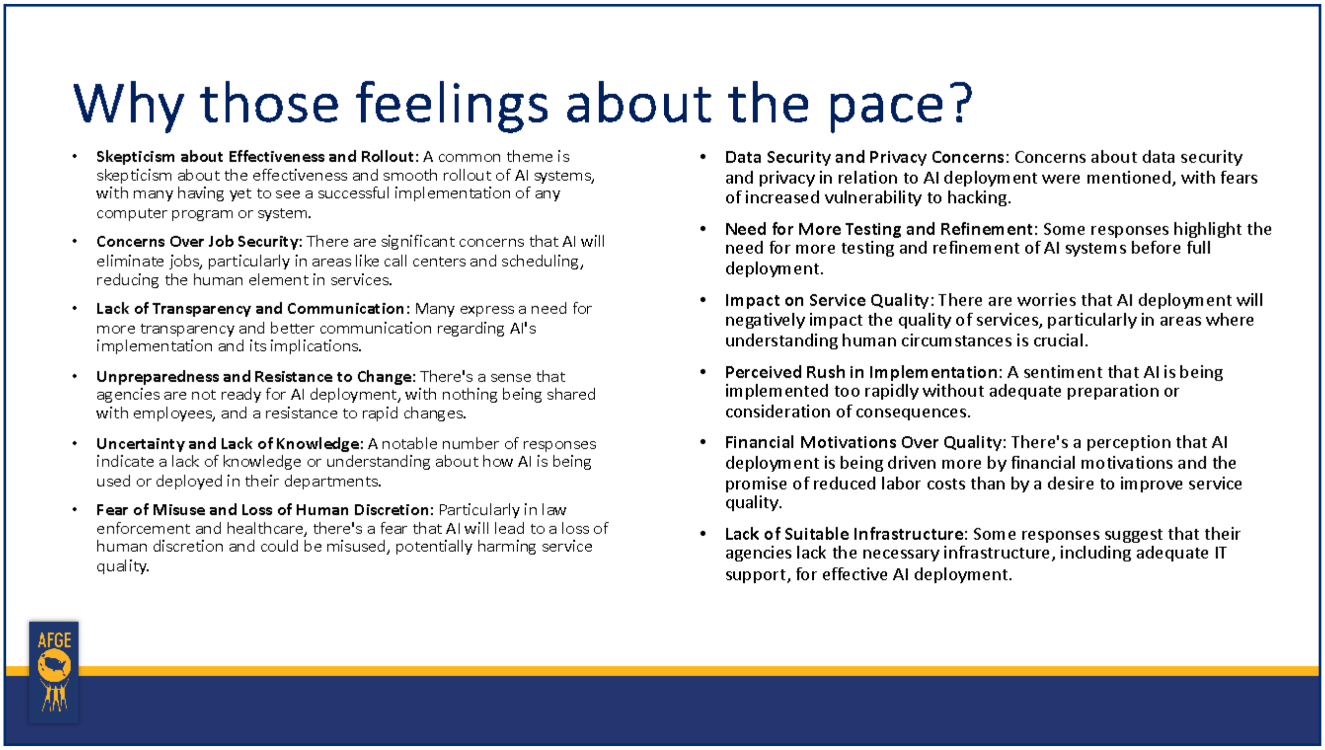
Is AI currently being used at your department/agency?

- Less than a quarter say yes, but almost half don't know.



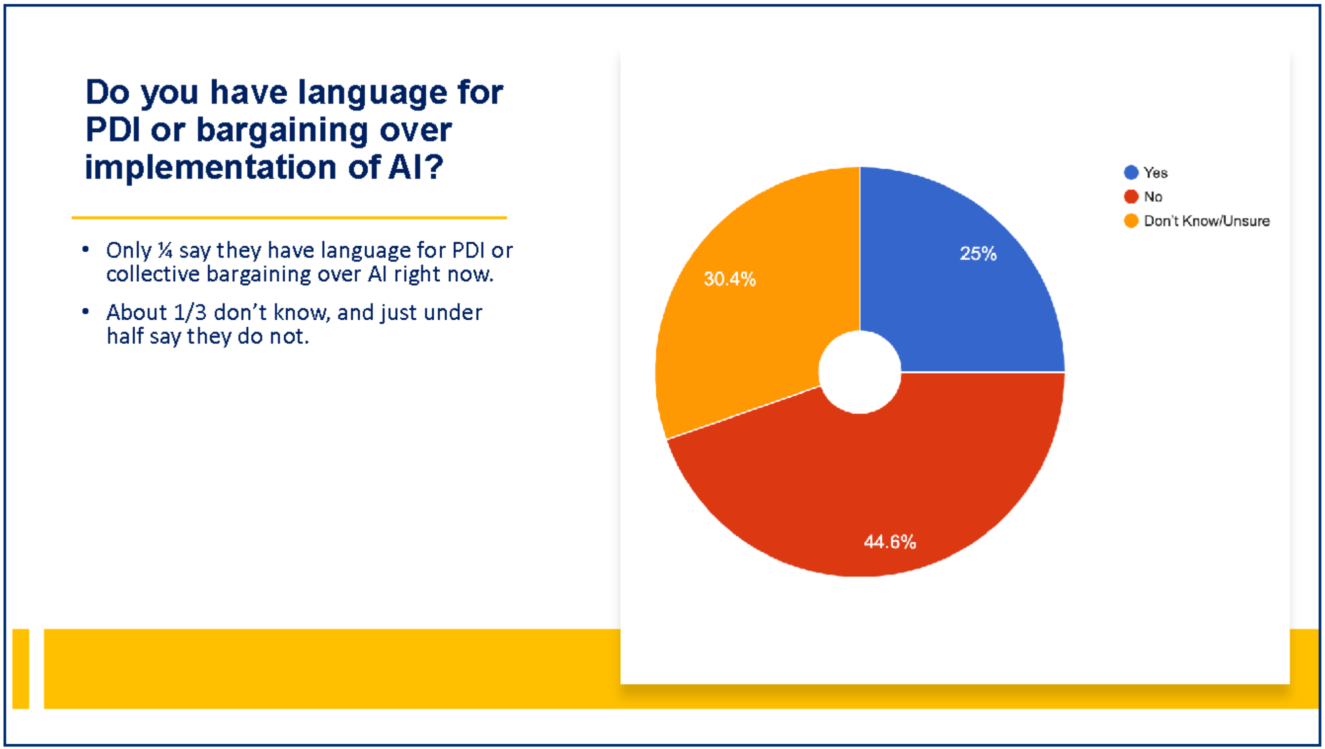
How do you feel about the pace of AI deployment in your department/agency?

- Less than ¼ say AI is being deployed at their agency, but nearly 50% say the pace of AI deployment is too fast.



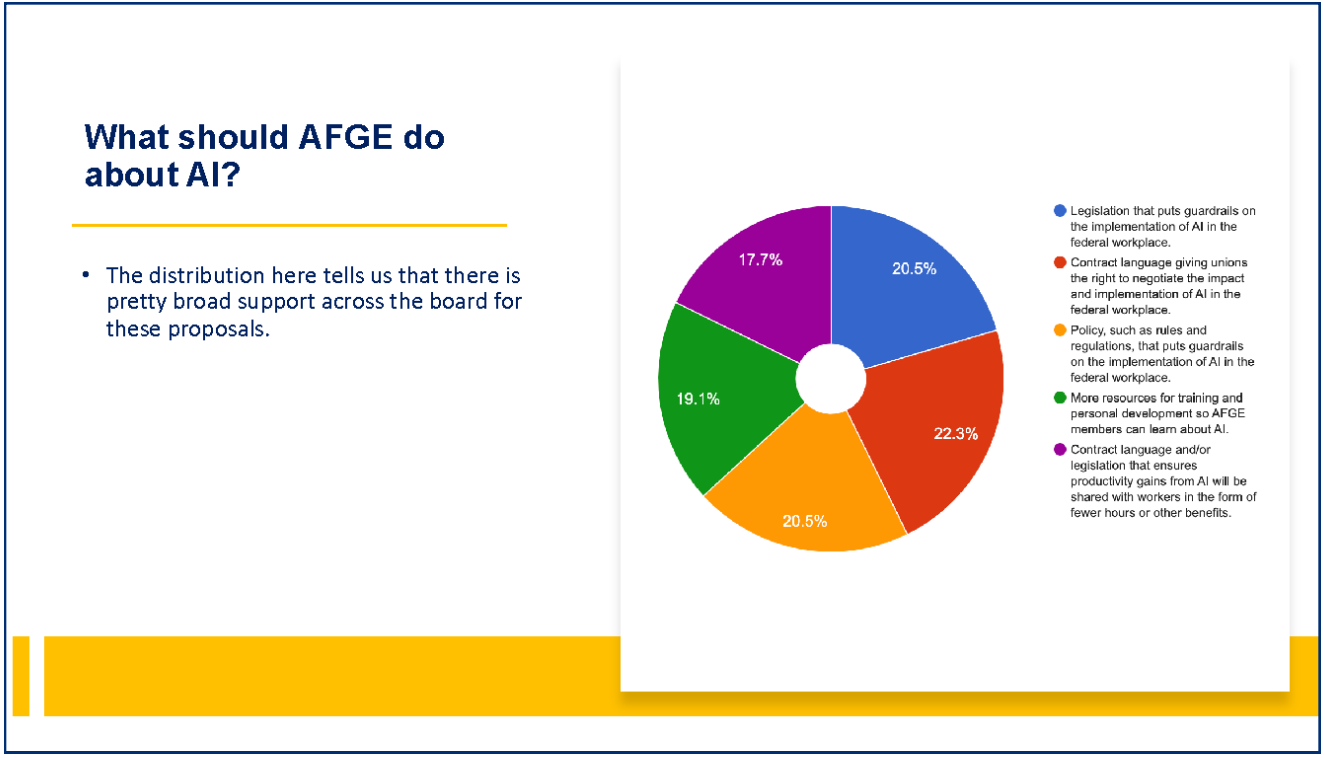
Why those feelings about the pace?

- **Skepticism about Effectiveness and Rollout:** A common theme is skepticism about the effectiveness and smooth rollout of AI systems, with many having yet to see a successful implementation of any computer program or system.
- **Concerns Over Job Security:** There are significant concerns that AI will eliminate jobs, particularly in areas like call centers and scheduling, reducing the human element in services.
- **Lack of Transparency and Communication:** Many express a need for more transparency and better communication regarding AI's implementation and its implications.
- **Unpreparedness and Resistance to Change:** There's a sense that agencies are not ready for AI deployment, with nothing being shared with employees, and a resistance to rapid changes.
- **Uncertainty and Lack of Knowledge:** A notable number of responses indicate a lack of knowledge or understanding about how AI is being used or deployed in their departments.
- **Fear of Misuse and Loss of Human Discretion:** Particularly in law enforcement and healthcare, there's a fear that AI will lead to a loss of human discretion and could be misused, potentially harming service quality.
- **Data Security and Privacy Concerns:** Concerns about data security and privacy in relation to AI deployment were mentioned, with fears of increased vulnerability to hacking.
- **Need for More Testing and Refinement:** Some responses highlight the need for more testing and refinement of AI systems before full deployment.
- **Impact on Service Quality:** There are worries that AI deployment will negatively impact the quality of services, particularly in areas where understanding human circumstances is crucial.
- **Perceived Rush in Implementation:** A sentiment that AI is being implemented too rapidly without adequate preparation or consideration of consequences.
- **Financial Motivations Over Quality:** There's a perception that AI deployment is being driven more by financial motivations and the promise of reduced labor costs than by a desire to improve service quality.
- **Lack of Suitable Infrastructure:** Some responses suggest that their agencies lack the necessary infrastructure, including adequate IT support, for effective AI deployment.



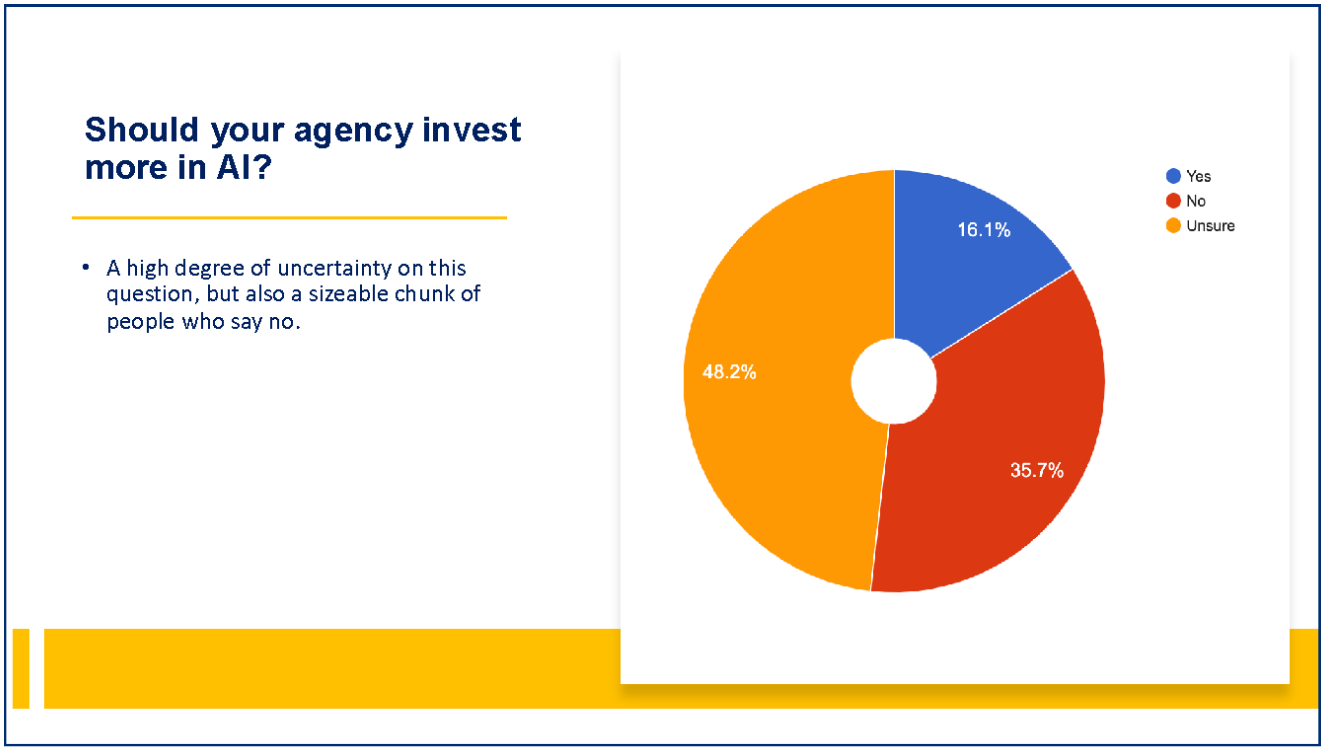
Do you have language for PDI or bargaining over implementation of AI?

- Only ¼ say they have language for PDI or collective bargaining over AI right now.
- About 1/3 don't know, and just under half say they do not.



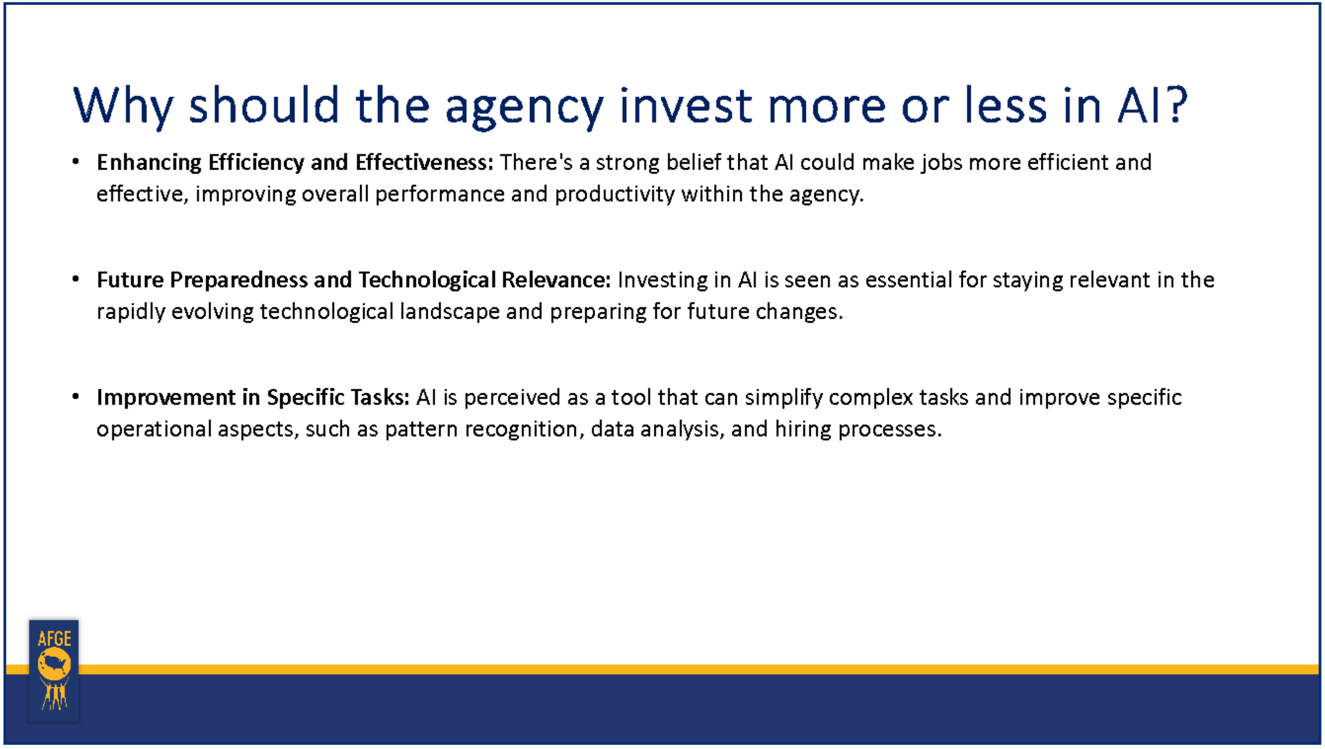
What should AFGE do about AI?

- The distribution here tells us that there is pretty broad support across the board for these proposals.



Should your agency invest more in AI?

- A high degree of uncertainty on this question, but also a sizeable chunk of people who say no.

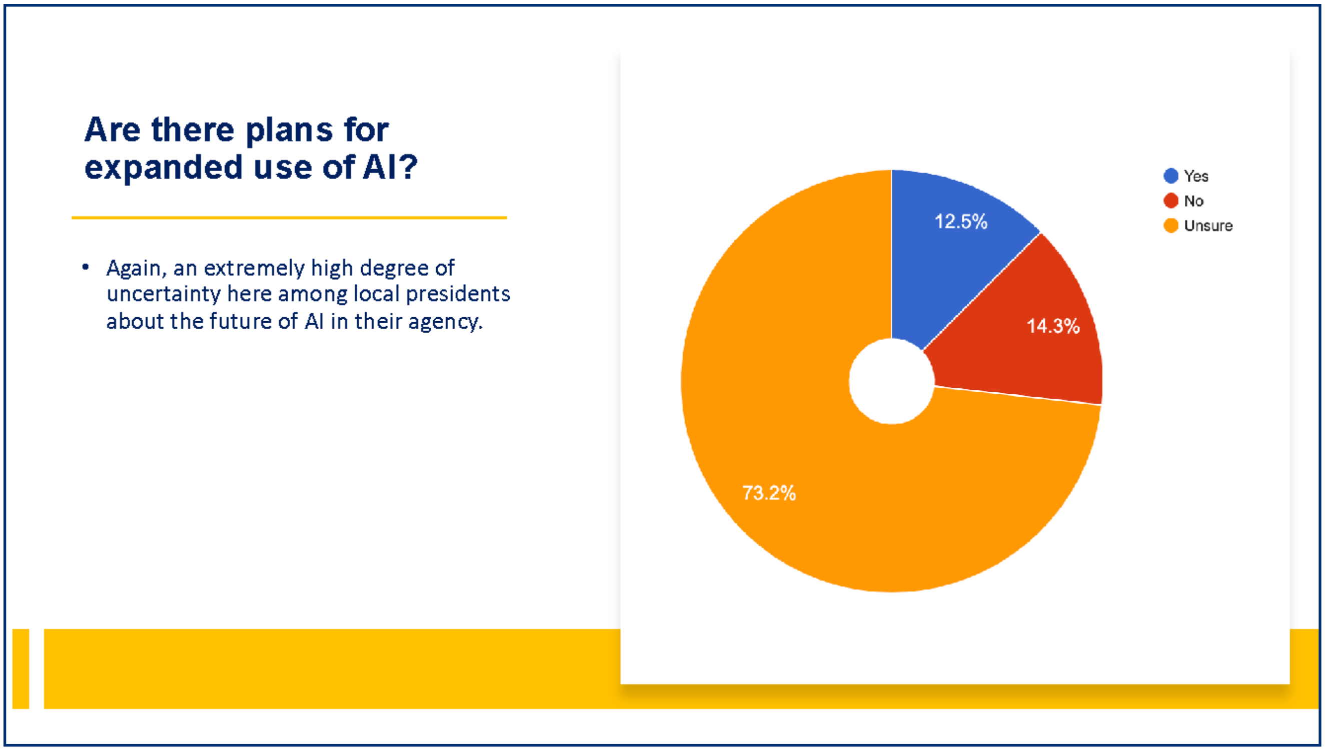


Why should the agency invest more or less in AI?

- **Enhancing Efficiency and Effectiveness:** There's a strong belief that AI could make jobs more efficient and effective, improving overall performance and productivity within the agency.

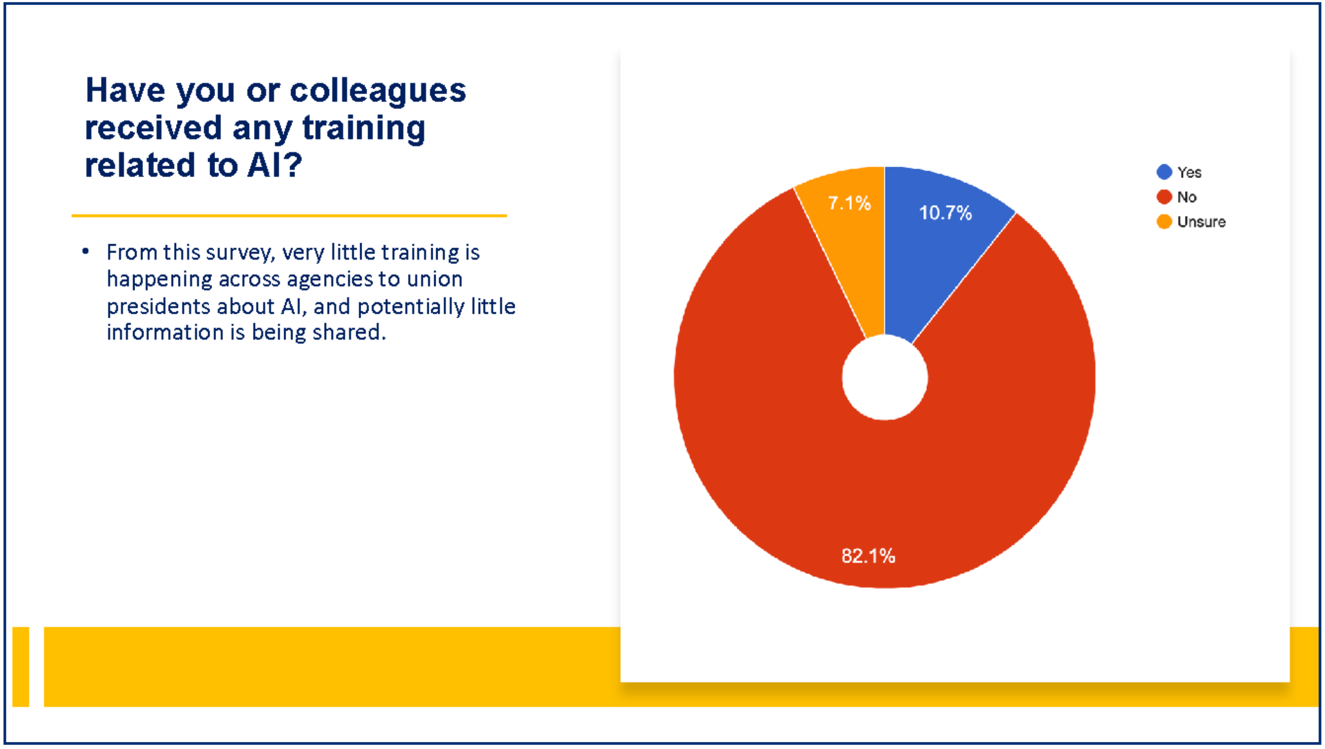
- **Future Preparedness and Technological Relevance:** Investing in AI is seen as essential for staying relevant in the rapidly evolving technological landscape and preparing for future changes.

- **Improvement in Specific Tasks:** AI is perceived as a tool that can simplify complex tasks and improve specific operational aspects, such as pattern recognition, data analysis, and hiring processes.



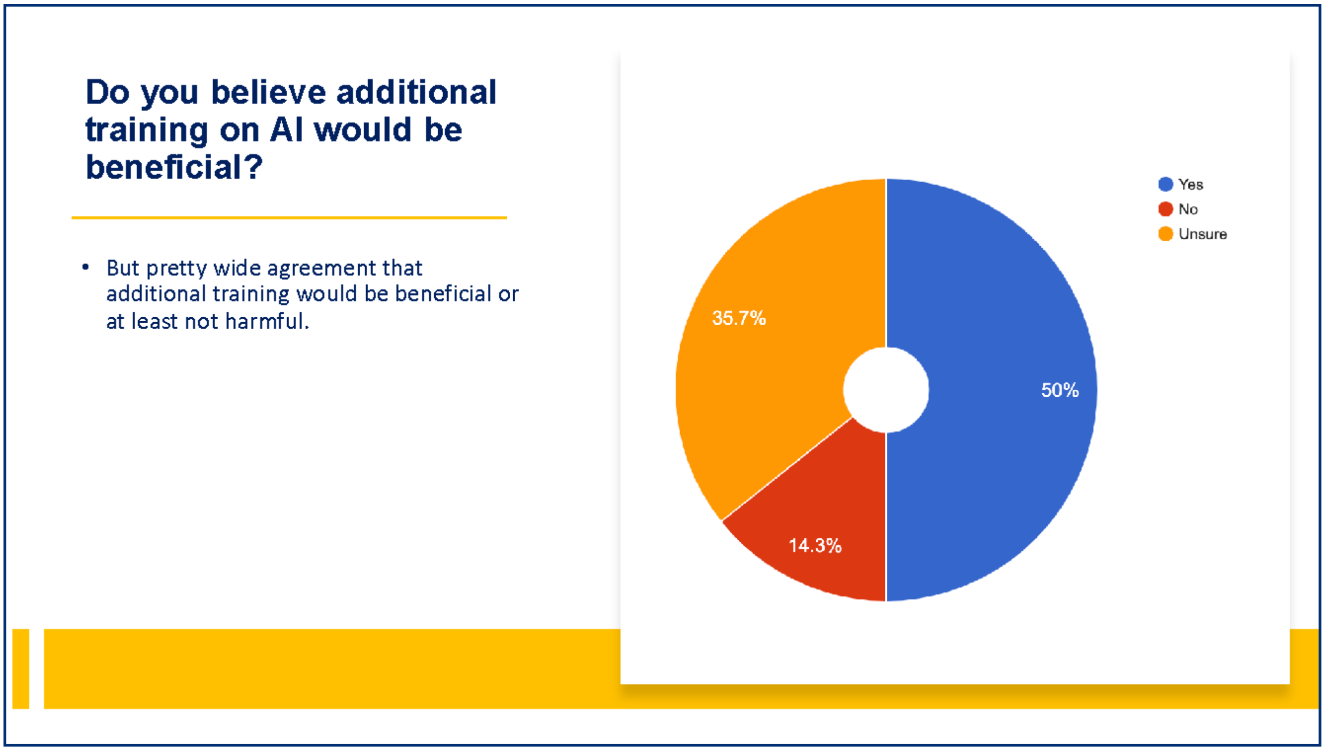
Are there plans for expanded use of AI?

- Again, an extremely high degree of uncertainty here among local presidents about the future of AI in their agency.



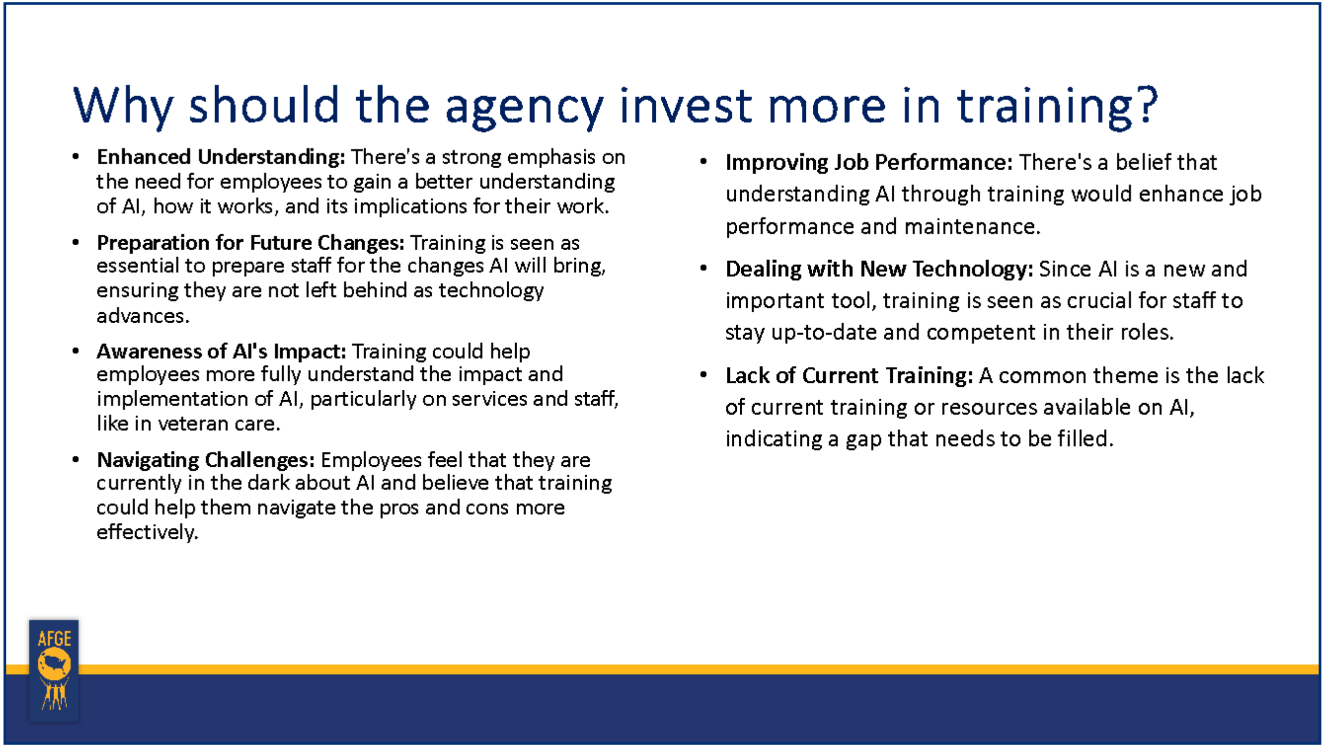
Have you or colleagues received any training related to AI?

- From this survey, very little training is happening across agencies to union presidents about AI, and potentially little information is being shared.



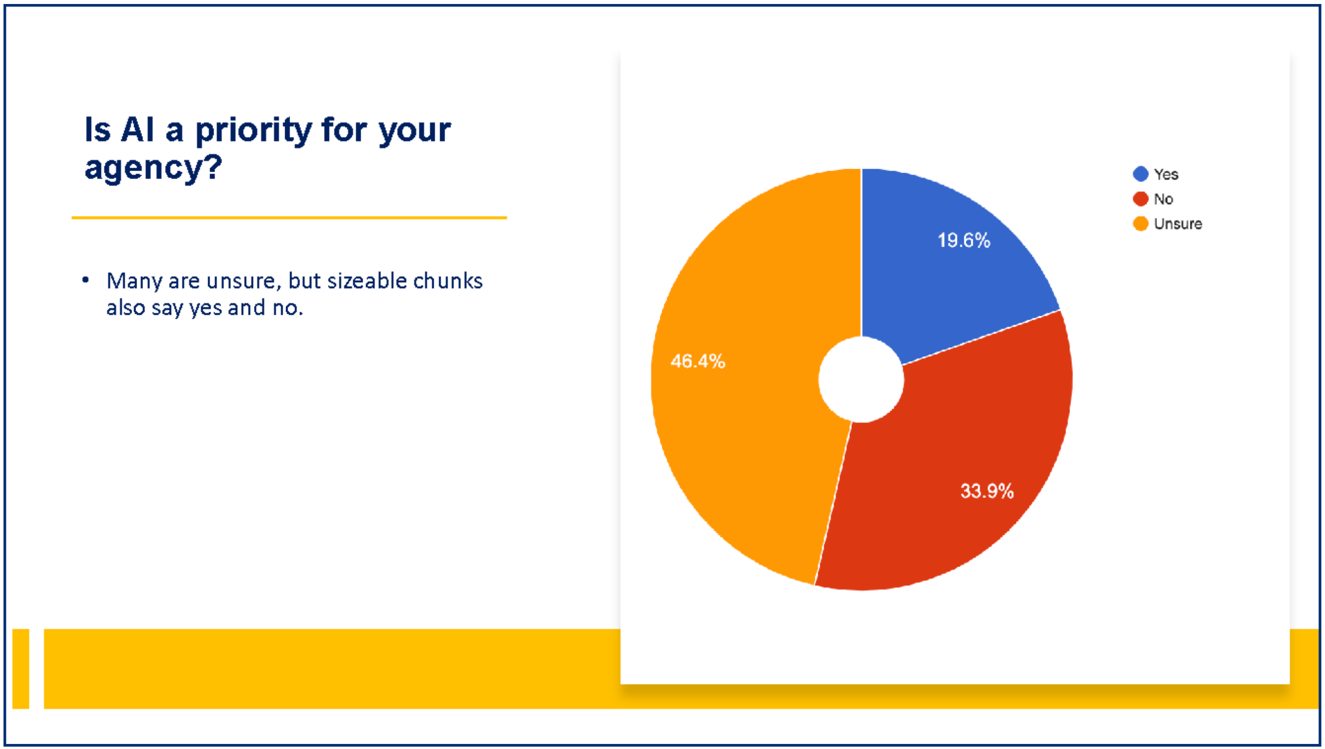
Do you believe additional training on AI would be beneficial?

- But pretty wide agreement that additional training would be beneficial or at least not harmful.



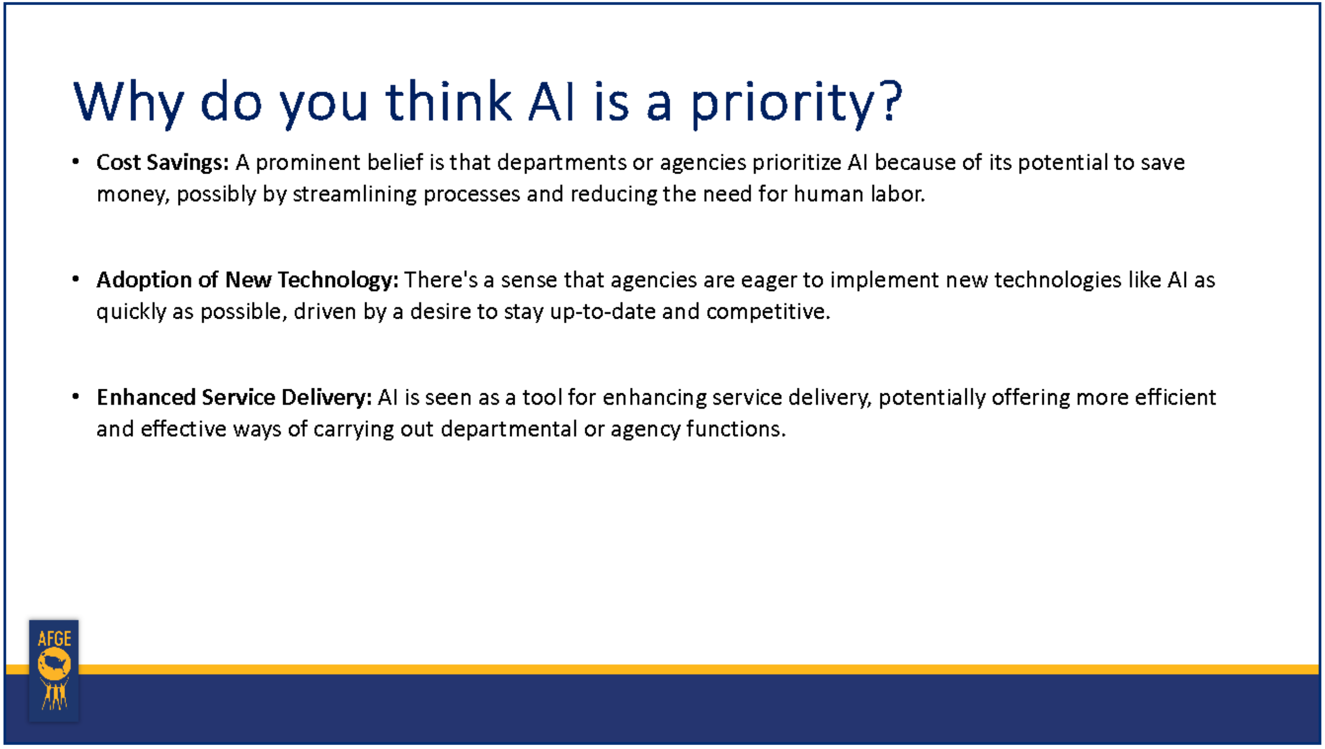
Why should the agency invest more in training?

- **Enhanced Understanding:** There's a strong emphasis on the need for employees to gain a better understanding of AI, how it works, and its implications for their work.
- **Preparation for Future Changes:** Training is seen as essential to prepare staff for the changes AI will bring, ensuring they are not left behind as technology advances.
- **Awareness of AI's Impact:** Training could help employees more fully understand the impact and implementation of AI, particularly on services and staff, like in veteran care.
- **Navigating Challenges:** Employees feel that they are currently in the dark about AI and believe that training could help them navigate the pros and cons more effectively.
- **Improving Job Performance:** There's a belief that understanding AI through training would enhance job performance and maintenance.
- **Dealing with New Technology:** Since AI is a new and important tool, training is seen as crucial for staff to stay up-to-date and competent in their roles.
- **Lack of Current Training:** A common theme is the lack of current training or resources available on AI, indicating a gap that needs to be filled.



Is AI a priority for your agency?

- Many are unsure, but sizeable chunks also say yes and no.



Why do you think AI is a priority?

- **Cost Savings:** A prominent belief is that departments or agencies prioritize AI because of its potential to save money, possibly by streamlining processes and reducing the need for human labor.

- **Adoption of New Technology:** There's a sense that agencies are eager to implement new technologies like AI as quickly as possible, driven by a desire to stay up-to-date and competitive.

- **Enhanced Service Delivery:** AI is seen as a tool for enhancing service delivery, potentially offering more efficient and effective ways of carrying out departmental or agency functions.

Themes from open comments

- **Need for Training and Preparedness:** There's a strong emphasis on the need for training to ensure employees are prepared for AI implementation and to maintain operations when technology fails. This includes understanding AI's role limitations and their work.
- **Concerns About Job Security and Human Element:** Many comments express concerns that AI could phase out human jobs, particularly on service-based industries that require personal connections and empathy. There's a fear that AI's logical approach may lack the human element crucial in certain fields.
- **Potential Benefits and Risks of AI:** Some see AI as a beneficial tool if used in conjunction with human oversight, but there are concerns about the risks, including security threats and the reliability of complete automation. The need for more information and cautious approach towards AI implementation is highlighted.
- **Technological Reliance and Vulnerability:** Some comments hint at concerns about over-reliance on technology, suggesting that when IT and communication systems fail, there's a lack of ability to continue essential functions manually. This point to a vulnerability in current operations and a need for balanced skills.
- **Financial Considerations:** There's a mention of AI being cost effective compared to human labor, indicating financial motivations behind AI adoption. This theme ties into the broader context of budgeting and resource allocation within agencies.
- **Role of Unions and Worker Representation:** Several comments reference unions, like AFGE, suggesting a need for these entities, to understand, embrace, and regulate AI to protect workers' interests and ensure fair implementation.
- **Legislative and Policy Advocacy:** A few responses call for changes in laws and policies to address broader issues related to workforce management and accountability, which could be indirectly related to the integration of AI in work environments.
- **Broader Ethical and Social Implications:** Some concerns allude to the wider ethical and social implications of AI, such as its impact on American values and the potential for AI to disrupt societal norms and labor dynamics.

Part 2: Impact Assessment and Implication Analysis

Introduction

AFGE members and the broader society are at a serious juncture with the ongoing evolution of this technology. For AFGE members, the immediate risk lies in the potential displacement of jobs as tasks are automated by AI. Roles traditionally filled by federal employees could be at risk, particularly entry-level positions that serve as gateways to careers in the public sector. The increasing reliance on AI for performance evaluations and the potential for algorithmic bias presents risks of unfair labor practices and discrimination, undermining job security and career advancement. This is compounded by privacy concerns, as AI monitoring of work habits intensifies.

On the flip side, the advent of AI opens up significant opportunities for AFGE members and the federation as a whole. The potential for AI to handle repetitive tasks could lead to job enrichment, allowing workers to engage in more meaningful and complex roles. AI can also improve decision-making and efficiency, offering enhanced support tools for various organizational roles. There is a chance to be at the forefront of advocating for ethical AI use that augments rather than replaces human workers, reinforcing AFGE's role as a protector of workers' rights.

For AFGE as an organization, the integration of AI poses the challenge of staying abreast of technological developments and ensuring that the union's legal strategies and organizing efforts are not undermined by flawed or biased AI systems. Yet, AI also represents a tool that can revolutionize AFGE's approach to organizing, legal research, and compliance, offering more efficient methods to support the federation's work.

Broadly for society, the implications of AI are profound. AI can enhance public services, making agencies more efficient and responsive, but there's a pressing need to manage the transition responsibly to protect public sector jobs and services. The use of AI in legislation and policymaking could lead to more efficient government but also risks creating a landscape where opaque 'microlegislation' and rapid changes challenge democratic processes and transparency.

Specifically, the federation must work to:

- Educate and upskill members to prepare for an AI-augmented workplace.
- Advocate for fair AI implementation policies that protect jobs and enhance worker capabilities.
- Develop technical expertise within AFGE to negotiate effectively with agencies as they adopt AI technologies.
- Craft robust responses to AI-induced changes in the labor market, both in organizing strategies and in legislative influence.
- Ensure that AI-generated efficiencies in the public sector benefit workers, potentially through higher wages or reduced work hours.
- Protect data privacy and security for both members and the general public as AI systems become more prevalent in government operations.

- Engage with broader society to navigate the ethical and practical implications of AI on services and democracy.

Addressing these challenges and leveraging opportunities requires a strategic, informed, and proactive approach from AFGE to harness AI's potential while safeguarding the rights and welfare of its members and the society they serve.

AI Enters the Revolution Stage

In November 2022, with the announcement of Open AI's generative ChatGPT, machine learning and AI moved from a slower evolutionary development to a revolutionary development. Some are referring to it as the latest phase of the industrial revolution. Underscoring the massive interest, the investment and business community is investing hundreds of billions of dollars in the development of new hardware and software products.

Since AI rocketed onto the scene, all manner of wild predictions have been made covering both ends of the spectrum of extreme fear to extreme optimism. There were calls for a "time out" to allow for guard rails to be developed. But with the genie out of the bottle, there was no way a "time out" was ever going to happen.

Some predictions foresee the development of AI moving over the next 50 years from controlled programmed machine learning to the development of "General Intelligence" which means AI would have the independent ability to learn and think as humans do.

Indeed, some fear that AI could develop into a "super intelligence" with little need for human beings in the future, leading to calamity for the human race. This report acknowledges this debate as a symbol of the potential power of AI. However, this report is focused on how the development of AI over the next 10 years will impact workers in general and workers that AFGE represents in the federal and DC government.

There have been all manner of predictions when it comes to the impact on workers. Some have predicted that half of all jobs will be lost due to AI. Others indicate that AI will lead to the greatest increase in productivity ever, setting the stage for increases in societal wealth.

What is clear is that AI has arrived and is here to stay. AI is still in its infancy but is likely to evolve very quickly. We believe that over the next ten years, virtually every occupation will be impacted by AI. Some jobs will be enriched while others will likely be eliminated. New jobs will likely be created. Much higher levels of worker productivity and effectiveness will absolutely be achieved.

Information on AI Impact Gleaned from Committee Research, Discussions, Other Unions

AI has the potential to negatively impact labor practices, with possibilities such as deskilling workers, eroding democracy, and infringing on workers' rights. However, there are also potentially beneficial opportunities for AI to help workers analyze data and find trends more quickly, make better decisions, automate routine tasks, and upskill work.

While it is impossible to halt the progress of technology, protecting and ensuring the dignity and respect of human workers within the context of these changes is our most important responsibility.

Warning Signs and Flaws: Digital Surveillance, Algorithms, Hallucinations, and Potential Bias

A critical theme of our work was the influence and consequences of AI surveillance and the potential biases in algorithms. Concerns were raised that AI tools, which are increasingly used in decision-making processes like hiring and firing, often reflect the systematized the biases of their training data. In effect, widespread adoption could automate the systemic discrimination we too often see in contemporary institutions.

Digital surveillance can best be described as comprehensive, continuous, instantaneous, interactive, and unavoidable. The types of data being collected by these systems can range from facts and figures to biometric, cognitive, and behavioral data. Indeed, the description was that of a privately-owned open-air surveillance state.

Concerns were raised about the emotional and health effects resulting from increased monitoring and the lack of face-to-face interaction. Survey data from CWA call center workers has demonstrated increased levels of stress, but no improvement in customer or job satisfaction as a result of AI deployment.

AI “hallucinations” refer to the phenomenon where artificial intelligence systems generate or interpret information in ways that are nonsensical or entirely disconnected from reality. This occurs primarily due to the limitations in how AI algorithms process and understand the data they are trained on. For instance, when an AI model trained on a vast dataset encounters a rare or unusual input, it may “hallucinate” by filling in gaps with irrelevant or imaginary details, resulting in outputs that can be bizarre or illogical. For instance, lawyers using AI to help draft legal briefs have seen AI invent non-existent case law in citations.

These hallucinations are indicative of fundamental flaws in AI, particularly in their understanding of context and real-world logic. They highlight the challenges in developing AI systems that can genuinely comprehend and accurately interpret the complexities of human language and the nuances of the real world. This limitation is a stark reminder of the current boundaries of AI capabilities and the need for continuous refinement and oversight in AI development.

The topic of predictive analysis and its lack of transparency was also raised, with concerns over the difficulty of holding decision-makers accountable when algorithms are involved. Similarly, the entanglement of work and life in the digital age was brought into focus, with instances such as employers gaining access to employees’ health data and social media activities.

The potential negative impact of predictive algorithms, including unfair labeling and discrimination, was discussed in the context of digital advertising and surveillance. It was pointed out how AI could be used to make the government more efficient but also how it could impact politics. It was also discussed how these efficiencies may come at the expense of government workers and a trusted pathway to the middle class for working class Americans.

We must have robust protections against algorithmic discrimination, data privacy measures, and the inclusion of human oversight and alternatives in all decision-making processes. The importance of broader public input into governance design and the need for further research into the impacts of data-centric technologies and AI was also highlighted.

Collective Bargaining Impacts

This discussion focused on several key themes around collective bargaining, labor law, and the impacts of AI on the workplace.

Workplace transformation and surveillance:
AI has the capacity to fundamentally alter workplaces and processes, leading to worker displacement. These technologies also facilitate enhanced surveillance and create new forms of supervision and management. The conversation drew attention to the question of when surveillance is considered unlawful, with specific attention on instances when it targets or discourages union activity or when its perceived benefits are outweighed by its chilling effect on such activity.

The Duty to Bargain:
A significant focus was placed on whether the introduction of AI in the workplace should trigger collective bargaining. Key considerations in this regard included whether the changes were significant, substantial, and material, and whether they represented a fundamental shift in business operations. A related theme revolved around the duty to bargain over new forms of surveillance and the right of bargaining representatives to request relevant information when new technology is introduced.

Mitigating Harmful Effects of AI through Collective Bargaining:
The discussion proposed several potential bargaining strategies, such as making broad and continuing requests for information regarding new technology and algorithms, and negotiating additional protections for employees. These could include measures such as requiring notice before the introduction of new technology or surveillance methods, promoting joint research and planning, setting limits on new technology and surveillance, protecting employee privacy, and addressing effects like displacement and training requirements.

Impacts on Specific Sectors:
Representatives from different labor organizations provided unique insights into the implications of AI and technological advancements on their respective fields.

National Nurses United (NNU) emphasized the need for technology to be skill-enhancing rather than deskill nursing personnel. There is a growing concern that heavy reliance on AI and technology may infringe on the nurses’ professional autonomy and independent judgment. Thus, NNU is reviewing all contracts to assess if they are adequate to handle the increasing influence of AI. To better equip their members, NNU is also initiating continuous education around AI and campaigns to educate the public on the potential pitfalls of AI in healthcare.

The potential effects of AI on the Administrative Law Judges (ALJs) at SSA were also discussed, with fears that automation would create AI-determinative decision making instead of AI-supported

human decision making. Another concern raised was the potential liability and lack of meaningful oversight when delegating authority to machines. There was also discussion about the potential for ALJs to lose protections under the Administrative Procedures Act if AI is deployed.

UNITE HERE presented a distinct perspective, highlighting how technology, particularly smartphones, have impacted housekeepers. Every interaction housekeepers have with these devices generate data that's useful for employers but also imposes additional workload. As part of their tech bargaining strategies, UNITE HERE has started maintaining daily logs of this extra work and used it as a basis to protect their autonomy and rights. Interestingly, the organization uses SQL and Python to analyze the data and look for potential contract violations. They've effectively automated the grievance procedure, allowing workers to raise concerns more efficiently.

WGA East expressed concerns over the use of AI in generating literary material. They argued against using AI-generated material as source material and insisted on the sanctity of human creativity and originality in the industry. Studio executives have so far balked at the demand, instead suggesting a yearly meeting to discuss new technologies.

Field Services and Education Implications

- **Technical Skill Gap:** Field service representatives will need to develop new skills to interact with AI-driven systems, suggesting a need for significant investment in training and development.

- **Enhanced Service Delivery:** AI can facilitate predictive maintenance and diagnostics, leading to more proactive and efficient field services, potentially increasing member satisfaction.

- **Policy Advocacy:** There's a critical need for AFGE to advocate for policies that govern AI use in field services, emphasizing fair labor practices and ethical standards.

- **Curriculum Development:** Educational initiatives must now include AI literacy, focusing on how AI impacts the public sector and union membership.

- **Resource Allocation:** Educators will need to determine how to best allocate resources between traditional learning methods and new AI-driven tools and platforms.
- **Workforce Adaptation:** Both sectors will need to guide their constituents in adapting to an AI-augmented workplace, which may involve reskilling and continuous learning.

- **Data Management:** The collection, analysis, and interpretation of data by AI will become more prevalent, necessitating a robust understanding of data privacy and security among both field services and education departments.

- **Regulatory Engagement:** Active participation in shaping regulations that impact AI deployment in the public sector will be critical. This involves both fields aligning their efforts to influence policy-making.

Opportunities:

- **Strategic Organizing:** Utilizing AI for data analysis can reveal insights that inform targeted organizing and educational campaigns, aligning union efforts with member needs and concerns.

- **Collaborative Learning:** Education departments can harness AI for creating collaborative learning platforms, enhancing member training and professional development.

Risks:

- **Job Displacement Anxiety:** Both fields must address the anxiety surrounding potential job displacement due to AI, providing assurance through policy advocacy and education on AI's role in augmenting jobs rather than replacing them.

- **Misinformation Control:** As AI generates content, the potential for misinformation increases, requiring stringent verification processes and member education on discerning credible information.

Organizing Implications

The challenges presented by AI advancements can be divided into external and internal factors that impact the workforce. Externally, the attrition of work to AI represents a significant shift in the labor landscape, where machines may replace human tasks, leading to job displacement. Furthermore, AI employee monitoring could introduce hyper-surveillance, scrutinizing productivity, work trends, habits, and even the nuances of remote work, potentially encroaching on personal boundaries and privacy. Additionally, AI-driven anti-union campaigns and AI-influenced Reductions in Force (RIFs) and furloughs could automate and streamline managerial decisions, often to the detriment of employees. Performance evaluations influenced by AI could lead to standardized appraisals that might not consider the unique contributions and circumstances of individual workers, while biases in AI human resources and labor-management relations could embed and perpetuate systemic discrimination. Internally, AI-produced organizing materials could suffer from poor quality, failing to capture the nuance and persuasive communication typically generated by humans.

On the flip side, these challenges present opportunities for organization and innovation. The very issues arising from AI can galvanize workers to unite and organize around the threats, turning adversity into a focal point for collective action. Organizing materials could be developed specifically to address the AI threat, educating workers on both the risks and the potential advantages. AI-based communications can streamline and personalize updates and spotlights on worker experiences and contract details, fostering a more engaged and informed membership. Organizing events can focus on practical AI applications in the workplace, highlighting ways to harness AI for positive outcomes such as efficiency and growth trend analysis. By understanding and leveraging these tools, the workforce can stay ahead of the curve, advocating for policies and practices that protect workers' interests in the age of AI.

The Human Impact of AI Tools:

The implications of AI tools in areas such as call center operations were explored, with surveys indicating that workers often found these tools stressful and did not perceive them as making their work easier or more interesting. Negative impacts included higher levels of customer abuse, increased absenteeism, higher turnover, and lower job satisfaction. The narrative of technology serving as an accountability avoidance strategy was also highlighted, leading to increased mental and physical stress among workers due to increased monitoring and surveillance.

Policy and Legislative Concerns

AI-related legislation and the policy landscape are critical areas of interest with numerous bills currently under consideration within the U.S. Congress and state legislatures. These cover issues ranging from bias and privacy to data protection and worker rights. Among these, the American Data Privacy and Protection Act stands out on a federal level. At the state level, legislation such as CT SB1103, VT H 410, DC B24-0558, AB 331 in California, the Artificial Intelligence Video Interview Act in Illinois, HB1202 in Maryland, NYC Local Law 114, AB 791 in California, SF 3035 in Minnesota, and s8992A/a.10020A in New York, all address different aspects of AI application and governance, especially in the workplace and public sectors.

Governments worldwide are placing emphasis on creating standards and certifications for AI to regulate its use. Several frameworks have been proposed and enacted, such as the EU AI Act, EU-US TTC, OECD, and G7/20. However, challenges exist due to the fluid nature of AI, the dominance of industry players in certification bodies, and the debate between a risk-based approach and a rights-based approach to AI regulation.

Bias and discrimination in AI have become major areas of concern, with fears that these technologies could perpetuate historical bias. Instances like unfair healthcare predictions and false recidivism predictions in the prison system highlight the potential societal impact of biased AI systems.

The labor market is also expected to see a profound impact due to the rise of AI, especially generative AI. Predictions suggest that a large number of jobs could be impacted and fields like administration, architecture, and law could see significant levels of automation. While there are potential positive aspects, like automation of disliked tasks, the negative implications like job elimination and shrinking job functions are worrying.

AI's rapid evolution and its ability to generate seemingly real content raises major concerns about misinformation and deepfakes. The potential for misuse in politics and by hate groups needs urgent attention and regulation.

Trade issues and global strategies around data localization rights, technology transfer obligations, free flow of data, and right out access to source code are currently contentious. Solutions that consider inclusive governance, periodic assessments, and fair representation in certification bodies are being sought.

The urgent need for AI regulations is a common theme worldwide. The Biden Administration's blueprint on AI and the EU's efforts towards regulation serve as models for what such governance could look like, emphasizing AI safety, discrimination protection, data privacy, and human alternatives to AI.

Lastly, the potential impact of AI on public sector jobs is a significant concern. High levels of efficiency brought about by AI could mean a significant reduction in government jobs, with implications for the societal fabric, particularly the middle class.

Overall, the current landscape necessitates proactive, comprehensive, and thoughtful regulations that protect societal and worker interests while allowing beneficial technological evolution. The labor movement and civil society play vital roles in ensuring that AI governance evolves in a fair and equitable manner.

Political, Legislative, Policy, and Mobilization Impacts

The advancement of AI technology presents a complex landscape for AFGE with implications for its legislative, political, and mobilization efforts. The strategic use of AI in targeting lawmakers for lobbying purposes represents a significant opportunity to enhance the efficacy of AFGE's advocacy efforts. By harnessing the analytical capabilities of AI to parse vast datasets, including voting patterns, social media interactions, and campaign finance data, AFGE can tailor communications and lobbying efforts to the individual profiles of lawmakers, potentially increasing the impact and resonance of their messages.

However, this approach is not without risks. The proliferation of AI tools may lead to a saturation of tailored messages, which could in turn cause lawmakers to become desensitized to such communications, thereby diminishing the effectiveness of traditional written advocacy. Moreover, opponents of the union, including advocates for reduced government spending and private contractors, are likely to employ similar AI strategies, possibly intensifying competition and creating a legislative arms race that could counteract AFGE's objectives.

The legislative drafting process is also poised for transformation by AI. Tools like ChatGPT and Google Bard demonstrate potential in generating legislative text, which could streamline the work of congressional staff and outside firms. However, this raises concerns about the legal accuracy of AI-generated texts and the potential for 'microlegislation' — small, targeted legislative provisions that could be drafted to benefit specific interests without broader stakeholder awareness. AFGE must prepare to utilize AI for rapidly analyzing legislative packages to identify and respond to such hidden provisions that may adversely affect federal programs and employment.

For AFGE's internal operations, the use of AI in creating written materials — from short emails to lengthy Congressional testimonies — can augment staff efforts, provided there is careful human review to ensure the accuracy and appropriateness of such AI-generated content. As AI evolves, there may be debates about its capacity for original thought versus its role in synthesizing existing human content, but the immediate reality is that AI can significantly affect AFGE's lobbying work by refining argument synthesis and stakeholder persuasion.

Externally, AI's potential to revolutionize public sector services comes with the threat of job displacement for federal employees. The capability of AI to deliver services traditionally provided by the public sector could lead to an increased push for privatization and contracting out, fueled by the current political climate that emphasizes cost-cutting and efficiency. The impact on AFGE membership could be profound, necessitating a proactive approach to advocacy for regulations governing the ethical use of AI in public service delivery.

Furthermore, the ability of AI to craft persuasive messages at scale also presents a risk of influencing AFGE membership behaviors, such as PAC contributions and union involvement. As AI-generated content becomes more indistinguishable from human-created content, the potential for mis- and disinformation increases, which could disrupt the union's internal cohesion and external advocacy.

In summary, AI offers AFGE powerful tools for legislative analysis, personalized lobbying, and efficient communication, yet it also introduces competitive pressures, risks to member engagement, and ethical considerations for content creation and legislative influence. AFGE's response must be strategic, incorporating AI capabilities into its operations while advocating for safeguards that protect the interests of its members and the integrity of public sector services.

Legal Implications

Challenges:

- **Legal Research Reliability:** There's a risk of relying on AI for legal research that may yield incorrect information, such as fictitious case law, which can have serious professional consequences.

- **Vendor Evolution:** As legal research vendors incorporate AI, there will be a need to critically assess these tools for accuracy and reliability.

- **Organizing Strategy:** AI has potential in aiding union organizing, but its application needs creative development and careful execution.

- **Compliance Automation:** While AI could potentially streamline compliance processes, it must be implemented in a way that does not compromise the accuracy or integrity of reporting.

- **Theft and Embezzlement Detection:** AI could assist in early detection of financial irregularities; however, developing and maintaining such systems requires significant expertise and resources.

- **Job Preservation:** As AI enhances productivity, there's an imperative to ensure that it complements rather than replaces human staff within AFGE.

Opportunities:

- **Enhanced Legal Research:** AI can significantly improve the breadth and depth of legal research, helping attorneys to be more efficient and strategic in their work.

- **Refined Organizing Tools:** AI could offer sophisticated methods for mapping, tracking, assessing, and mobilizing union organizing campaigns.

- **Improved Legal and Financial Compliance:** Through automation, AI has the potential to improve the accuracy of legal and financial compliance, reducing human error.

- **Proactive Financial Oversight:** AI systems could provide ongoing oversight, offering real-time alerts to potential financial mismanagement.

- **Efficiency in Operations:** AI's capability to perform routine tasks could allow AFGE staff to reallocate their time to more complex and high-value activities.

- **Internal Job Enrichment:** The adoption of AI could lead to the creation of new roles and responsibilities within AFGE, offering staff opportunities for professional growth.

Communications Implications

The integration of AI into communications presents a mix of transformative impacts for AFGE, its members, and the broader context in which they operate.

Implications for Internal Communications:

- Enhanced Efficiency: AI can automate routine communications tasks, allowing staff to focus on strategic initiatives and member engagement.
- Consistency and Professionalism: AI tools can generate consistent and professional communications materials, such as newsletters, emails, and social media posts, benefiting from uniform tone and style.
- Real-time Interaction: AI chatbots can provide immediate responses to member inquiries, leading to increased member satisfaction with the responsiveness of the union.

Implications for External Communications:

- Targeted Messaging: AI's data analysis capabilities enable the creation of highly targeted messaging for campaigns, potentially increasing their effectiveness.
- Monitoring and Sentiment Analysis: AI can monitor public sentiment and media trends, providing insights that can inform public relations strategies and reputation management.
- Rapid Response: AI can quickly generate content to respond to unfolding events, keeping the union's messaging timely and relevant.

Risks and Challenges:

- Misinformation and Disinformation: There is a risk that AI-generated content could contribute to the spread of misinformation if not properly supervised. Similarly, AI-generated "deepfake" content poses a threat to the credibility of union communications.
- Loss of Personal Touch: Over-reliance on AI for communications could result in a loss of personal touch and the nuanced understanding that comes from human interaction.

Opportunities:

- Personalization at Scale: AI enables personalization of communications to members' specific interests and needs, even as the membership size grows.

- Analytical Insights: AI’s ability to analyze engagement metrics can lead to more effective communication strategies by understanding what content performs best.
- Resource Allocation: By reducing the time spent on creating and distributing content, AI allows the union to reallocate resources to other critical areas such as member services and advocacy.

Information Systems Implications

Challenges

- **Evolving Technologies:** The implementation of AI technologies, especially in the generative AI realm, poses challenges ensuring data accuracy and reliability.
- **Privacy and Bias Concerns:** When deploying AI tools for employees and members, we must rigorously test for biases and ensure the privacy and security of member data.
- **International and Domestic Compliance:** For our European members, compliance with EU regulations, including established privacy and emerging AI regulations, is critical. Our small but significant interactions with EU members must be considered by GCO to ensure adherence to these laws. In addition, AI regulations may emerge in states or nationally that are important to keep abreast of.

Opportunities

- **Enhanced Decision Support Tools:** GPTs, fine-tuned on internal data, offer innovative support for local presidents and treasurers, aiding in information access and decision-making.
- **Conversational AI for Member Insights:** AI tools can conversationally provide membership insights, aiding in tracking financial or regulatory compliance, thus enhancing internal capabilities.
- **Efficiency in Membership Systems:** AI can enhance our membership processes, significantly improving data entry efficiency and reducing manual workload.
- **Reduction of Repetitive Work:** Generative AI tools can significantly reduce repetitive tasks, increasing productivity and allowing employees to focus on more complex, value-added activities.
- **Enhanced Member Communications:** By providing professional draft responses, generative AI can aid employees in communicating effectively with members, ensuring consistency and quality in member interactions, particularly beneficial for staff with varying communication skills.

Conclusions

In the wake of rapid advancements in artificial intelligence and automation, AFGE bargaining unit employees are poised at a crucial juncture. AI’s transformational impact could lead to a considerable shift in roles and responsibilities, particularly for those in administrative, clerical, and certain decision-making positions where AI-determinative decision-making threatens to supplant AI-supported human decision-making. Similarly, healthcare workers, including nurses, might confront significant changes as technology becomes more deeply integrated into their work environment, potentially impacting professional autonomy and judgment.

Concurrently, AI presents opportunities for enhancing productivity, decision-making, and trend analysis which could benefit AFGE members by alleviating routine tasks and opening avenues for upskilling. However, this technological revolution brings forth risks that need to be vigilantly managed. Potential discrimination in AI-driven hiring and firing decisions, biases in algorithms, and the erosion of workers' rights could undermine the core values of labor-management relations. The proliferation of digital surveillance could encroach on privacy and potentially target union activity. In the realm of collective bargaining, AI's integration into workplaces necessitates new frameworks to safeguard employee rights and to ensure that any surveillance methods employed are lawful and respect worker autonomy. AFGE must advocate for robust protections against algorithmic discrimination, maintain human oversight in AI systems, and ensure that AI tools are utilized to support, rather than replace, human workers.

The promise of AI to enhance efficiency in field services, optimize legal research, and refine educational outreach is evident. These advancements could lead to more predictive and personalized member services, improved compliance and oversight capabilities, and a more informed and engaged membership. However, alongside these opportunities are considerable challenges, including the risk of job displacement due to automation, potential biases in AI algorithms, and the need for extensive training to ensure that staff can harness AI responsibly and effectively. There is also a looming concern regarding data privacy and the ethical use of AI, which necessitates a proactive approach in policy development and member education to safeguard interests and foster trust.

As AFGE moves forward in this AI-driven landscape, it will be critical to maintain a balanced approach that leverages technology to innovate while also upholding the union's core values of worker advocacy and protection. Ensuring that AI adoption is in line with ethical guidelines and that there is transparency in its application will be key to mitigating potential risks. In parallel, AFGE must remain vigilant in advocating for fair AI-driven changes in the workplace, promoting legislation that secures members' rights in the face of automation, and pursuing initiatives that share the benefits of AI-related efficiencies. By doing so, AFGE can not only navigate the complexities of AI but also champion its potential to enhance union solidarity, worker empowerment, and the quality of public services.

Part 3: Action Plan Recommendations

Introduction

As the dawn of the Artificial Intelligence (AI) revolution beckons, a pivotal question emerges, shaping the narrative of the future workplace: Will AI's implementation be orchestrated "with workers," ensuring a quadruple win for labor, government, capital, and society? Or will it be enforced "to workers," serving only the interests of affluent capital owners while disregarding the broader societal good?

This narrative introduction sets the stage for a crucial action plan and recommendations. It underscores the pressing need for a strategic, proactive response from the American Federation of Government Employees (AFGE). History, laden with lessons of concentrated wealth's propensity to prioritize profit over people, calls upon us to act. The entertainment industry's recent confrontations, led by writers and actors, against AI displacement, echo a universal struggle for rightful compensation and representation in the face of burgeoning technology.

AFGE stands at the crossroads of change, recognizing that the nascent implementations of AI, as reported in departments like HUD, VA, and Global Media, are but the harbingers of a swift and expansive evolution. With AI's trajectory set to surge within the next decade, there's an undeniable urgency for AFGE to craft a strategic plan that not only keeps pace with but also directs AI development towards serving the common good.

The time for AFGE to craft and enact this plan is now — to establish a centralized hub for information on government-wide AI activities and to galvanize the labor movement for a collective voice in the AI arena. This proactive approach will enable AFGE to shape the implementation of AI in ways that protect our members' interests and uphold the mission-driven services they provide to the American people.

The following section lays out recommendations for actions AFGE should take along each vector of the federation's responsibilities.

Recommendations

Ongoing AI Development and Monitoring – Establish AFGE AI/Technology Institute:

- **Establish an AI Hub/Institute to stay ahead of AI developments and implementations and ensure AFGE has comprehensive knowledge of ongoing and forthcoming AI and technology changes in government agencies.**

  - **Dedicated Resources:**
    - Allocate dedicated staff focused on understanding AI impacts on AFGE members and developing AI strategy.
    - Maintain a shared database of critical AI-related information for the union.
    - Create a centralized hub for AI within AFGE, possibly named AFGE's AI/Technology Institute, to last for at least 10 years.

  - **Operational Structure:**
    - Operate the AI/Technology Institute under the direction of the National President (NP).
    - Coordinate efforts with the National Executive Council (NEC), Districts, other Departments, Councils, Locals, and AFGE employees.

- Acquire new set-aside funding from the NEC or Convention for operational needs.

- **AI/Technology Forums, Conferences:**
  - Establish forums or conferences comprising AFGE members who are experts in AI, technological change, and AI/Technology collective bargaining and enforcement.
  - Utilize these forums to enhance AFGE's union-wide knowledge and expertise in AI, engaging member-experts in evaluation of legislation, policy.

- **Collaborative Engagement:**
  - Have the AI/Technology Institute staff engage with AFL-CIO Institute, other unions, academic resources, and non-profits for knowledge exchange and action planning on AI regulations and enforcement.

- **Government Agency Liaison:**
  - Assign Institute staff to liaise with key government agencies for staying informed and influencing AI/Technology policy.

- **Corporate Contract Influence:**
  - Strategize to be involved in the pre-decision stages before corporate AI contracts are secured by the government.
  - Utilize OMB draft guidance on inventory, pilot testing, and impact studies to inform strategic involvement in contract considerations.

External Operations:

Lobbying and Policy Development:

- **Employ AI for targeting strategies in lobbying efforts.**
  - Develop an AI system that analyzes legislative voting records, public statements, and other relevant data to identify lawmakers who are most likely to support AFGE's position, allowing for more targeted and effective lobbying strategies.
  - Use AI-driven sentiment analysis on social media and news outlets to gauge the public and political mood, providing insights that can refine messaging and advocacy approaches to align with current trends and values.

- **Leverage AI to develop legislation and monitor large legislative packages.**
  - Implement AI tools capable of drafting legislative language and reviewing legal documents to assist in the creation of comprehensive and compliant legislative proposals.
  - Use AI to continuously scan and analyze the contents of omnibus bills and other large legislative packages for clauses and provisions that may affect union members, ensuring timely and informed responses to potential challenges.

- **Establish ethical standards for AI-generated materials.**
  - Formulate a union-wide policy on the ethical use of AI in content creation, which includes guidelines on transparency, accuracy, and accountability, ensuring all materials meet high standards of integrity.
  - Introduce a review process where AI-generated content is routinely checked by human experts before publication to maintain trust and authenticity in all communications.
  - Ensure such standard protect the rights of federal employees against having their likeness, voice, other private data used without their consent.

Member Engagement:

- **Educate members about AI and its potential impacts.**
  - Organize educational campaigns and workshops to inform members about how AI works, its benefits, and potential risks, empowering them with the knowledge to embrace technology confidently. Incorporate into ongoing trainings and conferences.
  - Provide resources and learning materials that cover real-life examples of AI impacts on employment, privacy, and union operations, fostering a community that is well-informed about AI developments.

- **Use AI to analyze growth trends for better member service.**
  - Implement data analysis tools powered by AI to identify patterns in membership engagement and growth, which can inform targeted strategies for member recruitment and retention.
  - Deploy AI to track and predict service demand across various departments, ensuring that resources are allocated efficiently to meet member needs promptly.

Communication and Outreach:

- **Enhance AFGE communications using AI-generated content and analysis.**
  - Utilize AI to craft precise and personalized messaging for different member segments, as well as various issues and potential issues, ensuring relevance, preparation, and higher engagement rates.
  - Incorporate AI-powered analytics to measure the effectiveness of communication campaigns, enabling data-driven decisions for future strategies.

- **Develop a coherent message on AI for different councils and locals.**
  - Establish a centralized AI messaging framework that can be localized, ensuring consistency across all levels of the organization while allowing for region-specific adaptations.
  - Provide training and resources to council and local leaders on the key points of AFGE's AI stance to maintain a unified voice when discussing AI-related topics with members.

- **Create AI-assisted communication tools for local communicators.**
  - Develop AI-based templates for routine communications, such as meeting notices and updates, to streamline the creation process for local union leaders.
  - Integrate AI tools that suggest content improvements, such as readability enhancements and language simplification, to aid local communicators in refining their messages.

- **Create dedicated web pages and newsletters for AI-related updates.**
  - Launch specialized web portals featuring the latest AI news, educational materials, and the impact of AI on union members, providing a one-stop source of trusted information.
  - Curate a regular newsletter that distills complex AI concepts into accessible summaries, keeping members informed and engaged with the latest AI developments.

- **Conduct surveys to gauge leader and member perspectives on AI.**

  - Design comprehensive surveys to capture insights on members' awareness, concerns, and expectations regarding AI, helping to shape AFGE’s AI policies and communication.

- Analyze survey results with AI to identify trends and areas needing attention, thus tailoring education and support services to member needs.

- **Foster engagement of members and potential members on AI topics.**
  - Organize interactive forums and Q&A sessions facilitated by AI systems to allow real-time member engagement on AI discussions.
  - Launch an AI-focused outreach campaign featuring webinars and virtual meetups that inform and solicit feedback on how AI is reshaping the workplace and the union’s response.

Representation - AFGE as the Leader in AI:

- **Host conferences to discuss AI’s impact on the workforce.**
  - Facilitate annual or biannual conferences bringing together experts, union members, and industry leaders to discuss the latest AI developments and their practical implications for labor and employment.
  - Provide workshops at these conferences that offer hands-on experience with AI tools and discussions on how AI changes job roles and the skills required for future jobs.

- **Advocate for collective bargaining and partnership engagements related to AI.**
  - Formulate negotiation strategies that include AI-related clauses in collective bargaining agreements, ensuring workers’ rights are protected as AI integration progresses. (See Appendix I for more).
  - Encourage the establishment of joint labor-management AI committees to ensure transparency and fairness in the implementation of AI technologies.

- **Gain access to AI inventories, impact studies, and pilot testing to inform bargaining, particularly for displaced workers.**
  - Negotiate for union representation on committees that oversee AI inventories and impact assessments within government agencies or private companies.
  - Implement a system for monitoring and evaluating the outcomes of AI pilot programs to prepare for and address the implications of workforce displacement in bargaining processes.

Policy Impact and Analysis:

- **Explore policy changes such as reduced work weeks, improved pensions, and wage structures to protect workers and agency missions.**
  - Investigate the potential for AI-driven efficiency gains to translate into reduced work hours for employees without loss of income, thereby improving work-life balance and job satisfaction.
  - Analyze the long-term benefits of adjusting pension plans and wage structures to ensure that workers are adequately compensated for AI-induced changes in job roles and requirements, e.g. by upskilling workers as routine tasks become automated and human work becomes more complex.

- **Utilize AI for data analysis and predictive modeling.**

- Apply AI algorithms to analyze membership data and predict trends in labor needs, helping to guide strategic decisions on worker training and development programs.
- Use predictive modeling to anticipate the impacts of economic and policy changes on employment, equipping the union with data to support advocacy efforts.

- **Implement AI tools for policy impact assessment.**
  - Integrate AI systems capable of simulating the effects of policy changes on worker demographics, job security, and union representation, allowing for evidence-based advocacy.
  - Employ AI-based scenario analysis to evaluate the potential outcomes of new regulations or policies, ensuring the union can proactively respond to protect its members' interests.

Implementation of AI for case management efficiency

- AI application to sort through extensive policy documents, identifying pertinent information for case assessments, identifying potential solutions and initial evaluation for local stewards.
- Ongoing pilot program at a VA local serves as a model, demonstrating AI's capacity to assist stewards with case preparation and strategy.

- **Use NLP for document analysis and automation of repetitive tasks.**
  - Harness NLP to streamline the processing of large volumes of text-based data, such as member feedback or legal documents, making information extraction more efficient and less labor-intensive.
  - Implement AI-driven systems to perform routine tasks such as data entry, scheduling, and report generation, freeing up staff to focus on higher-value strategic work.

Union Organization and Advocacy:

- **Organize around AI-related workplace threats.**
  - Conduct analysis and engage in ongoing monitoring of emerging AI-related risks in the workplace, and use these insights to organize targeted campaigns to address these threats, mobilize existing members, and organize new members.
  - Host workshops and training sessions that equip members with the skills to identify and advocate against unfair AI practices in their workplaces.

- **Leverage AI for membership segmentation and predictive analytics.**
  - Implement AI systems to segment the membership base by various factors like job type, demographics, or risk of AI impact, enabling personalized outreach and support.
  - Use predictive analytics to forecast shifts in the labor market and union membership, preparing the union to adapt its organizing strategies in advance.

- **Address AI-driven anti-union campaigns and potential job attrition.**
  - Monitor and counteract anti-union messaging amplified by AI tools through the development of rapid response protocols and strategic communication campaigns.
  - Analyze trends and patterns in employment data to anticipate job attrition risks due to AI, and create contingency plans for workforce and member support.

- **Advocate for responsible AI integration in government agencies.**
  - Promote transparency and accountability in government agencies' use of AI, ensuring that any integration of AI technologies is in line with ethical standards and workers' rights.

  - Engage in policy dialogue and provide recommendations on the responsible use of AI in public services, emphasizing the protection of jobs and the quality of services provided to the public.

Workforce Training on AI:

- **Educate members on AI implications for career trajectories.**
  - Develop a series of educational materials and webinars that outline potential career paths and changes in skill requirements due to the advent of AI, enabling members to plan and adapt their career plans proactively.
  - Provide case studies and real-world examples of how AI is transforming different sectors, helping members to understand the practical impact on their current and future job roles.

- **Offer reskilling and retraining opportunities to preempt potential reductions in force (RIFs).**
  - Partner with educational institutions and online learning platforms to provide members with access to courses and certifications in AI literacy and other future-focused skills.
  - Establish a career transition program within the union that assesses individual member skills, provides personalized reskilling pathways, and offers support in finding new opportunities within or outside their current field of work.

Enforcement and Advocacy:

- **Utilize grievances and litigation to enforce fair AI implementation.**
  - Assign team of relevant staff to research and understand AI-related changes in the workplace and formulates strategies to address unfair labor practices through grievances and litigation.
  - Train union representatives to identify contract violations related to AI implementation, ensuring that any deployment of AI technology adheres to existing collective bargaining agreements and workers' rights.

- **Challenge AI system flaws, including biases, discrimination, and inaccuracies.**
  - Invest in expertise to audit AI systems for bias and discrimination, and use findings to negotiate for fairer AI practices and systems that do not perpetuate workplace inequalities.
  - Establish a reporting mechanism for members to raise concerns about AI inaccuracies and biases, which can be used to build cases for improvements or the removal of flawed AI systems.

Leveraging AI for Data Analysis:

- **Use AI tools to extract insights from government databases on health, safety, and discrimination issues.**
  - Deploy advanced data mining and analytics AI to sift through extensive government databases, identifying patterns and key issues in health and safety violations that could affect union members.
  - Implement AI-driven natural language processing to monitor and review discrimination case reports, aiding in the rapid identification and response to systemic issues affecting members in the workplace.

Internal Operations:

Technology Integration and Pilots:

- **Implement low-risk pilot projects to explore AI applications:**
    - Rapidly test the potential of AI to improve operational efficiency and member services without significant upfront investment.
    - Use pilot projects to learn and adapt AI integration strategies, minimizing risk and preparing for broader rollouts.

- **Utilize Microsoft AI and OpenAI technologies, with a focus on quality and security:**
    - Leverage the advanced features and ongoing support from Microsoft's AI suite and OpenAI to ensure high-quality, secure solutions for AFGE's needs.
    - Prioritize technologies that are known for robust privacy policies and secure platforms to protect member data integrity.

- **Continue development and testing of AI tools like Microsoft Document Intelligence, AFGEMentor, and AFGELocalFinder:**
    - Develop AI tools tailored to specific union needs, like automating form processing with handwriting recognition for improved efficiency.
    - Enhance member support and engagement through conversational AI, providing real-time assistance and information to local union leaders and members.

- **Explore and understand the capabilities and limitations of LLM technologies:**
    - Investigate the advanced functionalities of LLMs for applications in natural language processing, document generation, and decision support.
    - Conduct thorough testing to identify any limitations or biases in LLM technologies to ensure responsible and ethical use within the union's operations.

Improving AFGE's Effectiveness and Efficiency:

- **Develop AI solutions to provide timely responses to queries and assistance requests.**
    - Design and deploy AI-driven chatbots to handle routine member inquiries, ensuring fast and accurate dissemination of information and freeing up staff for more complex issues.
    - Establish an AI-assisted internal knowledge base that allows for natural language querying, making it easier for staff and members to find information quickly and efficiently.

- **Implement AI tools for administrative tasks like drafting grievances.**
    - Create an AI system that can draft initial grievance documents by extracting relevant details from a database of past cases and member inputs, streamlining the grievance filing process.
    - Use AI to identify patterns and commonalities in grievances to assist in developing more effective bargaining strategies and proactive measures for workplace issues.

Training and Development:

- **Develop focused training programs for staff on AI technologies.**

  - Design a curriculum that covers AI basics to more advanced applications, ensuring staff across all levels have the knowledge to utilize AI tools relevant to their daily tasks.
  - Prioritize collaboration with other unions, nonprofits, and advocacy groups to gain a broader perspective on AI's impact in various sectors and incorporate diverse, real-world scenarios into training.

- **Educate staff about ethical AI usage.**
  - Integrate training on the ethical implications of AI, including bias detection, data privacy, and the importance of transparency in AI-driven decisions, to promote responsible AI deployment in union activities.
  - Establish a code of conduct and guidelines for ethical AI use within the organization, ensuring staff understand how to employ AI in a manner that aligns with AFGE's values and the welfare of its members.

Internal Policy and Governance:

- **Actively encourage staff participation in shaping internal AI policies.**
  - Form an interdisciplinary AI policy committee with representatives from various departments to ensure diverse perspectives are included in policy formulation, and develop comprehensive guidelines that address the nuanced implications of AI across different sectors of the union.
  - Conduct regular policy review sessions to assess the impact of AI policies on staff workflow, member services, and union operations, and to stay aligned with evolving legal standards and technological advancements.

- **Encourage cross-departmental collaboration on AI initiatives.**
  - Initiate cross-departmental AI projects to leverage the unique expertise of different teams, fostering innovative solutions and a cohesive approach to AI challenges and opportunities within the union.
  - Establish a shared digital platform for inter-departmental communication that promotes the exchange of AI resources, findings, and best practices, encouraging a culture of knowledge sharing and collaborative problem-solving.

Legal Research and Compliance:

- **Warn staff against undue reliance on AI for legal research.**
  - Conduct informational sessions to highlight the limitations of AI in legal research, emphasizing the importance of human oversight in verifying the validity and relevance of legal citations and case law.
  - Develop a checklist or guidelines for staff to cross-reference and validate the information provided by AI tools against official legal databases and resources.

- **Test AI tools developed by legal research vendors.**
  - Set up a pilot program with a control group to assess the accuracy and efficiency of AI tools in legal research compared to traditional methods.
  - Create a feedback loop where legal staff can report discrepancies or errors found in AI-generated legal research to improve the AI models through iterative training.

- **Use AI to improve legal compliance and reduce the risk of theft/embezzlement.**
  - Implement AI-driven analytics to identify patterns and anomalies in financial records that could indicate fraudulent activities, enhancing the union’s preventative measures against theft.
  - Integrate AI into the auditing process to continuously review financial transactions and flag irregularities for immediate investigation.

- **Utilize AI to monitor local legal fiduciary requirements and flag potential audit needs.**
  - Deploy AI systems capable of tracking and analyzing compliance with legal fiduciary requirements across all local chapters, ensuring timely adherence to regulations.
  - Use predictive AI models to forecast potential areas of non-compliance, allowing for proactive remedial action and training where needed to avoid fiduciary breaches.

Staff Jobs and AI:

- **Find ways AI can enhance productivity without cutting jobs.**
  - Identify repetitive and time-consuming tasks that can be automated by AI, allowing staff to redirect their focus towards strategic initiatives and complex problem-solving, thus enhancing job satisfaction and productivity.
  - Introduce AI as a tool to assist employees, not replace them, by providing training for staff to work alongside AI, thereby upskilling the workforce and creating new opportunities for growth within the union.

Member Services Improvements:

- **Utilize AI for automated content generation and personalization in the Graphics Department.**
  - Implement AI-driven design tools to rapidly generate and iterate on visual content, allowing for tailored graphics that can respond to member feedback and engagement metrics.
  - Personalize member communications by using AI to segment audiences and customize graphics according to the preferences and interests identified through data analysis.

- **Implement AI for print automation and predictive maintenance in Printing Operations.**
  - Deploy AI systems to streamline the workflow in printing operations, reducing lead times and minimizing manual errors in print jobs.
  - Use AI to monitor printing equipment performance in real-time, predicting maintenance needs to prevent downtime and extend the lifespan of printing hardware.

- **Integrate AI to optimize the Mailing Operation.**
  - Apply AI algorithms to manage mailing lists more efficiently, ensuring that communications are targeted and reducing waste in mailing operations.
  - Enhance sorting and delivery processes with AI to optimize logistics, track member engagement through mailed content, and provide actionable insights for future campaigns.

Building Services Management:

- **Use AI for predictive maintenance in building services.**
  - Integrate AI systems to analyze equipment performance data in real-time, predicting when maintenance is needed to prevent downtime and extend the lifespan of building infrastructure.
  - Develop a schedule optimization program using AI to efficiently allocate maintenance tasks, ensuring resources are used effectively and maintenance is conducted with minimal disruption to services.

Conclusion

AFGE must proactively approach the implementation of AI with foresight and strategic planning. The potential for AI to redefine the landscape of federal employment and union operations is significant, carrying with it the dual promise of efficiency and the risk of displacement. As such, AFGE must be an important voice in shaping the future of AI in the workplace — one that is inclusive, equitable, and reflective of the collective interests of labor, government, and society.

The union will also need to strengthen its internal operations through technology integration, AI pilot programs, and training initiatives that empower staff with the skills to harness AI ethically and effectively. With an eye on legal compliance and governance, AI tools can be utilized to enhance legal research, improve communications, enhance representation, and assist union staff in representing and safeguarding the rights of AFGE members.

By embodying the role of an informed, involved, and innovative participant in the AI dialogue, AFGE will ensure that AI development aligns with the ethos of a democratic society, where technology is harnessed not just for economic gain but for the betterment of all — a future where AI is implemented “with workers,” and not “to workers,” remains the steadfast goal.

Appendix I – Model Contract Language Proposal, Request for Information Template

Model Language on AI Negotiation Proposals

General

1. The Parties agree that AI will be used to augment, not replace, the work done by the bargaining unit employees.

2. The Parties agree the Agency will provide bargaining unit employees with an annual notice of what information is collected, how it will be used, how it can impact bargaining unit employees, what legitimate business purposes it serves, and how the Agency will ensure that the information is accurate.

3. The Parties agree that all use of AI in the Agency has a more than de minimis impact on the conditions of employment of bargaining unit employees.

4. The Parties agree that bargaining unit employees should be fully involved in the design and development of AI program(s) that they will be required to use.

5. The Agency will engage the Union in pre-decisional involvement concerning the introduction of AI, including any pilot program(s) that impacts conditions of employment. This involvement will begin when the Agency begins internal discussions about the possible use of AI.

6. The Parties agree that any use of AI impacting the conditions of employment of bargaining unit employees must be run as a pilot program before being implemented Agency-wide.

7. The Agency agrees to engage in negotiations to the fullest extent possible by law, rule, regulation, and executive order with the union concerning the substance, impact, and implementation of the pilot program(s).

8. The duration of AI Pilot programs will be one full year and will be evaluated at the end of that year for: efficiency, cost effectiveness, accuracy and impact on the working conditions of bargaining unit employees.

9. The pilot program(s) may be extended for an additional term of one year or subject to collective bargaining in a term or mid-term agreement.

10. The Parties agree to create an AI committee that shall include one or more Union representatives but shall at least have an equal number of union representatives as there are Agency representatives.

11. The AI committee shall evaluate the pilot program(s) and have access to all relevant data to accomplish that task. The AI committee shall also make recommendations where it finds necessary improvements need to be made to the pilot program(s).

12. Union participation in the AI committee does not waive any bargaining rights held by the union.

13. Annually, the Agency will provide the Union President with a list of all uses of AI throughout the Agency, specifically noting which uses are directly connected with bargaining unit work.

14. The Parties agree that due to the potential of negative impact to bargaining unit employees, AI will not be used to create performance reviews of bargaining unit employees.

15. The Parties agree the Agency must disclose any data created by AI that was used in evaluating a bargaining unit employee's performance.

16. AI will not be used in place of a deciding official in either disciplinary or adverse action decisions or to communicate with bargaining unit employees about either disciplinary or adverse action decisions.

17. The Parties agree the Agency will provide basic training for all bargaining unit employees on how AI works and how it being use in the workplace.

18. The Parties agree that when new AI program(s) are implemented, the Agency will provide training on use of the AI program(s) to bargaining unit employees and one or more Union representatives.

19. The Parties agree that training in the use of Agency AI program(s) will be open to bargaining unit employees both already using the programs and employees who may be required to use the program(s) in the future either in their current position or any future position in their job series.

20. The Parties agree that employees whose use of AI program(s) as part of their essential functions will be given at least six months to become fully successful in the use of the AI program(s). If an employee is not fully successful after the initial 6-month period, they will be provided an additional 6-month period which will include additional training and/or mentoring in areas they are not fully successful.

21. The Parties agree that it is best practice for Agency officials, who conduct annual performance evaluations, to receive training on the AI program(s) used by the bargaining unit employees before they can evaluate bargaining unit employee(s) use of the program(s).

22. The Parties agree that AI program(s) will not be used in the evaluation process for hiring bargaining unit employees unless the Agency has completed an impact assessment showing that the AI program(s) will not lead to unbiased selections (i.e., EEO disparate impact issues) and that the selections will reflect all rules applicable to federal hiring (e.g., veterans' preference or diversity goals). This assessment will be made available to Union representatives.

23. The Parties agree that the Agency will conduct an impact assessment annually on AI program(s) used in the evaluation process for hiring bargaining unit employees to ensure that the program(s) remain unbiased and that selections reflect all rules applicable to federal hiring (e.g., veterans' preference or diversity goals). This assessment will be made available to Union representatives.

24. The Parties agree not to synthetically reproduce the voice and/or likeness of a bargaining unit employee for any use.

25. The Parties agree that any use of AI augmented evidence produced in a disciplinary or adverse

action will be disclosed to the employee prior to the issuance either a proposal for disciplinary or adverse action or the issuance of a disciplinary or adverse action.

26. The Parties agree that, before the Agency contracts, or begins the process of contracting, for any service which includes AI, the Agency will make a written determination that the services do not include any amount of work currently or last performed by bargaining unit employees. The written determination should be made available to the Union and included as part of the official contract file required by Federal Acquisition Regulation (FAR) Part 4.803.

Model Request for Information Template for AI from Field Services

Date:
From: *Name and title of Union Officer*
To: *Name and title of Agency official*
Subject: Request for Information

1. This is a request for information by AFGE *local or council number*_____ in connection with its representational duties, pursuant to 5 U.S.C. Section 7114(b)(4). Information requested in this correspondence will provide adequate and effective representation, determining whether a grievance should be filed, or whether other actions (e.g., unfair labor practices) may be appropriate in accordance with applicable laws, rules, regulations, and policies from higher authority. The Union requests that the information be provided within 14 days of receipt.

2. Particularized Need: AFGE has a particularized need for the information requested in order to analyze the Agency's use of Artificial Intelligence (AI) programs and their impact on the conditions of employment of bargaining unit employees. This analysis will allow the *local/council* to (a) Adequately determine whether the Agency has misapplied laws, rules, regulations, agency policies, executive orders, and the collective bargaining agreement in its use of AI and the impacts on the conditions of employment of bargaining unit employees; (b) Adequately prepare for both substantive and Impact and Implementation negotiations regarding any changes the *name your agency* has made to conditions of employment of bargaining unit employees.

3. Information Requested: AFGE *Local or Council number*___ request a copy of all records, from the last two years within the Agency's statutory requirement responsive to the following:

    a. A list of any AI program(s) currently being used or that the agency has decide to implement but is noy yet being used in performing agency functions or managing the work force.

    b. Description of the work done by the AI program(s), the data collected, and the occupational codes of employees in related functions.

    c. Names and version or edition number(s)s of the AI program(s).

    d. The dates the Agency began using or intents to start using the AI program(s) and any rollout schedules.

    e. Any vendor or other third-party guidance provided to the Agency on the use of the AI program(s).

f. Any Agency guidance, policies, or practices on the use of the AI program(s)

g. Names of any bargaining unit employee(s) who have been educated on the AI program(s).

h. When bargaining unit employee(s) were educated on the AI program(s)

i. Scheduled education sessions for bargaining unit employees and/or supervisors on the AI program(s).

j. Names of any supervisor(s) who have been educated on the AI program(s).

k. When supervisor(s) were educated on the AI program(s).

l. A copy of the contract(s) between the Agency and the vendor providing the AI program(s). Specifically, any contract(s) that contains a liability waiver between the parties.

4. If any of the information requested is denied in whole or in part, please inform the Union, in writing, the name, position title and grade of the official making the decision and the specific statutory, regulatory, or contractual citation(s) which the decision is based.

5. Partial/Denial. In the event you deny any portion of the request, please provide the remaining information.

6. Possession. If any material responsive to a particular request is known to exist, but is not currently in the agency's, custody, or control, please identify the material and the person or entity who has possession, custody, or control thereof.

7. Please provide the Information Requested to __________ at ______________.

8. AFGE retains the right to submit further information requests if the need for more information arises. If you have any questions concerning this matter, please do not hesitate to email _________ at ______________

Brian DeWyngaert GovExec Article on AI in Federal Government

Want successful integration of AI at federal agencies? Engage employees through the unions

COMMENTARY | AI will bring dramatic, disruptive, productive changes that can improve how the work of government is carried out over the next 10 years. To prepare for it, organizations will need to learn together and plan together.

JULY 19, 2023

By Brian DeWyngaert Sr.
The Age of AI has arrived with the recent release of ChatGPT. Earlier this month, OPM released a memorandum with initial instructions on the AI in Government Act of 2020. AI will bring dramatic, disruptive, productive changes that can improve how the work of government is carried out over the next 10 years. But this could also mean serious technological failures leading to poor results and wasted dollars as well as negative consequences for employees. Will these AI developments be led, managed and planned via decision-making processes that lead to effective outcomes for the mission of the agency and for the employees who are tasked to carry out the mission?

Not only will AI introduce significant changes over the next 10 years, it will do so at a rate of speed that will be faster than prior technological changes. For this reason alone, successful organizations will need to learn together and plan together from this moment forward. The general talk of AI replacing employees is constantly in the media. This will absolutely make the workforce nervous and fearful about their own careers and livelihoods. The employees will want to know whether the coming changes will augment them to make them more effective in their job or simply replace them. This anxiety will need to be addressed in a positive way and constantly if the AI changes are to be implemented smoothly. The employees will need training in some cases and reskilling in other cases. Taking care of the agency's people must be priority number one alongside technological adoption if the leadership wants the changes to be successful.

There are 1.2 million federal government employees represented by employee unions across most agencies. Non-management employees are proud of their agency mission and their personal contribution in the same way managers and leaders are. These same employees have valuable first-hand front line knowledge and wisdom (that management often does not) on how the work gets done. This knowledge should not be overlooked and ignored when work is redesigned or new technologies and automation are brought into the workplace. If the agency leadership and management make decisions in a vacuum, the outcome is usually flawed implementation and less than desired results. If there is a union representing the employees and the interests of the employees are ignored as well, one can add conflict to the mix. Unfortunately, this path is chosen all too often for a variety of reasons.

With the coming transformations in technology and work redesign, the path to success will come through engaging the employees through the full engagement of the employees' union. It is important to recognize that the union is the collective voice of the employees and that the employees choose their representatives who will interface with management representatives. Thus to successfully engage the employees, the labor management process between management and the union should be based on a “full engagement framework.”

What does this mean and what does it look like?

It starts with the very basic premise that management and non-management employees are partners in the successful performance of the mission of the agency. The mission cannot be successfully achieved by management without the non-management employees and vice versa. Sounds too simple to even think about – right? Wrong. This principle is fundamental to how one approaches the decision-making process and the engagement of both employees and their union. Engagement with employees is most successful when managerial employees and non-managerial employees recognize that they are partners in achieving the mission of the agency. It is nearly impossible to truly engage the employees if management does not adhere to this fundamental principle.

When former President Clinton and Vice President Gore made Reinventing Government a key objective, AFGE proposed a new and different approach in labor management relations based on the concept that management and non-management employees were partners in the successful outcome of the mission. After months of dialogue, President Clinton issued Executive Order 12871—Labor-Management Partnerships on Oct. 1, 1993. The preamble stated:

The involvement of Federal Government employees and their union representatives is essential to achieving the National Performance Review’s Government reform objectives. Only by changing the nature of Federal labor management relations so that managers, employees, and employees’ elected union representatives serve as partners will it be possible to design and implement comprehensive changes necessary to reform Government.

Partnership properly reflected that the non-managerial employees are as committed to and vested in the success of the mission of their agencies as the managers. While both groups have different perspectives, different information and experiences, different interests and different roles and responsibilities, they are joined together in achieving the mission. Neither can achieve the mission without the other. As Vice President Gore was fond of saying, when two people are in a rowboat together, it isn’t helpful to simply say to the other person, that your end of the boat is sinking. Success or failure depends on their ability to engage together as partners.

Many old school agency leaders, operational managers, labor relations specialists and even some union leaders howled and verbalized their inability to accept the concept as they felt very threatened by the concept. However, there were a number of leaders/managers who saw the value and wisdom of engaging with their employees through the employees’ union in this different approach.

Engagement based on the partnership concept does not mean giving up the respective interests or the respective responsibilities from either side. Management has interests and responsibilities and so do the union representatives. It is precisely the pre-decisional dialogue around the intersection of those interests, the open sharing of information, the shared vision of the mission, the shared analytics and the shared planning that leads to better decisions with faster and fuller implementation due to upfront engagement and buy-in from the workforce. That is full engagement.

Two quick stories following the issuance of the Executive Order on Labor-Management Partnerships are worth sharing.

The U.S. Mint was a total disaster of an agency at the time. Mission accomplishment was a failure. The agency was losing money instead of making money. Its reputation for making highly collectible coins was in severe distress. These are manufacturing plants. They had antiquated equipment and technology.

On the employee state of affairs, the agency had a highly disgruntled workforce with high numbers of safety and health violations and injuries, EEO complaints, grievances and Unfair Labor Practice complaints. The Clinton administration appointed a new director who decided to use the new executive order to its full extent. He pulled together all his key managers and the AFGE union representatives for a joint strategic review and planning session. One of the top operational managers objected to the joint partnership approach and left the agency.

The strategic planning team's final plan was a complete overhaul and transformation of the agency. Everyone remembers the multi-year rollout of the new quarters minted for each state. The idea for the new coin venture, which came from this joint strategic review and planning effort, was key to the Mint's return to credibility and profitability. Investments in new technology, plant equipment and training reestablished the production quality of collectible coins thereby restoring both the desirability of collectible coins and the profitability of the Mint. The parties set up systems to jointly review and resolve all of the workforce's outstanding complaints and issues. The outcome was probably the quickest and most dramatic turnaround of an agency ever.

The second story is about Crane Naval Base, which is located in the land locked state of Indiana. Among various functions, it was a warehouse supply center. Management wanted to adopt some new technologies to automate the taking of supplies off the shelves for shipment. This would create a few new jobs but would also eliminate more jobs than it would create.

The base Commander decided to approach this difficult transformation in a full engagement/ partnership with the union. Clearly, the union/employees' concerns centered on their desire to keep working to provide for their families. The Commander was open to using the special authorities under the law and the executive order to negotiate special arrangements with AFGE that guaranteed the employees other jobs on the base with reskilling and no loss in pay. Some of the provisions may have bumped up against normal regulations, but the contract was key to the automation change.

The union and management came to the table with different perspectives and interests. Instead of management trying to drive the change with little regard for the union/employee interests or declaring key topics and proposals as non-negotiable under the law, they worked it out in a pre-decisional full engagement fashion to the satisfaction of both. It was a win-win allowing for the automation to take place in a timely fashion, for the employees to maintain their livelihoods and for the base to maintain a committed workforce who felt they were partners in the mission and not just capital costs to be reduced. The morale of the entire base workforce was uplifted instead of destroyed.

These two stories demonstrate the power of labor management engagement based on the partnership concept. With the very challenging age of AI upon us, the only path to success over the next 10 years is through the full engagement with the employees' union based on the partnership concept. But you don't have to wait for AI to engage as partners. It is the right approach each and every day. Agency management can see continuous improvements in operational performance and the employees will feel engaged and part of the team.

Brian DeWyngaert Sr. is the retired chief of staff and assistant to the president of AFGE, where he worked for 43 years. He has a bachelor's in Business from Georgetown University and a master's in Public Administration from the University of Baltimore.

Appendix II – Background Materials

2023-24 AFGE ARTIFICIAL INTELLIGENCE (AI) COMMITTEE CHARTER

PURPOSE OF THE AI COMMITTEE:
To proactively shape the future of work in a manner that champions the human workforce and ensures that advancements in AI enhance work, help human workers, and deliver the productivity gains to our working members.

RATIONALE:
The National President is establishing the AFGE Artificial Intelligence Committee ("the Committee") to help the federation better understand, prepare for, and respond to the implications of artificial intelligence (AI) on AFGE and its members. The Committee will conduct research and develop a comprehensive report, AI strategy, and action plan to be submitted to the National President. This document should assess the potential impacts of AI on AFGE-represented employees, units, and jobs, and determine proactive measures to recommend to the National President in order to safeguard our members' rights and interests.

MEMBERSHIP/SMEs:

- Ex - Officio: Everett Kelley, National President
- Chair: Tatishka Thomas, National Vice President, District 5
- Members: Diana Hicks (NEC), Ruark Hotopp (NEC), Edwin Osorio (Local 3369), Dave Bump (NVAC), Brittany Coleman (Local 252 DOE), Damien Luviano (Local 1739/NVAC), Yvonne Renee Evans (District 7 Coordinator)
- Staff: Andrew Huddleston, Brian DeWyngaert, Tracie St John, Anitha Vemury, Taylor Higley, Jeff Sievert, Richard Loeb, David Borer, others as needed to support the committee's work.

FUNDING AND SUPPORT:

- Sufficient resources will be devoted to support the effective function of the Committee, including the assignment of support staff by the Chair to take minutes and handle administrative tasks.
- The committee will be provided reasonable access to AFGE documents and materials that may be required to do their assigned tasks.
- The Committee shall actively engage with AFL-CIO Technology Institute and AFL-CIO-sponsored roundtables. These partnerships will enable the exchange of strategies, insights, and knowledge. The Committee will also coordinate as-needed with member-leaders and outside AI experts for continual learning and improved understanding.

GOALS/OBJECTIVES/MEASURES OF SUCCESS:

- Members of the AI committee commit to supporting this work.
- Deliver specific recommendations for consideration by the National President.

KEY ISSUES TO ADDRESS:

- **Exploration & Understanding**: Understand the nature of AI, its capabilities, and its potential evolution in the foreseeable future.
- **Impact Assessment**: Identify AFGE-represented units/jobs at risk due to AI advancements and automation. Identify potential risks around discrimination, hiring, discipline, union activity, collective bargaining, and other routine labor-management relations functions. Likewise, identify potential opportunities in the deployment of AI.
- **Implication Analysis**: Analyze what these changes mean for our members, their agencies, AFGE, and society more broadly. Identify specific risks and opportunities as they relate to AFGE members and the federation as a whole.
- **Action Plan Development**: Develop recommendations for a course of action to protect and empower AFGE members during AI's progression. Include in this report recommended actions to help AFGE leaders and members throughout the federation better understand AI, AI's potential risks and opportunities, and strategies to mitigate AI risks at the federation, district, council, and local level.

NORMS:

- Observe AFGE Code of Conduct
- Civil and Issue-Oriented Discussion
- Apolitical
- All Committee members have an equal voice in these discussions
- Partnership at all levels
- No personal attacks on individual officers, members, or staff
- Maintain confidentiality of committee documents and discussions
- All decisions made by unanimous consent to ensure unity
- Endeavor to deliver all materials 24 hours before the schedules meeting

MEETINGS:

- The Committee commits to meet for the duration of six months, commencing in September 2023.
- The Committee should expect to attend one or two meetings per month along with additional action items that may result from the Committee's work.
- The duration of the Committee may be extended at the recommendation of the Committee with approval of the National President.
- These meetings can take place using the appropriate technology via virtual platform.
- 50% of Committee members present shall constitute a quorum

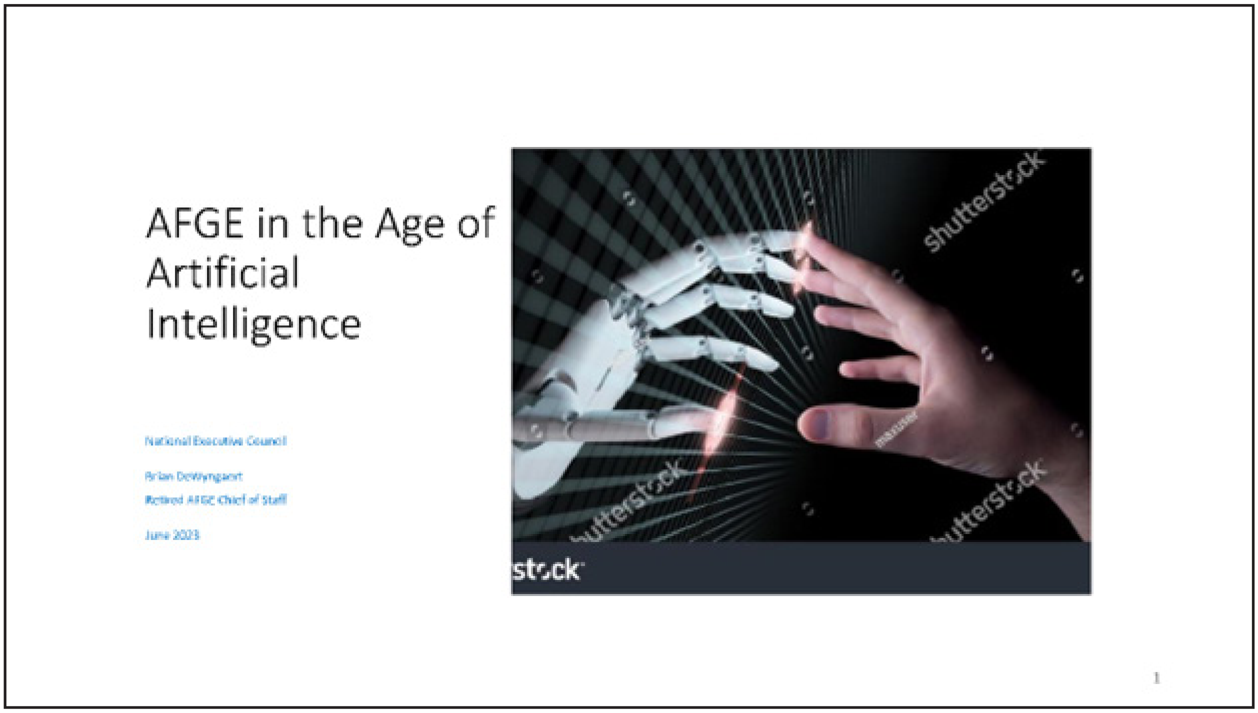
REPORTING RESPONSIBILITY:

- Adhere to timelines established by the Chair of this Committee.
- Committee reports will be maintained in the office of the National President
- **Progress Reporting**: The Committee will provide written monthly reports to the National President on the progress of the Committee's work. The Committee may be called upon to provide further briefings to other federation bodies at the direction of the National President.
- **Final Report:** The Committee will submit to the National President a final written report detailing its work in each of the areas outlined above in Section II (Key Responsibilities) and recommendations for future actions.
- The goal will be to complete all work by March 18, 2024.

AMENDMENT PROCESS:

- Changes to the document must be proposed in writing and presented to the Chair/NP designee.
- This Charter is a living document, and therefore amendable by unanimous consent of the Committee membership.

BRIAN DEWYNGAERT POWERPOINT ON AFGE AND AI



AFGE in the Age of Artificial Intelligence

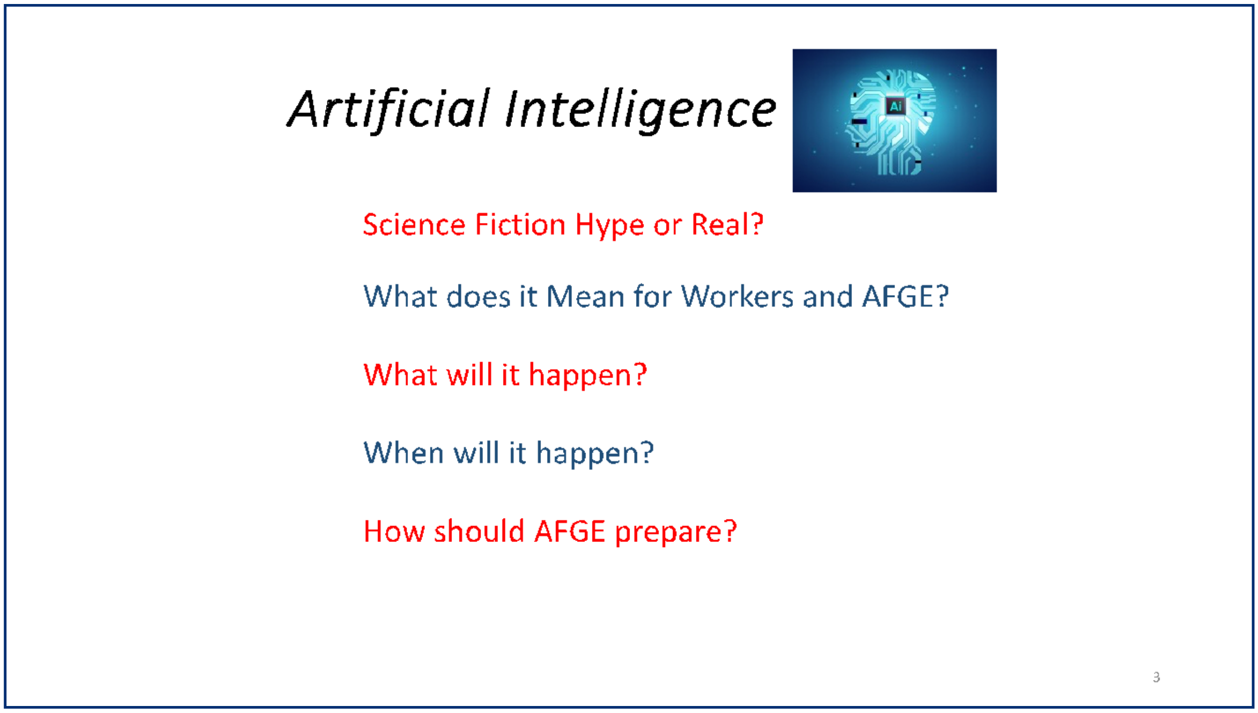
National Executive Council

Brian DeWyngaert

Retired AFGE Chief of Staff

June 2023

1



Artificial Intelligence

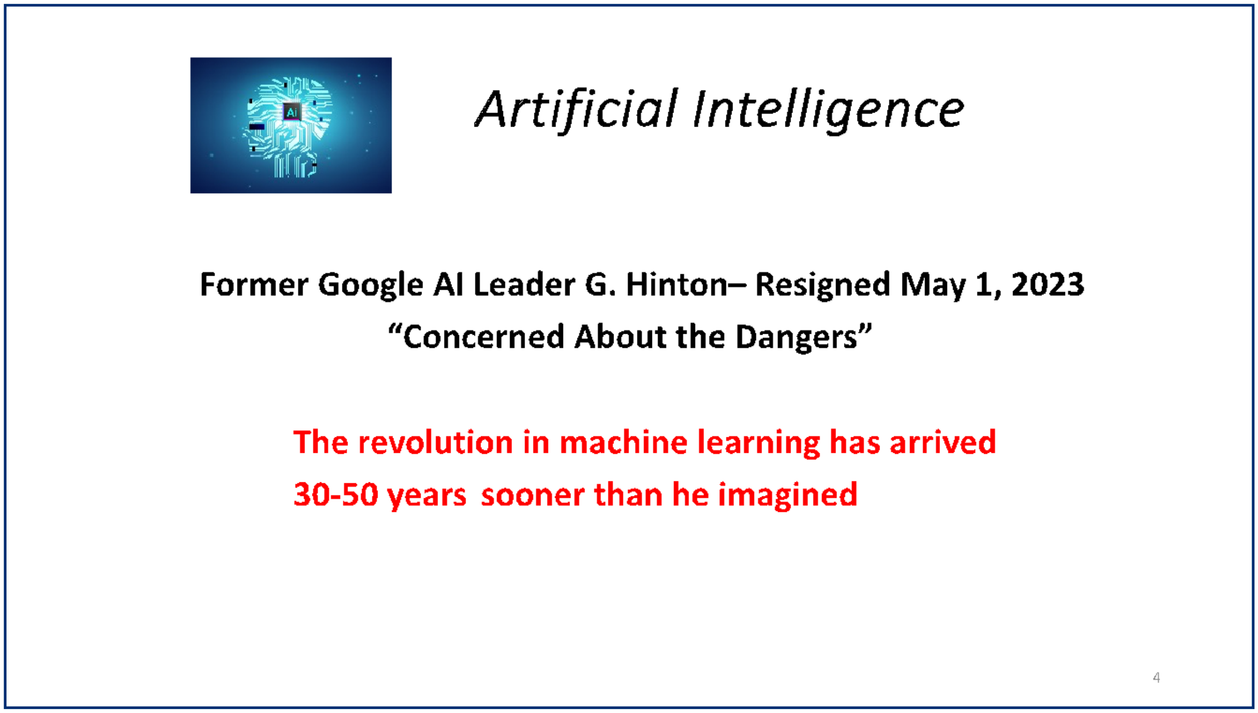
Science Fiction Hype or Real?

What does it Mean for Workers and AFGE?

What will it happen?

When will it happen?

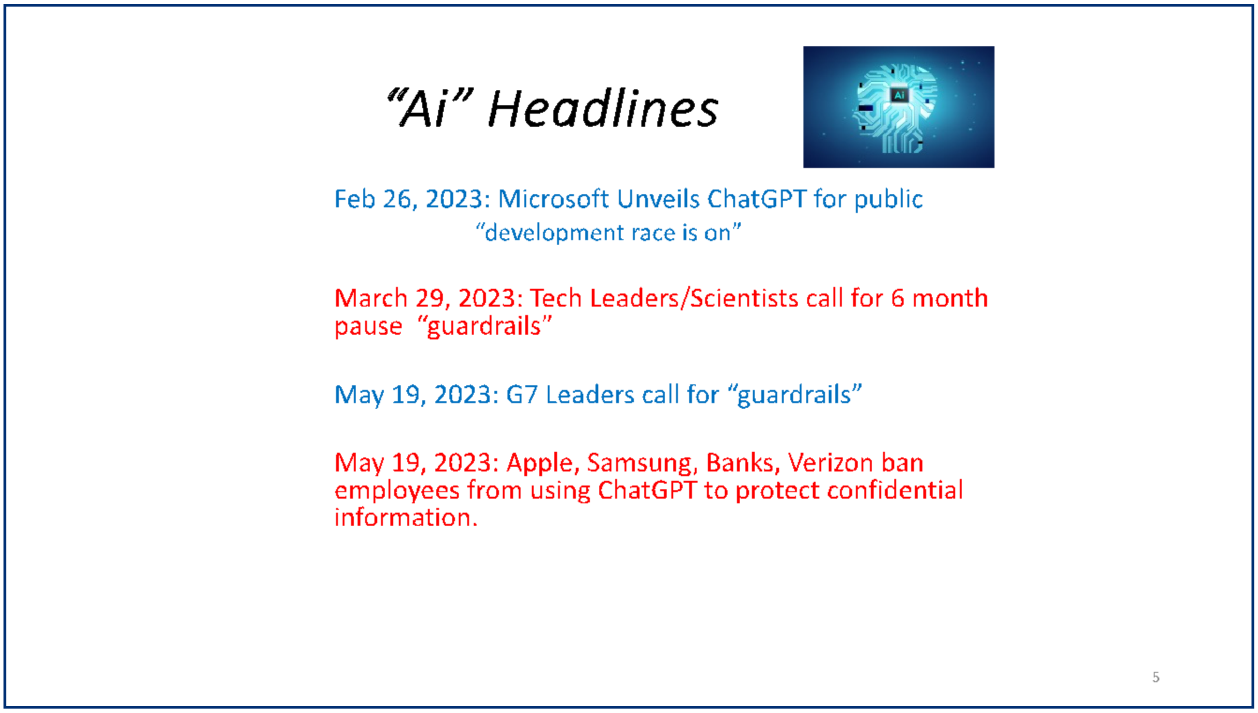
How should AFGE prepare?



Artificial Intelligence

Former Google AI Leader G. Hinton– Resigned May 1, 2023
"Concerned About the Dangers"

The revolution in machine learning has arrived
30-50 years sooner than he imagined



“Ai” Headlines

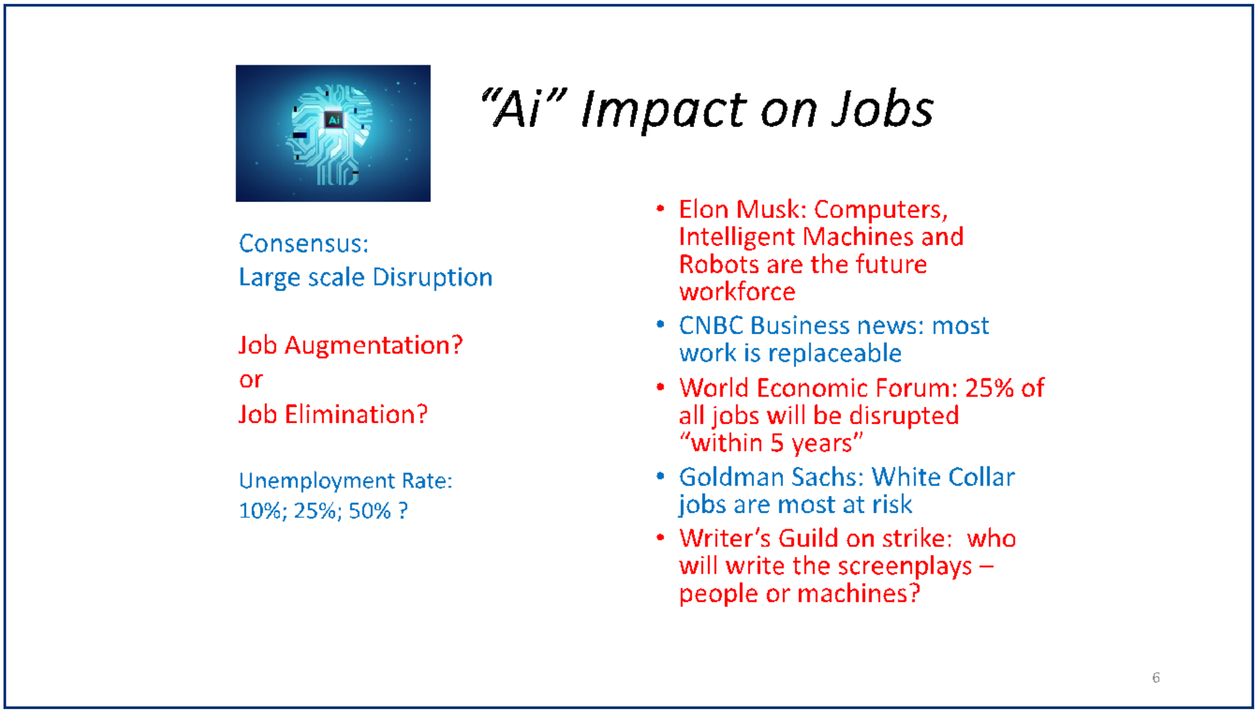
Feb 26, 2023: Microsoft Unveils ChatGPT for public
“development race is on”

March 29, 2023: Tech Leaders/Scientists call for 6 month pause “guardrails”

May 19, 2023: G7 Leaders call for “guardrails”

May 19, 2023: Apple, Samsung, Banks, Verizon ban employees from using ChatGPT to protect confidential information.

5



“Ai” Impact on Jobs

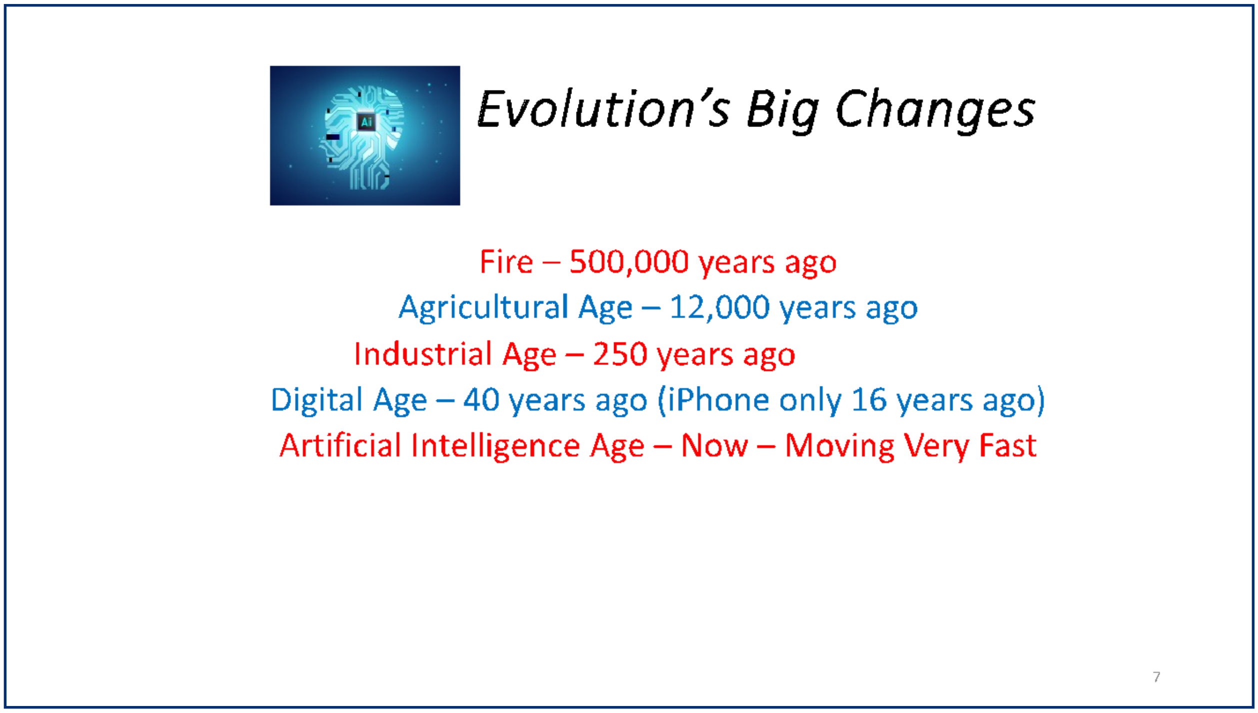
Consensus:
Large scale Disruption

Job Augmentation?
or
Job Elimination?

Unemployment Rate:
10%; 25%; 50% ?

- Elon Musk: Computers, Intelligent Machines and Robots are the future workforce
- CNBC Business news: most work is replaceable
- World Economic Forum: 25% of all jobs will be disrupted “within 5 years”
- Goldman Sachs: White Collar jobs are most at risk
- Writer’s Guild on strike: who will write the screenplays – people or machines?

6



Evolution's Big Changes

Fire – 500,000 years ago

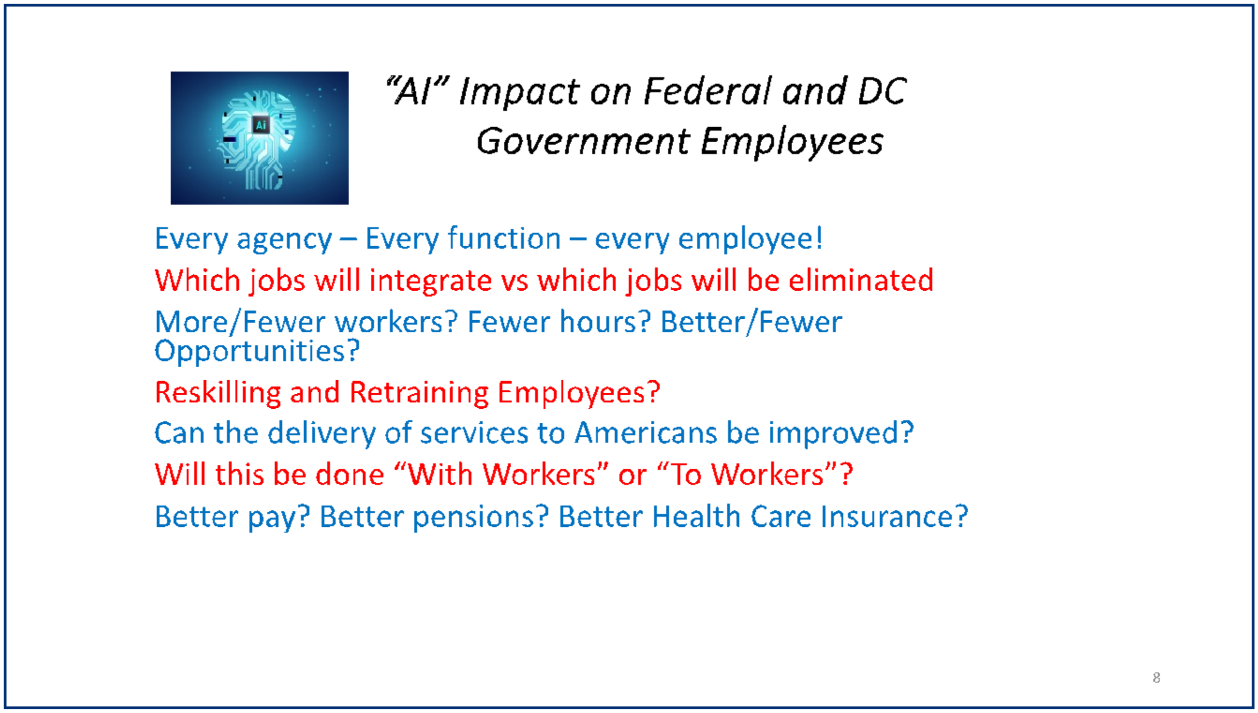
Agricultural Age – 12,000 years ago

Industrial Age – 250 years ago

Digital Age – 40 years ago (iPhone only 16 years ago)

Artificial Intelligence Age – Now – Moving Very Fast

7



"AI" Impact on Federal and DC Government Employees

Every agency – Every function – every employee!

Which jobs will integrate vs which jobs will be eliminated

More/Fewer workers? Fewer hours? Better/Fewer Opportunities?

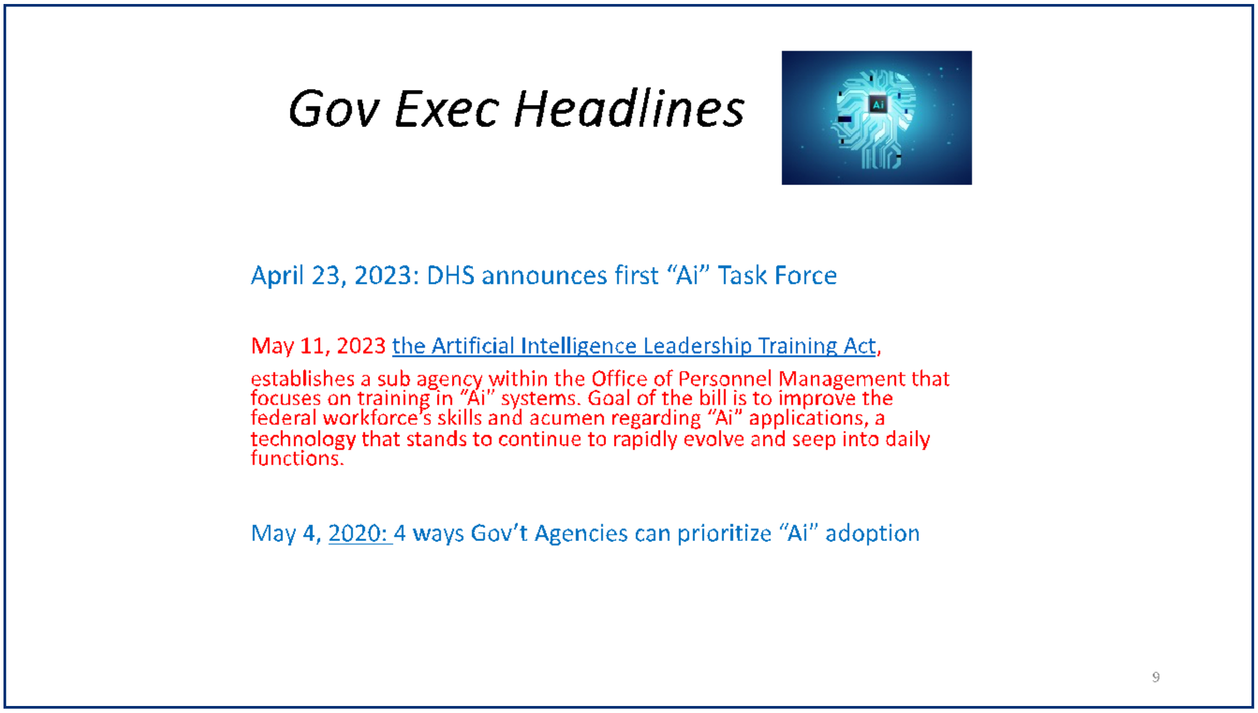
Reskilling and Retraining Employees?

Can the delivery of services to Americans be improved?

Will this be done "With Workers" or "To Workers"?

Better pay? Better pensions? Better Health Care Insurance?

8



Gov Exec Headlines

April 23, 2023: DHS announces first "Ai" Task Force

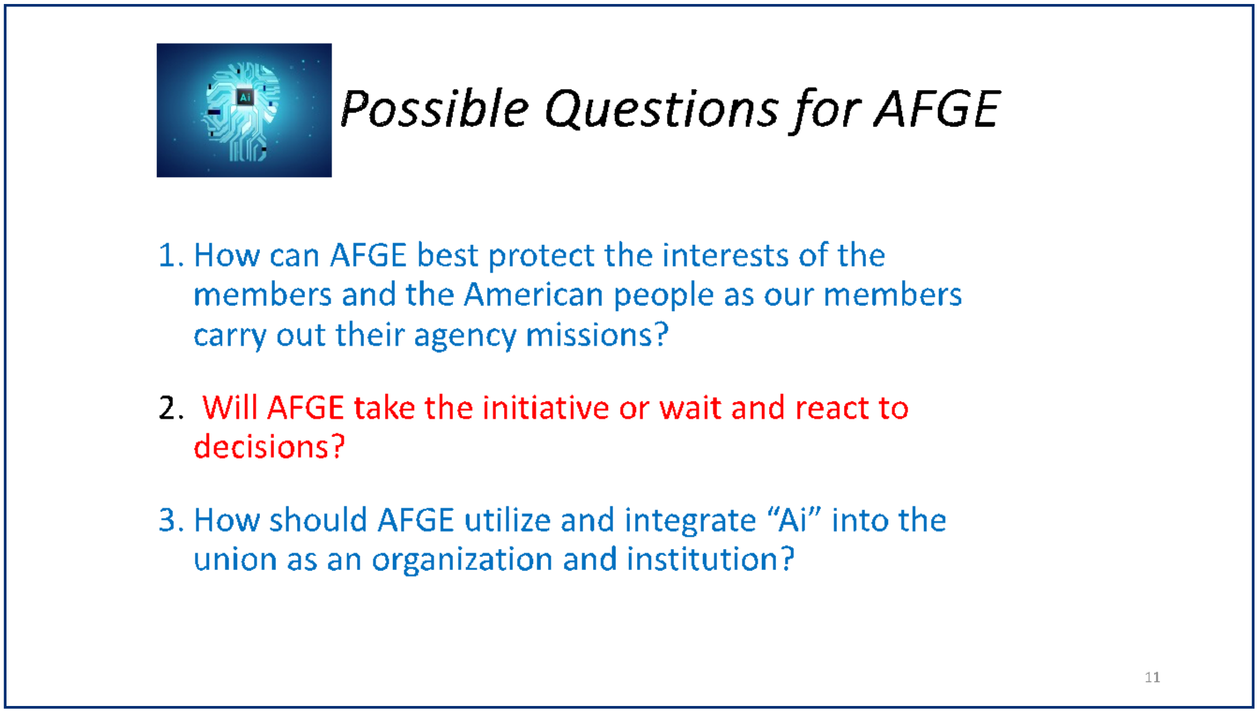
May 11, 2023 the Artificial Intelligence Leadership Training Act,

establishes a sub agency within the Office of Personnel Management that focuses on training in "Ai" systems. Goal of the bill is to improve the federal workforce's skills and acumen regarding "Ai" applications, a technology that stands to continue to rapidly evolve and seep into daily functions.

May 4, 2020: 4 ways Gov't Agencies can prioritize "Ai" adoption

Challenge
or
Opportunity

AFGE in the Age of Artificial Intelligence

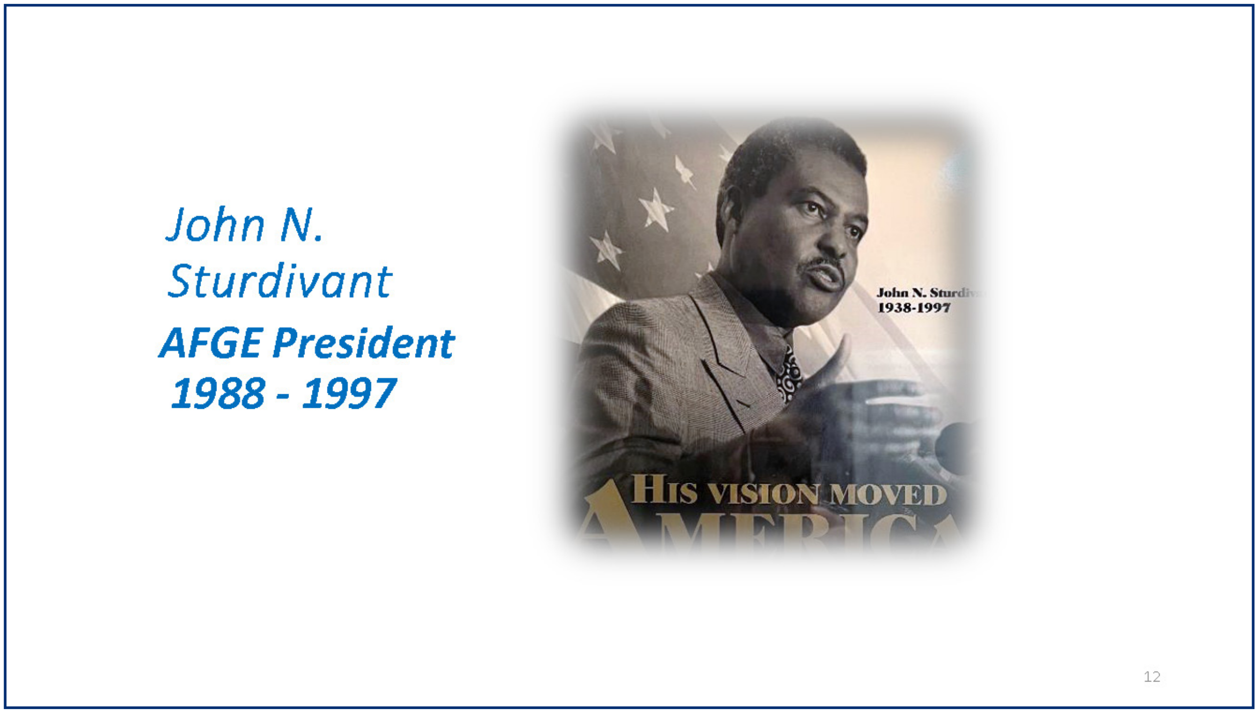


Possible Questions for AFGE

1. How can AFGE best protect the interests of the members and the American people as our members carry out their agency missions?

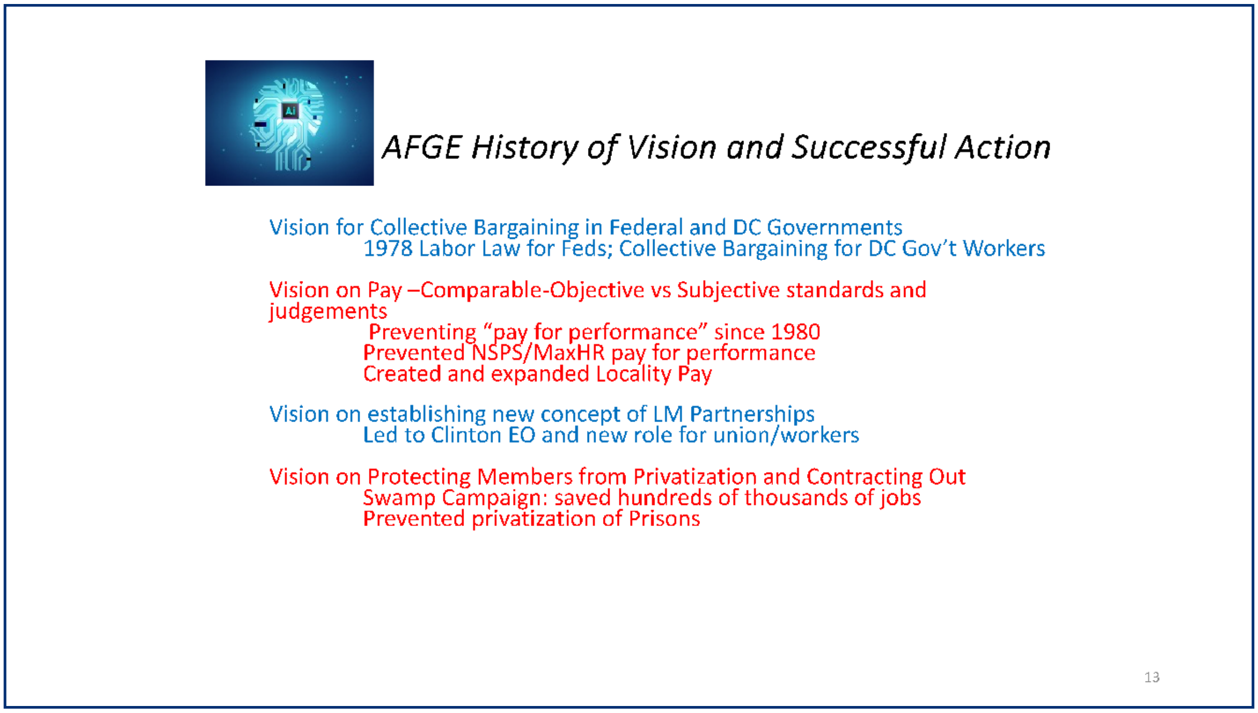
2. Will AFGE take the initiative or wait and react to decisions?

3. How should AFGE utilize and integrate “Ai” into the union as an organization and institution?



John N. Sturdivant

AFGE President 1988 - 1997



AFGE History of Vision and Successful Action

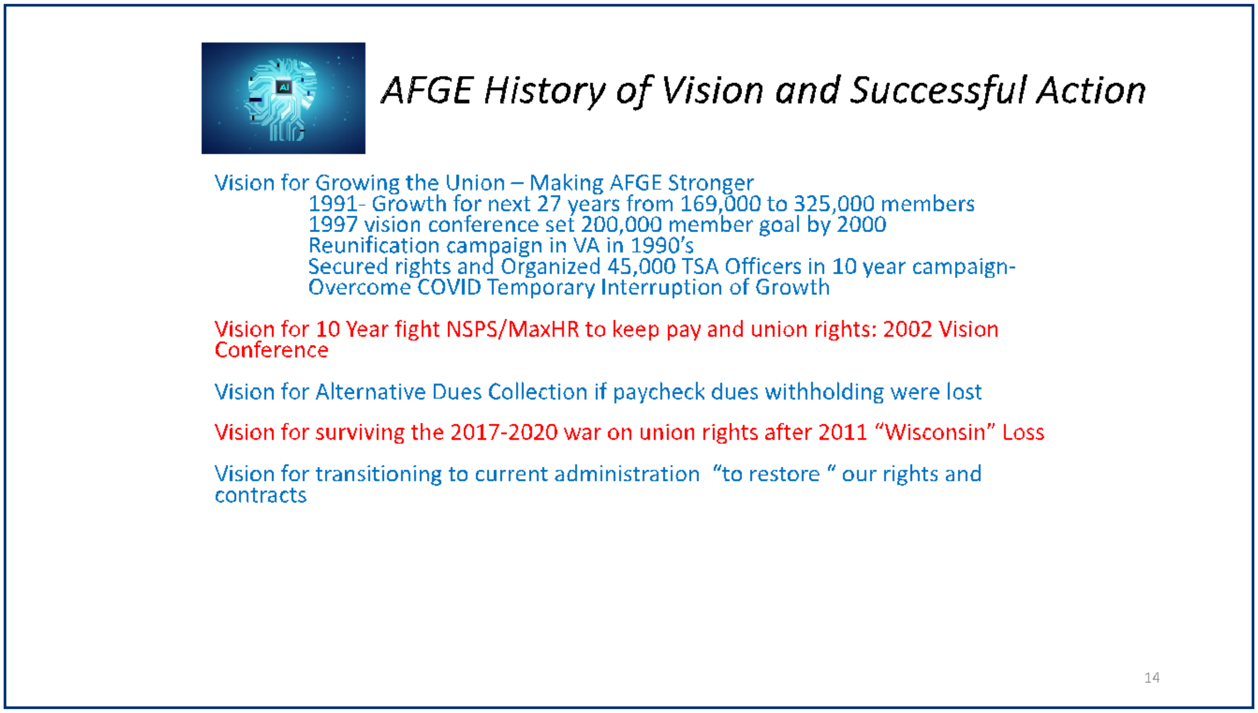
Vision for Collective Bargaining in Federal and DC Governments
1978 Labor Law for Feds; Collective Bargaining for DC Gov't Workers

Vision on Pay –Comparable-Objective vs Subjective standards and judgements
Preventing "pay for performance" since 1980
Prevented NSPS/MaxHR pay for performance
Created and expanded Locality Pay

Vision on establishing new concept of LM Partnerships
Led to Clinton EO and new role for union/workers

Vision on Protecting Members from Privatization and Contracting Out
Swamp Campaign: saved hundreds of thousands of jobs
Prevented privatization of Prisons

13



AFGE History of Vision and Successful Action

Vision for Growing the Union – Making AFGE Stronger
1991- Growth for next 27 years from 169,000 to 325,000 members
1997 vision conference set 200,000 member goal by 2000
Reunification campaign in VA in 1990's
Secured rights and Organized 45,000 TSA Officers in 10 year campaign-
Overcome COVID Temporary Interruption of Growth

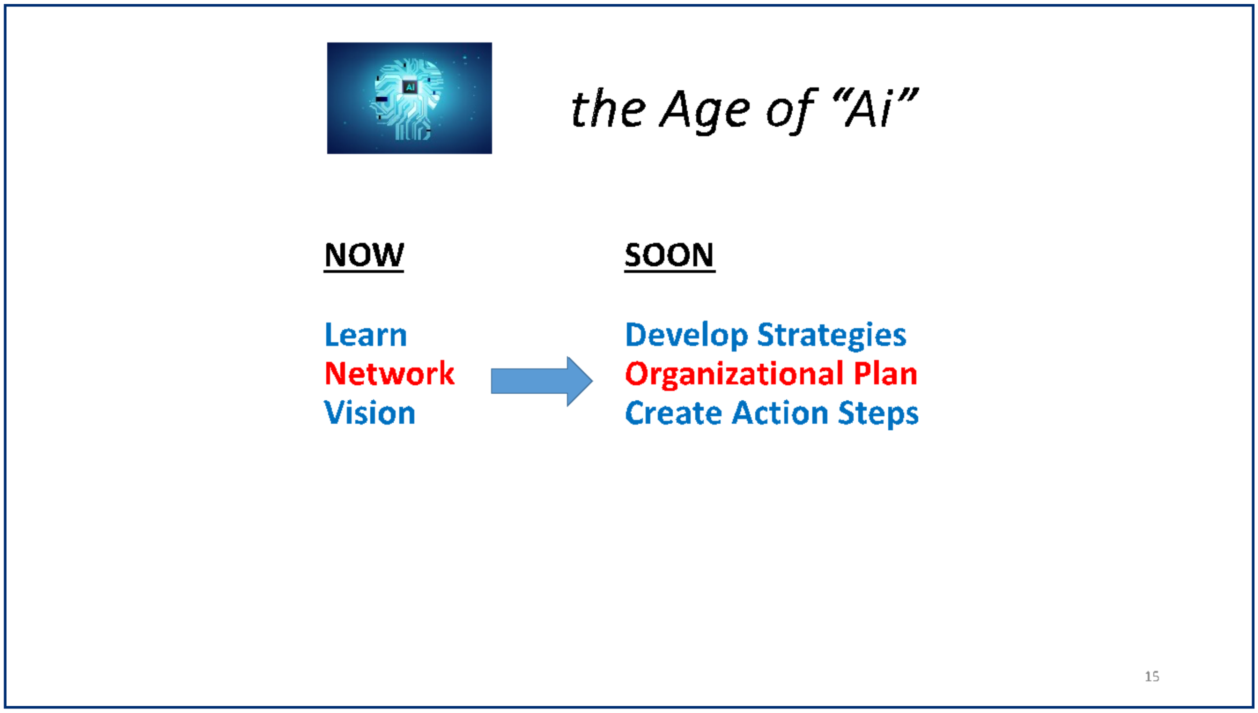
Vision for 10 Year fight NSPS/MaxHR to keep pay and union rights: 2002 Vision Conference

Vision for Alternative Dues Collection if paycheck dues withholding were lost

Vision for surviving the 2017-2020 war on union rights after 2011 "Wisconsin" Loss

Vision for transitioning to current administration "to restore " our rights and contracts

14



the Age of "Ai"

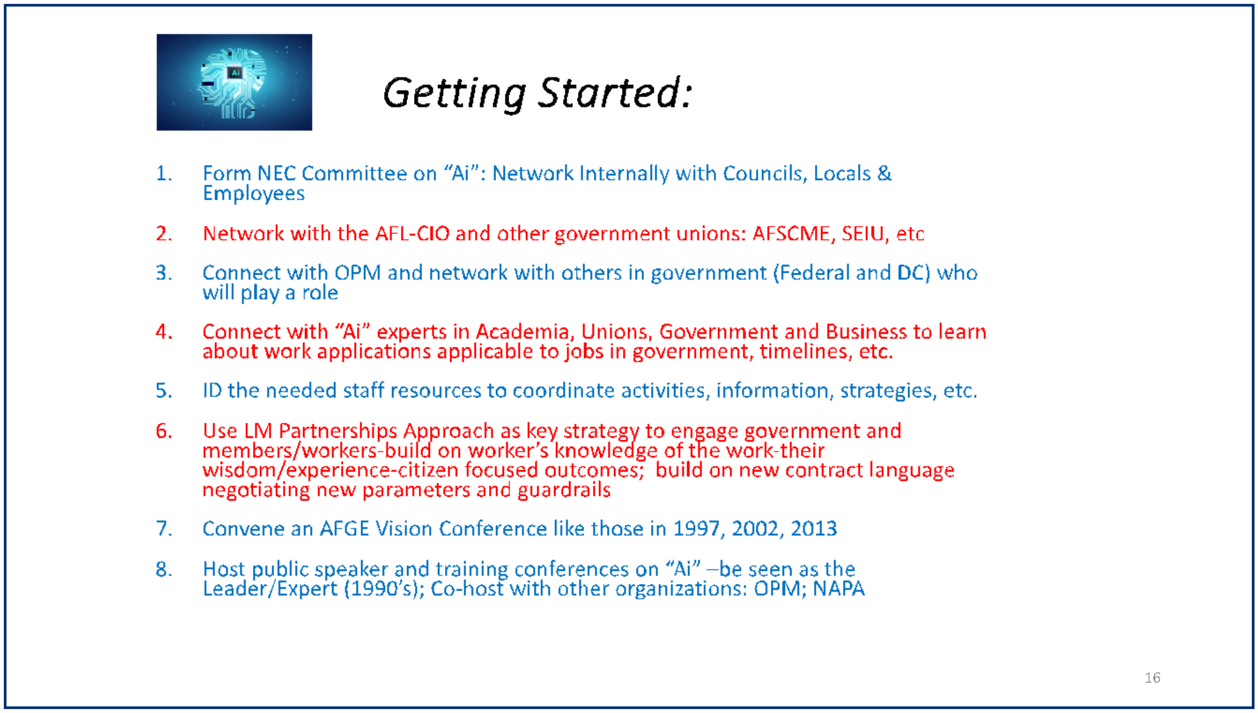
NOW

Learn
Network
Vision

SOON

Develop Strategies
Organizational Plan
Create Action Steps

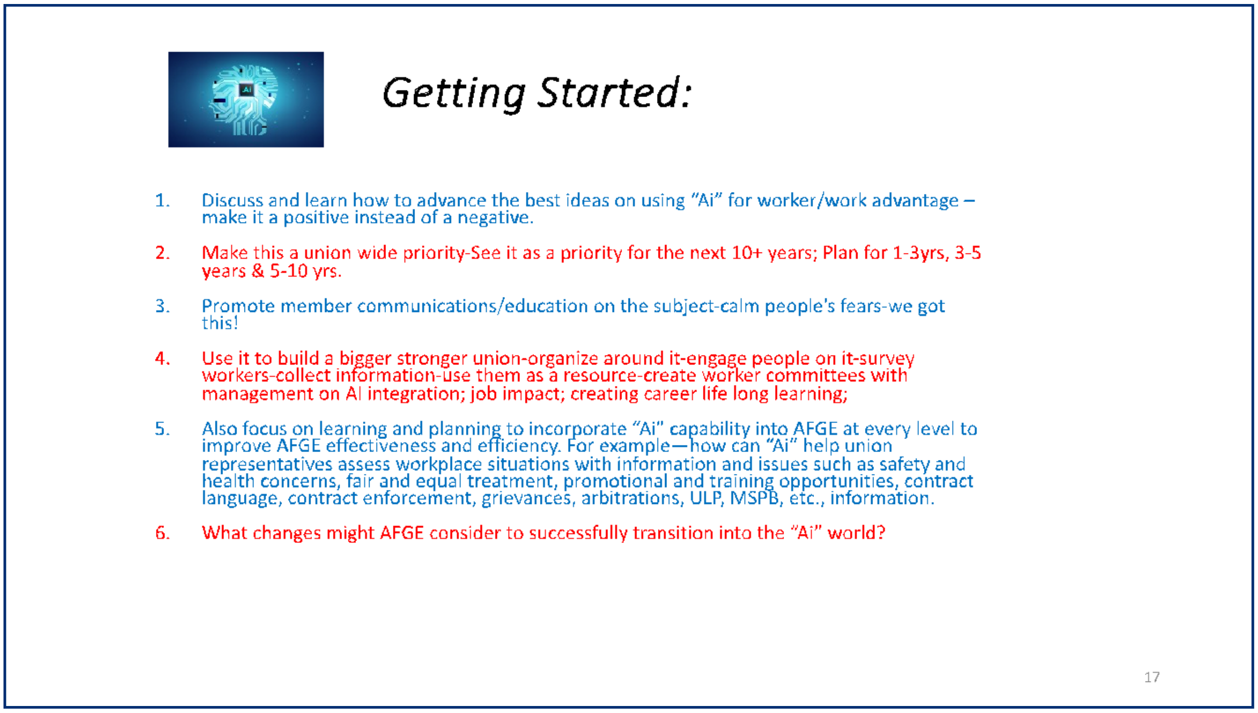
15



Getting Started:

1. Form NEC Committee on "Ai": Network Internally with Councils, Locals & Employees
2. Network with the AFL-CIO and other government unions: AFSCME, SEIU, etc
3. Connect with OPM and network with others in government (Federal and DC) who will play a role
4. Connect with "Ai" experts in Academia, Unions, Government and Business to learn about work applications applicable to jobs in government, timelines, etc.
5. ID the needed staff resources to coordinate activities, information, strategies, etc.
6. Use LM Partnerships Approach as key strategy to engage government and members/workers-build on worker's knowledge of the work-their wisdom/experience-citizen focused outcomes; build on new contract language negotiating new parameters and guardrails
7. Convene an AFGE Vision Conference like those in 1997, 2002, 2013
8. Host public speaker and training conferences on "Ai" –be seen as the Leader/Expert (1990's); Co-host with other organizations: OPM; NAPA

16



Getting Started:

1. Discuss and learn how to advance the best ideas on using "Ai" for worker/work advantage – make it a positive instead of a negative.
2. Make this a union wide priority-See it as a priority for the next 10+ years; Plan for 1-3yrs, 3-5 years & 5-10 yrs.
3. Promote member communications/education on the subject-calm people's fears-we got this!
4. Use it to build a bigger stronger union-organize around it-engage people on it-survey workers-collect information-use them as a resource-create worker committees with management on AI integration; job impact; creating career life long learning;
5. Also focus on learning and planning to incorporate "Ai" capability into AFGE at every level to improve AFGE effectiveness and efficiency. For example—how can "Ai" help union representatives assess workplace situations with information and issues such as safety and health concerns, fair and equal treatment, promotional and training opportunities, contract language, contract enforcement, grievances, arbitrations, ULP, MSPB, etc., information.
6. What changes might AFGE consider to successfully transition into the "Ai" world?

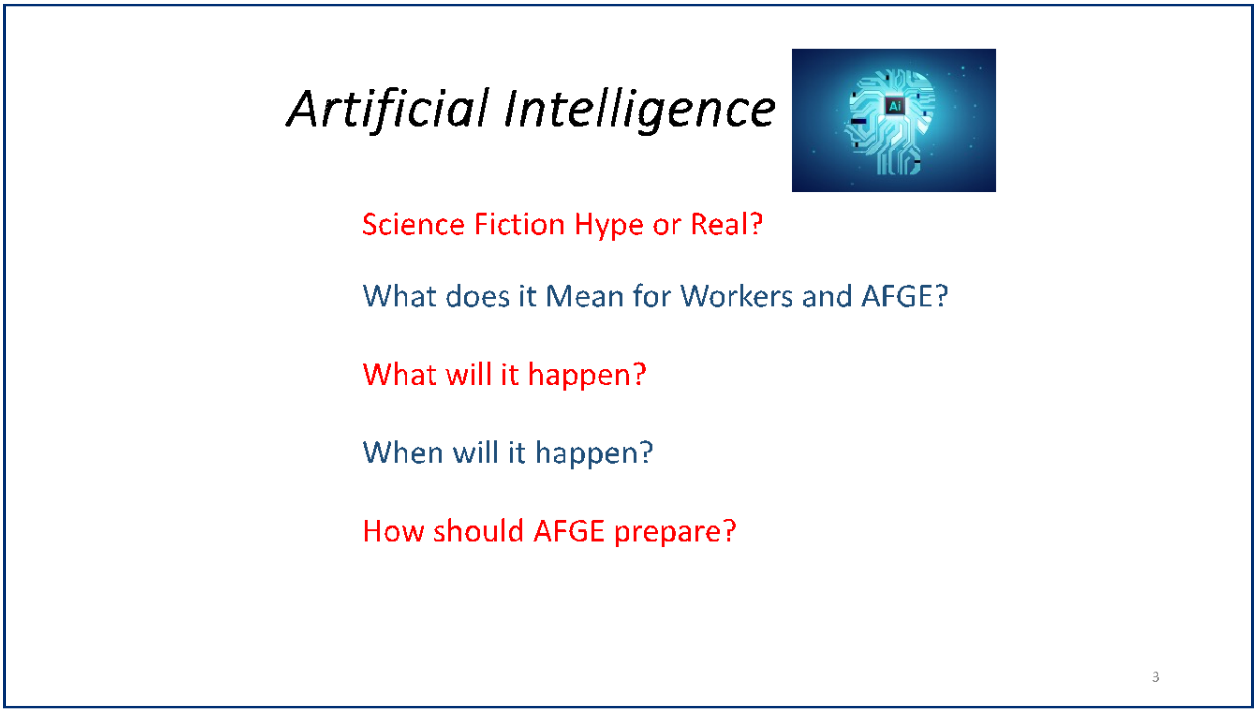
17

AFGE in the Age of Artificial Intelligence

Questions?

18

Andrew Huddleston Powerpoint on AFGE and AI



Artificial Intelligence

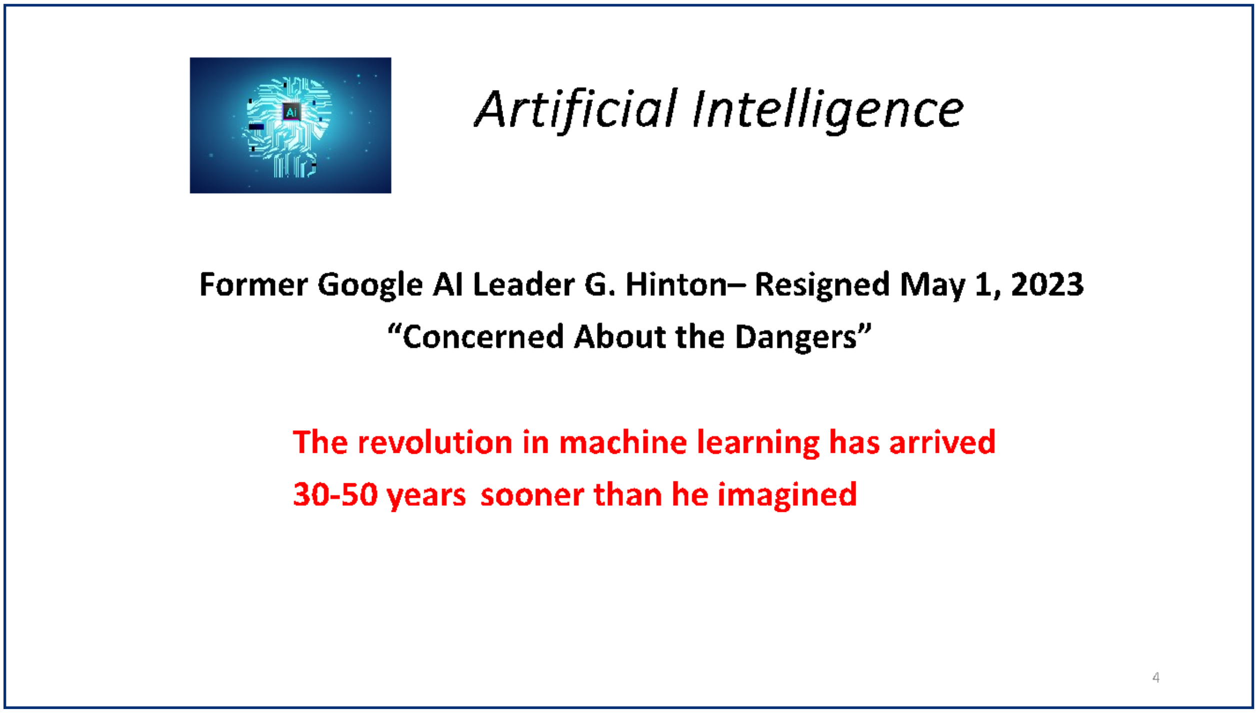
Science Fiction Hype or Real?

What does it Mean for Workers and AFGE?

What will it happen?

When will it happen?

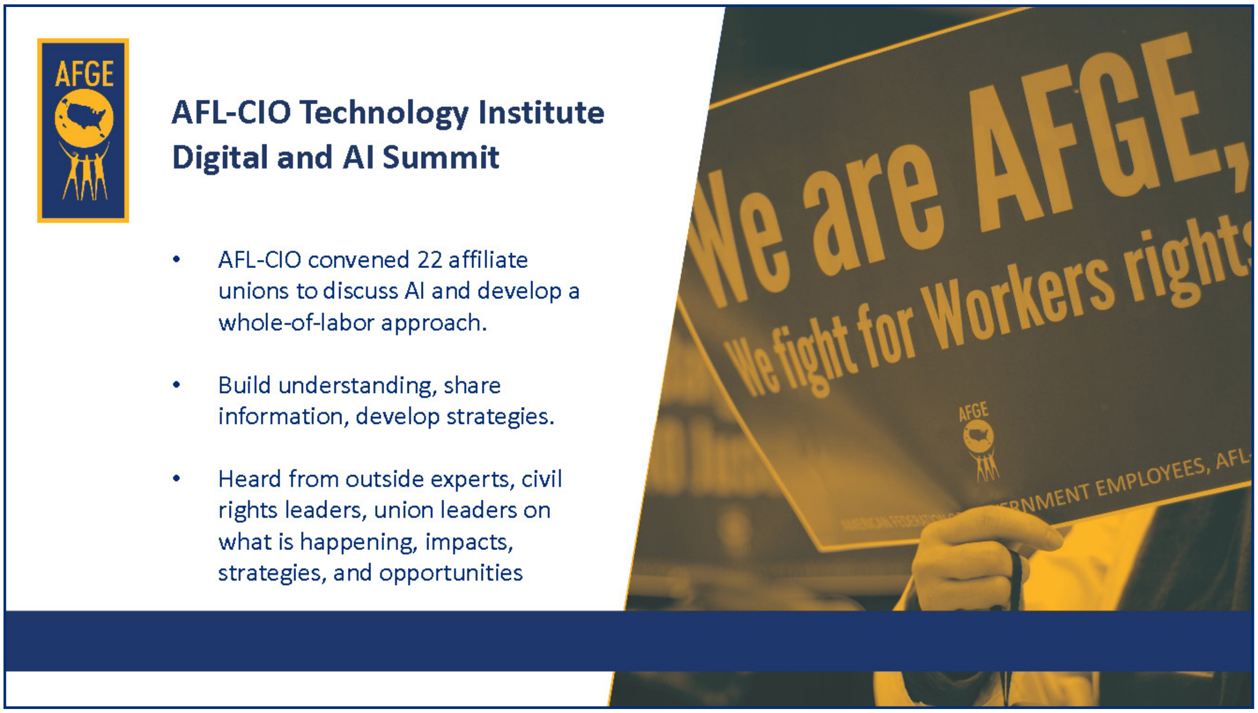
How should AFGE prepare?



Artificial Intelligence

Former Google AI Leader G. Hinton– Resigned May 1, 2023
“Concerned About the Dangers”

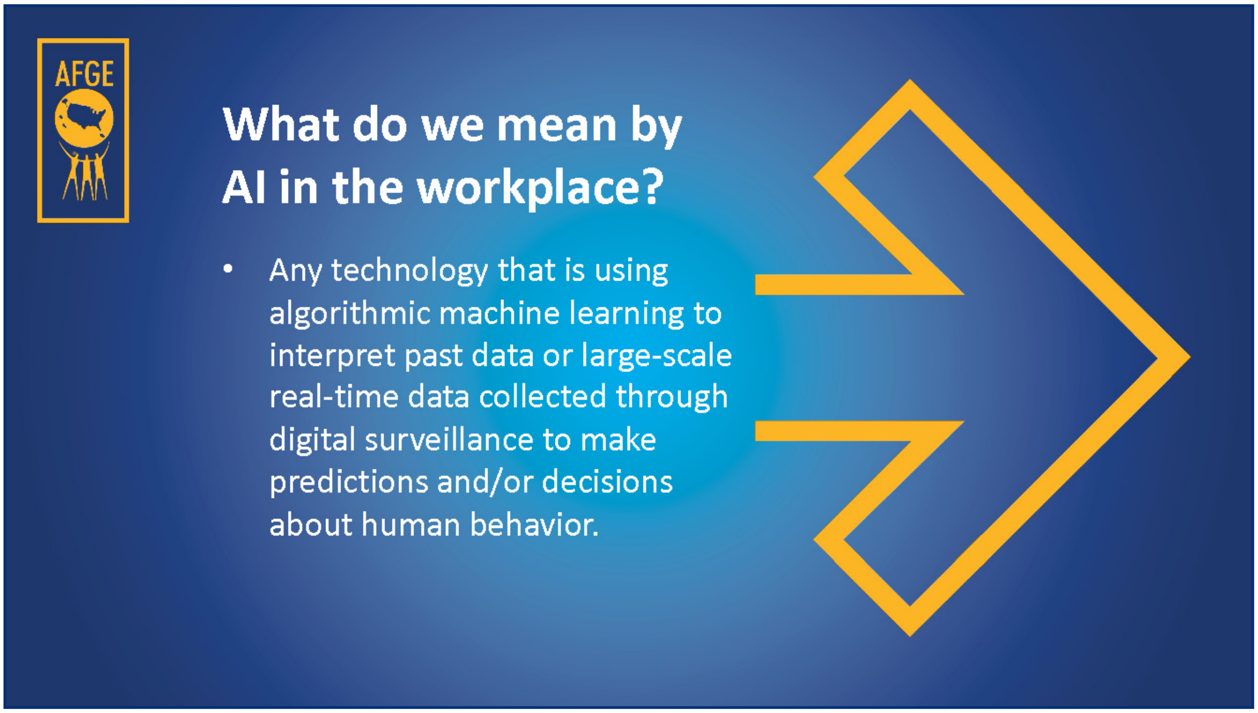
The revolution in machine learning has arrived
30-50 years sooner than he imagined



AFL-CIO Technology Institute Digital and AI Summit

- AFL-CIO convened 22 affiliate unions to discuss AI and develop a whole-of-labor approach.
- Build understanding, share information, develop strategies.
- Heard from outside experts, civil rights leaders, union leaders on what is happening, impacts, strategies, and opportunities

AFGE
We are AFGE,
We fight for Workers rights
AFGE
AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-



What do we mean by AI in the workplace?

- Any technology that is using algorithmic machine learning to interpret past data or large-scale real-time data collected through digital surveillance to make predictions and/or decisions about human behavior.

HUMAN RIGHTS
WOMEN'S RIGHTS ARE HUMAN RIGHTS
AMERICAN FEDERATION OF GOVERNMENT

How are these tools being deployed in the economy?

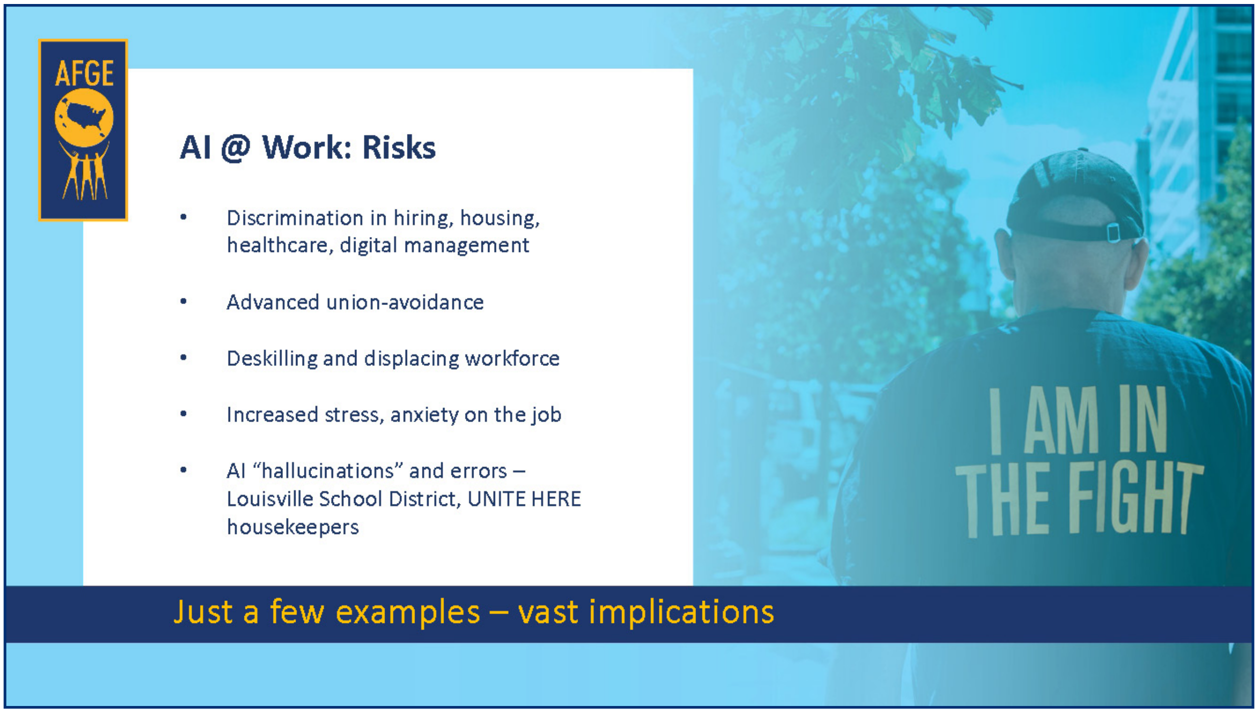
- Digital surveillance of workers
- Predictive analysis tools used in hiring, day-to-day management
- Union avoidance efforts
- Healthcare, housing
- Elections and political advertising

Just a few examples – vast implications

AI In the Workplace

- Electronic health records, predictive analysis and predictive staffing in healthcare
- Management of cleaning staff
- Sentiment analysis and digital surveillance of call-center and customer service workers
- AI in production, assembly
- AI-assisted decision making

Just a few examples – vast implications

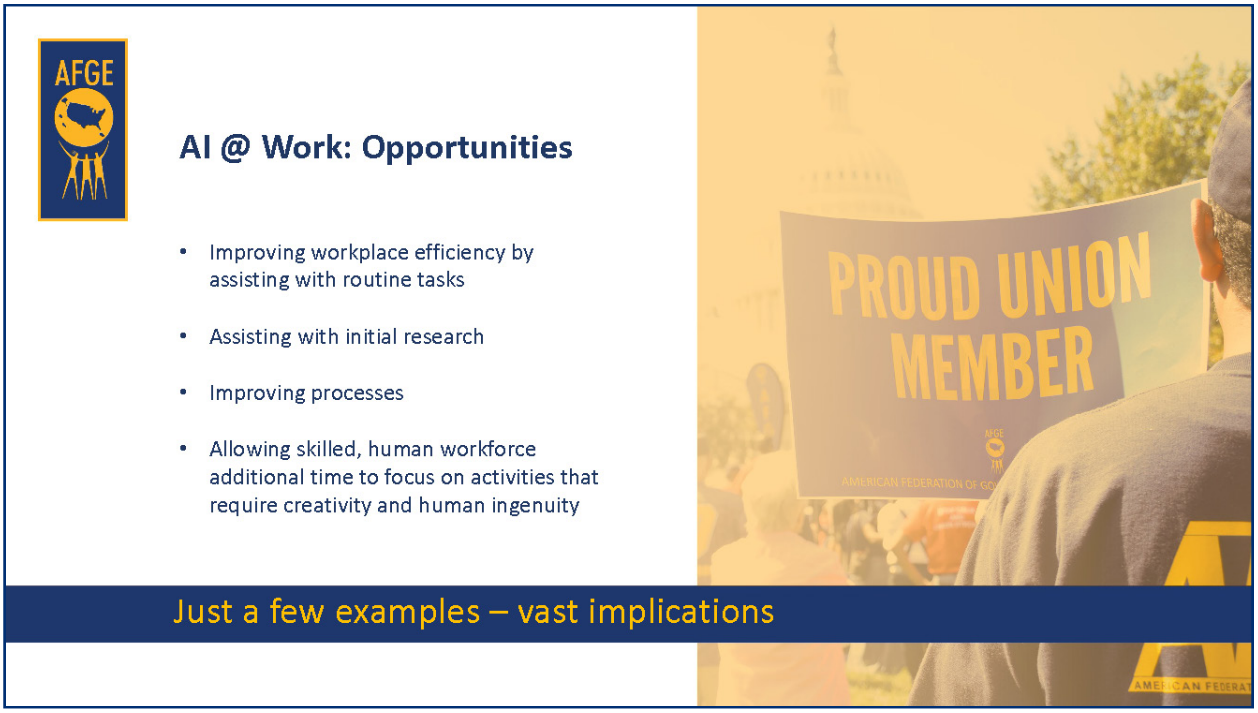


AI @ Work: Risks

- Discrimination in hiring, housing, healthcare, digital management
- Advanced union-avoidance
- Deskilling and displacing workforce
- Increased stress, anxiety on the job
- AI "hallucinations" and errors – Louisville School District, UNITE HERE housekeepers

Just a few examples – vast implications

I AM IN
THE FIGHT



AI @ Work: Opportunities

- Improving workplace efficiency by assisting with routine tasks
- Assisting with initial research
- Improving processes
- Allowing skilled, human workforce additional time to focus on activities that require creativity and human ingenuity

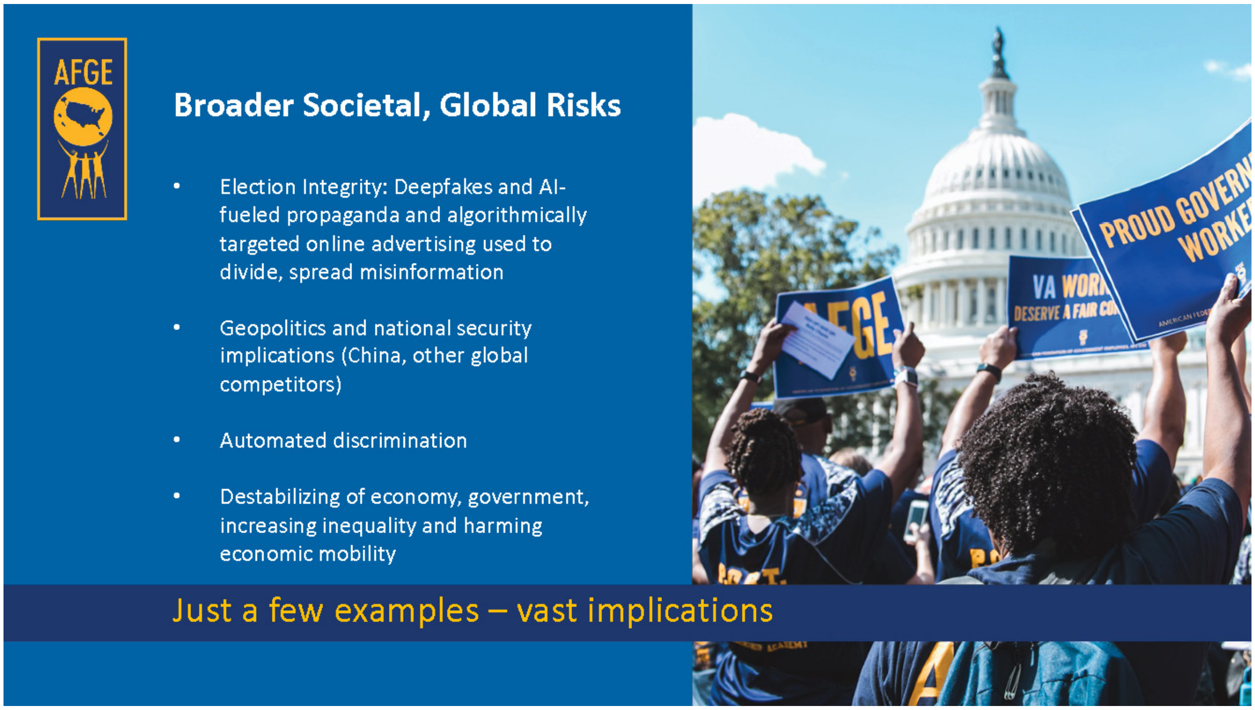
Just a few examples – vast implications

PROUD UNION
MEMBER
AFGE
AMERICAN FEDERATION OF GO
AMERICAN FEDERAT

AI in the Government

- Dozens of pieces of federal legislation about AI have already been introduced, hundreds in states
- Big Tech in active conversations with agencies, senior government leaders about how to use AI to assist agency missions
- WH developed blueprints for AI, National Security Strategy, OMB guidance for agencies

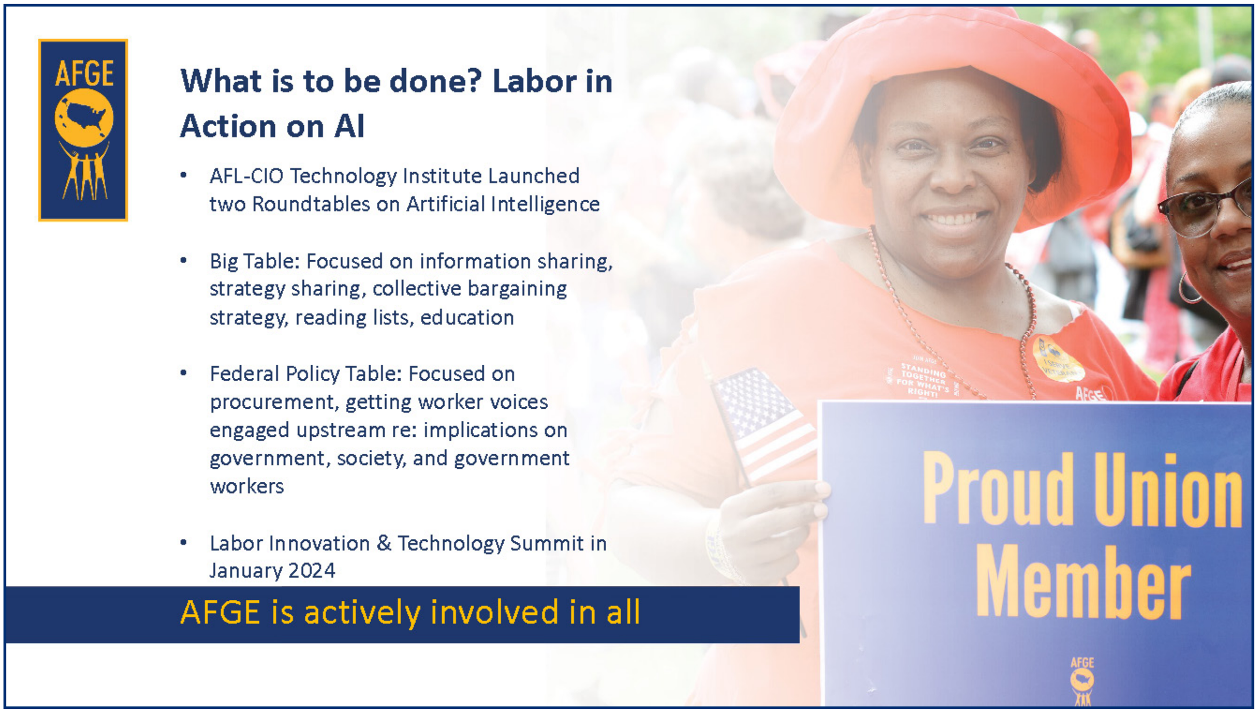
Broader Implications for Democracy, Government


AFGE
PROUD GOVERNMENT WORKERS
VA WORKERS DESERVE A FAIR CONTRACT
AFGE

Broader Societal, Global Risks

- Election Integrity: Deepfakes and AI-fueled propaganda and algorithmically targeted online advertising used to divide, spread misinformation
- Geopolitics and national security implications (China, other global competitors)
- Automated discrimination
- Destabilizing of economy, government, increasing inequality and harming economic mobility

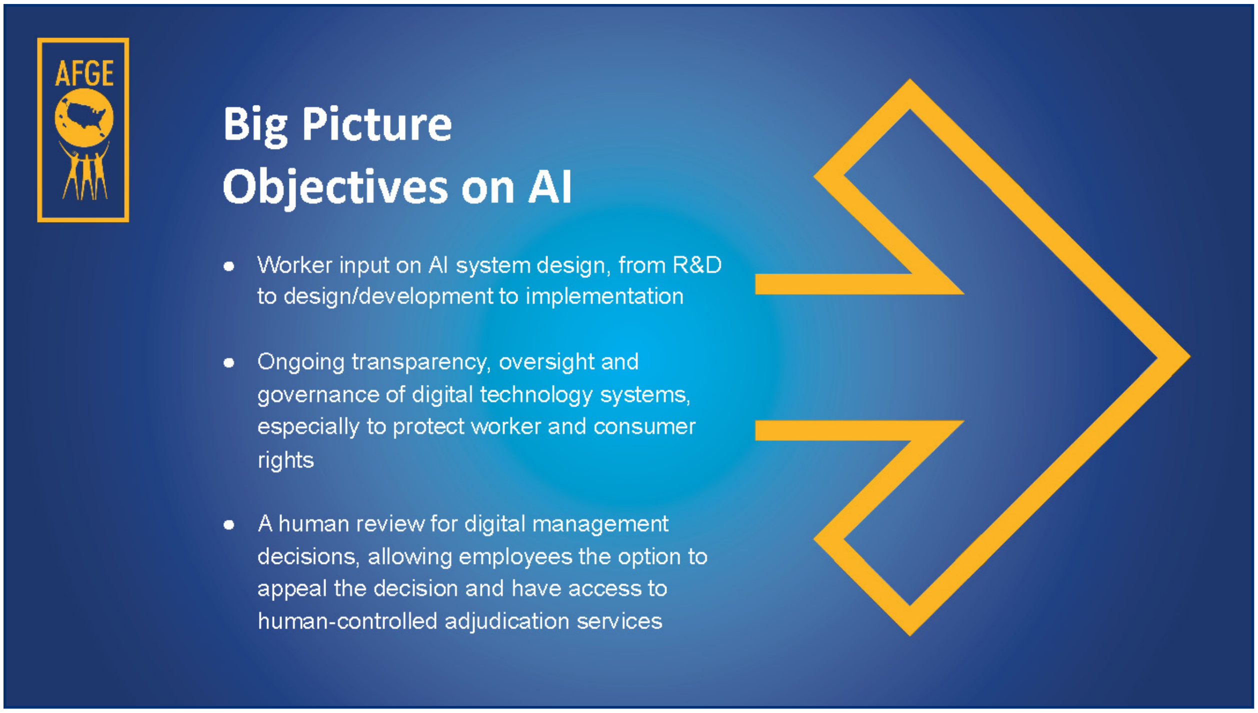
Just a few examples – vast implications


AFGE
Proud Union Member
AFGE

What is to be done? Labor in Action on AI

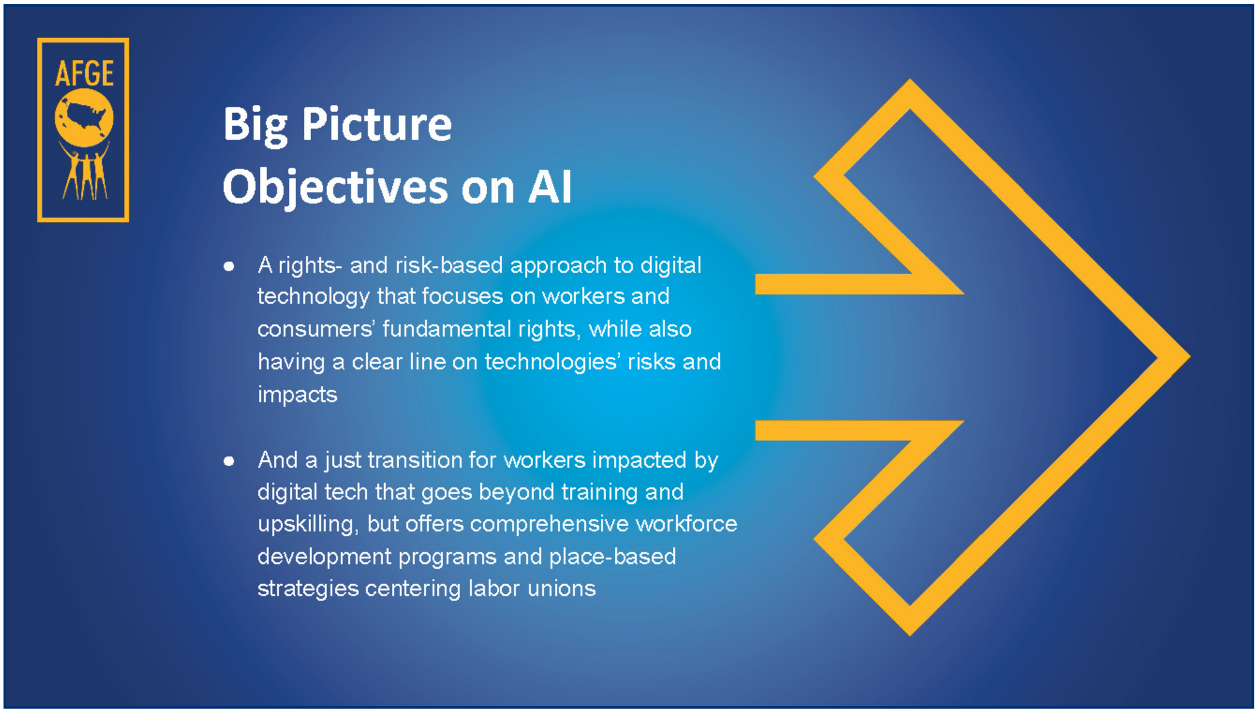
- AFL-CIO Technology Institute Launched two Roundtables on Artificial Intelligence
- Big Table: Focused on information sharing, strategy sharing, collective bargaining strategy, reading lists, education
- Federal Policy Table: Focused on procurement, getting worker voices engaged upstream re: implications on government, society, and government workers
- Labor Innovation & Technology Summit in January 2024

AFGE is actively involved in all



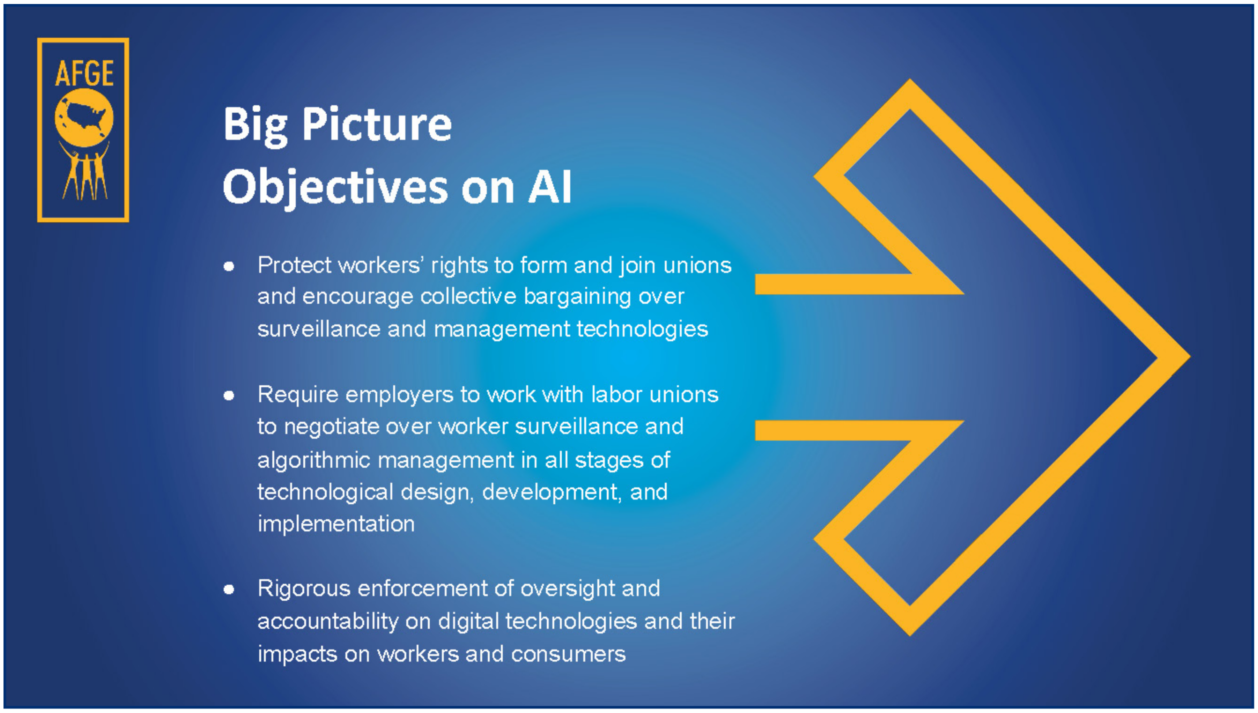
Big Picture Objectives on AI

- Worker input on AI system design, from R&D to design/development to implementation
- Ongoing transparency, oversight and governance of digital technology systems, especially to protect worker and consumer rights
- A human review for digital management decisions, allowing employees the option to appeal the decision and have access to human-controlled adjudication services



Big Picture Objectives on AI

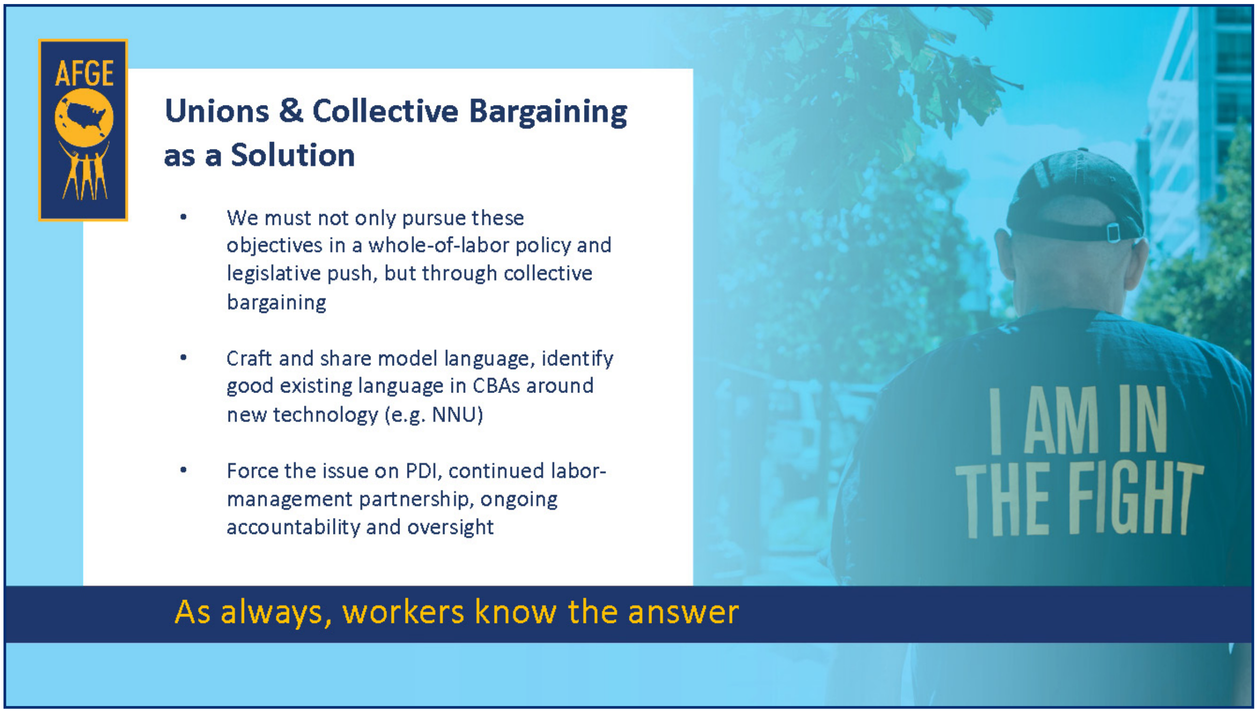
- A rights- and risk-based approach to digital technology that focuses on workers and consumers' fundamental rights, while also having a clear line on technologies' risks and impacts
- And a just transition for workers impacted by digital tech that goes beyond training and upskilling, but offers comprehensive workforce development programs and place-based strategies centering labor unions



AFGE

Big Picture Objectives on AI

- Protect workers' rights to form and join unions and encourage collective bargaining over surveillance and management technologies
- Require employers to work with labor unions to negotiate over worker surveillance and algorithmic management in all stages of technological design, development, and implementation
- Rigorous enforcement of oversight and accountability on digital technologies and their impacts on workers and consumers

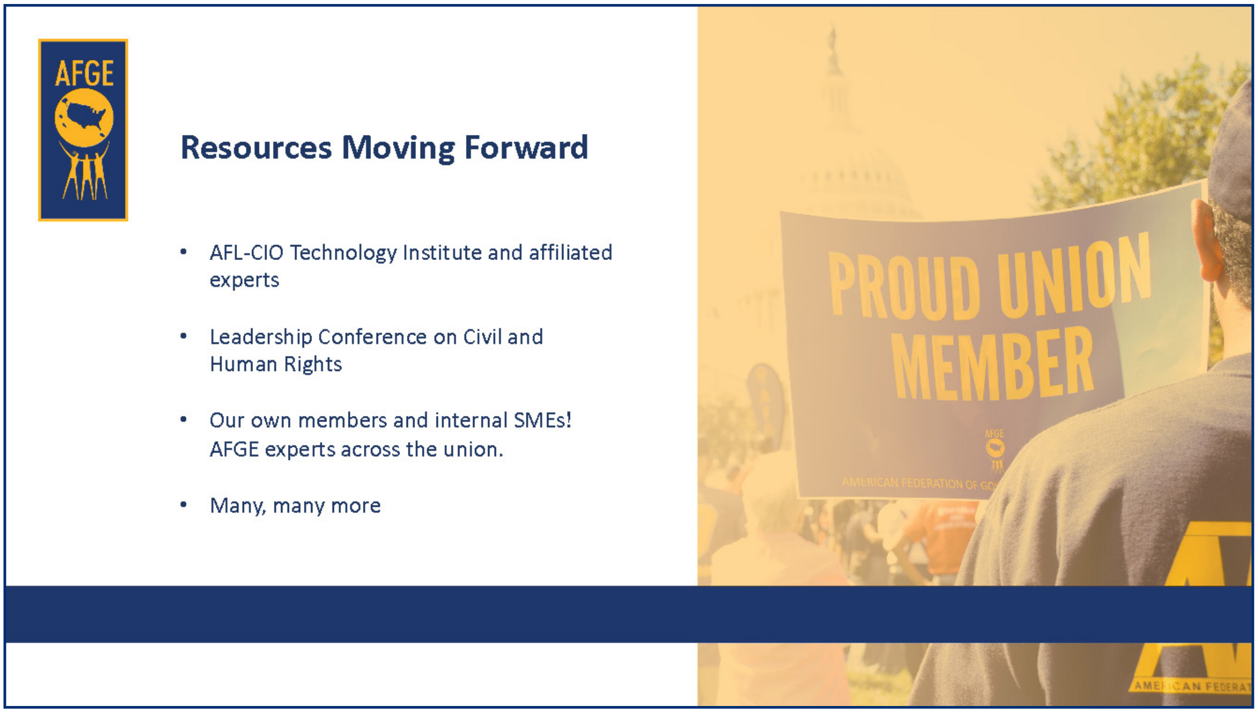


AFGE

Unions & Collective Bargaining as a Solution

- We must not only pursue these objectives in a whole-of-labor policy and legislative push, but through collective bargaining
- Craft and share model language, identify good existing language in CBAs around new technology (e.g. NNU)
- Force the issue on PDI, continued labor-management partnership, ongoing accountability and oversight

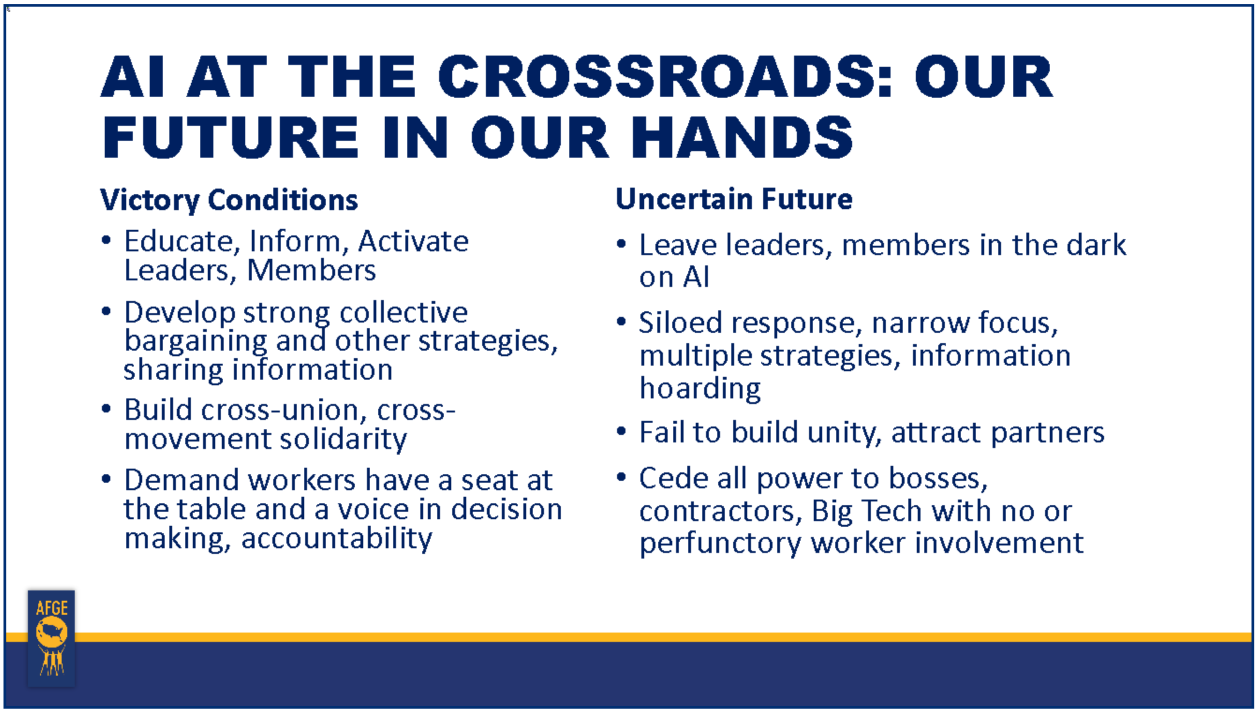
As always, workers know the answer



Resources Moving Forward

- AFL-CIO Technology Institute and affiliated experts
- Leadership Conference on Civil and Human Rights
- Our own members and internal SMEs! AFGE experts across the union.
- Many, many more

PROUD UNION MEMBER
AFGE
AMERICAN FEDERATION OF GO
AMERICAN FEDERAT



AI AT THE CROSSROADS: OUR FUTURE IN OUR HANDS

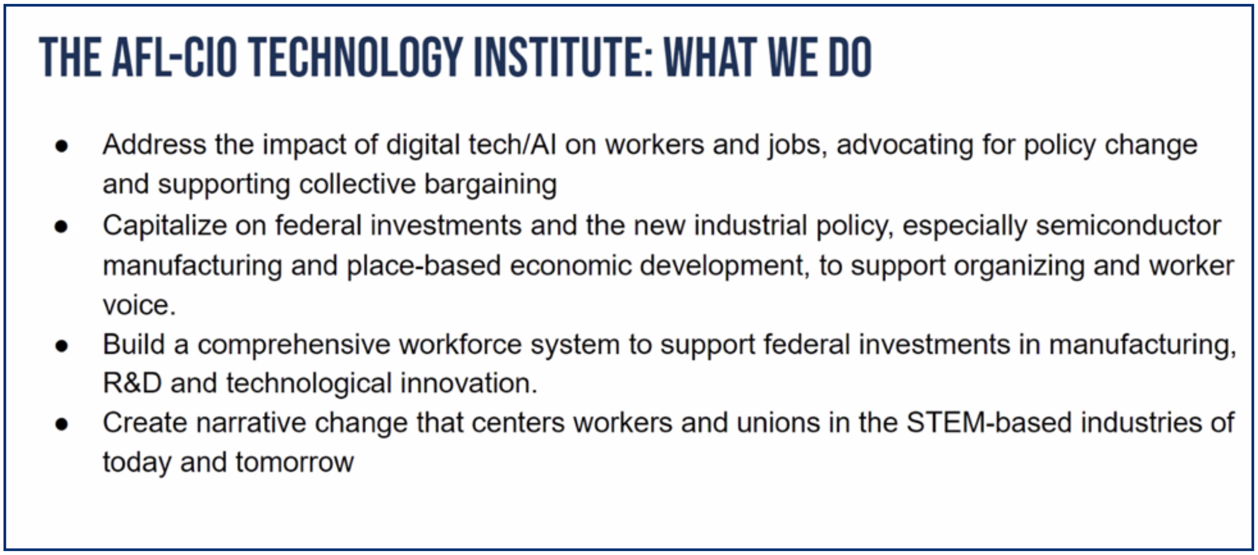
Victory Conditions

- Educate, Inform, Activate Leaders, Members
- Develop strong collective bargaining and other strategies, sharing information
- Build cross-union, cross-movement solidarity
- Demand workers have a seat at the table and a voice in decision making, accountability

Uncertain Future

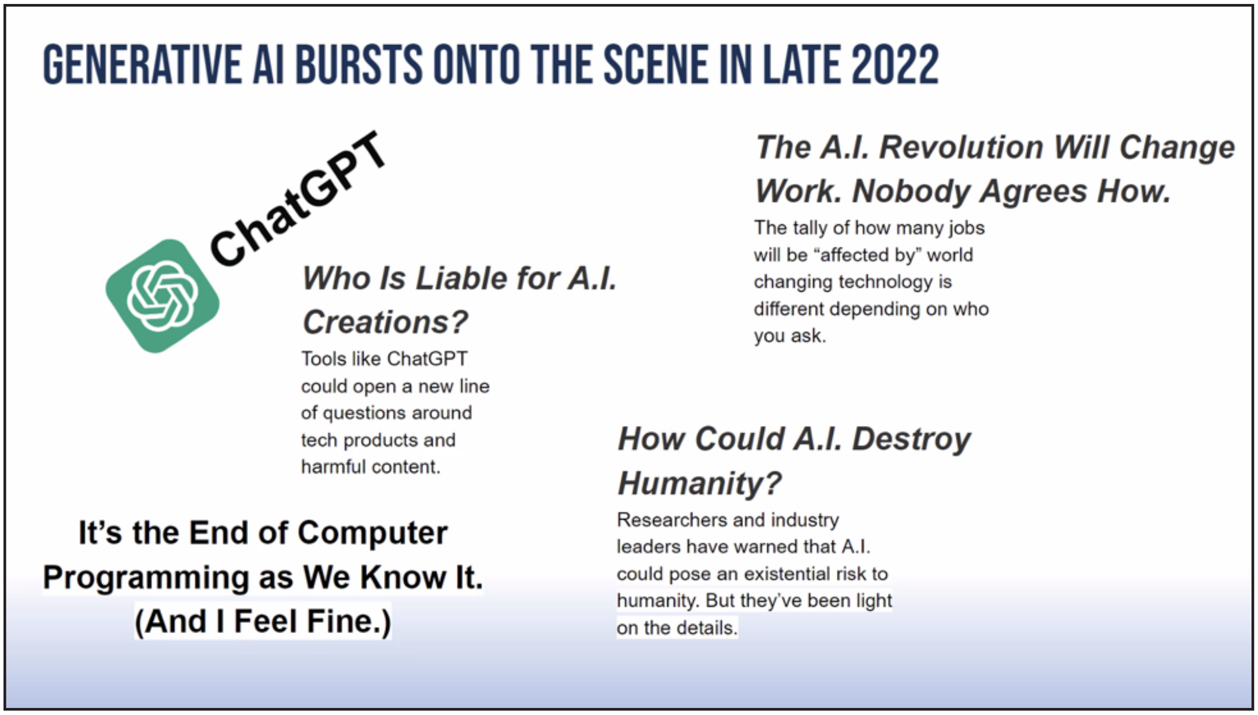
- Leave leaders, members in the dark on AI
- Siloed response, narrow focus, multiple strategies, information hoarding
- Fail to build unity, attract partners
- Cede all power to bosses, contractors, Big Tech with no or perfunctory worker involvement

Garret Schneider Presentation on AI from AFL-CIO Tech Institute



THE AFL-CIO TECHNOLOGY INSTITUTE: WHAT WE DO

- Address the impact of digital tech/AI on workers and jobs, advocating for policy change and supporting collective bargaining
- Capitalize on federal investments and the new industrial policy, especially semiconductor manufacturing and place-based economic development, to support organizing and worker voice.
- Build a comprehensive workforce system to support federal investments in manufacturing, R&D and technological innovation.
- Create narrative change that centers workers and unions in the STEM-based industries of today and tomorrow



GENERATIVE AI BURSTS ONTO THE SCENE IN LATE 2022

Who Is Liable for A.I. Creations?

Tools like ChatGPT could open a new line of questions around tech products and harmful content.

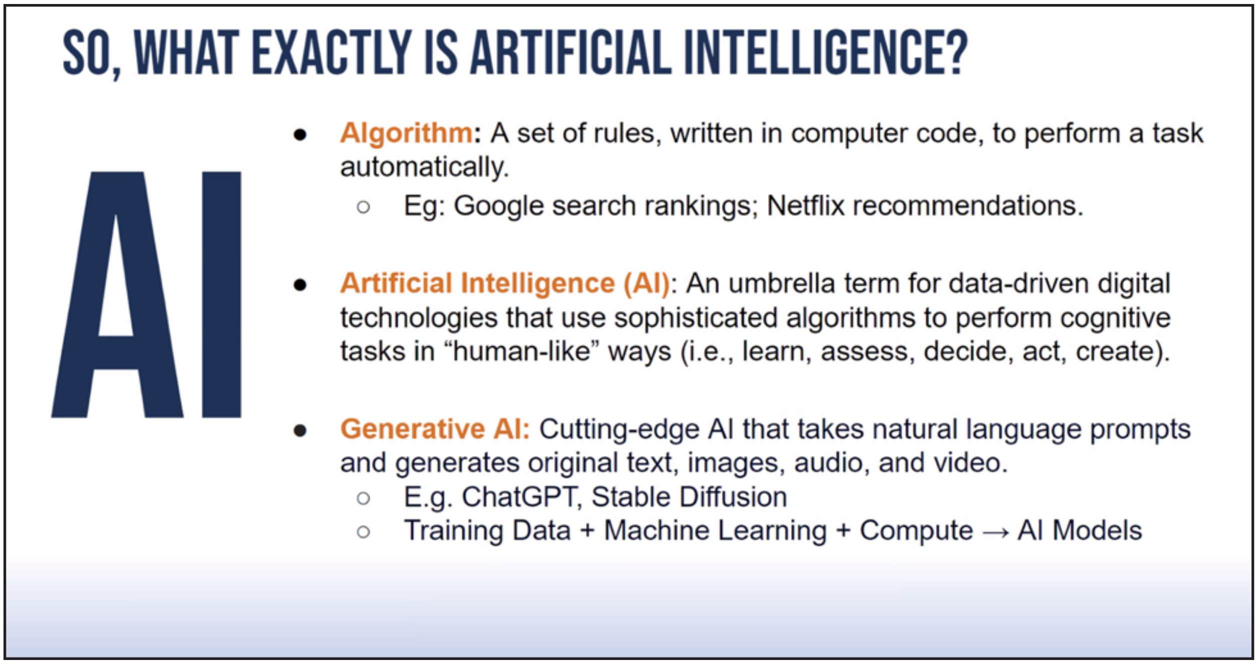
The A.I. Revolution Will Change Work. Nobody Agrees How.

The tally of how many jobs will be "affected by" world changing technology is different depending on who you ask.

How Could A.I. Destroy Humanity?

Researchers and industry leaders have warned that A.I. could pose an existential risk to humanity. But they've been light on the details.

It's the End of Computer Programming as We Know It. (And I Feel Fine.)



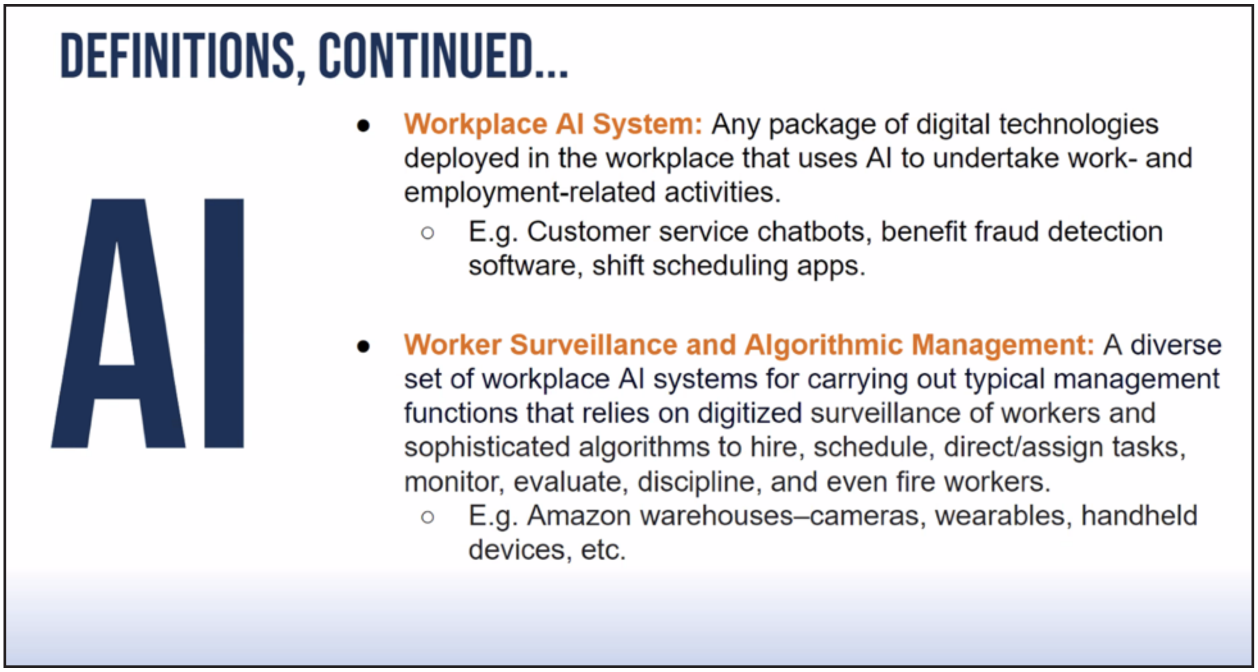
SO, WHAT EXACTLY IS ARTIFICIAL INTELLIGENCE?

AI

- **Algorithm:** A set of rules, written in computer code, to perform a task automatically.
  - Eg: Google search rankings; Netflix recommendations.

- **Artificial Intelligence (AI)**: An umbrella term for data-driven digital technologies that use sophisticated algorithms to perform cognitive tasks in "human-like" ways (i.e., learn, assess, decide, act, create).

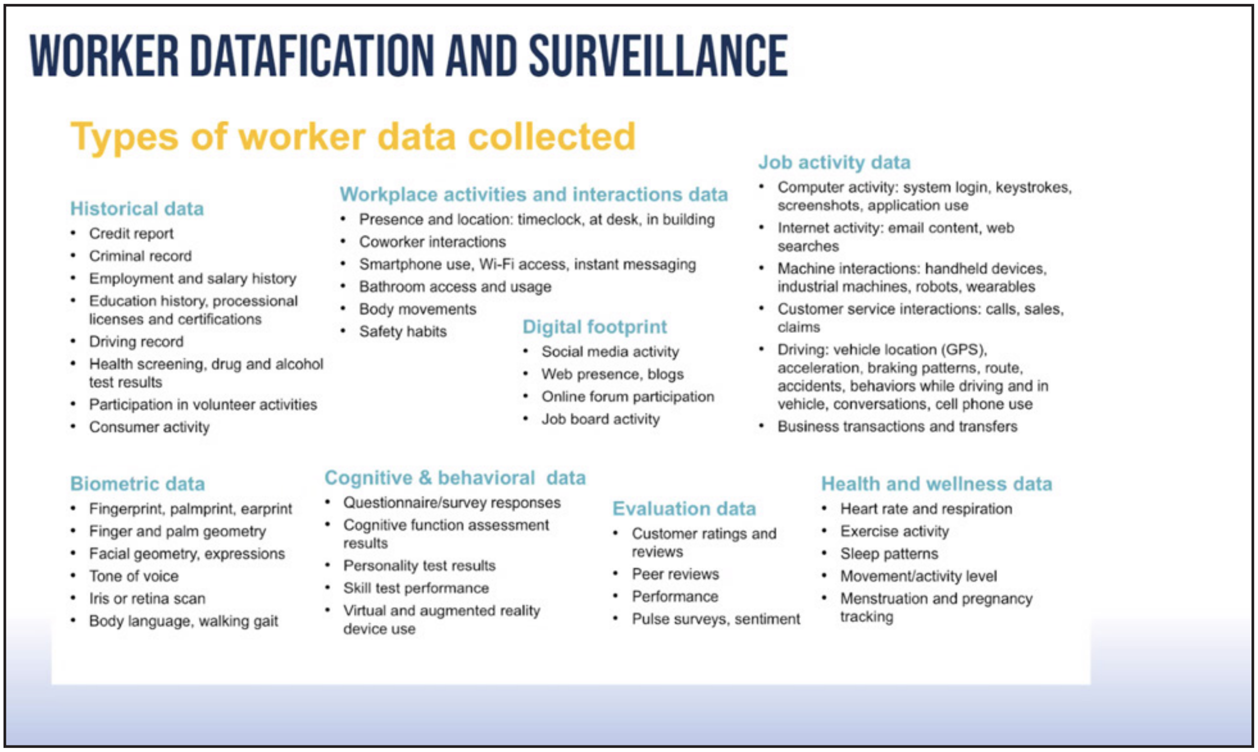
- **Generative AI:** Cutting-edge AI that takes natural language prompts and generates original text, images, audio, and video.
  - E.g. ChatGPT, Stable Diffusion
  - Training Data + Machine Learning + Compute → AI Models



DEFINITIONS, CONTINUED...

AI

- **Workplace AI System:** Any package of digital technologies deployed in the workplace that uses AI to undertake work- and employment-related activities.
  - E.g. Customer service chatbots, benefit fraud detection software, shift scheduling apps.
- **Worker Surveillance and Algorithmic Management:** A diverse set of workplace AI systems for carrying out typical management functions that relies on digitized surveillance of workers and sophisticated algorithms to hire, schedule, direct/assign tasks, monitor, evaluate, discipline, and even fire workers.
  - E.g. Amazon warehouses–cameras, wearables, handheld devices, etc.



WORKER DATAFICATION AND SURVEILLANCE

Types of worker data collected

Historical data

- Credit report
- Criminal record
- Employment and salary history
- Education history, processional licenses and certifications
- Driving record
- Health screening, drug and alcohol test results
- Participation in volunteer activities
- Consumer activity

Workplace activities and interactions data

- Presence and location: timeclock, at desk, in building
- Coworker interactions
- Smartphone use, Wi-Fi access, instant messaging
- Bathroom access and usage
- Body movements
- Safety habits

Digital footprint

- Social media activity
- Web presence, blogs
- Online forum participation
- Job board activity

Job activity data

- Computer activity: system login, keystrokes, screenshots, application use
- Internet activity: email content, web searches
- Machine interactions: handheld devices, industrial machines, robots, wearables
- Customer service interactions: calls, sales, claims
- Driving: vehicle location (GPS), acceleration, braking patterns, route, accidents, behaviors while driving and in vehicle, conversations, cell phone use
- Business transactions and transfers

Biometric data

- Fingerprint, palmprint, earprint
- Finger and palm geometry
- Facial geometry, expressions
- Tone of voice
- Iris or retina scan
- Body language, walking gait

Cognitive & behavioral data

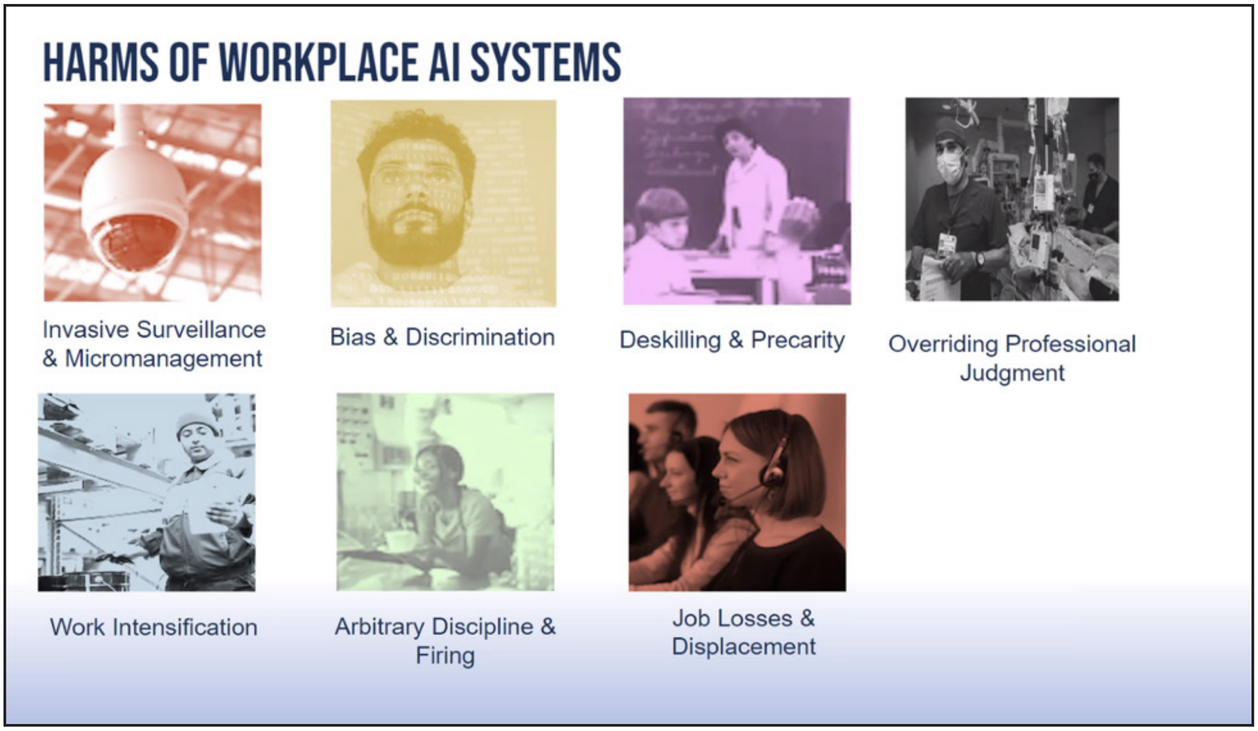
- Questionnaire/survey responses
- Cognitive function assessment results
- Personality test results
- Skill test performance
- Virtual and augmented reality device use

Evaluation data

- Customer ratings and reviews
- Peer reviews
- Performance
- Pulse surveys, sentiment

Health and wellness data

- Heart rate and respiration
- Exercise activity
- Sleep patterns
- Movement/activity level
- Menstruation and pregnancy tracking



HARMS OF WORKPLACE AI SYSTEMS

Invasive Surveillance & Micromanagement

Bias & Discrimination

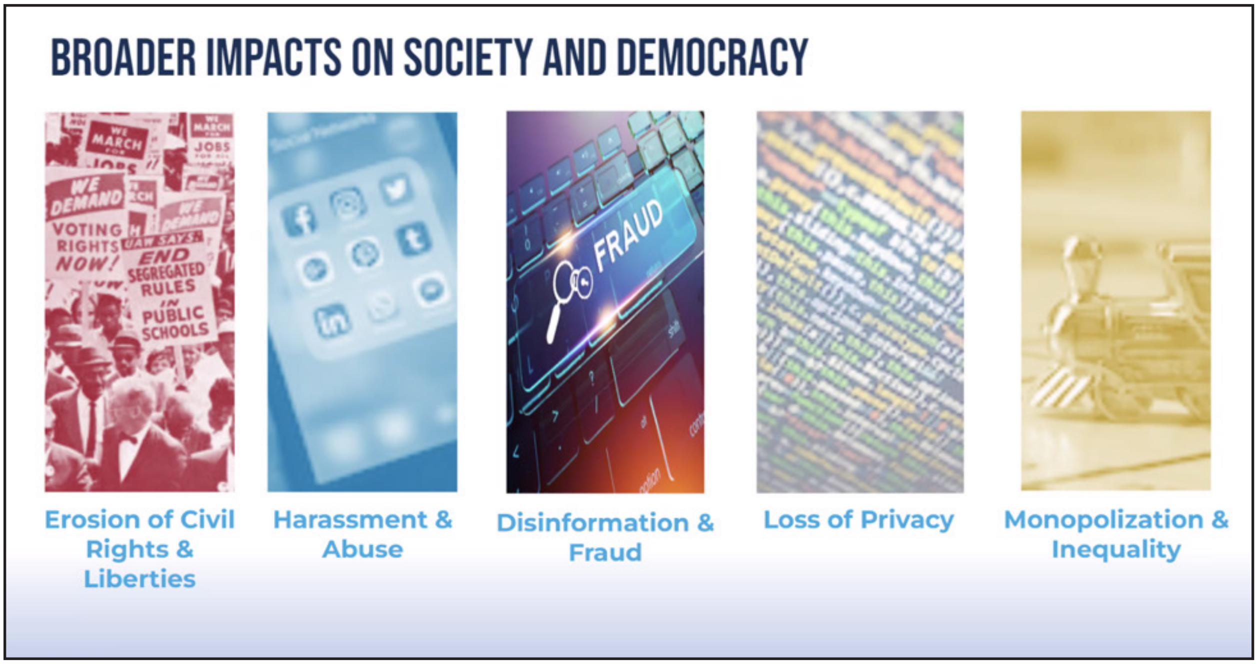
Deskilling & Precarity

Overriding Professional Judgment

Work Intensification

Arbitrary Discipline & Firing

Job Losses & Displacement



BROADER IMPACTS ON SOCIETY AND DEMOCRACY

WE MARCH FOR JOBS
WE DEMAND VOTING RIGHTS NOW!
UAW SAYS: END SEGREGATED RULES IN PUBLIC SCHOOLS
FRAUD

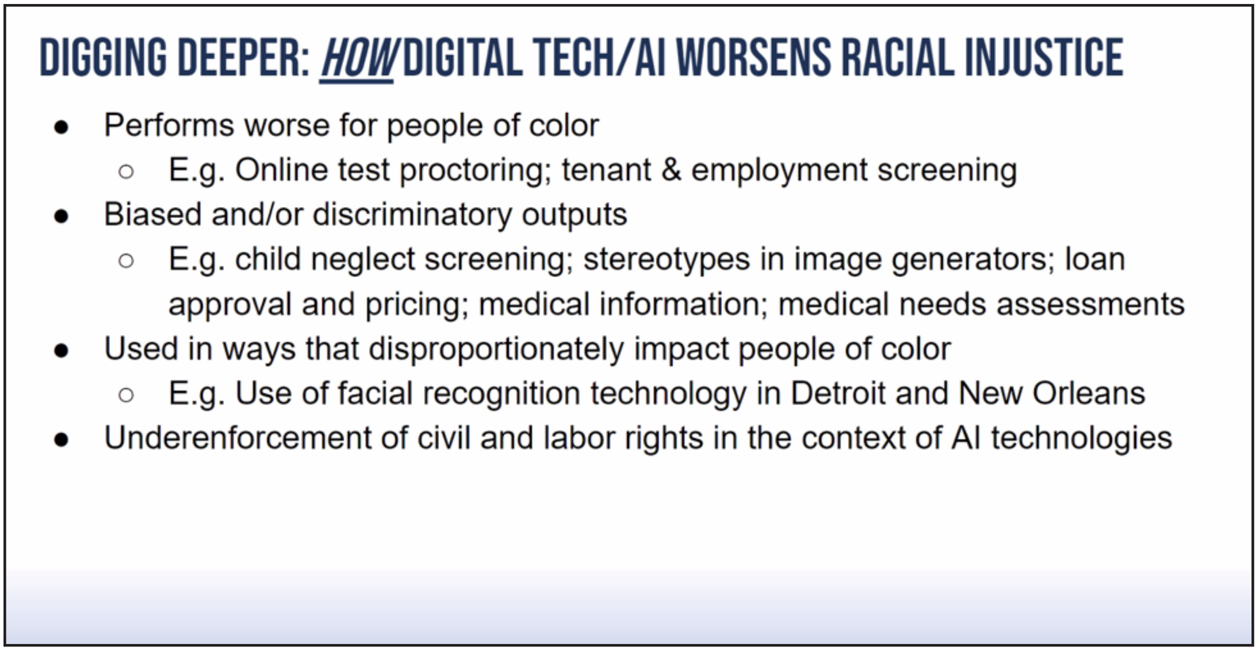
Erosion of Civil Rights & Liberties

Harassment & Abuse

Disinformation & Fraud

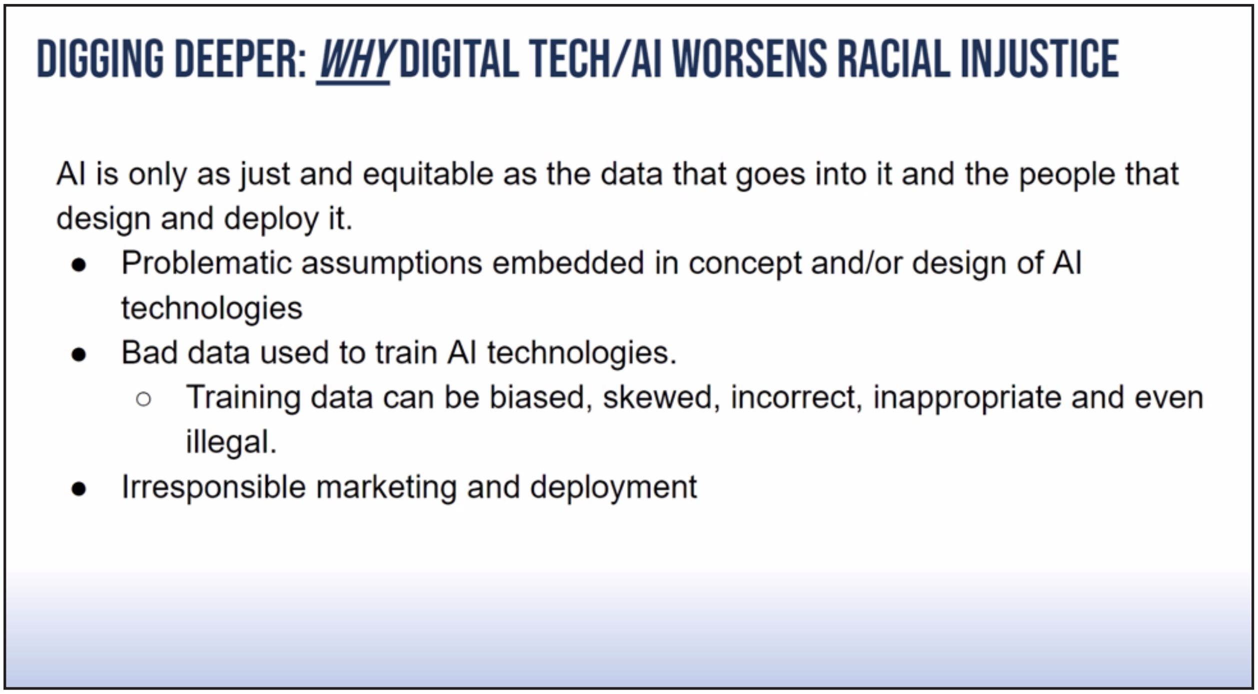
Loss of Privacy

Monopolization & Inequality



DIGGING DEEPER: *HOW* DIGITAL TECH/AI WORSENS RACIAL INJUSTICE

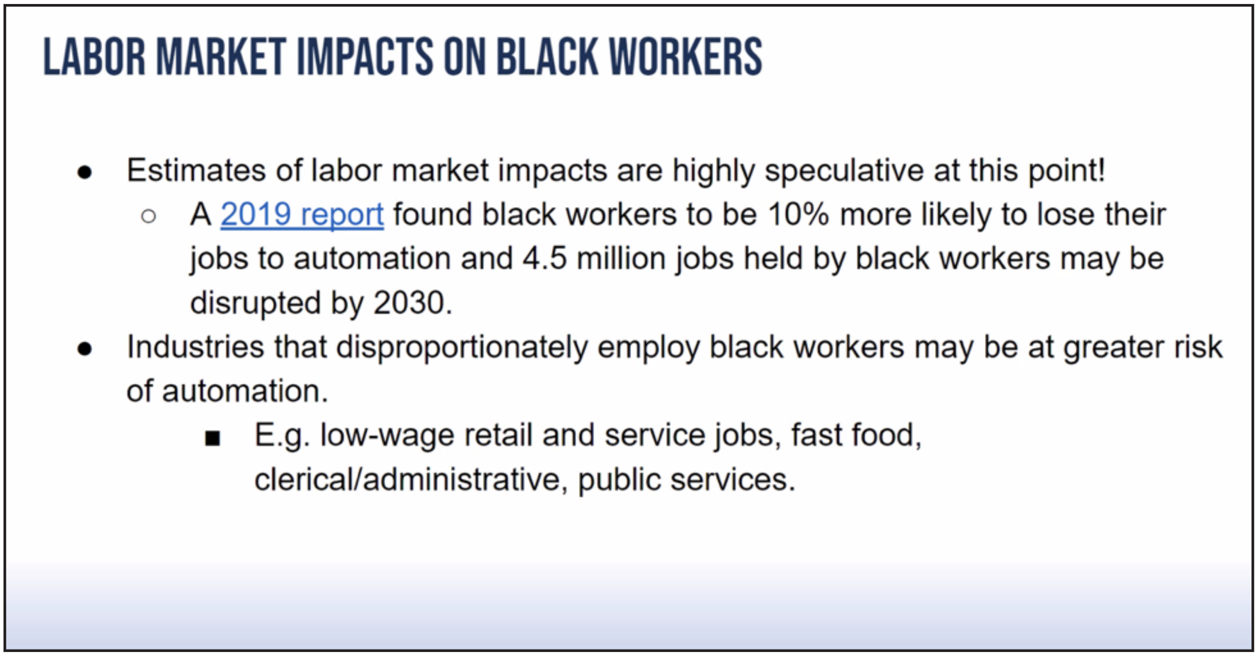
- Performs worse for people of color
  - E.g. Online test proctoring; tenant & employment screening
- Biased and/or discriminatory outputs
  - E.g. child neglect screening; stereotypes in image generators; loan approval and pricing; medical information; medical needs assessments
- Used in ways that disproportionately impact people of color
  - E.g. Use of facial recognition technology in Detroit and New Orleans
- Underenforcement of civil and labor rights in the context of AI technologies



DIGGING DEEPER: *WHY* DIGITAL TECH/AI WORSENS RACIAL INJUSTICE

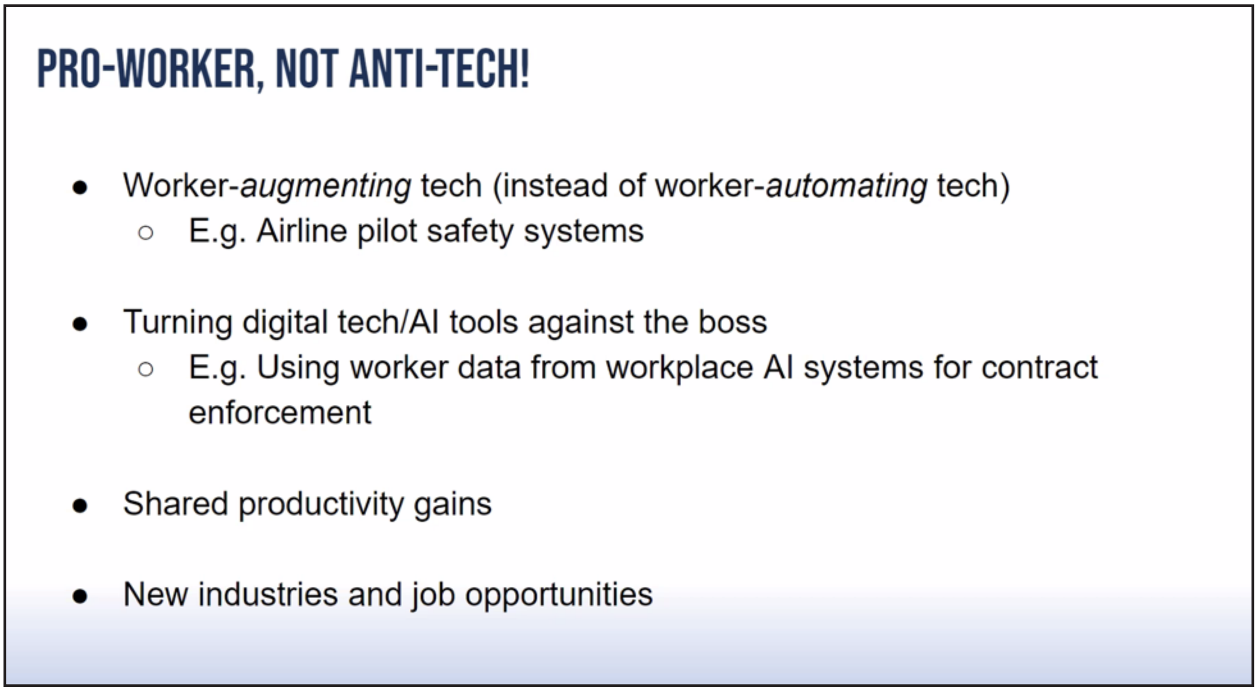
AI is only as just and equitable as the data that goes into it and the people that design and deploy it.

- Problematic assumptions embedded in concept and/or design of AI technologies
- Bad data used to train AI technologies.
  - Training data can be biased, skewed, incorrect, inappropriate and even illegal.
- Irresponsible marketing and deployment



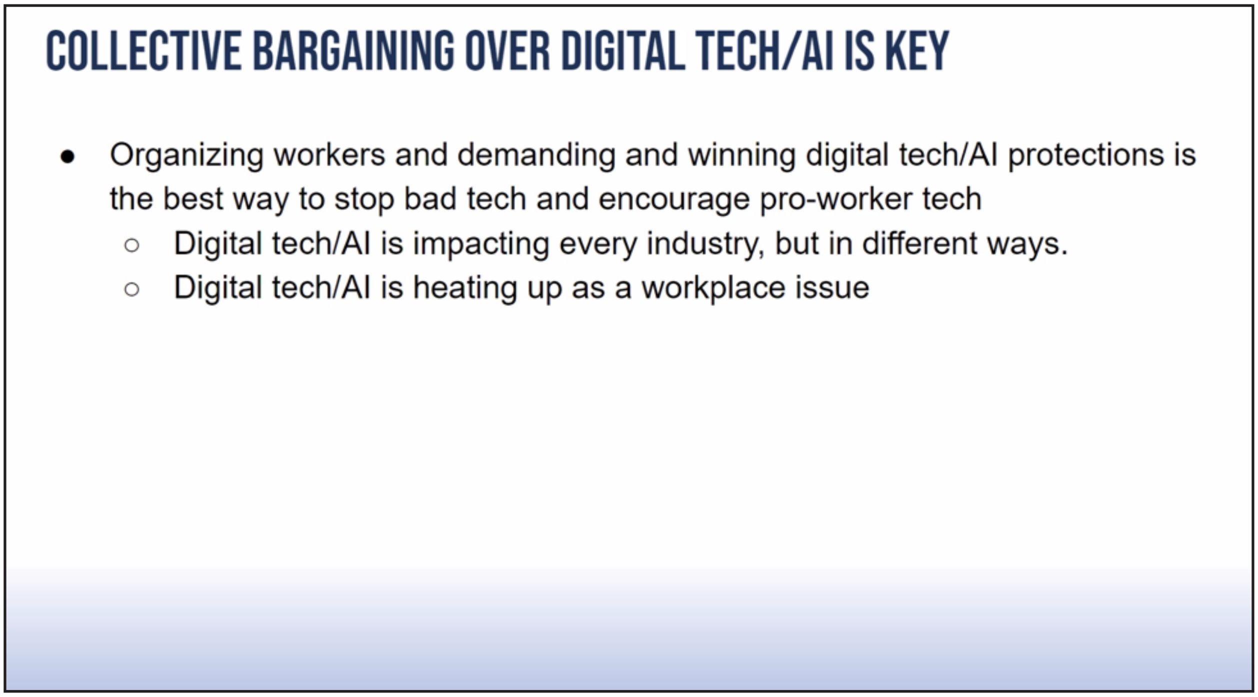
LABOR MARKET IMPACTS ON BLACK WORKERS

- Estimates of labor market impacts are highly speculative at this point!
  - A 2019 report found black workers to be 10% more likely to lose their jobs to automation and 4.5 million jobs held by black workers may be disrupted by 2030.
- Industries that disproportionately employ black workers may be at greater risk of automation.
    - E.g. low-wage retail and service jobs, fast food, clerical/administrative, public services.



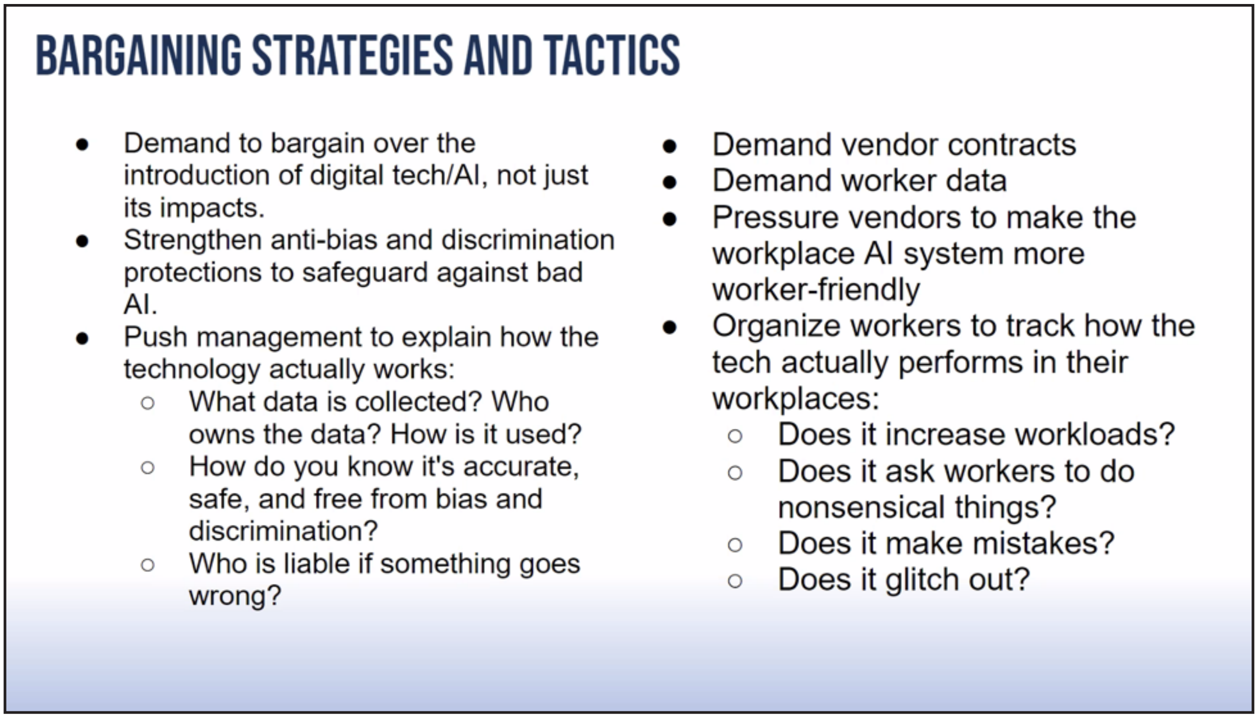
PRO-WORKER, NOT ANTI-TECH!

- Worker-*augmenting* tech (instead of worker-*automating* tech)
  - E.g. Airline pilot safety systems
- Turning digital tech/AI tools against the boss
  - E.g. Using worker data from workplace AI systems for contract enforcement
- Shared productivity gains
- New industries and job opportunities



COLLECTIVE BARGAINING OVER DIGITAL TECH/AI IS KEY

- Organizing workers and demanding and winning digital tech/AI protections is the best way to stop bad tech and encourage pro-worker tech
    - Digital tech/AI is impacting every industry, but in different ways.
    - Digital tech/AI is heating up as a workplace issue



BARGAINING STRATEGIES AND TACTICS

- Demand to bargain over the introduction of digital tech/AI, not just its impacts.
- Strengthen anti-bias and discrimination protections to safeguard against bad AI.
- Push management to explain how the technology actually works:
    - What data is collected? Who owns the data? How is it used?
    - How do you know it's accurate, safe, and free from bias and discrimination?
    - Who is liable if something goes wrong?
- Demand vendor contracts
- Demand worker data
- Pressure vendors to make the workplace AI system more worker-friendly
- Organize workers to track how the tech actually performs in their workplaces:
    - Does it increase workloads?
    - Does it ask workers to do nonsensical things?
    - Does it make mistakes?
    - Does it glitch out?

GLOSSARY OF DIGITAL/AI TERM

This glossary consists of key terms from the digital world and digitized workplaces. They are in alphabetical order.

Algorithm: In its simplest form, an algorithm is a set of rules in computer programming code to solve a problem or perform a task. An algorithm is fed data. It is a person, such as a manager or programmer, who sets the goal of the task or problem and writes algorithms to tell the computer system what to do and how to do it. These are the so-called instructions. The computer system is then able to independently perform tasks by following the instructions outlined by the algorithm. (For more information, see: What is an algorithm? See also the section below "Machine Learning"

Algorithmic system: An algorithmic system is a system that uses one or more algorithms, usually as part of computer software, to produce output that can be used to make decisions.

Algorithmic management: The concept of algorithmic management can be broadly defined as the delegation of management functions to algorithmic and automated systems. According to the organization Data & Society, algorithmic management is a diverse set of technological tools and techniques that structure working conditions and remotely manage the workforce.

Artificial intelligence (AI): Artificial intelligence refers to machines (e.g. computer systems) that are able to mimic human abilities to perceive their environment, learn, reason and act (perform tasks). In the broadest sense, AI refers to machines that can learn, reason and act by themselves. They can make their own decisions when faced with new situations, in the same way that humans and animals can.

The vast majority of systems that are called artificial intelligence today are actually machine learning systems (see below). In addition to machine learning and automated decision-making systems, there are some other types of artificial intelligence that have specific applications in the workplace:

Computer Vision (CV): analysis of visual information (static images or video streams) to recognize and classify images, objects, activities or events, individual faces, intentions. Some CV systems are designed to monitor human-to-human interaction.

Natural Language Processing (NLP): is the analysis of written and spoken language to recognize and classify words and to understand and generate written and spoken language. Other types of NLP applications are machine translation, chatbots, social media analysis, voice assistants, text summarization, information retrieval and emotional analysis.

Speech recognition: Analyzing audio (e.g. phone calls, conversations, voice commands) to recognize and process spoken language into text. Speech recognition can also be used to process text into spoken language.

Robotics: Hardware systems that can perform physical tasks such as movement and

interact with and adapt to changes in the physical world. Robots run on software systems that have varying degrees of complexity; the most advanced robots rely on learning algorithms, computer vision and natural language processing.
For more information see this short video: Artificial Intelligence Explained in 2 min and this article: What is AI?)

Automated decision-making systems (ADS): Semi-automated decision-making systems can be used to support human decision-making by providing recommendations to humans, while fully-automated ADS systems execute the decision without human involvement. Examples of ADS in use are fraud detection, social welfare eligibility determination, scheduling optimization, driving route optimization, planning and task allocation. Thus, there is often an overlap between ADS and "algorithmic management."

Big data: Extremely large and complex data sets that are analyzed using very high computing power and speed. Data is continuously collected from a variety of sources, including business transactions, IoT devices, sensors, RFID tags, industrial equipment, videos, social media, etc. Big data is used by artificial intelligence or machine learning to reveal patterns, trends, and associations, especially in the context of human behavior and interactions.

Data: Data can be seen as the smallest unit of information that can be used as a basis for calculation, reasoning or discussion. Data must be processed to be meaningful. See more under

Data analytics, Employee data and Personal data respectively.

Data analytics: Data analytics is a broad term that encompasses many different types of analysis designed to extract insights, identify trends, optimize processes or solve problems. Two common types of advanced data analysis techniques used in the workplace are predictive and prescriptive analytics. Predictive analytics uses techniques such as forecasting, statistical modeling or machine learning to make predictions about what outcome is likely to happen in the future. Prescriptive analytics uses techniques such as machine learning to recommend a course of action that will deliver the desired results. These forms of advanced analytics are increasingly embedded in automated digital systems that combine data collection and analysis to make predictions and decisions.

Controller and processor: Concepts used in data protection regulations. In short, the controller determines why (for what purpose) and how (by what means) personal data is processed. A data processor, on the other hand, is someone who processes personal data on behalf of the controller - i.e. on the instructions of the controller.

Data protection: In the US, data protection regulations vary across states. The General Data Protection Regulation (GDPR) in Europe is said to be the gold standard setting a number of requirements towards employers, including: transparency, data minimization and impact assessments. See the descriptions for these in this document.

Data minimization: The principle of "data minimization" is especially known from the European Data Protection Regulation, the GDPR. It implies that a data controller should limit the collection of personal data to what is directly relevant and necessary to achieve a specific purpose. They should also only retain the data for as long as necessary to fulfill that purpose. In other words, controllers should only collect the personal data they really need and should only keep it for as long as they need it.

This means that employers are not allowed to collect a lot of data because they might need it one day. They are also not allowed to permanently store data and personal information about their employees because it goes against the protection of individual rights.

Data Protection Impact assessments (DPIA): Required by law in 2023 in California, Colorado and Virginia. The requirements are similar in many ways to the existing requirements for DPIA's under the European Union's General Data Protection Regulation (the "GDPR"). Although the terms differ among jurisdictions, the basic concepts are substantially similar.
See the UK DPA's detailed guidance on DPIAs here. The European Commission's here

Digital systems: Digital systems include hardware and software designed to collect, store, process and communicate information (data) in digital (binary numbers) form. Key components of digital systems include 1) input and output devices (e.g. keyboard, camera, microphone, monitor, speakers), 2) memory and 3) central processing unit (CPU). Computers and smartphones are examples of digital systems. Algorithms are also a key component of digital computing systems. Digital systems can be connected to form a network (see also Internet of Things).

Electronic monitoring: Electronic monitoring is a particularly invasive form of data collection that involves systematic and continuous monitoring and recording of employee behavior and actions. Although not new, electronic monitoring has become more common with the development of internet-connected devices with built-in sensors that can capture a wide range of data about employees' location, activities and interactions with coworkers (see Internet of Things definition). Electronic monitoring is often embedded in the measurement of the work process rather than specifically focusing on tracking the employee.

Employee data - collecting data from workers: Employers can collect a wide range of data about employees. Some of this data is collected in the workplace, such as computer activity, location in the building, customer reviews, bathroom usage, coworker interactions and smartphone app interactions. Other types of data are purchased from third parties, such as social media activity, credit reports, driving history and consumer activity. Some of this data, such as criminal background checks, has been collected by employers abroad for decades. In some countries, employers have partnered with wellness programs and technology providers to collect biometric and health and wellness data as new wearable sensors have become available. Data collected from employees is personal data (see below)

Generative AI: Typically takes on 2 forms:

- Large language models (LLMs), such as the one that underpins ChatGPT, which generate plausible-sounding text in response to a human prompt in the form of a request (e.g. 'write a sonnet about the risks of AI in the style of Shakespeare')
- Multi-modal models, such as Stable Diffusion, Midjourney, or OpenAI's DALL-E 2,typically take text prompts (e.g. 'a purple penguin wearing sunglasses') and generate images as an

output. Some models, such as GPT-4, can also take images as input (e.g. a photo of your fridge's contents) to produce text as the output (e.g. a recipe for the ingredients you have). Multi-modal models that can generate audio and video outputs are also in development.

Generative AI systems are trained on huge datasets of text, images, and other media in order to produce similar but synthetic content. These systems make predictions about the text likely to follow a given prompt: they generate content as their output - hence the term 'generative AI.' Such systems can imitate the work of writers or artists included in their training data – but they will also replicate any biases from the content they are trained on, such as racist language or sexist imagery.

Read more about Generative AI by Access Now here

Human oversight/human in command: These two concepts are used in the context of artificial intelligence systems that are designed to support human autonomy and decision-making, as prescribed by the principle of respect for human autonomy. This requires that AI systems must both enable a democratic, thriving and just society by supporting user agency and promoting fundamental rights, and allow for human oversight (stewardship of the systems). Read more in the document The Ethics Guidelines for Trustworthy Artificial Intelligence (AI).

Internet of Things (IoT): IoT refers to a system of devices ("things") connected to the internet to transmit and receive data, such as physical objects, industrial machines, WiFi-connected cameras, workplace and handheld devices, wearables (e.g. wristbands), smartwatches and fitness trackers, etc. IoT devices use embedded sensors (see sensor definition) to collect data and then share the data through a wireless network to other internet-connected devices (e.g. smartphones) for remote monitoring and interaction (control) or computers for processing, storage and in some cases real-time analysis and use. (For more information, see this video: What is the internet of things).

Machine learning, deep learning and neural networks: These are subcategories of AI and cover the more advanced algorithms and algorithmic systems. A common term is that they are "learning algorithms". They enable computers to perform a specific task without a human explicitly writing the rules (instructions) for how the computer should perform the task. What happens is that the algorithm is given data, a goal and feedback when it's on the right path. It then learns on its own how to continue. We humans can control what data goes in and we can see the result that comes out, but these forms of artificial intelligence are often so complicated that we can't always understand how the algorithm arrived at a certain result (for more information, see article: What is machine learning?).

Personal data: GDPR defines personal data as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Online identifiers such as IP addresses are now considered personal data unless they are anonymized. Pseudonymized personal data is also subject to GDPR if it is possible to identify whose data it is by reverse engineering.

“Privacy by design and default”: Privacy-by-design and/or default is about how data protection is built into a company’s products, services and business processes from the outset.

● Privacy-by-design is an approach that ensures that a company incorporates data protection as an integral part of its business processes, value chain and product lifecycle. From the production phase to the product reaching the end user.

● Privacy-by-default means that products are set up from the start to ensure the highest level of personal data protection.

Profiling: Profiling, in short, is the classification of a person’s personality, behavior, interests and habits. It’s important to remember that profiling is also done on everything we DON’T do, have interests or habits. Profiling is typically used to make predictions and is based on analysis of collected data (for more information, see this webpage from the UK Data Protection Board). Profiling can have immediate effects – someone is hired, promoted, disciplined or fire. And importantly, profiling can have future effects as profiles created can open or close opportunities for future workers.

Sensors: Sensors detect, measure and transmit information about the environmental context around the sensor and/or physical and behavioral characteristics of a human wearing the sensor. They can capture precise measurements of the physical environment and can distinguish human characteristics, activities and interactions with machines and devices. Sensors can be embedded in a variety of objects (see Internet of Things definition), wearables, personal devices (e.g. smartphones), etc.

Transparency: Transparency requirements in the private sector vary by state: In the CCPA-CPRA transparency requirements cover 1. What types of information are collected; 2. For what purpose they are being collected; 3. Specifics of what is being collected; 4. Disclosure of where data is being shared. In Virginia, the VCDPA requirements include: 1. Stating what categories of personal data are collected; 2. Obtaining affirmative consent for sensitive data before collecting it; 3. Providing an option for access and correct personal information; 4. Providing opt-out mechanisms; 5. Providing data protection assessments; 6. Honor deletion requests; 7. Provide data breach notifications.

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

(full text accessed on March 8, 2024 here: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/)

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. Artificial intelligence (AI) holds extraordinary potential for both promise and peril. Responsible AI use has the potential to help solve urgent challenges while making our world more prosperous, productive, innovative, and secure. At the same time, irresponsible use could exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security. Harnessing AI for good and realizing its myriad benefits requires mitigating its substantial risks. This endeavor demands a society-wide effort that includes government, the private sector, academia, and civil society.

My Administration places the highest urgency on governing the development and use of AI safely and responsibly, and is therefore advancing a coordinated, Federal Government-wide approach to doing so. The rapid speed at which AI capabilities are advancing compels the United States to lead in this moment for the sake of our security, economy, and society.

In the end, AI reflects the principles of the people who build it, the people who use it, and the data upon which it is built. I firmly believe that the power of our ideals; the foundations of our society; and the creativity, diversity, and decency of our people are the reasons that America thrived in past eras of rapid change. They are the reasons we will succeed again in this moment. We are more than capable of harnessing AI for justice, security, and opportunity for all.

Sec. 2. Policy and Principles. It is the policy of my Administration to advance and govern the development and use of AI in accordance with eight guiding principles and priorities. When undertaking the actions set forth in this order, executive departments and agencies (agencies) shall, as appropriate and consistent with applicable law, adhere to these principles, while, as feasible, taking into account the views of other agencies, industry, members of academia, civil society, labor unions, international allies and partners, and other relevant organizations:

(a) Artificial Intelligence must be safe and secure. Meeting this goal requires robust, reliable, repeatable, and standardized evaluations of AI systems, as well as policies, institutions, and, as appropriate, other mechanisms to test, understand, and mitigate risks from these systems before they are put to use. It also requires addressing AI systems' most pressing security risks — including with respect to biotechnology, cybersecurity, critical infrastructure, and other national security dangers — while navigating AI's opacity and complexity. Testing and evaluations, including post-deployment performance monitoring, will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies. Finally, my Administration will help develop effective labeling and content provenance mechanisms, so that Americans are able to determine when content is generated using AI and when it is not. These actions will provide a vital foundation for an approach that addresses AI's risks without unduly reducing its benefits.

(b) 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. This effort requires investments in AI-related education, training, development, research, and capacity, while simultaneously tackling novel intellectual property (IP) questions and other problems to protect inventors and creators. Across the Federal Government, my Administration will support programs to provide Americans the skills they need for the age of AI and attract the world's AI talent to our shores — not just to study, but to stay — so that the companies and technologies of the future are made in America. The Federal Government will promote a fair, open, and competitive ecosystem and marketplace for AI and related technologies so that small developers and entrepreneurs can continue to drive innovation. Doing so requires stopping unlawful collusion and addressing risks from dominant firms' use of key assets such as semiconductors, computing power, cloud storage, and data to disadvantage competitors, and it requires supporting a marketplace that harnesses the benefits of AI to provide new opportunities for small businesses, workers, and entrepreneurs.

(c) The responsible development and use of AI require a commitment to supporting American workers. As AI creates new jobs and industries, all workers need a seat at the table, including through collective bargaining, to ensure that they benefit from these opportunities. My Administration will seek to adapt job training and education to support a diverse workforce and help provide access to opportunities that AI creates. In the workplace itself, AI should not be deployed in ways that undermine rights, worsen job quality, encourage undue worker surveillance, lessen market competition, introduce new health and safety risks, or cause harmful labor-force disruptions. The critical next steps in AI development should be built on the views of workers, labor unions, educators, and employers to support responsible uses of AI that improve workers' lives, positively augment human work, and help all people safely enjoy the gains and opportunities from technological innovation.

(d) Artificial Intelligence policies must be consistent with my Administration's dedication to advancing equity and civil rights. My Administration cannot — and will not — tolerate the use of AI to disadvantage those who are already too often denied equal opportunity and justice. From hiring to housing to healthcare, we have seen what happens when AI use deepens discrimination and bias, rather than improving quality of life. Artificial Intelligence systems deployed irresponsibly have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms. My Administration will build on the important steps that have already been taken — such as issuing the Blueprint for an AI Bill of Rights, the AI Risk Management Framework, and Executive Order 14091 of February 16, 2023 (Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government) — in seeking to ensure that AI complies with all Federal laws and to promote robust technical evaluations, careful oversight, engagement with affected communities, and rigorous regulation. It is necessary to hold those developing and deploying AI accountable to standards that protect against unlawful discrimination and abuse, including in the justice system and the Federal Government. Only then can Americans trust AI to advance civil rights, civil liberties, equity, and justice for all.

(e) The interests of Americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected. Use of new technologies, such as AI, does not excuse organizations from their legal obligations, and hard-won consumer protections are more important than ever in moments of technological change. The Federal Government will enforce existing consumer protection laws and principles and enact appropriate safeguards against fraud, unintended bias, discrimination, infringements on privacy, and other harms from AI. Such protections are especially important in critical fields like healthcare, financial services, education, housing, law, and transportation, where mistakes by or misuse of AI could harm patients, cost consumers or small businesses, or jeopardize safety or rights. At the same time, my Administration will promote responsible uses of AI that protect consumers, raise the quality of goods and services, lower their prices, or expand selection and availability.

(f) Americans' privacy and civil liberties must be protected as AI continues advancing. Artificial Intelligence is making it easier to extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires. Artificial Intelligence's capabilities in these areas can increase the risk that personal data could be exploited and exposed. To combat this risk, the Federal Government will ensure that the collection, use, and retention of data is lawful, is secure, and mitigates privacy and confidentiality risks. Agencies shall use available policy and technical tools, including privacy-enhancing technologies (PETs) where appropriate, to protect privacy and to combat the broader legal and societal risks — including the chilling of First Amendment rights — that result from the improper collection and use of people's data.

(g) 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. These efforts start with people, our Nation's greatest asset. My Administration will take steps to attract, retain, and develop public service-oriented AI professionals, including from underserved communities, across disciplines — including technology, policy, managerial, procurement, regulatory, ethical, governance, and legal fields — and ease AI professionals' path into the Federal Government to help harness and govern AI. The Federal Government will work to ensure that all members of its workforce receive adequate training to understand the benefits, risks, and limitations of AI for their job functions, and to modernize Federal Government information technology infrastructure, remove bureaucratic obstacles, and ensure that safe and rights-respecting AI is adopted, deployed, and used.

(h) 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. This leadership is not measured solely by the technological advancements our country makes. Effective leadership also means pioneering those systems and safeguards needed to deploy technology responsibly — and building and promoting those safeguards with the rest of the world. My Administration will engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges. The Federal Government will seek to promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms.

Sec. 3. Definitions. For purposes of this order:

(a) The term "agency" means each agency described in 44 U.S.C. 3502(1), except for the independent regulatory agencies described in 44 U.S.C. 3502(5).

(b) The term “artificial intelligence” or “AI” has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

(c) The term “AI model” means a component of an information system that implements AI technology and uses computational, statistical, or machine-learning techniques to produce outputs from a given set of inputs.

(d) The term “AI red-teaming” means a structured testing effort to find flaws and vulnerabilities in an AI system, often in a controlled environment and in collaboration with developers of AI. Artificial Intelligence red-teaming is most often performed by dedicated “red teams” that adopt adversarial methods to identify flaws and vulnerabilities, such as harmful or discriminatory outputs from an AI system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

(e) The term “AI system” means any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

(f) The term “commercially available information” means any information or data about an individual or group of individuals, including an individual’s or group of individuals’ device or location, that is made available or obtainable and sold, leased, or licensed to the general public or to governmental or non-governmental entities.

(g) The term “crime forecasting” means the use of analytical techniques to attempt to predict future crimes or crime-related information. It can include machine-generated predictions that use algorithms to analyze large volumes of data, as well as other forecasts that are generated without machines and based on statistics, such as historical crime statistics.

(h) The term “critical and emerging technologies” means those technologies listed in the February 2022 Critical and Emerging Technologies List Update issued by the National Science and Technology Council (NSTC), as amended by subsequent updates to the list issued by the NSTC.

(i) The term “critical infrastructure” has the meaning set forth in section 1016(e) of the USA PATRIOT Act of 2001, 42 U.S.C. 5195c(e).

(j) The term “differential-privacy guarantee” means protections that allow information about a group to be shared while provably limiting the improper access, use, or disclosure of personal information about particular entities.

(k) The term “dual-use foundation model” means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters, such as by:

(i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons;

(ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or

(iii) permitting the evasion of human control or oversight through means of deception or obfuscation.

Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities.

(l) The term “Federal law enforcement agency” has the meaning set forth in section 21(a) of Executive Order 14074 of May 25, 2022 (Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety).

(m) The term “floating-point operation” means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base.

(n) The term “foreign person” has the meaning set forth in section 5(c) of Executive Order 13984 of January 19, 2021 (Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities).

(o) The terms “foreign reseller” and “foreign reseller of United States Infrastructure as a Service Products” mean a foreign person who has established an Infrastructure as a Service Account to provide Infrastructure as a Service Products subsequently, in whole or in part, to a third party.

(p) The term “generative AI” means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include images, videos, audio, text, and other digital content.

(q) The terms “Infrastructure as a Service Product,” “United States Infrastructure as a Service Product,” “United States Infrastructure as a Service Provider,” and “Infrastructure as a Service Account” each have the respective meanings given to those terms in section 5 of Executive Order 13984.

(r) The term “integer operation” means any mathematical operation or assignment involving only integers, or whole numbers expressed without a decimal point.

(s) The term “Intelligence Community” has the meaning given to that term in section 3.5(h) of Executive Order 12333 of December 4, 1981 (United States Intelligence Activities), as amended.

(t) The term “machine learning” means a set of techniques that can be used to train AI algorithms to improve performance at a task based on data.

(u) The term “model weight” means a numerical parameter within an AI model that helps determine the model’s outputs in response to inputs.

(v) The term “national security system” has the meaning set forth in 44 U.S.C. 3552(b)(6).

(w) The term “omics” means biomolecules, including nucleic acids, proteins, and metabolites, that make up a cell or cellular system.

(x) The term “Open RAN” means the Open Radio Access Network approach to telecommunications-network standardization adopted by the O-RAN Alliance, Third Generation Partnership Project, or any similar set of published open standards for multi-vendor network equipment interoperability.

(y) The term “personally identifiable information” has the meaning set forth in Office of Management and Budget (OMB) Circular No. A-130.

(z) The term “privacy-enhancing technology” means any software or hardware solution, technical process, technique, or other technological means of mitigating privacy risks arising from data processing, including by enhancing predictability, manageability, disassociability, storage, security, and confidentiality. These technological means may include secure multiparty computation, homomorphic encryption, zero-knowledge proofs, federated learning, secure enclaves, differential privacy, and synthetic-data-generation tools. This is also sometimes referred to as “privacy-preserving technology.”

(aa) The term “privacy impact assessment” has the meaning set forth in OMB Circular No. A-130.

(bb) The term “Sector Risk Management Agency” has the meaning set forth in 6 U.S.C. 650(23).

(cc) The term “self-healing network” means a telecommunications network that automatically diagnoses and addresses network issues to permit self-restoration.

(dd) The term “synthetic biology” means a field of science that involves redesigning organisms, or the biomolecules of organisms, at the genetic level to give them new characteristics. Synthetic nucleic acids are a type of biomolecule redesigned through synthetic-biology methods.

(ee) The term “synthetic content” means information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI.

(ff) The term “testbed” means a facility or mechanism equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI and PETs, to help evaluate the functionality, usability, and performance of those tools or technologies.

(gg) The term “watermarking” means the act of embedding information, which is typically difficult to remove, into outputs created by AI — including into outputs such as photos, videos, audio clips, or text — for the purposes of verifying the authenticity of the output or the identity or characteristics of its provenance, modifications, or conveyance.

Sec. 4. Ensuring the Safety and Security of AI Technology.

4.1. Developing Guidelines, Standards, and Best Practices for AI Safety and Security. (a) Within

270 days of the date of this order, to help ensure the development of safe, secure, and trustworthy AI systems, the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology (NIST), in coordination with the Secretary of Energy, the Secretary of Homeland Security, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall:

(i) Establish guidelines and best practices, with the aim of promoting consensus industry standards, for developing and deploying safe, secure, and trustworthy AI systems, including:

(A) developing a companion resource to the AI Risk Management Framework, NIST AI 100-1, for generative AI;

(B) developing a companion resource to the Secure Software Development Framework to incorporate secure development practices for generative AI and for dual-use foundation models; and

(C) launching an initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity.

(ii) Establish appropriate guidelines (except for AI used as a component of a national security system), including appropriate procedures and processes, to enable developers of AI, especially of dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems. These efforts shall include:

(A) coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models; and

(B) in coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as to support the design, development, and deployment of associated PETs, consistent with section 9(b) of this order.

(b) Within 270 days of the date of this order, to understand and mitigate AI security risks, the Secretary of Energy, in coordination with the heads of other Sector Risk Management Agencies (SRMAs) as the Secretary of Energy may deem appropriate, shall develop and, to the extent permitted by law and available appropriations, implement a plan for developing the Department of Energy's AI model evaluation tools and AI testbeds. The Secretary shall undertake this work using existing solutions where possible, and shall develop these tools and AI testbeds to be capable of assessing near-term extrapolations of AI systems' capabilities. At a minimum, the Secretary shall develop tools to evaluate AI capabilities to generate outputs that may represent nuclear, nonproliferation, biological, chemical, critical infrastructure, and energy-security threats or hazards. The Secretary shall do this work solely for the purposes of guarding against these threats, and shall also develop model guardrails that reduce such risks. The Secretary shall, as appropriate, consult with private AI laboratories, academia, civil society, and third-party evaluators, and shall use existing solutions.

4.2. Ensuring Safe and Reliable AI. (a) Within 90 days of the date of this order, to ensure and verify the continuous availability of safe, reliable, and effective AI in accordance with the Defense Production Act, as amended, 50 U.S.C. 4501 et seq., including for the national defense and the protection of critical infrastructure, the Secretary of Commerce shall require:

(i) Companies developing or demonstrating an intent to develop potential dual-use foundation models to provide the Federal Government, on an ongoing basis, with information, reports, or records regarding the following:

(A) any ongoing or planned activities related to training, developing, or producing dual-use foundation models, including the physical and cybersecurity protections taken to assure the integrity of that training process against sophisticated threats;

(B) the ownership and possession of the model weights of any dual-use foundation models, and the physical and cybersecurity measures taken to protect those model weights; and

(C) the results of any developed dual-use foundation model's performance in relevant AI red-team testing based on guidance developed by NIST pursuant to subsection 4.1(a)(ii) of this section, and a description of any associated measures the company has taken to meet safety objectives, such as mitigations to improve performance on these red-team tests and strengthen overall model security. Prior to the development of guidance on red-team testing standards by NIST pursuant to subsection 4.1(a)(ii) of this section, this description shall include the results of any red-team testing that the company has conducted relating to lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors; the discovery of software vulnerabilities and development of associated exploits; the use of software or tools to influence real or virtual events; the possibility for self-replication or propagation; and associated measures to meet safety objectives; and

(ii) Companies, individuals, or other organizations or entities that acquire, develop, or possess a potential large-scale computing cluster to report any such acquisition, development, or possession, including the existence and location of these clusters and the amount of total computing power available in each cluster.

(b) The Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Secretary of Energy, and the Director of National Intelligence, shall define, and thereafter update as needed on a regular basis, the set of technical conditions for models and computing clusters that would be subject to the reporting requirements of subsection 4.2(a) of this section. Until such technical conditions are defined, the Secretary shall require compliance with these reporting requirements for:

(i) any model that was trained using a quantity of computing power greater than 1026 integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 1023 integer or floating-point operations; and

(ii) any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 1020 integer or floating-point operations per second for training AI.

(c) Because I find that additional steps must be taken to deal with the national emergency related to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities), as amended by Executive Order 13757 of December 28, 2016 (Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities), and further amended by Executive Order 13984, to address the use of United States Infrastructure as a Service (IaaS) Products by foreign malicious cyber actors, including to impose additional record-keeping obligations with respect to foreign transactions and to assist in the investigation of transactions involving foreign malicious cyber actors, I hereby direct the Secretary of Commerce, within 90 days of the date of this order, to:

(i) Propose regulations that require United States IaaS Providers to submit a report to the Secretary of Commerce when a foreign person transacts with that United States IaaS Provider to train a large AI model with potential capabilities that could be used in malicious cyber-enabled activity (a "training run"). Such reports shall include, at a minimum, the identity of the foreign person and the existence of any training run of an AI model meeting the criteria set forth in this section, or other criteria defined by the Secretary in regulations, as well as any additional information identified by the Secretary.

(ii) Include a requirement in the regulations proposed pursuant to subsection 4.2(c)(i) of this section that United States IaaS Providers prohibit any foreign reseller of their United States IaaS Product from providing those products unless such foreign reseller submits to the United States IaaS Provider a report, which the United States IaaS Provider must provide to the Secretary of Commerce, detailing each instance in which a foreign person transacts with the foreign reseller to use the United States IaaS Product to conduct a training run described in subsection 4.2(c)(i) of this section. Such reports shall include, at a minimum, the information specified in subsection 4.2(c)(i) of this section as well as any additional information identified by the Secretary.

(iii) Determine the set of technical conditions for a large AI model to have potential capabilities that could be used in malicious cyber-enabled activity, and revise that determination as necessary and appropriate. Until the Secretary makes such a determination, a model shall be considered to have potential capabilities that could be used in malicious cyber-enabled activity if it requires a quantity of computing power greater than 1026 integer or floating-point operations and is trained on a computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum compute capacity of 1020 integer or floating-point operations per second for training AI.

(d) Within 180 days of the date of this order, pursuant to the finding set forth in subsection 4.2(c) of this section, the Secretary of Commerce shall propose regulations that require United States IaaS Providers to ensure that foreign resellers of United States IaaS Products verify the identity of any foreign person that obtains an IaaS account (account) from the foreign reseller. These regulations shall, at a minimum:

(i) Set forth the minimum standards that a United States IaaS Provider must require of foreign resellers of its United States IaaS Products to verify the identity of a foreign person who opens an account or maintains an existing account with a foreign reseller, including:

(A) the types of documentation and procedures that foreign resellers of United States IaaS

Products must require to verify the identity of any foreign person acting as a lessee or sub-lessee of these products or services;

(B) records that foreign resellers of United States IaaS Products must securely maintain regarding a foreign person that obtains an account, including information establishing:

(1) the identity of such foreign person, including name and address;

(2) the means and source of payment (including any associated financial institution and other identifiers such as credit card number, account number, customer identifier, transaction identifiers, or virtual currency wallet or wallet address identifier);

(3) the electronic mail address and telephonic contact information used to verify a foreign person's identity; and

(4) the Internet Protocol addresses used for access or administration and the date and time of each such access or administrative action related to ongoing verification of such foreign person's ownership of such an account; and

(C) methods that foreign resellers of United States IaaS Products must implement to limit all third-party access to the information described in this subsection, except insofar as such access is otherwise consistent with this order and allowed under applicable law;

(ii) Take into consideration the types of accounts maintained by foreign resellers of United States IaaS Products, methods of opening an account, and types of identifying information available to accomplish the objectives of identifying foreign malicious cyber actors using any such products and avoiding the imposition of an undue burden on such resellers; and

(iii) Provide that the Secretary of Commerce, in accordance with such standards and procedures as the Secretary may delineate and in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, may exempt a United States IaaS Provider with respect to any specific foreign reseller of their United States IaaS Products, or with respect to any specific type of account or lessee, from the requirements of any regulation issued pursuant to this subsection. Such standards and procedures may include a finding by the Secretary that such foreign reseller, account, or lessee complies with security best practices to otherwise deter abuse of United States IaaS Products.

(e) The Secretary of Commerce is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by the International Emergency Economic Powers Act, 50 U.S.C. 1701 et seq., as may be necessary to carry out the purposes of subsections 4.2(c) and (d) of this section. Such actions may include a requirement that United States IaaS Providers require foreign resellers of United States IaaS Products to provide United States IaaS Providers verifications relative to those subsections.

4.3. Managing AI in Critical Infrastructure and in Cybersecurity. (a) To ensure the protection of critical
infrastructure, the following actions shall be taken:

(i) Within 90 days of the date of this order, and at least annually thereafter, the head of each agency with relevant regulatory authority over critical infrastructure and the heads of relevant SRMAs, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security for consideration of cross-sector risks, shall evaluate and provide to the Secretary of Homeland Security an assessment of potential risks related to the use of AI in critical infrastructure sectors involved, including ways in which deploying AI may make critical infrastructure systems more vulnerable to critical failures, physical attacks, and cyber attacks, and shall consider ways to mitigate these vulnerabilities. Independent regulatory agencies are encouraged, as they deem appropriate, to contribute to sector-specific risk assessments.

(ii) Within 150 days of the date of this order, the Secretary of the Treasury shall issue a public report on best practices for financial institutions to manage AI-specific cybersecurity risks.

(iii) Within 180 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of Commerce and with SRMAs and other regulators as determined by the Secretary of Homeland Security, shall incorporate as appropriate the AI Risk Management Framework, NIST AI 100-1, as well as other appropriate security guidance, into relevant safety and security guidelines for use by critical infrastructure owners and operators.

(iv) Within 240 days of the completion of the guidelines described in subsection 4.3(a)(iii) of this section, the Assistant to the President for National Security Affairs and the Director of OMB, in consultation with the Secretary of Homeland Security, shall coordinate work by the heads of agencies with authority over critical infrastructure to develop and take steps for the Federal Government to mandate such guidelines, or appropriate portions thereof, through regulatory or other appropriate action. Independent regulatory agencies are encouraged, as they deem appropriate, to consider whether to mandate guidance through regulatory action in their areas of authority and responsibility.

(v) The Secretary of Homeland Security shall establish an Artificial Intelligence Safety and Security Board as an advisory committee pursuant to section 871 of the Homeland Security Act of 2002 (Public Law 107-296). The Advisory Committee shall include AI experts from the private sector, academia, and government, as appropriate, and provide to the Secretary of Homeland Security and the Federal Government's critical infrastructure community advice, information, or recommendations for improving security, resilience, and incident response related to AI usage in critical infrastructure.

(b) To capitalize on AI's potential to improve United States cyber defenses:

(i) The Secretary of Defense shall carry out the actions described in subsections 4.3(b)(ii) and (iii) of this section for national security systems, and the Secretary of Homeland Security shall carry out these actions for non-national security systems. Each shall do so in consultation with the heads of other relevant agencies as the Secretary of Defense and the Secretary of Homeland Security may deem appropriate.

(ii) As set forth in subsection 4.3(b)(i) of this section, within 180 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall, consistent with applicable law, each develop plans for, conduct, and complete an operational pilot project to identify, develop, test, evaluate, and deploy AI capabilities, such as large-language models, to aid in the discovery and remediation of vulnerabilities in critical United States Government software, systems, and networks.

(iii) As set forth in subsection 4.3(b)(i) of this section, within 270 days of the date of this order, the Secretary of Defense and the Secretary of Homeland Security shall each provide a report to the Assistant to the President for National Security Affairs on the results of actions taken pursuant to the plans and operational pilot projects required by subsection 4.3(b)(ii) of this section, including a description of any vulnerabilities found and fixed through the development and deployment of AI capabilities and any lessons learned on how to identify, develop, test, evaluate, and deploy AI capabilities effectively for cyber defense.

4.4. Reducing Risks at the Intersection of AI and CBRN Threats. (a) To better understand and mitigate the risk of AI being misused to assist in the development or use of CBRN threats — with a particular focus on biological weapons — the following actions shall be taken:

(i) Within 180 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Energy and the Director of the Office of Science and Technology Policy (OSTP), shall evaluate the potential for AI to be misused to enable the development or production of CBRN threats, while also considering the benefits and application of AI to counter these threats, including, as appropriate, the results of work conducted under section 8(b) of this order. The Secretary of Homeland Security shall:

(A) consult with experts in AI and CBRN issues from the Department of Energy, private AI laboratories, academia, and third-party model evaluators, as appropriate, to evaluate AI model capabilities to present CBRN threats — for the sole purpose of guarding against those threats — as well as options for minimizing the risks of AI model misuse to generate or exacerbate those threats; and

(B) submit a report to the President that describes the progress of these efforts, including an assessment of the types of AI models that may present CBRN risks to the United States, and that makes recommendations for regulating or overseeing the training, deployment, publication, or use of these models, including requirements for safety evaluations and guardrails for mitigating potential threats to national security.

(ii) Within 120 days of the date of this order, the Secretary of Defense, in consultation with the Assistant to the President for National Security Affairs and the Director of OSTP, shall enter into a contract with the National Academies of Sciences, Engineering, and Medicine to conduct — and submit to the Secretary of Defense, the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, the Director of OSTP, and the Chair of the Chief Data Officer Council — a study that:

(A) assesses the ways in which AI can increase biosecurity risks, including risks from generative AI models trained on biological data, and makes recommendations on how to mitigate these risks;

(B) considers the national security implications of the use of data and datasets, especially those associated with pathogens and omics studies, that the United States Government hosts, generates, funds the creation of, or otherwise owns, for the training of generative AI models, and makes recommendations on how to mitigate the risks related to the use of these data and datasets;

(C) assesses the ways in which AI applied to biology can be used to reduce biosecurity risks, including recommendations on opportunities to coordinate data and high-performance computing resources; and

(D) considers additional concerns and opportunities at the intersection of AI and synthetic biology that the Secretary of Defense deems appropriate.

(b) To reduce the risk of misuse of synthetic nucleic acids, which could be substantially increased by AI's capabilities in this area, and improve biosecurity measures for the nucleic acid synthesis industry, the following actions shall be taken:

(i) Within 180 days of the date of this order, the Director of OSTP, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Health and Human Services (HHS), the Secretary of Energy, the Secretary of Homeland Security, the Director of National Intelligence, and the heads of other relevant agencies as the Director of OSTP may deem appropriate, shall establish a framework, incorporating, as appropriate, existing United States Government guidance, to encourage providers of synthetic nucleic acid sequences to implement comprehensive, scalable, and verifiable synthetic nucleic acid procurement screening mechanisms, including standards and recommended incentives. As part of this framework, the Director of OSTP shall:

(A) establish criteria and mechanisms for ongoing identification of biological sequences that could be used in a manner that would pose a risk to the national security of the United States; and

(B) determine standardized methodologies and tools for conducting and verifying the performance of sequence synthesis procurement screening, including customer screening approaches to support due diligence with respect to managing security risks posed by purchasers of biological sequences identified in subsection 4.4(b)(i)(A) of this section, and processes for the reporting of concerning activity to enforcement entities.

(ii) Within 180 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in coordination with the Director of OSTP, and in consultation with the Secretary of State, the Secretary of HHS, and the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall initiate an effort to engage with industry and relevant stakeholders, informed by the framework developed under subsection 4.4(b)(i) of this section, to develop and refine for possible use by synthetic nucleic acid sequence providers:

(A) specifications for effective nucleic acid synthesis procurement screening;

(B) best practices, including security and access controls, for managing sequence-of-concern databases to support such screening;

(C) technical implementation guides for effective screening; and

(D) conformity-assessment best practices and mechanisms.

(iii) Within 180 days of the establishment of the framework pursuant to subsection 4.4(b)

(i) of this section, all agencies that fund life-sciences research shall, as appropriate and consistent with applicable law, establish that, as a requirement of funding, synthetic nucleic acid procurement is conducted through providers or manufacturers that adhere to the framework, such as through an attestation from the provider or manufacturer. The Assistant to the President for National Security Affairs and the Director of OSTP shall coordinate the process of reviewing such funding requirements to facilitate consistency in implementation of the framework across funding agencies.

(iv) In order to facilitate effective implementation of the measures described in subsections 4.4(b)(i)-(iii) of this section, the Secretary of Homeland Security, in consultation with the heads of other relevant agencies as the Secretary of Homeland Security may deem appropriate, shall:

(A) within 180 days of the establishment of the framework pursuant to subsection 4.4(b)(i) of this section, develop a framework to conduct structured evaluation and stress testing of nucleic acid synthesis procurement screening, including the systems developed in accordance with subsections 4.4(b)(i)-(ii) of this section and implemented by providers of synthetic nucleic acid sequences; and

(B) following development of the framework pursuant to subsection 4.4(b)(iv)(A) of this section, submit an annual report to the Assistant to the President for National Security Affairs, the Director of the Office of Pandemic Preparedness and Response Policy, and the Director of OSTP on any results of the activities conducted pursuant to subsection 4.4(b)(iv)(A) of this section, including recommendations, if any, on how to strengthen nucleic acid synthesis procurement screening, including customer screening systems.

4.5. Reducing the Risks Posed by Synthetic Content.

To foster capabilities for identifying and labeling synthetic content produced by AI systems, and to establish the authenticity and provenance of digital content, both synthetic and not synthetic, produced by the Federal Government or on its behalf:

(a) Within 240 days of the date of this order, the Secretary of Commerce, in consultation with the heads of other relevant agencies as the Secretary of Commerce may deem appropriate, shall submit a report to the Director of OMB and the Assistant to the President for National Security Affairs identifying the existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for:

(i) authenticating content and tracking its provenance;

(ii) labeling synthetic content, such as using watermarking;

(iii) detecting synthetic content;

(iv) preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual);

(v) testing software used for the above purposes; and

(vi) auditing and maintaining synthetic content.

(b) Within 180 days of submitting the report required under subsection 4.5(a) of this section, and updated periodically thereafter, the Secretary of Commerce, in coordination with the Director of OMB, shall develop guidance regarding the existing tools and practices for digital content authentication and synthetic content detection measures. The guidance shall include measures for the purposes listed in subsection 4.5(a) of this section.

(c) Within 180 days of the development of the guidance required under subsection 4.5(b) of this section, and updated periodically thereafter, the Director of OMB, in consultation with the Secretary of State; the Secretary of Defense; the Attorney General; the Secretary of Commerce, acting through the Director of NIST; the Secretary of Homeland Security; the Director of National Intelligence; and the heads of other agencies that the Director of OMB deems appropriate, shall — for the purpose of strengthening public confidence in the integrity of official United States Government digital content — issue guidance to agencies for labeling and authenticating such content that they produce or publish.

(d) The Federal Acquisition Regulatory Council shall, as appropriate and consistent with applicable law, consider amending the Federal Acquisition Regulation to take into account the guidance established under subsection 4.5 of this section.

4.6. Soliciting Input on Dual-Use Foundation Models with Widely Available Model Weights. When the weights for a dual-use foundation model are widely available — such as when they are publicly posted on the Internet — there can be substantial benefits to innovation, but also substantial security risks, such as the removal of safeguards within the model. To address the risks and potential benefits of dual-use foundation models with widely available weights, within 270 days of the date of this order, the Secretary of Commerce, acting through the Assistant Secretary of Commerce for Communications and Information, and in consultation with the Secretary of State, shall:

(a) solicit input from the private sector, academia, civil society, and other stakeholders through a public consultation process on potential risks, benefits, other implications, and appropriate policy and regulatory approaches related to dual-use foundation models for which the model weights are widely available, including:

(i) risks associated with actors fine-tuning dual-use foundation models for which the model weights are widely available or removing those models' safeguards;

(ii) benefits to AI innovation and research, including research into AI safety and risk management, of dual-use foundation models for which the model weights are widely available; and

(iii) potential voluntary, regulatory, and international mechanisms to manage the risks and maximize the benefits of dual-use foundation models for which the model weights are widely available; and

(b) based on input from the process described in subsection 4.6(a) of this section, and in consultation with the heads of other relevant agencies as the Secretary of Commerce deems appropriate, submit a report to the President on the potential benefits, risks, and implications of dual-use foundation models for which the model weights are widely available, as well as policy and regulatory recommendations pertaining to those models.

4.7. Promoting Safe Release and Preventing the Malicious Use of Federal Data for AI Training.To improve public data access and manage security risks, and consistent with the objectives of the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435) to expand public access to Federal data assets in a machine-readable format while also taking into account security considerations, including the risk that information in an individual data asset in isolation does not pose a security risk but, when combined with other available information, may pose such a risk:

(a) within 270 days of the date of this order, the Chief Data Officer Council, in consultation with the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, the Secretary of Homeland Security, and the Director of National Intelligence, shall develop initial guidelines for performing security reviews, including reviews to identify and manage the potential security risks of releasing Federal data that could aid in the development of CBRN weapons as well as the development of autonomous offensive cyber capabilities, while also providing public access to Federal Government data in line with the goals stated in the Open, Public, Electronic, and Necessary Government Data Act (title II of Public Law 115-435); and

(b) within 180 days of the development of the initial guidelines required by subsection 4.7(a) of this section, agencies shall conduct a security review of all data assets in the comprehensive data inventory required under 44 U.S.C. 3511(a)(1) and (2)(B) and shall take steps, as appropriate and consistent with applicable law, to address the highest-priority potential security risks that releasing that data could raise with respect to CBRN weapons, such as the ways in which that data could be used to train AI systems.

4.8. Directing the Development of a National Security Memorandum. To develop a coordinated executive branch approach to managing AI's security risks, the Assistant to the President for National Security Affairs and the Assistant to the President and Deputy Chief of Staff for Policy shall oversee an interagency process with the purpose of, within 270 days of the date of this order, developing and submitting a proposed National Security Memorandum on AI to the President. The memorandum shall address the governance of AI used as a component of a national security system or for military and intelligence purposes. The memorandum shall take into account current efforts to govern the development and use of AI for national security systems. The memorandum shall outline actions for the Department of Defense, the Department of State, other relevant agencies, and the Intelligence Community to address the national security risks and potential benefits posed by AI. In particular, the memorandum shall:

(a) provide guidance to the Department of Defense, other relevant agencies, and the Intelligence Community on the continued adoption of AI capabilities to advance the United States national security mission, including through directing specific AI assurance and risk-management practices for national security uses of AI that may affect the rights or safety of United States persons and, in appropriate contexts, non-United States persons; and

(b) direct continued actions, as appropriate and consistent with applicable law, to address the potential use of AI systems by adversaries and other foreign actors in ways that threaten the capabilities or objectives of the Department of Defense or the Intelligence Community, or that otherwise pose risks to the security of the United States or its allies and partners.

Sec. 5. Promoting Innovation and Competition.

5.1. Attracting AI Talent to the United States. (a) Within 90 days of the date of this order, to attract and retain talent in AI and other critical and emerging technologies in the United States economy, the Secretary of State and the Secretary of Homeland Security shall take appropriate steps to:

(i) streamline processing times of visa petitions and applications, including by ensuring timely availability of visa appointments, for noncitizens who seek to travel to the United States to work on, study, or conduct research in AI or other critical and emerging technologies; and

(ii) facilitate continued availability of visa appointments in sufficient volume for applicants with expertise in AI or other critical and emerging technologies.

(b) Within 120 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to establish new criteria to designate countries and skills on the Department of State's Exchange Visitor Skills List as it relates to the 2-year foreign residence requirement for certain J-1 nonimmigrants, including those skills that are critical to the United States;

(ii) consider publishing updates to the 2009 Revised Exchange Visitor Skills List (74 FR 20108); and

(iii) consider implementing a domestic visa renewal program under 22 C.F.R. 41.111(b) to facilitate the ability of qualified applicants, including highly skilled talent in AI and critical and emerging technologies, to continue their work in the United States without unnecessary interruption.

(c) Within 180 days of the date of this order, the Secretary of State shall:

(i) consider initiating a rulemaking to expand the categories of nonimmigrants who qualify for the domestic visa renewal program covered under 22 C.F.R. 41.111(b) to include academic J-1 research scholars and F-1 students in science, technology, engineering, and mathematics (STEM); and

(ii) establish, to the extent permitted by law and available appropriations, a program to identify and attract top talent in AI and other critical and emerging technologies at universities, research institutions, and the private sector overseas, and to establish and increase connections with that talent to educate them on opportunities and resources for research and employment in the United States, including overseas educational components to inform top STEM talent of nonimmigrant and immigrant visa options and potential expedited adjudication of their visa petitions and applications.

(d) Within 180 days of the date of this order, the Secretary of Homeland Security shall:

(i) review and initiate any policy changes the Secretary determines necessary and appropriate to clarify and modernize immigration pathways for experts in AI and other critical and emerging technologies, including O-1A and EB-1 noncitizens of extraordinary ability; EB-2 advanced-degree holders and noncitizens of exceptional ability; and startup founders in AI and other critical and emerging technologies using the International Entrepreneur Rule; and

(ii) continue its rulemaking process to modernize the H-1B program and enhance its integrity and usage, including by experts in AI and other critical and emerging technologies, and consider initiating a rulemaking to enhance the process for noncitizens, including experts in AI and other critical and emerging technologies and their spouses, dependents, and children, to adjust their status to lawful permanent resident.

(e) Within 45 days of the date of this order, for purposes of considering updates to the "Schedule A" list of occupations, 20 C.F.R. 656.5, the Secretary of Labor shall publish a request for information (RFI) to solicit public input, including from industry and worker-advocate communities, identifying AI and other STEM-related occupations, as well as additional occupations across the economy, for which there is an insufficient number of ready, willing, able, and qualified United States workers.

(f) The Secretary of State and the Secretary of Homeland Security shall, consistent with applicable law and implementing regulations, use their discretionary authorities to support and attract foreign nationals with special skills in AI and other critical and emerging technologies seeking to work, study, or conduct research in the United States.

(g) Within 120 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of State, the Secretary of Commerce, and the Director of OSTP, shall develop and publish informational resources to better attract and retain experts in AI and other critical and emerging technologies, including:

(i) a clear and comprehensive guide for experts in AI and other critical and emerging technologies to understand their options for working in the United States, to be published in multiple relevant languages on AI.gov; and

(ii) a public report with relevant data on applications, petitions, approvals, and other key indicators of how experts in AI and other critical and emerging technologies have utilized the immigration system through the end of Fiscal Year 2023.

5.2. Promoting Innovation. (a) To develop and strengthen public-private partnerships for advancing innovation, commercialization, and risk-mitigation methods for AI, and to help promote safe, responsible, fair, privacy-protecting, and trustworthy AI systems, the Director of NSF shall take the following steps:

(i) Within 90 days of the date of this order, in coordination with the heads of agencies that the Director of NSF deems appropriate, launch a pilot program implementing the National AI Research Resource (NAIRR), consistent with past recommendations of the NAIRR Task Force. The program shall pursue the infrastructure, governance mechanisms, and user interfaces to pilot an initial integration of distributed computational, data, model, and training resources to be made available to the research community in support of AI-related research and development. The Director of NSF shall identify Federal and private sector computational, data, software, and training resources appropriate for inclusion in the NAIRR pilot program. To assist with such work, within 45 days of the date of this order, the heads of agencies whom the Director of NSF identifies for coordination pursuant to this subsection shall each submit to the Director of NSF a report identifying the agency resources that could be developed and integrated into such a pilot program. These reports shall include a description of such resources, including their current status and availability; their format, structure, or technical specifications; associated agency expertise that will be provided; and the benefits and risks associated with their inclusion in the NAIRR pilot program. The heads of independent regulatory agencies are encouraged to take similar steps, as they deem appropriate.

(ii) Within 150 days of the date of this order, fund and launch at least one NSF Regional Innovation Engine that prioritizes AI-related work, such as AI-related research, societal, or workforce needs.

(iii) Within 540 days of the date of this order, establish at least four new National AI Research Institutes, in addition to the 25 currently funded as of the date of this order.

(b) Within 120 days of the date of this order, to support activities involving high-performance and data-intensive computing, the Secretary of Energy, in coordination with the Director of NSF, shall, in a manner consistent with applicable law and available appropriations, establish a pilot program to enhance existing successful training programs for scientists, with the goal of training 500 new researchers by 2025 capable of meeting the rising demand for AI talent.

(c) To promote innovation and clarify issues related to AI and inventorship of patentable subject matter, the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office (USPTO Director) shall:

(i) within 120 days of the date of this order, publish guidance to USPTO patent examiners and applicants addressing inventorship and the use of AI, including generative AI, in the inventive process, including illustrative examples in which AI systems play different roles in inventive processes and how, in each example, inventorship issues ought to be analyzed;

(ii) subsequently, within 270 days of the date of this order, issue additional guidance to USPTO patent examiners and applicants to address other considerations at the intersection of AI and IP, which could include, as the USPTO Director deems necessary, updated guidance on patent eligibility to address innovation in AI and critical and emerging technologies; and

(iii) within 270 days of the date of this order or 180 days after the United States Copyright Office of the Library of Congress publishes its forthcoming AI study that will address copyright issues raised by AI, whichever comes later, consult with the Director of the United States Copyright Office and issue recommendations to the President on potential executive actions relating to copyright and AI. The recommendations shall address any copyright and related issues discussed in the United States Copyright Office's study, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training.

(d) Within 180 days of the date of this order, to assist developers of AI in combatting AI-related IP risks, the Secretary of Homeland Security, acting through the Director of the National Intellectual Property Rights Coordination Center, and in consultation with the Attorney General, shall develop a training, analysis, and evaluation program to mitigate AI-related IP risks. Such a program shall:

(i) include appropriate personnel dedicated to collecting and analyzing reports of AI-related IP theft, investigating such incidents with implications for national security, and, where appropriate and consistent with applicable law, pursuing related enforcement actions;

(ii) implement a policy of sharing information and coordinating on such work, as appropriate and consistent with applicable law, with the Federal Bureau of Investigation; United States Customs and Border Protection; other agencies; State and local agencies; and appropriate international organizations, including through work-sharing agreements;

(iii) develop guidance and other appropriate resources to assist private sector actors with mitigating the risks of AI-related IP theft;

(iv) share information and best practices with AI developers and law enforcement personnel to identify incidents, inform stakeholders of current legal requirements, and evaluate AI systems for IP law violations, as well as develop mitigation strategies and resources; and

(v) assist the Intellectual Property Enforcement Coordinator in updating the Intellectual Property Enforcement Coordinator Joint Strategic Plan on Intellectual Property Enforcement to address AI-related issues.

(e) To advance responsible AI innovation by a wide range of healthcare technology developers that promotes the welfare of patients and workers in the healthcare sector, the Secretary of HHS shall identify and, as appropriate and consistent with applicable law and the activities directed in section 8 of this order, prioritize grantmaking and other awards, as well as undertake related efforts, to support responsible AI development and use, including:

(i) collaborating with appropriate private sector actors through HHS programs that may support the advancement of AI-enabled tools that develop personalized immune-response profiles for patients, consistent with section 4 of this order;

(ii) prioritizing the allocation of 2024 Leading Edge Acceleration Project cooperative agreement awards to initiatives that explore ways to improve healthcare-data quality to support the responsible development of AI tools for clinical care, real-world-evidence programs, population health, public health, and related research; and

(iii) accelerating grants awarded through the National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity (AIM-AHEAD) program and showcasing current AIM-AHEAD activities in underserved communities.

(f) To advance the development of AI systems that improve the quality of veterans' healthcare, and in order to support small businesses' innovative capacity, the Secretary of Veterans Affairs shall:

(i) within 365 days of the date of this order, host two 3-month nationwide AI Tech Sprint competitions; and

(ii) as part of the AI Tech Sprint competitions and in collaboration with appropriate partners, provide participants access to technical assistance, mentorship opportunities, individualized expert feedback on products under development, potential contract opportunities, and other programming and resources.

(g) Within 180 days of the date of this order, to support the goal of strengthening our Nation's resilience against climate change impacts and building an equitable clean energy economy for the future, the Secretary of Energy, in consultation with the Chair of the Federal Energy Regulatory Commission, the Director of OSTP, the Chair of the Council on Environmental Quality, the Assistant to the President and National Climate Advisor, and the heads of other relevant agencies as the Secretary of Energy may deem appropriate, shall:

(i) issue a public report describing the potential for AI to improve planning, permitting, investment, and operations for electric grid infrastructure and to enable the provision of clean, affordable, reliable, resilient, and secure electric power to all Americans;

(ii) develop tools that facilitate building foundation models useful for basic and applied science, including models that streamline permitting and environmental reviews while improving environmental and social outcomes;

(iii) collaborate, as appropriate, with private sector organizations and members of academia to support development of AI tools to mitigate climate change risks;

(iv) take steps to expand partnerships with industry, academia, other agencies, and international allies and partners to utilize the Department of Energy's computing capabilities and AI testbeds to build foundation models that support new applications in science and energy, and for national security, including partnerships that increase community preparedness for climate-related risks, enable clean-energy deployment (including addressing delays in permitting reviews), and enhance grid reliability and resilience; and

(v) establish an office to coordinate development of AI and other critical and emerging technologies across Department of Energy programs and the 17 National Laboratories.

(h) Within 180 days of the date of this order, to understand AI's implications for scientific research, the President's Council of Advisors on Science and Technology shall submit to the President and make publicly available a report on the potential role of AI, especially given recent developments in AI, in research aimed at tackling major societal and global challenges. The report shall include a discussion of issues that may hinder the effective use of AI in research and practices needed to ensure that AI is used responsibly for research.

5.3. Promoting Competition. (a) The head of each agency developing policies and regulations related to AI shall use their authorities, as appropriate and consistent with applicable law, to promote competition in AI and related technologies, as well as in other markets. Such actions include addressing risks arising from concentrated control of key inputs, taking steps to stop unlawful collusion and prevent dominant firms from disadvantaging competitors, and working to provide new opportunities for small businesses and entrepreneurs. In particular, the Federal Trade Commission is encouraged to consider, as it deems appropriate, whether to exercise the Commission's existing authorities, including its rulemaking authority under the Federal Trade Commission Act, 15 U.S.C. 41 et seq., to ensure fair competition in the AI marketplace and to ensure that consumers and workers are protected from harms that may be enabled by the use of AI.

(b) To promote competition and innovation in the semiconductor industry, recognizing that semiconductors power AI technologies and that their availability is critical to AI competition, the Secretary of Commerce shall, in implementing division A of Public Law 117-167, known as the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022, promote competition by:

(i) implementing a flexible membership structure for the National Semiconductor Technology Center that attracts all parts of the semiconductor and microelectronics ecosystem, including startups and small firms;

(ii) implementing mentorship programs to increase interest and participation in the semiconductor industry, including from workers in underserved communities;

(iii) increasing, where appropriate and to the extent permitted by law, the availability of resources to startups and small businesses, including:

(A) funding for physical assets, such as specialty equipment or facilities, to which startups and small businesses may not otherwise have access;

(B) datasets — potentially including test and performance data — collected, aggregated, or shared by CHIPS research and development programs;

(C) workforce development programs;

(D) design and process technology, as well as IP, as appropriate; and

(E) other resources, including technical and intellectual property assistance, that could accelerate commercialization of new technologies by startups and small businesses, as appropriate; and

(iv) considering the inclusion, to the maximum extent possible, and as consistent with applicable law, of competition-increasing measures in notices of funding availability for commercial research-and-development facilities focused on semiconductors, including measures that increase access to facility capacity for startups or small firms developing semiconductors used to power AI technologies.

(c) To support small businesses innovating and commercializing AI, as well as in responsibly adopting and deploying AI, the Administrator of the Small Business Administration shall:

(i) prioritize the allocation of Regional Innovation Cluster program funding for clusters that support planning activities related to the establishment of one or more Small Business AI Innovation and Commercialization Institutes that provide support, technical assistance, and other resources to small businesses seeking to innovate, commercialize, scale, or otherwise advance the development of AI;

(ii) prioritize the allocation of up to $2 million in Growth Accelerator Fund Competition bonus prize funds for accelerators that support the incorporation or expansion of AI-related curricula, training, and technical assistance, or other AI-related resources within their programming; and

(iii) assess the extent to which the eligibility criteria of existing programs, including the State Trade Expansion Program, Technical and Business Assistance funding, and capital-access programs — such as the 7(a) loan program, 504 loan program, and Small Business Investment Company (SBIC) program — support appropriate expenses by small businesses related to the adoption of AI and, if feasible and appropriate, revise eligibility criteria to improve support for these expenses.

(d) The Administrator of the Small Business Administration, in coordination with resource partners, shall conduct outreach regarding, and raise awareness of, opportunities for small businesses to use capital-access programs described in subsection 5.3(c) of this section for eligible AI-related purposes, and for eligible investment funds with AI-related expertise — particularly those seeking to serve or with experience serving underserved communities — to apply for an SBIC license.

Sec. 6. Supporting Workers.(a) To advance the Government's understanding of AI's implications for workers, the following actions shall be taken within 180 days of the date of this order:

(i) The Chairman of the Council of Economic Advisers shall prepare and submit a report to the President on the labor-market effects of AI.

(ii) To evaluate necessary steps for the Federal Government to address AI-related workforce disruptions, the Secretary of Labor shall submit to the President a report analyzing the abilities of agencies to support workers displaced by the adoption of AI and other technological advancements. The report shall, at a minimum:

(A) assess how current or formerly operational Federal programs designed to assist workers facing job disruptions — including unemployment insurance and programs authorized by the Workforce Innovation and Opportunity Act (Public Law 113-128) — could be used to respond to possible future AI-related disruptions; and

(B) identify options, including potential legislative measures, to strengthen or develop additional Federal support for workers displaced by AI and, in consultation with the Secretary of Commerce and the Secretary of Education, strengthen and expand education and training opportunities that provide individuals pathways to occupations related to AI.

(b) To help ensure that AI deployed in the workplace advances employees' well-being:

(i) The Secretary of Labor shall, within 180 days of the date of this order and in consultation with other agencies and with outside entities, including labor unions and workers, as the Secretary of Labor deems appropriate, develop and publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefits. The principles and best practices shall include specific steps for employers to take with regard to AI, and shall cover, at a minimum:

(A) job-displacement risks and career opportunities related to AI, including effects on job skills and evaluation of applicants and workers;

(B) labor standards and job quality, including issues related to the equity, protected-activity, compensation, health, and safety implications of AI in the workplace; and

(C) implications for workers of employers' AI-related collection and use of data about them, including transparency, engagement, management, and activity protected under worker-protection laws.

(ii) After principles and best practices are developed pursuant to subsection (b)(i) of this section, the heads of agencies shall consider, in consultation with the Secretary of Labor, encouraging the adoption of these guidelines in their programs to the extent appropriate for each program and consistent with applicable law.

(iii) To support employees whose work is monitored or augmented by AI in being compensated appropriately for all of their work time, the Secretary of Labor shall issue guidance to make clear that employers that deploy AI to monitor or augment employees' work must continue to comply with protections that ensure that workers are compensated for their hours worked, as defined under the Fair Labor Standards Act of 1938, 29 U.S.C. 201 et seq., and other legal requirements.

(c) To foster a diverse AI-ready workforce, the Director of NSF shall prioritize available resources to support AI-related education and AI-related workforce development through existing programs. The Director shall additionally consult with agencies, as appropriate, to identify further opportunities for agencies to allocate resources for those purposes. The actions by the Director shall use appropriate fellowship programs and awards for these purposes.

Sec. 7. Advancing Equity and Civil Rights.

7.1. Strengthening AI and Civil Rights in the Criminal Justice System. (a) To address unlawful discrimination and other harms that may be exacerbated by AI, the Attorney General shall:

(i) consistent with Executive Order 12250 of November 2, 1980 (Leadership and Coordination of Nondiscrimination Laws), Executive Order 14091, and 28 C.F.R. 0.50-51, coordinate with and support agencies in their implementation and enforcement of existing Federal laws to address civil rights and civil liberties violations and discrimination related to AI;

(ii) direct the Assistant Attorney General in charge of the Civil Rights Division to convene, within 90 days of the date of this order, a meeting of the heads of Federal civil rights offices — for which meeting the heads of civil rights offices within independent regulatory agencies will be encouraged to join — to discuss comprehensive use of their respective authorities and offices to: prevent and address discrimination in the use of automated systems, including algorithmic discrimination; increase coordination between the Department of Justice's Civil Rights Division and Federal civil rights offices concerning issues related to AI and algorithmic discrimination; improve external stakeholder engagement to promote public awareness of potential discriminatory uses and effects of AI; and develop, as appropriate, additional training, technical assistance, guidance, or other resources; and

(iii) consider providing, as appropriate and consistent with applicable law, guidance, technical assistance, and training to State, local, Tribal, and territorial investigators and prosecutors on best practices for investigating and prosecuting civil rights violations and discrimination related to automated systems, including AI.

(b) To promote the equitable treatment of individuals and adhere to the Federal Government's fundamental obligation to ensure fair and impartial justice for all, with respect to the use of AI in the criminal justice system, the Attorney General shall, in consultation with the Secretary of Homeland Security and the Director of OSTP:

(i) within 365 days of the date of this order, submit to the President a report that addresses the use of AI in the criminal justice system, including any use in:

(A) sentencing;

(B) parole, supervised release, and probation;

(C) bail, pretrial release, and pretrial detention;

(D) risk assessments, including pretrial, earned time, and early release or transfer to home-confinement determinations;

(E) police surveillance;

(F) crime forecasting and predictive policing, including the ingestion of historical crime data into AI systems to predict high-density "hot spots";

(G) prison-management tools; and

(H) forensic analysis;

(ii) within the report set forth in subsection 7.1(b)(i) of this section:

(A) identify areas where AI can enhance law enforcement efficiency and accuracy, consistent with protections for privacy, civil rights, and civil liberties; and

(B) recommend best practices for law enforcement agencies, including safeguards and appropriate use limits for AI, to address the concerns set forth in section 13(e)(i) of Executive Order 14074 as well as the best practices and the guidelines set forth in section 13(e)(iii) of Executive Order 14074; and

(iii) supplement the report set forth in subsection 7.1(b)(i) of this section as appropriate with recommendations to the President, including with respect to requests for necessary legislation.

(c) To advance the presence of relevant technical experts and expertise (such as machine-learning engineers, software and infrastructure engineering, data privacy experts, data scientists, and user experience researchers) among law enforcement professionals:

(i) The interagency working group created pursuant to section 3 of Executive Order 14074 shall, within 180 days of the date of this order, identify and share best practices for recruiting and hiring law enforcement professionals who have the technical skills mentioned in subsection 7.1(c) of this section, and for training law enforcement professionals about responsible application of AI.

(ii) Within 270 days of the date of this order, the Attorney General shall, in consultation with the Secretary of Homeland Security, consider those best practices and the guidance developed under section 3(d) of Executive Order 14074 and, if necessary, develop additional general recommendations for State, local, Tribal, and territorial law enforcement agencies and criminal justice agencies seeking to recruit, hire, train, promote, and retain highly qualified and service-oriented officers and staff with relevant technical knowledge. In considering this guidance, the Attorney General shall consult with State, local, Tribal, and territorial law enforcement agencies, as appropriate.

(iii) Within 365 days of the date of this order, the Attorney General shall review the work conducted pursuant to section 2(b) of Executive Order 14074 and, if appropriate, reassess the existing capacity to investigate law enforcement deprivation of rights under color of law resulting from the use of AI, including through improving and increasing training of Federal law enforcement officers, their supervisors, and Federal prosecutors on how to investigate and prosecute cases related to AI involving the deprivation of rights under color of law pursuant to 18 U.S.C. 242.

7.2. Protecting Civil Rights Related to Government Benefits and Programs. (a) To advance equity and civil rights, consistent with the directives of Executive Order 14091, and in addition to complying with the guidance on Federal Government use of AI issued pursuant to section 10.1(b) of this order, agencies shall use their respective civil rights and civil liberties offices and authorities — as appropriate and consistent with applicable law — to prevent and address unlawful discrimination and other harms that result from uses of AI in Federal Government programs and benefits administration. This directive does not apply to agencies' civil or criminal enforcement authorities. Agencies shall consider opportunities to ensure that their respective civil rights and civil liberties offices are appropriately consulted on agency decisions regarding the design, development, acquisition, and use of AI in Federal Government programs and benefits administration. To further these objectives, agencies shall also consider opportunities to increase coordination, communication, and engagement about AI as appropriate with community-based organizations; civil-rights and civil-liberties organizations; academic institutions; industry; State, local, Tribal, and territorial governments; and other stakeholders.

(b) To promote equitable administration of public benefits:

(i) The Secretary of HHS shall, within 180 days of the date of this order and in consultation with relevant agencies, publish a plan, informed by the guidance issued pursuant to section 10.1(b) of this order, addressing the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services administered by the Secretary, such as to promote: assessment of access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers; and analysis of whether algorithmic systems in use by benefit programs achieve equitable and just outcomes.

(ii) The Secretary of Agriculture shall, within 180 days of the date of this order and as informed by the guidance issued pursuant to section 10.1(b) of this order, issue guidance to State, local, Tribal, and territorial public-benefits administrators on the use of automated or algorithmic systems in implementing benefits or in providing customer support for benefit programs administered by the Secretary, to ensure that programs using those systems:

(A) maximize program access for eligible recipients;

(B) employ automated or algorithmic systems in a manner consistent with any requirements for using merit systems personnel in public-benefits programs;

(C) identify instances in which reliance on automated or algorithmic systems would require notification by the State, local, Tribal, or territorial government to the Secretary;

(D) identify instances when applicants and participants can appeal benefit determinations to a human reviewer for reconsideration and can receive other customer support from a human being;

(E) enable auditing and, if necessary, remediation of the logic used to arrive at an individual decision or determination to facilitate the evaluation of appeals; and

(F) enable the analysis of whether algorithmic systems in use by benefit programs achieve equitable outcomes.

7.3. Strengthening AI and Civil Rights in the Broader Economy. (a) Within 365 days of the date of this order, to prevent unlawful discrimination from AI used for hiring, the Secretary of Labor shall publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.

(b) To address discrimination and biases against protected groups in housing markets and consumer financial markets, the Director of the Federal Housing Finance Agency and the Director of the Consumer Financial Protection Bureau are encouraged to consider using their authorities, as they deem appropriate, to require their respective regulated entities, where possible, to use appropriate methodologies including AI tools to ensure compliance with Federal law and:

(i) evaluate their underwriting models for bias or disparities affecting protected groups; and

(ii) evaluate automated collateral-valuation and appraisal processes in ways that minimize bias.

(c) Within 180 days of the date of this order, to combat unlawful discrimination enabled by automated or algorithmic tools used to make decisions about access to housing and in other real estate-related transactions, the Secretary of Housing and Urban Development shall, and the Director of the Consumer Financial Protection Bureau is encouraged to, issue additional guidance:

(i) addressing the use of tenant screening systems in ways that may violate the Fair Housing Act (Public Law 90-284), the Fair Credit Reporting Act (Public Law 91-508), or other relevant Federal laws, including how the use of data, such as criminal records, eviction records, and credit information, can lead to discriminatory outcomes in violation of Federal law; and

(ii) addressing how the Fair Housing Act, the Consumer Financial Protection Act of 2010 (title X of Public Law 111-203), or the Equal Credit Opportunity Act (Public Law 93-495) apply to the advertising of housing, credit, and other real estate-related transactions through digital platforms, including those that use algorithms to facilitate advertising delivery, as well as on best practices to avoid violations of

Federal law.

(d) To help ensure that people with disabilities benefit from AI's promise while being protected from its risks, including unequal treatment from the use of biometric data like gaze direction, eye tracking, gait analysis, and hand motions, the Architectural and Transportation Barriers Compliance Board is encouraged, as it deems appropriate, to solicit public participation and conduct community engagement; to issue technical assistance and recommendations on the risks and benefits of AI in using biometric data as an input; and to provide people with disabilities access to information and communication technology and transportation services.

Sec. 8. Protecting Consumers, Patients, Passengers, and Students. (a) Independent regulatory agencies are encouraged, as they deem appropriate, to consider using their full range of authorities to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, including risks to financial stability, and to consider rulemaking, as well as emphasizing or clarifying where existing regulations and guidance apply to AI, including clarifying the responsibility of regulated entities to conduct due diligence on and monitor any third-party AI services they use, and emphasizing or clarifying requirements and expectations related to the transparency of AI models and regulated entities' ability to explain their use of AI models.

(b) To help ensure the safe, responsible deployment and use of AI in the healthcare, public-health, and human-services sectors:

(i) Within 90 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an HHS AI Task Force that shall, within 365 days of its creation, develop a strategic plan that includes policies and frameworks — possibly including regulatory action, as appropriate — on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health), and identify appropriate guidance and
resources to promote that deployment, including in the following areas:

(A) development, maintenance, and use of predictive and generative AI-enabled technologies in healthcare delivery and financing — including quality measurement, performance improvement, program integrity, benefits administration, and patient experience — taking into account considerations such as appropriate human oversight of the application of AI-generated output;

(B) long-term safety and real-world performance monitoring of AI-enabled technologies in the health and human services sector, including clinically relevant or significant modifications and performance across population groups, with a means to communicate product updates to regulators, developers, and users;

(C) incorporation of equity principles in AI-enabled technologies used in the health and human services sector, using disaggregated data on affected populations and representative population data sets when developing new models, monitoring algorithmic performance against discrimination and bias in existing models, and helping to identify and mitigate discrimination and bias in current systems;

(D) incorporation of safety, privacy, and security standards into the software-development lifecycle for protection of personally identifiable information, including measures to address AI-enhanced cybersecurity threats in the health and human services sector;

(E) development, maintenance, and availability of documentation to help users determine appropriate and safe uses of AI in local settings in the health and human services sector;

(F) work to be done with State, local, Tribal, and territorial health and human services agencies to advance positive use cases and best practices for use of AI in local settings; and

(G) identification of uses of AI to promote workplace efficiency and satisfaction in the health and human services sector, including reducing administrative burdens.

(ii) Within 180 days of the date of this order, the Secretary of HHS shall direct HHS components, as the Secretary of HHS deems appropriate, to develop a strategy, in consultation with relevant agencies, to determine whether AI-enabled technologies in the health and human services sector maintain appropriate levels of quality, including, as appropriate, in the areas described in subsection (b)(i) of this section. This work shall include the development of AI assurance policy — to evaluate important aspects of the performance of AI-enabled healthcare tools — and infrastructure needs for enabling pre-market assessment and post-market oversight of AI-enabled healthcare-technology algorithmic system performance against real-world data.

(iii) Within 180 days of the date of this order, the Secretary of HHS shall, in consultation with relevant agencies as the Secretary of HHS deems appropriate, consider appropriate actions to advance the prompt understanding of, and compliance with, Federal nondiscrimination laws by health and human services providers that receive Federal financial assistance, as well as how those laws relate to AI. Such actions may include:

(A) convening and providing technical assistance to health and human services providers and payers about their obligations under Federal nondiscrimination and privacy laws as they relate to AI and the potential consequences of noncompliance; and

(B) issuing guidance, or taking other action as appropriate, in response to any complaints or other reports of noncompliance with Federal nondiscrimination and privacy laws as they relate to AI.

(iv) Within 365 days of the date of this order, the Secretary of HHS shall, in consultation with the Secretary of Defense and the Secretary of Veterans Affairs, establish an AI safety program that, in partnership with voluntary federally listed Patient Safety Organizations:

(A) establishes a common framework for approaches to identifying and capturing clinical errors resulting from AI deployed in healthcare settings as well as specifications for a central tracking repository for associated incidents that cause harm, including through bias or discrimination, to patients, caregivers, or other parties;

(B) analyzes captured data and generated evidence to develop, wherever appropriate, recommendations, best practices, or other informal guidelines aimed at avoiding these harms; and

(C) disseminates those recommendations, best practices, or other informal guidance to appropriate stakeholders, including healthcare providers.

(v) Within 365 days of the date of this order, the Secretary of HHS shall develop a strategy for regulating the use of AI or AI-enabled tools in drug-development processes. The strategy shall, at a minimum:

(A) define the objectives, goals, and high-level principles required for appropriate regulation throughout each phase of drug development;

(B) identify areas where future rulemaking, guidance, or additional statutory authority may be necessary to implement such a regulatory system;

(C) identify the existing budget, resources, personnel, and potential for new public/private partnerships necessary for such a regulatory system; and

(D) consider risks identified by the actions undertaken to implement section 4 of this order.

(c) To promote the safe and responsible development and use of AI in the transportation sector, in consultation with relevant agencies:

(i) Within 30 days of the date of this order, the Secretary of Transportation shall direct the Nontraditional and Emerging Transportation Technology (NETT) Council to assess the need for information, technical assistance, and guidance regarding the use of AI in transportation. The Secretary of Transportation shall further direct the NETT Council, as part of any such efforts, to:

(A) support existing and future initiatives to pilot transportation-related applications of AI, as they align with policy priorities articulated in the Department of Transportation's (DOT) Innovation Principles, including, as appropriate, through technical assistance and connecting stakeholders;

(B) evaluate the outcomes of such pilot programs in order to assess when DOT, or other Federal or State agencies, have sufficient information to take regulatory actions, as appropriate, and recommend appropriate actions when that information is available; and

(C) establish a new DOT Cross-Modal Executive Working Group, which will consist of members from different divisions of DOT and coordinate applicable work among these divisions, to solicit and use relevant input from appropriate stakeholders.

(ii) Within 90 days of the date of this order, the Secretary of Transportation shall direct appropriate Federal Advisory Committees of the DOT to provide advice on the safe and responsible use of AI in transportation. The committees shall include the Advanced Aviation Advisory Committee, the Transforming Transportation Advisory Committee, and the Intelligent Transportation Systems Program Advisory Committee.

(iii) Within 180 days of the date of this order, the Secretary of Transportation shall direct the Advanced Research Projects Agency-Infrastructure (ARPA-I) to explore the transportation-related opportunities and challenges of AI — including regarding software-defined AI enhancements impacting autonomous mobility ecosystems. The Secretary of Transportation shall further encourage ARPA-I to prioritize the allocation of grants to those opportunities, as appropriate. The work tasked to ARPA-I shall include soliciting input on these topics through a public consultation process, such as an RFI.

(d) To help ensure the responsible development and deployment of AI in the education sector, the Secretary of Education shall, within 365 days of the date of this order, develop resources, policies, and guidance regarding AI. These resources shall address safe, responsible, and nondiscriminatory uses of AI in education, including the impact AI systems have on vulnerable and underserved communities, and shall be developed in consultation with stakeholders as appropriate. They shall also include the development of an "AI toolkit" for education leaders implementing recommendations from the Department of Education's AI and the Future of Teaching and Learning report, including appropriate human review of AI decisions, designing AI systems to enhance trust and safety and align with privacy-related laws and regulations in the educational context, and developing education-specific guardrails.

(e) The Federal Communications Commission is encouraged to consider actions related to how AI will affect communications networks and consumers, including by:

(i) examining the potential for AI to improve spectrum management, increase the efficiency of non-Federal spectrum usage, and expand opportunities for the sharing of non-Federal spectrum;

(ii) coordinating with the National Telecommunications and Information Administration to create opportunities for sharing spectrum between Federal and non-Federal spectrum operations;

(iii) providing support for efforts to improve network security, resiliency, and interoperability using next-generation technologies that incorporate AI, including self-healing networks, 6G, and Open RAN; and

(iv) encouraging, including through rulemaking, efforts to combat unwanted robocalls and robotexts that are facilitated or exacerbated by AI and to deploy AI technologies that better serve consumers by blocking unwanted robocalls and robotexts.

Sec. 9. Protecting Privacy. (a) To mitigate privacy risks potentially exacerbated by AI — including by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals — the Director of OMB shall:

(i) evaluate and take steps to identify commercially available information (CAI) procured by agencies, particularly CAI that contains personally identifiable information and including CAI procured from data brokers and CAI procured and processed indirectly through vendors, in appropriate agency inventory and reporting processes (other than when it is used for the purposes of national security);

(ii) evaluate, in consultation with the Federal Privacy Council and the Interagency Council on Statistical Policy, agency standards and procedures associated with the collection, processing, maintenance, use, sharing, dissemination, and disposition of CAI that contains personally identifiable information (other than when it is used for the purposes of national security) to inform potential guidance to agencies on ways to mitigate privacy and confidentiality risks from agencies' activities related to CAI;

(iii) within 180 days of the date of this order, in consultation with the Attorney General, the

Assistant to the President for Economic Policy, and the Director of OSTP, issue an RFI to inform potential revisions to guidance to agencies on implementing the privacy provisions of the E-Government Act of 2002 (Public Law 107-347). The RFI shall seek feedback regarding how privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI; and

(iv) take such steps as are necessary and appropriate, consistent with applicable law, to support and advance the near-term actions and long-term strategy identified through the RFI process, including issuing new or updated guidance or RFIs or consulting other agencies or the Federal Privacy Council.

(b) Within 365 days of the date of this order, to better enable agencies to use PETs to safeguard Americans' privacy from the potential threats exacerbated by AI, the Secretary of Commerce, acting through the Director of NIST, shall create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI. The guidelines shall, at a minimum, describe the significant factors that bear on differential-privacy safeguards and common risks to realizing differential privacy in practice.

(c) To advance research, development, and implementation related to PETs:

(i) Within 120 days of the date of this order, the Director of NSF, in collaboration with the Secretary of Energy, shall fund the creation of a Research Coordination Network (RCN) dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of PETs. The RCN shall serve to enable privacy researchers to share information, coordinate and collaborate in research, and develop standards for the privacy-research community.

(ii) Within 240 days of the date of this order, the Director of NSF shall engage with agencies to identify ongoing work and potential opportunities to incorporate PETs into their operations. The Director of NSF shall, where feasible and appropriate, prioritize research — including efforts to translate research discoveries into practical applications — that encourage the adoption of leading-edge PETs solutions for agencies' use, including through research engagement through the RCN described in subsection (c)(i) of this section.

(iii) The Director of NSF shall use the results of the United States-United Kingdom PETs Prize Challenge to inform the approaches taken, and opportunities identified, for PETs research and adoption.

Sec. 10. Advancing Federal Government Use of AI.

10.1. Providing Guidance for AI Management. (a) To coordinate the use of AI across the Federal Government, within 60 days of the date of this order and on an ongoing basis as necessary, the Director of OMB shall convene and chair an interagency council to coordinate the development and use of AI in agencies' programs and operations, other than the use of AI in national security systems. The Director of OSTP shall serve as Vice Chair for the interagency council. The interagency council's membership shall include, at minimum, the heads of the agencies identified in 31 U.S.C. 901(b), the Director of National Intelligence, and other agencies as identified by the Chair. Until agencies designate their permanent Chief AI Officers consistent with the guidance described in subsection 10.1(b) of this section, they shall be represented on the interagency council by an appropriate official at the Assistant Secretary level or equivalent, as determined by the head of each agency.

(b) To provide guidance on Federal Government use of AI, within 150 days of the date of this order and updated periodically thereafter, the Director of OMB, in coordination with the Director of OSTP, and in consultation with the interagency council established in subsection 10.1(a) of this section, shall issue guidance to agencies to strengthen the effective and appropriate use of AI, advance AI innovation, and manage risks from AI in the Federal Government. The Director of OMB's guidance shall specify, to the extent appropriate and consistent with applicable law:

(i) the requirement to designate at each agency within 60 days of the issuance of the guidance a Chief Artificial Intelligence Officer who shall hold primary responsibility in their agency, in coordination with other responsible officials, for coordinating their agency's use of AI, promoting AI innovation in their agency, managing risks from their agency's use of AI, and carrying out the responsibilities described in section 8(c) of Executive Order 13960 of December 3, 2020 (Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government), and section 4(b) of Executive Order 14091;

(ii) the Chief Artificial Intelligence Officers' roles, responsibilities, seniority, position, and reporting structures;

(iii) for the agencies identified in 31 U.S.C. 901(b), the creation of internal Artificial Intelligence Governance Boards, or other appropriate mechanisms, at each agency within 60 days of the issuance of the guidance to coordinate and govern AI issues through relevant senior leaders from across the agency;

(iv) required minimum risk-management practices for Government uses of AI that impact people's rights or safety, including, where appropriate, the following practices derived from OSTP's Blueprint for an AI Bill of Rights and the NIST AI Risk Management Framework: conducting public consultation; assessing data quality; assessing and mitigating disparate impacts and algorithmic discrimination; providing notice of the use of AI; continuously monitoring and evaluating deployed AI; and granting human consideration and remedies for adverse decisions made using AI;

(v) specific Federal Government uses of AI that are presumed by default to impact rights or safety;

(vi) recommendations to agencies to reduce barriers to the responsible use of AI, including barriers related to information technology infrastructure, data, workforce, budgetary restrictions, and cybersecurity processes;

(vii) requirements that agencies identified in 31 U.S.C. 901(b) develop AI strategies and pursue high-impact AI use cases;

(viii) in consultation with the Secretary of Commerce, the Secretary of Homeland Security, and the heads of other appropriate agencies as determined by the Director of OMB, recommendations to agencies regarding:

(A) external testing for AI, including AI red-teaming for generative AI, to be developed in coordination with the Cybersecurity and Infrastructure Security Agency;

(B) testing and safeguards against discriminatory, misleading, inflammatory, unsafe, or deceptive outputs, as well as against producing child sexual abuse material and against producing non-consensual intimate imagery of real individuals (including intimate digital depictions of the body or body parts of an identifiable individual), for generative AI;

(C) reasonable steps to watermark or otherwise label output from generative AI;

(D) application of the mandatory minimum risk-management practices defined under subsection 10.1(b)(iv) of this section to procured AI;

(E) independent evaluation of vendors' claims concerning both the effectiveness and risk mitigation of their AI offerings;

(F) documentation and oversight of procured AI;

(G) maximizing the value to agencies when relying on contractors to use and enrich Federal Government data for the purposes of AI development and operation;

(H) provision of incentives for the continuous improvement of procured AI; and

(I) training on AI in accordance with the principles set out in this order and in other references related to AI listed herein; and

(ix) requirements for public reporting on compliance with this guidance.

(c) To track agencies' AI progress, within 60 days of the issuance of the guidance established in subsection 10.1(b) of this section and updated periodically thereafter, the Director of OMB shall develop a method for agencies to track and assess their ability to adopt AI into their programs and operations, manage its risks, and comply with Federal policy on AI. This method should draw on existing related efforts as appropriate and should address, as appropriate and consistent with applicable law, the practices, processes, and capabilities necessary for responsible AI adoption, training, and governance across, at a minimum, the areas of information technology infrastructure, data, workforce, leadership, and risk management.

(d) To assist agencies in implementing the guidance to be established in subsection 10.1(b) of this section:

(i) within 90 days of the issuance of the guidance, the Secretary of Commerce, acting through the Director of NIST, and in coordination with the Director of OMB and the Director of OSTP, shall develop guidelines, tools, and practices to support implementation of the minimum risk-management practices described in subsection 10.1(b)(iv) of this section; and

(ii) within 180 days of the issuance of the guidance, the Director of OMB shall develop an initial means to ensure that agency contracts for the acquisition of AI systems and services align with the guidance described in subsection 10.1(b) of this section and advance the other aims identified in section 7224(d)(1) of the Advancing American AI Act (Public Law 117-263, div. G, title LXXII, subtitle B).

(e) To improve transparency for agencies' use of AI, the Director of OMB shall, on an annual basis, issue instructions to agencies for the collection, reporting, and publication of agency AI use cases, pursuant to section 7225(a) of the Advancing American AI Act. Through these instructions, the Director shall, as appropriate, expand agencies' reporting on how they are managing risks from their AI use cases and update or replace the guidance originally established in section 5 of Executive Order 13960.

(f) To advance the responsible and secure use of generative AI in the Federal Government:

(i) As generative AI products become widely available and common in online platforms, agencies are discouraged from imposing broad general bans or blocks on agency use of generative AI. Agencies should instead limit access, as necessary, to specific generative AI services based on specific risk assessments; establish guidelines and limitations on the appropriate use of generative AI; and, with appropriate safeguards in place, provide their personnel and programs with access to secure and reliable generative AI capabilities, at least for the purposes of experimentation and routine tasks that carry a low risk of impacting Americans' rights. To protect Federal Government information, agencies are also encouraged to employ risk-management practices, such as training their staff on proper use, protection, dissemination, and disposition of Federal information; negotiating appropriate terms of service with vendors; implementing measures designed to ensure compliance with record-keeping, cybersecurity, confidentiality, privacy, and data protection requirements; and deploying other measures to prevent misuse of Federal Government information in generative AI.

(ii) Within 90 days of the date of this order, the Administrator of General Services, in coordination with the Director of OMB, and in consultation with the Federal Secure Cloud Advisory Committee and other relevant agencies as the Administrator of General Services may deem appropriate, shall develop and issue a framework for prioritizing critical and emerging technologies offerings in the Federal Risk and Authorization Management Program authorization process, starting with generative AI offerings that have the primary purpose of providing large language model-based chat interfaces, code-generation and debugging tools, and associated application programming interfaces, as well as prompt-based image generators. This framework shall apply for no less than 2 years from the date of its issuance. Agency Chief Information Officers, Chief Information Security Officers, and authorizing officials are also encouraged to prioritize generative AI and other critical and emerging technologies in granting authorities for agency operation of information technology systems and any other applicable release or oversight processes, using continuous authorizations and approvals wherever feasible.

(iii) Within 180 days of the date of this order, the Director of the Office of Personnel Management (OPM), in coordination with the Director of OMB, shall develop guidance on the use of generative AI for work by the Federal workforce.

(g) Within 30 days of the date of this order, to increase agency investment in AI, the Technology Modernization Board shall consider, as it deems appropriate and consistent with applicable law, prioritizing funding for AI projects for the Technology Modernization Fund for a period of at least 1 year. Agencies are encouraged to submit to the Technology Modernization Fund project funding proposals that include AI — and particularly generative AI — in service of mission delivery.

(h) Within 180 days of the date of this order, to facilitate agencies' access to commercial AI capabilities, the Administrator of General Services, in coordination with the Director of OMB, and in collaboration with the Secretary of Defense, the Secretary of Homeland Security, the Director of National Intelligence, the Administrator of the National Aeronautics and Space Administration, and the head of any other agency identified by the Administrator of General Services, shall take steps consistent with applicable law to facilitate access to Federal Government-wide acquisition solutions for specified types of AI services and products, such as through the creation of a resource guide or other tools to assist the acquisition workforce. Specified types of AI capabilities shall include generative AI and specialized computing infrastructure.

(i) The initial means, instructions, and guidance issued pursuant to subsections 10.1(a)-(h) of this section shall not apply to AI when it is used as a component of a national security system, which shall be addressed by the proposed National Security Memorandum described in subsection 4.8 of this order.

10.2. Increasing AI Talent in Government. (a) Within 45 days of the date of this order, to plan a national surge in AI talent in the Federal Government, the Director of OSTP and the Director of OMB, in consultation with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Assistant to the President and Domestic Policy Advisor, and the Assistant to the President and Director of the Gender Policy Council, shall identify priority mission areas for increased Federal Government AI talent, the types of talent that are highest priority to recruit and develop to ensure adequate implementation of this order and use of relevant enforcement and regulatory authorities to address AI risks, and accelerated hiring pathways.

(b) Within 45 days of the date of this order, to coordinate rapid advances in the capacity of the Federal AI workforce, the Assistant to the President and Deputy Chief of Staff for Policy, in coordination with the Director of OSTP and the Director of OMB, and in consultation with the National Cyber Director, shall convene an AI and Technology Talent Task Force, which shall include the Director of OPM, the Director of the General Services Administration's Technology Transformation Services, a representative from the Chief Human Capital Officers Council, the Assistant to the President for Presidential Personnel, members of appropriate agency technology talent programs, a representative of the Chief Data Officer Council, and a representative of the interagency council convened under subsection 10.1(a) of this section. The Task Force's purpose shall be to accelerate and track the hiring of AI and AI-enabling talent across the Federal Government, including through the following actions:

(i)   within 180 days of the date of this order, tracking and reporting progress to the President on increasing AI capacity across the Federal Government, including submitting to the President a report and recommendations for further increasing capacity;

(ii)   identifying and circulating best practices for agencies to attract, hire, retain, train, and empower AI talent, including diversity, inclusion, and accessibility best practices, as well as to plan and budget adequately for AI workforce needs;

(iii) coordinating, in consultation with the Director of OPM, the use of fellowship programs and agency technology-talent programs and human-capital teams to build hiring capabilities, execute hires, and place AI talent to fill staffing gaps; and

(iv)   convening a cross-agency forum for ongoing collaboration between AI professionals to share best practices and improve retention.

(c) Within 45 days of the date of this order, to advance existing Federal technology talent programs, the United States Digital Service, Presidential Innovation Fellowship, United States Digital Corps, OPM, and technology talent programs at agencies, with support from the AI and Technology Talent Task Force described in subsection 10.2(b) of this section, as appropriate and permitted by law, shall develop and begin to implement plans to support the rapid recruitment of individuals as part of a Federal Government-wide AI talent surge to accelerate the placement of key AI and AI-enabling talent in high-priority areas and to advance agencies' data and technology strategies.

(d) To meet the critical hiring need for qualified personnel to execute the initiatives in this order, and to improve Federal hiring practices for AI talent, the Director of OPM, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, conduct an evidence-based review on the need for hiring and workplace flexibility, including Federal Government-wide direct-hire authority for AI and related data-science and technical roles, and, where the Director of OPM finds such authority is appropriate, grant it; this review shall include the following job series at all General Schedule (GS) levels: IT Specialist (2210), Computer Scientist (1550), Computer Engineer (0854), and Program Analyst (0343) focused on AI, and any subsequently developed job series derived from these job series;

(ii) within 60 days of the date of this order, consider authorizing the use of excepted service appointments under 5 C.F.R. 213.3102(i)(3) to address the need for hiring additional staff to implement directives of this order;

(iii) within 90 days of the date of this order, coordinate a pooled-hiring action informed by subject-matter experts and using skills-based assessments to support the recruitment of AI talent across agencies;

(iv) within 120 days of the date of this order, as appropriate and permitted by law, issue guidance for agency application of existing pay flexibilities or incentive pay programs for AI, AI-enabling, and other key technical positions to facilitate appropriate use of current pay incentives;

(v) within 180 days of the date of this order, establish guidance and policy on skills-based, Federal Government-wide hiring of AI, data, and technology talent in order to increase access to those with nontraditional academic backgrounds to Federal AI, data, and technology roles;

(vi) within 180 days of the date of this order, establish an interagency working group, staffed with both human-resources professionals and recruiting technical experts, to facilitate Federal Government-wide hiring of people with AI and other technical skills;

(vii) within 180 days of the date of this order, review existing Executive Core Qualifications (ECQs) for Senior Executive Service (SES) positions informed by data and AI literacy competencies and, within 365 days of the date of this order, implement new ECQs as appropriate in the SES assessment process;

(viii) within 180 days of the date of this order, complete a review of competencies for civil engineers (GS-0810 series) and, if applicable, other related occupations, and make recommendations for ensuring that adequate AI expertise and credentials in these occupations in the Federal Government reflect the increased use of AI in critical infrastructure; and

(ix) work with the Security, Suitability, and Credentialing Performance Accountability Council to assess mechanisms to streamline and accelerate personnel-vetting requirements, as appropriate, to support AI and fields related to other critical and emerging technologies.

(e) To expand the use of special authorities for AI hiring and retention, agencies shall use all appropriate hiring authorities, including Schedule A(r) excepted service hiring and direct-hire authority, as applicable and appropriate, to hire AI talent and AI-enabling talent rapidly. In addition to participating in OPM-led pooled hiring actions, agencies shall collaborate, where appropriate, on agency-led pooled hiring under the Competitive Service Act of 2015 (Public Law 114-137) and other shared hiring. Agencies shall also, where applicable, use existing incentives, pay-setting authorities, and other compensation flexibilities, similar to those used for cyber and information technology positions, for AI and data-science professionals, as well as plain-language job titles, to help recruit and retain these highly skilled professionals. Agencies shall ensure that AI and other related talent needs (such as technology governance and privacy) are reflected in strategic workforce planning and budget formulation.

(f) To facilitate the hiring of data scientists, the Chief Data Officer Council shall develop a position-description library for data scientists (job series 1560) and a hiring guide to support agencies in hiring data scientists.

(g) To help train the Federal workforce on AI issues, the head of each agency shall implement — or increase the availability and use of — AI training and familiarization programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields. Such training programs should, for example, empower Federal employees, managers, and leaders to develop and maintain an operating knowledge of emerging AI technologies to assess opportunities to use these technologies to enhance the delivery of services to the public, and to mitigate risks associated with these technologies. Agencies that provide professional-development opportunities, grants, or funds for their staff should take appropriate steps to ensure that employees who do not serve in traditional technical roles, such as policy, managerial, procurement, or legal fields, are nonetheless eligible to receive funding for programs and courses that focus on AI, machine learning, data science, or other related subject areas.

(h) Within 180 days of the date of this order, to address gaps in AI talent for national defense, the Secretary of Defense shall submit a report to the President through the Assistant to the President for National Security Affairs that includes:

(i) recommendations to address challenges in the Department of Defense's ability to hire certain noncitizens, including at the Science and Technology Reinvention Laboratories;

(ii) recommendations to clarify and streamline processes for accessing classified information for certain noncitizens through Limited Access Authorization at Department of Defense laboratories;

(iii) recommendations for the appropriate use of enlistment authority under 10 U.S.C. 504(b)(2) for experts in AI and other critical and emerging technologies; and

(iv) recommendations for the Department of Defense and the Department of Homeland Security to work together to enhance the use of appropriate authorities for the retention of certain noncitizens of vital importance to national security by the Department of Defense and the Department of Homeland Security.

Sec. 11. Strengthening American Leadership Abroad. (a) To strengthen United States leadership of global efforts to unlock AI's potential and meet its challenges, the Secretary of State, in coordination with the Assistant to the President for National Security Affairs, the Assistant to the President for Economic Policy, the Director of OSTP, and the heads of other relevant agencies as appropriate, shall:

(i) lead efforts outside of military and intelligence areas to expand engagements with international allies and partners in relevant bilateral, multilateral, and multi-stakeholder fora to advance those allies' and partners' understanding of existing and planned AI-related guidance and policies of the United States, as well as to enhance international collaboration; and

(ii) lead efforts to establish a strong international framework for managing the risks and harnessing the benefits of AI, including by encouraging international allies and partners to support voluntary commitments similar to those that United States companies have made in pursuit of these objectives and coordinating the activities directed by subsections (b), (c), (d), and (e) of this section, and to develop common regulatory and other accountability principles for foreign nations, including to manage the risk that AI systems pose.

(b) To advance responsible global technical standards for AI development and use outside of military and intelligence areas, the Secretary of Commerce, in coordination with the Secretary of State and the heads of other relevant agencies as appropriate, shall lead preparations for a coordinated effort with key international allies and partners and with standards development organizations, to drive the development and implementation of AI-related consensus standards, cooperation and coordination, and information sharing. In particular, the Secretary of Commerce shall:

(i) within 270 days of the date of this order, establish a plan for global engagement on promoting and developing AI standards, with lines of effort that may include:

(A) AI nomenclature and terminology;

(B) best practices regarding data capture, processing, protection, privacy, confidentiality, handling, and analysis;

(C) trustworthiness, verification, and assurance of AI systems; and

(D) AI risk management;

(ii) within 180 days of the date the plan is established, submit a report to the President on priority actions taken pursuant to the plan; and

(iii) ensure that such efforts are guided by principles set out in the NIST AI Risk Management

Framework and United States Government National Standards Strategy for Critical and Emerging Technology.

(c) Within 365 days of the date of this order, to promote safe, responsible, and rights-affirming development and deployment of AI abroad:

(i) The Secretary of State and the Administrator of the United States Agency for International Development, in coordination with the Secretary of Commerce, acting through the director of NIST, shall publish an AI in Global Development Playbook that incorporates the AI Risk Management Framework's principles, guidelines, and best practices into the social, technical, economic, governance, human rights, and security conditions of contexts beyond United States borders. As part of this work, the Secretary of State and the Administrator of the United States Agency for International Development shall draw on lessons learned from programmatic uses of AI in global development.

(ii) The Secretary of State and the Administrator of the United States Agency for International Development, in collaboration with the Secretary of Energy and the Director of NSF, shall develop a Global AI Research Agenda to guide the objectives and implementation of AI-related research in contexts beyond United States borders. The Agenda shall:

(A) include principles, guidelines, priorities, and best practices aimed at ensuring the safe, responsible, beneficial, and sustainable global development and adoption of AI; and

(B) address AI's labor-market implications across international contexts, including by recommending risk mitigations.

(d) To address cross-border and global AI risks to critical infrastructure, the Secretary of Homeland Security, in coordination with the Secretary of State, and in consultation with the heads of other relevant agencies as the Secretary of Homeland Security deems appropriate, shall lead efforts with international allies and partners to enhance cooperation to prevent, respond to, and recover from potential critical infrastructure disruptions resulting from incorporation of AI into critical infrastructure systems or malicious use of AI.

(i) Within 270 days of the date of this order, the Secretary of Homeland Security, in coordination with the Secretary of State, shall develop a plan for multilateral engagements to encourage the adoption of the AI safety and security guidelines for use by critical infrastructure owners and operators developed in section 4.3(a) of this order.

(ii) Within 180 days of establishing the plan described in subsection (d)(i) of this section, the Secretary of Homeland Security shall submit a report to the President on priority actions to mitigate cross-border risks to critical United States infrastructure.

Sec. 12. Implementation. (a) There is established, within the Executive Office of the President, the White House Artificial Intelligence Council (White House AI Council). The function of the White House AI Council is to coordinate the activities of agencies across the Federal Government to ensure the effective formulation, development, communication, industry engagement related to, and timely implementation of AI-related policies, including policies set forth in this order.

(b) The Assistant to the President and Deputy Chief of Staff for Policy shall serve as Chair of the White House AI Council.

(c) In addition to the Chair, the White House AI Council shall consist of the following members, or their designees:

(i) the Secretary of State;

(ii) the Secretary of the Treasury;

(iii) the Secretary of Defense;

(iv) the Attorney General;

(v) the Secretary of Agriculture;

(vi) the Secretary of Commerce;

(vii) the Secretary of Labor;

(viii) the Secretary of HHS;

(ix) the Secretary of Housing and Urban Development;

(x) the Secretary of Transportation;

(xi) the Secretary of Energy;

(xii) the Secretary of Education;

(xiii) the Secretary of Veterans Affairs;

(xiv) the Secretary of Homeland Security;

(xv) the Administrator of the Small Business Administration;

(xvi) the Administrator of the United States Agency for International Development;

(xvii) the Director of National Intelligence;

(xviii) the Director of NSF;

(xix) the Director of OMB;

(xx) the Director of OSTP;

(xxi) the Assistant to the President for National Security Affairs;

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

March 28, 2024

M-24-10

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young

SUBJECT: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

Artificial intelligence (AI) is one of the most powerful technologies of our time, and the President has been clear that we must seize the opportunities AI presents while managing its risks. Consistent with the AI in Government Act of 2020,[1] the Advancing American AI Act,[2] and Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, this memorandum directs agencies to advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public.[3]

1. OVERVIEW

While AI is improving operations and service delivery across the Federal Government, agencies must effectively manage its use. As such, this memorandum establishes new agency requirements and guidance for AI governance, innovation, and risk management, including through specific minimum risk management practices for uses of AI that impact the rights and safety of the public.

Strengthening AI Governance. Managing AI risk and promoting AI innovation requires effective AI governance. As required by Executive Order 14110, each agency must designate a Chief AI Officer (CAIO) within 60 days of the date of the issuance of this memorandum. This memorandum describes the roles, responsibilities, seniority, position, and reporting structures for agency CAIOs, including expanded reporting through agency AI use case inventories. Because AI is deeply interconnected with other technical and policy areas including data, information technology (IT), security, privacy, civil rights and civil liberties, customer experience, and

[1] Pub. L. No. 116-260, div. U, title 1, § 104 (codified at 40 U.S.C. § 11301 note), https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf.

[2] Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301 note), https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf.

[3] This memorandum accounts for public comments that OMB received following its publication of a draft version of this memorandum on November 1, 2023. OMB has separately published an explanation and response to public comments, available at https://www.regulations.gov/document/OMB-2023-0020-0001.

workforce management, CAIOs must work in close coordination with existing responsible officials and organizations within their agencies.

Advancing Responsible AI Innovation. With appropriate safeguards in place, AI can be a helpful tool for modernizing agency operations and improving Federal Government service to the public. To that end, agencies must increase their capacity to responsibly adopt AI, including generative AI, and take steps to enable sharing and reuse of AI models, code, and data. This memorandum requires each agency identified in the Chief Financial Officers Act (CFO Act)[4] to develop an enterprise strategy for how they will advance the responsible use of AI. This memorandum also provides recommendations for how agencies should reduce barriers to the responsible use of AI, including barriers related to IT infrastructure, data, cybersecurity, workforce, and the particular challenges of generative AI.

Managing Risks from the Use of AI. While agencies will realize significant benefits from AI, they must also manage a range of risks from the use of AI. Agencies are subject to existing risk management requirements relevant to AI, and this memorandum does not replace or supersede these requirements. Instead, it establishes new requirements and recommendations that, both independently and collectively, address the specific risks from relying on AI to inform or carry out agency decisions and actions, particularly when such reliance impacts the rights and safety of the public. To address these risks, this memorandum requires agencies to follow minimum practices when using safety-impacting AI and rights-impacting AI, and enumerates specific categories of AI that are presumed to impact rights and safety. Finally, this memorandum also establishes a series of recommendations for managing AI risks in the context of Federal procurement.[5]

2. SCOPE

Agency adoption of AI poses many challenges, some novel and specific to AI and some well-known. While agencies must give due attention to all aspects of AI, this memorandum is more narrowly scoped to address a subset of AI risks, as well as governance and innovation issues that are directly tied to agencies' use of AI. The risks addressed in this memorandum result from any reliance on AI outputs to inform, influence, decide, or execute agency decisions or actions, which could undermine the efficacy, safety, equitableness, fairness, transparency, accountability, appropriateness, or lawfulness of such decisions or actions.[6]

[4] 31 U.S.C. § 901(b).

[5] Consistent with provisions of the AI in Government Act of 2020, the Advancing American AI Act, and Executive Order 14110 directing the publication of this memorandum, this memorandum sets forth multiple independent requirements and recommendations for agencies, and OMB intends that these requirements and recommendations be treated as severable. For example, the memorandum's provisions regarding the strengthening of AI governance in Section 2 are capable of operating independently, and serve an independent purpose, from the required risk management practices set forth in Section 5. Likewise, each of Section 5's individual risk management practices serves an independent purpose and can function independently from the other risk management practices. Accordingly, while this memorandum governs only agencies' own use of AI and does not create rights or obligations for the public, in the event that a court were to stay or enjoin application of a particular provision of this memorandum, or its application to a particular factual circumstance, OMB would intend that the remainder of the memorandum remain operative.

[6] The subset of AI risks addressed in this memorandum is generally referred to in this document as "risks from the use of AI", and a full definition for this term is provided in Section 6.

This memorandum does not address issues that are present regardless of whether AI is used versus any other software, such as issues with respect to Federal information and information systems in general. In addition, this memorandum does not supersede other, more general Federal policies that apply to AI but are not focused specifically on AI, such as policies that relate to enterprise risk management, information resources management, privacy, accessibility, Federal statistical activities, IT, or cybersecurity.

Agencies must continue to comply with applicable OMB policies in other domains relevant to AI, and to coordinate compliance across the agency with all appropriate officials. All agency responsible officials retain their existing authorities and responsibilities established in other laws and policies.

a. Covered Agencies. Except as specifically noted, this memorandum applies to all agencies defined in 44 U.S.C. § 3502(1).[7] As noted in the relevant sections, some requirements in this memorandum apply only to Chief Financial Officers Act (CFO Act) agencies as identified in 31 U.S.C. § 901(b), and other requirements do not apply to elements of the Intelligence Community, as defined in 50 U.S.C. § 3003.

b. Covered AI. This memorandum provides requirements and recommendations that, as described in more detail below, apply to new and existing AI that is developed, used, or procured by or on behalf of covered agencies. This memorandum does not, by contrast, govern:

i. agencies' regulatory actions designed to prescribe law or policy regarding non-agency uses of AI;
ii. agencies' evaluations of particular AI applications because the AI provider is the target or potential target of a regulatory enforcement, law enforcement, or national security action;[8]
iii. agencies' development of metrics, methods, and standards to test and measure AI, where such metrics, methods, and standards are for use by the general public or the government as a whole, rather than to test AI for a particular agency application[9]; or
iv. agencies' use of AI to carry out basic research or applied research, except where the purpose of such research is to develop particular AI applications within the agency.

[7] The term "agency," as used in both the AI in Government Act of 2020 and the Advancing American AI Act, is defined as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency," but does not include the Government Accountability Office; the Federal Election Commission; the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. 44 U.S.C. § 3502(1); *see* AI in Government Act of 2020 § 102(2) (defining "agency" by reference to § 3502); Advancing American AI Act § 7223(1) (same). As a result, independent regulatory agencies as defined in 44 U.S.C. § 3502(5), which were not included in the definitions of "agency" in Executive Order 13960 and Executive Order 14110, *are* covered by this memorandum.

[8] AI is not in scope when it is the target or potential target of such an action, but it is in scope when the AI is used to *carry out* an enforcement or national security action. For example, when evaluating an AI tool to determine whether it violates the law, the AI would not be in scope; if agencies were using that same tool to assess a different target, then the AI would be in scope.

[9] Examples include agency actions to develop, for general use, standards or testing methodologies for evaluating or red-teaming AI capabilities.

The requirements and recommendations of this memorandum apply to system functionality that implements or is reliant on AI, rather than to the entirety of an information system that incorporates AI. As noted in the relevant sections, some requirements in this memorandum apply only in specific circumstances in which agencies use AI, such as when the AI may impact rights or safety.

c. Applicability to National Security Systems. This memorandum does not cover AI when it is being used as a component of a National Security System.[10]

3. STRENGTHENING ARTIFICIAL INTELLIGENCE GOVERNANCE

The head of each covered agency is responsible for pursuing AI innovation and ensuring that their agency complies with AI requirements in relevant law and policy, including the requirement that risks from the agency's use of AI are adequately managed. Doing so requires a strong governance structure and agencies are encouraged to strategically draw upon their policy, programmatic, research and evaluation, and regulatory functions to support the implementation of this memorandum's requirements and recommendations. The head of each covered agency must also consider the financial, human, information, and infrastructure resources necessary for implementation, prioritizing current resources or requesting additional resources via the budget process, as needed to support the responsibilities identified in this memorandum.

To improve accountability for AI issues, agencies must designate a Chief AI Officer, consistent with Section 10.1(b) of Executive Order 14110. CAIOs bear primary responsibility on behalf of the head of their agency for implementing this memorandum and coordinating implementation with other agencies. This section defines CAIOs' roles, responsibilities, seniority, position, and reporting structure.

a. Actions

i. **Designating Chief AI Officers**. Within 60 days of the issuance of this memorandum, the head of each agency must designate a CAIO. To ensure the CAIO can fulfill the responsibilities laid out in this memorandum, agencies that have already designated a CAIO must evaluate whether they need to provide that individual with additional authority or appoint a new CAIO. Agencies must identify these officers to OMB through OMB's Integrated Data Collection process or an OMB-designated successor process. When the designated individual changes or the position is vacant, agencies must notify OMB within 30 days.

ii. **Convening Agency AI Governance Bodies**. Within 60 days of the issuance of this memorandum, each CFO Act agency must convene its relevant senior officials to

[10] AI innovation and risk for National Security Systems must be managed appropriately, but these systems are governed through other policy. For example, Section 4.8 of Executive Order 14110 directs the development of a National Security Memorandum to govern the use of AI as a component of a National Security System, and agencies also have existing guidelines in place, such as the Department of Defense's (DoD) *Responsible Artificial Intelligence Strategy and Implementation Pathway* and the Office of the Director of National Intelligence's *Principles of Artificial Intelligence Ethics for the Intelligence Community*, as well as policies governing specific high-risk national security applications of AI, such as DoD Directive 3000.09, *Autonomy in Weapon Systems*.

coordinate and govern issues tied to the use of AI within the Federal Government, consistent with Section 10.1(b) of Executive Order 14110 and the detailed guidance in Section 3(c) of this memorandum.

iii. **Compliance Plans**. Consistent with Section 104(c) and (d) of the AI in Government Act of 2020, within 180 days of the issuance of this memorandum or any update to this memorandum, and every two years thereafter until 2036, each agency must submit to OMB and post publicly on the agency's website either a plan to achieve consistency with this memorandum, or a written determination that the agency does not use and does not anticipate using covered AI. Agencies must also include plans to update any existing internal AI principles and guidelines to ensure consistency with this memorandum.[11] OMB will provide templates for these compliance plans.

iv. **AI Use Case Inventories**. Each agency (except for the Department of Defense and the Intelligence Community) must individually inventory each of its AI use cases at least annually, submit the inventory to OMB, and post a public version on the agency's website. OMB will issue detailed instructions for the inventory and its scope through its Integrated Data Collection process or an OMB-designated successor process. Beginning with the use case inventory for 2024, agencies will be required, as applicable, to identify which use cases are safety-impacting and rights-impacting AI and report additional detail on the risks—including risks of inequitable outcomes—that such uses pose and how agencies are managing those risks.

v. **Reporting on AI Use Cases Not Subject to Inventory**. Some AI use cases are not required to be individually inventoried, such as those in the Department of Defense or those whose sharing would be inconsistent with applicable law and governmentwide policy. On an annual basis, agencies must still report and release aggregate metrics about such use cases that are otherwise within the scope of this memorandum, the number of such cases that impact rights and safety, and their compliance with the practices of Section 5(c) of this memorandum. OMB will issue detailed instructions for this reporting through its Integrated Data Collection process or an OMB-designated successor process.

b. Roles, Responsibilities, Seniority, Position, and Reporting Structure of Chief Artificial Intelligence Officers

Consistent with Section 10.1(b)(ii) of Executive Order 14110, this memorandum defines CAIOs' roles, responsibilities, seniority, position, and reporting structures as follows:

i. **Roles.** CAIOs must have the necessary skills, knowledge, training, and expertise to perform the responsibilities described in this section. At CFO Act agencies, a primary role of the CAIO must be coordination, innovation, and risk management for their agency's use of AI specifically, as opposed to data or IT issues in general. Agencies may choose to designate an existing official, such as a Chief Information Officer (CIO), Chief Data Officer (CDO), Chief Technology Officer, or similar official with relevant or

[11] Given the importance of context-specific guidance on AI, agencies are encouraged to continue implementing their agency's AI principles and guidelines, so long as they do not conflict with this memorandum.

complementary authorities and responsibilities, provided they have significant expertise in AI and meet the other requirements in this section.

ii. **Responsibilities.** Executive Order 14110 tasks CAIOs with primary responsibility in their agencies, in coordination with other responsible officials, for coordinating their agency's use of AI, promoting AI innovation, managing risks from the use of AI, and carrying out the agency responsibilities defined in Section 8(c) of Executive Order 13960[12] and Section 4(b) of Executive Order 14091.[13] In addition, CAIOs, in coordination with other responsible officials and appropriate stakeholders, are responsible for:

Coordinating Agency Use of AI

A. serving as the senior advisor for AI to the head of the agency and other senior agency leadership and within their agency's senior decision-making forums;
B. instituting the requisite governance and oversight processes to achieve compliance with this memorandum and enable responsible use of AI in the agency, in coordination with relevant agency officials;
C. maintaining awareness of agency AI activities, including through the creation and maintenance of the annual AI use case inventory;
D. developing a plan for compliance with this memorandum, as detailed in Section 3(a)(iii) of this memorandum, and an agency AI strategy, as detailed in Section 4(a) of this memorandum;
E. working with and advising the agency CFO on the resourcing requirements necessary to implement this memorandum and providing recommendations on priority investment areas to build upon existing enterprise capacity;
F. advising the Chief Human Capital Officer (CHCO) and where applicable, the Chief Learning Officer, on improving workforce capacity and securing and maintaining the skillsets necessary for using AI to further the agency's mission and adequately manage its risks;
G. sharing relevant information with agency officials involved in the agency's major AI policymaking initiatives;
H. supporting agency involvement with appropriate interagency coordination bodies related to their agency's AI activities, including representing the agency on the council described in Section 10.1(a) of Executive Order 14110;
I. supporting and coordinating their agency's involvement in AI standards-setting bodies, as appropriate, and encouraging agency adoption of voluntary consensus standards for AI, as appropriate and consistent with OMB Circular No. A-119, if applicable;[14]

[12] Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,* https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf.

[13] Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, https://www.govinfo.gov/content/pkg/FR-2023-02-22/pdf/2023-03779.pdf.

[14] OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* (Feb. 10, 1998), https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf.

J. promoting equity and inclusion within the agency's AI governance structures and incorporating diverse perspectives into the decision-making process;

Promoting AI Innovation

K. working with their agency to identify and prioritize appropriate uses of AI that will advance both their agency's mission and equitable outcomes;
L. identifying and removing barriers to the responsible use of AI in the agency, including through the advancement of AI-enabling enterprise infrastructure, data access and governance, workforce development measures, policy, and other resources for AI innovation;
M. working with their agency's CIO, CDO, and other relevant officials to ensure that custom-developed AI code and the data used to develop and test AI are appropriately inventoried, shared, and released in agency code and data repositories in accordance with Section 4(d) of this memorandum;
N. advocating within their agency and to the public on the opportunities and benefits of AI to the agency's mission;

Managing Risks from the Use of AI

O. managing an agency program that supports the enterprise in identifying and managing risks from the use of AI, especially for safety-impacting and rights-impacting AI;
P. working with relevant senior agency officials to establish or update processes to measure, monitor, and evaluate the ongoing performance and effectiveness of the agency's AI applications and whether the AI is advancing the agency's mission and meeting performance objectives;
Q. overseeing agency compliance with requirements to manage risks from the use of AI, including those established in this memorandum and in relevant law and policy;
R. conducting risk assessments, as necessary, of the agency's AI applications to ensure compliance with this memorandum;
S. working with relevant agency officials to develop supplementary AI risk management guidance particular to the agency's mission, including working in coordination with officials responsible for privacy and civil rights and civil liberties on identifying safety-impacting and rights-impacting AI within the agency;
T. waiving individual applications of AI from elements of Section 5 of this memorandum through the processes detailed in that section; and
U. in partnership with relevant agency officials (e.g., authorizing, procurement, legal, data governance, human capital, and oversight officials), establishing controls to ensure that their agency does not use AI that is not in compliance with this memorandum, including by assisting these relevant agency officials in evaluating Authorizations to Operate based on risks from the use of AI.

iii. **Seniority.** For CFO Act agencies, the CAIO must be a position at the Senior Executive Service, Scientific and Professional, or Senior Leader level, or equivalent. In other agencies, the CAIO must be at least a GS-15 or equivalent.

iv. **Position and Reporting Structure.** CAIOs must have the necessary authority to perform the responsibilities in this section and must be positioned highly enough to engage regularly with other agency leadership, to include the Deputy Secretary or equivalent. Further, CAIOs must coordinate with other responsible officials at their agency to ensure that the agency's use of AI complies with and is appropriate in light of applicable law and governmentwide guidance.

c. Internal Agency AI Coordination

Agencies must ensure that AI issues receive adequate attention from the agency's senior leadership. Consistent with Section 10.1(b) of Executive Order 14110, agencies must take appropriate steps, such as through the convening of an AI governance body, to coordinate internally among officials responsible for aspects of AI adoption and risk management. Likewise, the CAIO must be involved, at appropriate times, in broader agency-wide risk management bodies and processes,[15] including in the development of the agency risk management strategy.[16] The agency's AI coordination mechanisms should be aligned to the needs of the agency based on, for example, the degree to which the agency currently uses AI, the degree to which AI could improve the agency's mission, and the risks posed by the agency's current and potential uses of AI.

Each CFO Act agency is required to establish an AI Governance Board to convene relevant senior officials to govern the agency's use of AI, including to remove barriers to the use of AI and to manage its associated risks. Those agencies are permitted to rely on existing governance bodies[17] to fulfill this requirement as long as they currently satisfy or are made to satisfy both of the following:

i. Agency AI Governance Boards must be chaired by the Deputy Secretary of the agency or equivalent and vice-chaired by the agency CAIO, and these roles should not be assigned to other officials. The full Board, including the Deputy Secretary, must convene on at least a semi-annual basis. Working through this Board, CAIOs will support their respective Deputy Secretaries in coordinating AI activities across the agency and implementing relevant sections of Executive Order 14110.

[15] *See, e.g.,* OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf.

[16] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource*, Appx. I, sec. 5(b) (July 28, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

[17] An example of a qualifying body includes agency Data Governance Bodies, established by OMB Memorandum M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, https://www.whitehouse.gov/wp-content/uploads/2019/07/m-19-23.pdf.

ii. Agency AI Governance Boards must include appropriate representation from senior agency officials responsible for key enablers of AI adoption and risk management, including at least IT, cybersecurity, data, privacy, civil rights and civil liberties, equity, statistics, human capital, procurement, budget, legal, agency management, customer experience, program evaluation, and officials responsible for implementing AI within an agency's program office(s). Agencies should also consider including representation from their respective Office of the Inspector General.

Agencies are encouraged to have their AI Governance Boards consult external experts as appropriate and consistent with applicable law. Experts' individual viewpoints can help broaden the perspective of an existing governance board and inject additional technical, ethics, civil rights and civil liberties, or sector-specific expertise, as well as methods for engaging the workforce.

4. ADVANCING RESPONSIBLE ARTIFICIAL INTELLIGENCE INNOVATION

If implemented responsibly, AI can improve operations and deliver efficiencies across the Federal Government. Agencies must improve their ability to use AI in ways that benefit the public and increase mission effectiveness, while recognizing the limitations and risks of AI and when it is not suited for a given task. In particular, agencies are encouraged to prioritize AI development and adoption for the public good and where the technology can be helpful in understanding and tackling large societal challenges, such as using AI to improve the accessibility of government services, reduce food insecurity, address the climate crisis, improve public health, advance equitable outcomes, protect democracy and human rights, and grow economic competitiveness in a way that benefits people across the United States.

To achieve this, agencies should build upon existing internal enterprise capacity to support responsible AI innovation, take actions to strengthen their AI and AI-enabling talent,[18] and improve their ability to develop and procure AI. Agencies should both explore joint efforts to scale these opportunities as well as take steps to responsibly share their AI resources across the Federal Government and with the public.

a. AI Strategies

Within 365 days of the issuance of this memorandum, each CFO Act agency must develop and release publicly on the agency's website a strategy for identifying and removing barriers to the responsible use of AI and achieving enterprise-wide improvements in AI maturity, including:

i. the agency's current and planned uses of AI that are most impactful to an agency's mission or service delivery;[19]

[18] Agencies should also ensure that they consider and satisfy applicable collective bargaining obligations regarding their implementation of AI.

[19] Consistent with Sections 7225(d) and 7228 of the Advancing American AI Act, this requirement applies to CFO Act agencies except for the Department of Defense, and does not apply to elements of the Intelligence Community,

ii. a current assessment of the agency's AI maturity and the agency's AI maturity goals;

iii. the agency's plans to effectively govern its use of AI, including through its Chief AI Officer, AI Governance Boards, and improvements to its AI use case inventory;

iv. a plan for developing sufficient enterprise capacity for AI innovation, including mature AI-enabling infrastructure for the data, computing, development, testing, cybersecurity compliance, deployment, and continuous-monitoring infrastructure necessary to build, test, and maintain AI;

v. a plan for providing sufficient AI tools and capacity to support the agency's research and development (R&D) work consistent with the R&D priorities developed by OMB and the Office of Science and Technology Policy, the National AI R&D Strategic Plan, and agency-specific R&D plans;

vi. a plan for establishing operational and governance processes as well as developing the necessary infrastructure to manage risks from the use of AI;

vii. a current assessment of the agency's AI and AI-enabling workforce capacity and projected AI and AI-enabling workforce needs, as well as a plan to recruit, hire, train, retain, and empower AI practitioners and achieve AI literacy for non-practitioners involved in AI to meet those needs;

viii. the agency's plan to encourage diverse perspectives throughout the AI development or procurement lifecycle, including how to determine whether a particular use of AI is meeting the agency's equity goals and civil rights commitments; and

ix. specific, prioritized areas and planning for future AI investment, leveraging the annual budget process as appropriate.

b. Removing Barriers to the Responsible Use of AI

Embracing innovation requires removing unnecessary and unhelpful barriers to the use of AI while retaining and strengthening the guardrails that ensure its responsible use. Agencies should create internal environments where those developing and deploying AI have sufficient flexibility and where limited AI resources and expertise are not diverted away from AI innovation and risk management. Agencies should take steps to remove barriers to responsible use of AI, paying special attention to the following recommendations:

i. **IT Infrastructure.** Agencies should ensure that their AI projects have access to adequate IT infrastructure, including high-performance computing infrastructure specialized for AI training and inference, where necessary. Agencies should also ensure adequate access for AI developers to the software tools, open-source libraries, and deployment and

as defined in 50 U.S.C. § 3003(4). Information that would be protected from release if requested under 5 U.S.C. § 552 need not be included in the strategy.

monitoring capabilities necessary to rapidly develop, test, and maintain AI applications.

ii. **Data.** Agencies should develop adequate infrastructure and capacity to sufficiently share, curate, and govern agency data for use in training, testing, and operating AI. This includes an agency's capacity to maximize appropriate access to and sharing of both internally held data and agency data managed by third parties. Agencies should also explore the possible utility of and legal authorities supporting the use of publicly available information, and encourage its use where appropriate and consistent with the data practices outlined in this memorandum. Any data used to help develop, test, or maintain AI applications, regardless of source, should be assessed for quality, representativeness, and bias. These activities should be supported by resources to enable sound data governance and management practices, particularly as they relate to data collection, curation, labeling, and stewardship.

iii. **Cybersecurity.** Agencies should update, as necessary, processes for information system authorization and continuous monitoring to better address the needs of AI applications, including to advance the use of continuous authorizations for AI. Consistent with Section 10.1(f) of Executive Order 14110, agency authorizing officials are encouraged to prioritize review of generative AI and other critical and emerging technologies in Authorizations to Operate and any other applicable release or oversight processes.

iv. **Generative AI.** In addition to following the guidance provided in Section 10.1(f) of Executive Order 14110, agencies should assess potential beneficial uses of generative AI in their missions and establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk.

c. AI Talent

Consistent with Section 10.2 of Executive Order 14110, agencies are strongly encouraged to prioritize recruiting, hiring, developing, and retaining talent in AI and AI-enabling roles to increase enterprise capacity for responsible AI innovation. Agencies should:

i. follow the hiring practices described in the forthcoming AI and Tech Hiring Playbook created by the Office of Personnel Management (OPM), including encouraging applications from individuals with diverse perspectives, making best use of available hiring and retention authorities and using descriptive job titles and skills-based assessments;

ii. designate an AI Talent Lead who, for at least the duration of the AI Talent Task Force, will be accountable for reporting to agency leadership, tracking AI hiring across the agency, and providing data to OPM and OMB on hiring needs and progress. The AI Talent Task Force, established in Section 10.2(b) of EO 14110, will provide AI Talent Leads with engagement opportunities to enhance their AI hiring practices and to drive impact through collaboration across agencies, including sharing position descriptions, coordinating marketing and outreach, shared hiring actions, and, if appropriate, sharing applicant information across agencies; and

iii. in consultation with Federal employees and their union representatives, where applicable, provide resources and training to develop AI talent internally and increase AI training offerings for Federal employees, including opportunities that provide Federal employees pathways to AI occupations and that assist employees affected by the application of AI to their work.

d. AI Sharing and Collaboration

Openness, sharing, and reuse of AI significantly enhance both innovation and transparency, and must also be done responsibly to avoid undermining the rights, safety, and security of the public. Agencies must share their AI code, models, and data, and do so in a manner that facilitates re-use and collaboration Government-wide and with the public, subject to applicable law, governmentwide guidance, and the following considerations:

i. **Sharing and Releasing AI Code and Models.** Agencies must proactively share their custom-developed code[20]—including models and model weights—for AI applications in active use and must release and maintain that code as open source software on a public repository,[21] unless:
   A. the sharing of the code is restricted by law or regulation, including patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulations, and Federal laws and regulations governing classified information;
   B. the sharing of the code would create an identifiable risk to national security, confidentiality of Government information, individual privacy, or the rights or safety of the public;
   C. the agency is prevented by a contractual obligation from doing so; or
   D. the sharing of the code would create an identifiable risk to agency mission, programs, or operations, or to the stability, security, or integrity of an agency's systems or personnel.

   Agencies should prioritize sharing custom-developed code, such as commonly used packages or functions, that has the greatest potential for re-use by other agencies or the public.

ii. **Sharing and Releasing AI Data Assets.** Data used to develop and test AI is likely to constitute a "data asset" for the purposes of implementing the Open, Public, Electronic

[20] A full definition for "custom-developed code" is provided in Section 6.

[21] For guidance and best practices related to sharing code and releasing it as open source, agencies should consult OMB Memorandum M-16-21, *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (Aug. 8, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_21.pdf. Agencies are additionally encouraged to draw upon existing collaboration methods to facilitate the sharing and release of code and models, including the council described in Section 10.1(a) of Executive Order 14110, the General Services Administration's AI Community of Practice, and https://www.code.gov, as well as other publicly available code repositories.

and Necessary (OPEN) Government Data Act,[22] and agencies must, if required by that Act and pursuant to safety and security considerations in Section 4.7 of Executive Order 14110, release such data assets publicly as open government data assets.[23] When sharing AI data assets, agencies should promote data interoperability, including by coordinating internally and with other relevant agencies on interoperability criteria and using standardized data formats where feasible and appropriate.

iii. **Partial Sharing and Release.** Where some portion of an AI project's code, models, or data cannot be shared or released publicly pursuant to subsections (i) and (ii) of this section, the rest should still be shared or released where practicable, such as by releasing the data used to evaluate a model even if the model itself cannot be safely released, or by sharing a model within the Federal Government even if the model cannot be publicly released. Where code, models, or data cannot be released without restrictions on who can access it, agencies should also, where practicable, share them through Federally controlled infrastructure that allows controlled access by entities outside the Federal Government, such as via the National AI Research Resource.

iv. **Procuring AI for Sharing and Release.** When procuring custom-developed code for AI, data to train and test AI, and enrichments to existing data (such as labeling services), agencies are encouraged to do so in a manner that allows for the sharing and public release of the relevant code, models, and data.

v. **Unintended Disclosure of Data from AI Models.** When agencies are deciding whether to share and release AI models and model weights, they should assess the risk that the models can be induced to reveal sensitive details of the data used to develop them. Agencies' assessment of risk should include a model-specific risk analysis.[24]

e. Harmonization of Artificial Intelligence Requirements

Interpreting and implementing AI management requirements in a consistent manner across Federal agencies will create efficiencies as well as opportunities for sharing resources and best practices. To assist in this effort and consistent with Section 10.1(a) of Executive Order 14110, OMB, in collaboration with the Office of Science and Technology Policy, will coordinate the development and use of AI in agencies' programs and operations—including the implementation of this memorandum—across Federal agencies through an interagency council. This will include at a minimum:

i. promoting shared templates and formats;

ii. sharing best practices and lessons learned, including for achieving meaningful participation from affected communities and the public in AI development and

[22] Title II of the Foundations for Evidence-Based Policymaking Act of 2018, P.L. 115-435.

[23] Where such data is already publicly available, agencies are not required to duplicate it, but should maintain and share the provenance of such data and how others can access it.

[24] The risks of unintended disclosure differ by model, and agencies should also not assume that an AI model poses the same privacy and confidentiality risks as the data used to develop it.

procurement, updating organizational processes to better accommodate AI, removing barriers to responsible AI innovation, responding to AI incidents that may have resulted in harm to an individual, and building a diverse AI workforce to meet the agency's needs;

iii. sharing technical resources for implementation of this memorandum's risk management practices, such as for testing, continuous monitoring, and evaluation; and

iv. highlighting exemplary uses of AI for agency adoption, particularly uses which help address large societal challenges.

5. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

Agencies have a range of policies, procedures, and officials in place to manage risks related to agency information and systems. To better address risks from the use of AI, and particularly risks to the rights and safety of the public, all agencies are required to implement minimum practices, detailed below, to manage risks from safety-impacting AI and rights-impacting AI.[25] However, Section 5(a) through (c) of this memorandum do not apply to elements of the Intelligence Community.[26]

a. Actions

i. **Implementation of Risk Management Practices and Termination of Non-Compliant AI**. By December 1, 2024, agencies must implement the minimum practices in Section 5(c) of this memorandum for safety-impacting and rights-impacting AI, or else stop using any AI in their operations that is not compliant with the minimum practices, consistent with the details and caveats in that section.

ii. **Certification and Publication of Determinations and Waivers.** By December 1, 2024, and annually thereafter, each agency must certify the ongoing validity of the determinations made under subsection (b) and the waivers granted under subsection (c) of this section. To the extent consistent with law and governmentwide policy, the agency must publicly release a summary detailing each individual determination and waiver, as well its justification. Alternatively, if an agency has no active determinations or waivers, it must publicly indicate that fact and report it to OMB. OMB will issue detailed instructions for these summaries through its Integrated Data Collection process or an OMB-designated successor process.

[25] Agencies are not required to incorporate these practices into criteria for granting federal financial assistance (FFA). However, they are encouraged, consistent with applicable law, to consider the minimum practices when choosing such criteria.

[26] Although elements of the Intelligence Community are not required to implement these practices, they are encouraged to do so.

b. Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting

All AI that matches the definitions of "safety-impacting AI" or "rights-impacting AI" as defined in Section 6 must follow the minimum practices in Section 5(c) by the applicable deadline. Agencies must review each current or planned use of AI to assess whether it matches the definition of safety-impacting AI or rights-impacting AI. When conducting such an assessment, as reflected by the definitions of safety-impacting AI and rights-impacting AI in Section 6 of this memorandum, agencies must look to whether the particular AI output serves as a principal basis for a decision or action.

Additionally, AI used for one of the purposes identified in Appendix I is automatically *presumed* to be safety-impacting or rights-impacting. However, the agency CAIO, in coordination with other relevant officials, may determine (or revisit a prior determination) that a particular AI application or component[27] subject to this presumption does not match the definitions of "safety-impacting AI" or "rights-impacting AI" and is therefore not subject to the minimum practices. The agency CAIO may make or revisit such a determination only with a documented context-specific and system-specific risk assessment and may revisit a prior determination at any time. This responsibility shall not be delegated to other officials. In addition to the certification and publication requirements in Section 5(a)(ii) of this memorandum, CAIOs must centrally track these determinations, reassess them if there are significant changes to the conditions or context in which the AI is used, and report to OMB within 30 days of making or changing a determination, detailing the scope, justification, and supporting evidence.

c. Minimum Practices for Safety-Impacting and Rights-Impacting Artificial Intelligence

Except as prevented by applicable law and governmentwide guidance, agencies must apply the minimum risk management practices in this section to safety-impacting and rights-impacting AI by December 1, 2024, or else stop using the AI until they achieve compliance. Prior to December 1, 2024, agency CAIOs should work with their agencies' relevant officials to bring potentially non-compliant AI into conformity, which may include requests that third-party vendors voluntarily take appropriate action (e.g., via updated documentation or testing measures). To ensure compliance with this requirement, relevant agency officials must use existing mechanisms wherever possible, (for example, the Authorization to Operate process).[28] An agency may also request an extension or grant a waiver to this requirement through its CAIO using the processes detailed below.

[27] CAIOs may also make these determinations across groups of AI applications or components that are closely related by design or deployment context, provided that: (1) those systems have undergone a risk assessment that adequately considers the risks from each individual system or from all possible systems in the group; and (2) the systems are substantially identical in their risk profiles.

[28] While agencies must use existing authorization and oversight processes to enforce these practices, the practices are most effective when applied early in the research, design, and development of AI systems, and agencies should plan for and adopt the practices throughout the relevant AI systems' lifecycles and as early as possible, as appropriate.

Agencies must document their implementation of these practices and be prepared to report them to OMB, either as a component of the annual AI use case inventory, periodic accountability reviews, or upon request as determined by OMB.

The practices in this section represent an initial baseline for managing risk from the use of AI. Agencies must identify additional context-specific risks that are associated with their use of AI and address them as appropriate. Such risk considerations may include impacts to safety, security, civil rights, civil liberties, privacy, democratic values, human rights, equal opportunities, worker well-being, access to critical resources and services, agency trust and credibility, and market competition. To address these potential risk management gaps, agencies are encouraged to promote and to incorporate, as appropriate, additional best practices for AI risk management, such as from the National Institute of Standards and Technology (NIST) AI Risk Management Framework,[29] the Blueprint for an AI Bill of Rights,[30] relevant international standards,[31] and the workforce principles and best practices for employers established pursuant to Section 6(b)(i) of Executive Order 14110. Agencies are also encouraged to continue developing their own agency-specific practices, as appropriate and consistent with this memorandum and the principles in Executive Order 13960, Executive Order 14091, and Executive Order 14110.

The practices in this section also do not supersede, modify, or direct an interpretation of existing requirements mandated by law or governmentwide policy, and responsible agency officials must coordinate to ensure that the adoption of these practices does not conflict with other applicable law or governmentwide guidance.

i. **Exclusions from Minimum Practices.** Agencies are not required to follow the minimum practices outlined in this section when using AI *solely* to:
   A. evaluate a potential vendor, commercial capability, or freely available AI capability that is not otherwise used in agency operations, exclusively for the purpose of making a procurement or acquisition decision; or
   B. achieve its conformity with the requirements of this section, such as using an AI application in controlled testing conditions to carry out the minimum testing requirements below.[32]

ii. **Extensions for Minimum Practices.** Agencies may request from OMB an extension of up to one year, for a particular use of AI that cannot feasibly meet the minimum requirements in this section by that date. OMB will not grant renewals beyond the initial one-year extension. Any extension requests shall be submitted prior to October 15, 2024. The request must be accompanied by a detailed justification for why the agency cannot achieve compliance for the use of AI in question and what practices the agency has in

[29] *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST Publication AI 100-1, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[30] *Blueprint for an AI Bill of Rights*, White House Office of Science and Technology Policy, https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[31] For example, ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management, https://www.iso.org/standard/77304.html.

[32] This exclusion must not be applied to any use of AI in real-world conditions, except as specifically allowed by this section.

place to mitigate the risks from noncompliance, as well as a plan for how the agency will come to implement the full set of required minimum practices from this section. OMB will issue detailed instructions for extension requests through its Integrated Data Collection process or an OMB-designated successor process.

iii. **Waivers from Minimum Practices.** In coordination with other relevant officials, an agency CAIO may waive one or more of the requirements in this section for a specific covered AI application or component[33] after making a written determination, based upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. An agency CAIO may also revoke a previously issued waiver at any time. This responsibility shall not be delegated to other officials. In addition to the certification and publication requirements in Section 5(a)(ii) of this memorandum, CAIOs must centrally track waivers, reassess them if there are significant changes to the conditions or context in which the AI is used, and report to OMB within 30 days of granting or revoking any waiver, detailing the scope, justification, and supporting evidence.

iv. **Minimum Practices for Either Safety-Impacting or Rights-Impacting AI.**
No later than December 1, 2024, agencies must follow these practices *before* using new or existing covered safety-impacting or rights-impacting AI:

A. **Complete an AI impact assessment**. Agencies should update their impact assessments periodically and leverage them throughout the AI's lifecycle. In their impact assessments, agencies must document at least the following:

1. *The intended purpose for the AI and its expected benefit*, supported by specific metrics or qualitative analysis. Metrics should be quantifiable measures of positive outcomes for the agency's mission—for example to reduce costs, wait time for customers, or risk to human life—that can be measured using performance measurement or program evaluation methods after the AI is deployed to demonstrate the value of using AI.[34] Where quantification is not feasible, qualitative analysis should demonstrate an expected positive outcome, such as for improvements to customer experience, and it should demonstrate that AI is better suited to accomplish the relevant task as compared to alternative strategies.

2. *The potential risks of using AI*, as well as what, if any, additional mitigation measures, beyond these minimum practices, the agency will take to help

[33] CAIOs may also grant waivers applicable to groups of AI applications or components that are closely related by design or deployment context, provided that: (1) those systems have undergone a risk assessment that adequately considers the risks from each individual system or from all possible systems in the group; and (2) the systems are substantially identical in their risk profiles.

[34] For supervised and semi-supervised AI, agencies should use a target variable which can be reliably measured and adequately represents the desired real-world outcomes.

reduce these risks. Agencies should document the stakeholders[35] who will be most impacted by the use of the system and assess the possible failure modes of the AI and of the broader system, both in isolation and as a result of human users and other likely variables outside the scope of the system itself. Agencies should be especially attentive to the potential risks to underserved communities. The expected benefits of the AI functionality should be considered against its potential risks, and if the benefits do not meaningfully outweigh the risks, agencies should not use the AI.

3. *The quality and appropriateness of the relevant data*. Agencies must assess the quality of the data used in the AI's design, development, training, testing, and operation and its fitness to the AI's intended purpose. In conducting assessments, if the agency cannot obtain such data after a reasonable effort to do so, it must obtain sufficient descriptive information from the vendor (e.g., AI or data provider) to satisfy the reporting requirements in this paragraph. At a minimum, agencies must document:
   a. the data collection and preparation process, which must also include the provenance of any data used to train, fine-tune, or operate the AI;
   b. the quality[36] and representativeness[37] of the data for its intended purpose;
   c. how the data is relevant to the task being automated and may reasonably be expected to be useful for the AI's development, testing, and operation;
   d. whether the data contains sufficient breadth to address the range of real-world inputs the AI might encounter and how data gaps and shortcomings have been addressed either by the agency or vendor; and
   e. if the data is maintained by the Federal Government, whether that data is publicly disclosable as an open government data asset, in accordance with applicable law and policy.[38]

B. **Test the AI for performance in a real-world context**. Agencies must conduct adequate testing to ensure the AI, as well as components that rely on it, will work in its intended real-world context. Such testing should follow domain-specific best practices, when available, and should take into account both the specific technology used and feedback from human operators, reviewers, employees, and

[35] Stakeholders will vary depending on how AI is being used. For example, if an agency is using AI to control a water treatment process, stakeholders may include (1) local residents; (2) state, local, tribal, and territorial government representatives; and (3) environmental experts.

[36] Consistent with OMB Memorandum M-19-15, *Improving Implementation of the Information Quality Act*, https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf, if applicable. Agencies should also consider the National Science and Technology Council's report *Protecting the Integrity of Government Science*, https://www.whitehouse.gov/wp-content/uploads/2022/01/01-22-Protecting_the_Integrity_of_Government_Science.pdf.

[37] Agencies should assess whether the data used can produce or amplify inequitable outcomes as a result of poor data representativeness or harmful bias. Such outcomes can result from historical discrimination, such as the perpetuation of harmful gender-based and racial stereotypes in society.

[38] *See* 44 U.S.C. § 3502(20).

customers who use the service or are impacted by the system's outcomes. Testing conditions should mirror as closely as possible the conditions in which the AI will be deployed. Through test results, agencies should demonstrate that the AI will achieve its expected benefits and that associated risks will be sufficiently mitigated, or else the agency should not use the AI. In conducting such testing, if an agency does not have access to the underlying source code, models, or data, the agency must use alternative test methodologies, such as querying the AI service and observing the outputs or providing evaluation data to the vendor and obtaining results. Agencies are also encouraged to leverage pilots and limited releases, with strong monitoring, evaluation, and safeguards in place, to carry out the final stages of testing before a wider release.

C. **Independently evaluate the AI**. Agencies, through the CAIO, an agency AI oversight board, or other appropriate agency office with existing test and evaluation responsibilities, must review relevant AI documentation to ensure that the system works appropriately and as intended, and that its expected benefits outweigh its potential risks. At a minimum, this documentation must include the completed impact assessment and results from testing AI performance in a real-world context referenced in paragraphs (A) and (B) of this subsection. Agencies must incorporate this independent evaluation into an applicable release or oversight process, such as the Authorization to Operate process. The independent reviewing authority must not have been directly involved in the system's development.

No later than December 1, 2024 and on an ongoing basis *while* using new or existing covered safety-impacting or rights-impacting AI, agencies must ensure these practices are followed for the AI:

D. **Conduct ongoing monitoring.** In addition to pre-deployment testing, agencies must institute ongoing procedures to monitor degradation of the AI's functionality and to detect changes in the AI's impact on rights and safety. Agencies should also scale up the use of new or updated AI features incrementally where possible to provide adequate time to monitor for adverse performance or outcomes. Agencies should monitor and defend the AI from AI-specific exploits,[39] particularly those that would adversely impact rights and safety.

E. **Regularly evaluate risks from the use of AI.** The monitoring process in paragraph (D) must include periodic human reviews to determine whether the deployment context, risks, benefits, and agency needs have evolved. Agencies must also determine whether the current implementation of the memorandum's minimum practices adequately mitigates new and existing risks, or whether

[39] For example, the AI-specific exploits outlined in the MITRE ATLAS framework, *see* https://atlas.mitre.org/ and NIST's taxonomy for adversarial machine learning, *see* https://csrc.nist.gov/pubs/ai/100/2/e2023/final.

updated risk response options are required.[40] At a minimum, human review is required at least on an annual basis and after significant modifications to the AI or to the conditions or context in which the AI is used, and the review must include renewed testing for performance of the AI in a real-world context.[41] Reviews must also include oversight and consideration by an appropriate internal agency authority not directly involved in the system's development or operation.

F. **Mitigate emerging risks to rights and safety.** Upon identifying new or significantly altered risks to rights or safety through ongoing monitoring, periodic review, or other mechanisms, agencies must take steps to mitigate those risks, including, as appropriate, through updating the AI to reduce its risks or implementing procedural or manual mitigations, such as more stringent human intervention requirements. As significant modifications make the existing implementation of the other minimum practices in this section less effective, such as by making training or documentation inaccurate, agencies must update or repeat those practices, as appropriate. Where the AI's risks to rights or safety exceed an acceptable level and where mitigation strategies do not sufficiently reduce risk, agencies must stop using the AI as soon as is practicable.[42]

G. **Ensure adequate human training and assessment.** Agencies must ensure there is sufficient training, assessment, and oversight for operators of the AI to interpret and act on the AI's output, combat any human-machine teaming issues (such as automation bias), and ensure the human-based components of the system effectively manage risks from the use of AI. Training should be conducted on a periodic basis, determined by the agency, and should be specific to the AI product or service being operated and how it is being used.

H. **Provide additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety.** Agencies must assess their rights-impacting and safety-impacting uses of AI to identify any decisions or actions in which the AI is not permitted to act without additional human oversight, intervention, and accountability. When immediate human intervention is not practicable for such an action or decision, agencies must ensure that the AI functionality has an appropriate fail-safe that minimizes the risk of significant harm.[43]

[40] In some cases, this may require a program evaluation, as defined under requirements of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, to determine the extent to which the AI is advancing the agency's mission and objectives.

[41] For customer-facing services, agencies should consider customer feedback in their human review criteria.

[42] Agencies are responsible for determining how to safely decommission AI that was already in use at the time of this memorandum's release, without significant disruptions to essential government functions.

[43] For example, an AI-enabled safety mechanism may require an immediate and automated action to prevent a harm from occurring. It would not be practicable in this case to require human intervention to approve the activation of the safety mechanism. However, agencies must still determine the appropriate oversight and accountability processes for such a use of AI.

I. **Provide public notice and plain-language documentation.** Agencies must ensure, to the extent consistent with applicable law and governmentwide guidance, including concerning protection of privacy and of sensitive law enforcement, national security, and other protected information, that the AI's entry in the use case inventory provides accessible documentation in plain language of the system's functionality to serve as public notice of the AI to its users and the general public. Where people interact with a service relying on the AI and are likely to be impacted by the AI, agencies must also provide reasonable and timely notice[44] about the use of the AI and a means to directly access any public documentation about it in the use case inventory. Where agencies' use cases are not included in their public inventories, they may still be required to report relevant information to OMB and must ensure adequate transparency in their use of AI, as appropriate and consistent with applicable law.

v. **Additional Minimum Practices for Rights-Impacting AI.**

No later than December 1, 2024, agencies must follow the above minimum practices for AI that is *either* safety-impacting *or* rights-impacting. In addition, no later than December 1, 2024, agencies must also follow these minimum practices *before* initiating use of new or existing rights-impacting AI:

A. **Identify and assess AI's impact on equity and fairness, and mitigate algorithmic discrimination when it is present.** Agencies must:

1. Identify and document in their AI impact assessment when using data that contains information about a class protected by Federal nondiscrimination laws (e.g., race, age, etc.). Given the risks arising when AI may correlate demographic information with other types of information, agencies should also assess and document whether the AI model could foreseeably use other attributes as proxies for a protected characteristic and whether such use would significantly influence model performance;
2. Assess the AI in a real-world context to determine whether the AI model results in significant disparities in the model's performance (e.g., accuracy, precision, reliability in predicting outcomes) across demographic groups;
3. Mitigate disparities that lead to, or perpetuate, unlawful discrimination or harmful bias, or that decrease equity as a result of the government's use of the AI; and
4. Consistent with applicable law, cease use of the AI for agency decision-making if the agency is unable to adequately mitigate any associated risk of unlawful discrimination against protected classes. Agencies should maintain appropriate documentation to accompany this decision-making, and should disclose it publicly to the extent consistent with applicable law and governmentwide policy.

[44] Wherever feasible, agencies should provide notice to a user before the AI takes an action that significantly impacts them.

B. **Consult and incorporate feedback from affected communities and the public.** Consistent with applicable law and governmentwide guidance, agencies must consult affected communities, including underserved communities, and they must solicit public feedback, where appropriate, in the design, development, and use of the AI and use such feedback to inform agency decision-making regarding the AI. The consultation and feedback process must include seeking input on the agency's approach to implementing the minimum risk management practices established in Section 5(c) of this memorandum, such as applicable opt-out procedures. Agencies should consider and manage the risks of public consultation in contexts like fraud prevention and law enforcement investigations, where consulting with the targeted individual is impractical but consulting with a representative group may be appropriate.[45]

Agencies are strongly encouraged to solicit feedback on an ongoing basis from affected communities in particular as well as from the public broadly, especially after significant modifications to the AI or the conditions or context in which it is used.[46] In the course of assessing such feedback, if an agency determines that the use of AI in a given context would cause more harm than good, the agency should not use the AI.

To carry out such consultations and feedback processes, agencies must take appropriate steps to solicit input from the communities and individuals affected by the AI, which could include:[47]

1. direct usability testing, such as observing users interacting with the system;
2. general solicitations of comments from the public, such as a request for information in the *Federal Register* or a "Tell Us About Your Experience" sheet with an open-ended space for responses;
3. post-transaction customer feedback collections;[48]
4. public hearings or meetings, such as a listening session;
5. outreach to relevant Federal employee groups and Federal labor organizations, including on the appropriate fulfillment of collective bargaining obligations, where applicable; or
6. any other transparent process that seeks public input, comments, or feedback from the affected groups in a meaningful, equitable, accessible,

[45] For example, an agency using an AI tool to detect Federal benefits fraud is not required to consult with the target of their investigation. However, an agency should discern when it is appropriate to consult with civil society groups, academia, or other experts in the field to understand the technology's impact.

[46] The affected communities will vary depending on an agency's deployment context, but may include customers (for example, individuals, businesses, or organizations that interact with an agency) or Federal employee groups and employees' union representatives, when applicable.

[47] Agencies are encouraged to engage with OMB on whether they are required to submit information collection requests for OMB clearance under the Paperwork Reduction Act (44 U.S.C. § 3507) for the purposes of these consultations and feedback processes.

[48] Information on post-transaction customer feedback surveys can be found in OMB Circular A-11, Section 280 – Managing Customer Experience and Improving Service Delivery, https://www.whitehouse.gov/wp-content/uploads/2018/06/s280.pdf.

and effective manner.

No later than December 1, 2024 and on an ongoing basis *while* using new or existing covered rights-impacting AI, agencies must ensure these practices are followed for the AI:

C. **Conduct ongoing monitoring and mitigation for AI-enabled discrimination.** As part of the ongoing monitoring requirement established in Section 5(c)(iv)(D), agencies must also monitor rights-impacting AI to specifically assess and mitigate AI-enabled discrimination against protected classes, including discrimination that might arise from unforeseen circumstances, changes to the system after deployment, or changes to the context of use or associated data. Where sufficient mitigation is not possible, agencies must safely discontinue use of the AI functionality.

D. **Notify negatively affected individuals.** Consistent with applicable law and governmentwide guidance, agencies must notify individuals when use of the AI results in an adverse decision or action that specifically concerns them, such as the denial of benefits or deeming a transaction fraudulent.[49] Agencies should consider the timing of their notice and when it is appropriate to provide notice in multiple languages and through alternative formats and channels, depending on the context of the AI's use. The notice must also include a clear and accessible means of contacting the agency and, where applicable, provide information to the individual on their right to appeal. Agencies must also abide by any existing obligations to provide explanations for such decisions and actions.[50]

E. **Maintain human consideration and remedy processes**. Where practicable and consistent with applicable law and governmentwide guidance, agencies must provide timely human consideration and potential remedy, if appropriate, to the use of the AI via a fallback and escalation system in the event that an impacted individual would like to appeal or contest the AI's negative impacts on them. Agencies that already maintain an appeal or secondary human review process for adverse actions, or for agency officials' substantive or procedural errors, can leverage and expand such processes, as appropriate, or establish new processes to meet this requirement. These remedy processes should not place unnecessary burden on the impacted individual, and agencies should follow OMB guidance on

[49] In some instances, such as an active law enforcement investigation, providing immediate notice may be inappropriate or impractical, or disclosure may be more appropriate at a later stage (for example, prior to a defendant's trial).

[50] Explanations might include, for example, how and why the AI-driven decision or action was taken. This does not mean that agencies must provide a perfect breakdown of how a machine learning system came to a conclusion, as exact explanations of AI decisions may not be technically feasible. However, agencies should still characterize the general nature of such AI decisions through context such as the data that the decision relied upon, the design of the AI, and the broader decision-making context in which the system operates. Such explanations should be technologically valid, meaningful, useful, and as simply stated as possible, and higher-risk decisions should be accompanied by more comprehensive explanations.

calculating administrative burden.[51] Whenever agencies are unable to provide an opportunity for an individual to appeal due to law, governmentwide guidance, or impracticability, they must create appropriate alternative mechanisms for human oversight of the AI.

F. **Maintain options to opt-out for AI-enabled decisions**. Agencies must provide and maintain a mechanism for individuals to conveniently opt-out from the AI functionality in favor of a human alternative, where practicable and consistent with applicable law and governmentwide guidance. An opt-out mechanism must be prominent, readily available, and accessible, and it is especially critical where the affected people have a reasonable expectation of an alternative or where lack of an alternative would meaningfully limit availability of a service or create unwarranted harmful impacts. Agencies should also seek to ensure that the opt-out mechanism itself does not impose discriminatory burdens on access to a government service. Agencies are not required to provide the ability to opt-out if the AI functionality is solely used for the prevention, detection, and investigation of fraud[52] or cybersecurity incidents, or the conduct of a criminal investigation. Pursuant to the authority for waivers defined in Section 5(c)(ii), CAIOs are additionally permitted to waive this opt-out requirement if they can demonstrate that a human alternative would result in a service that is less fair (e.g., produces a disparate impact on protected classes) or if an opt-out would impose undue hardship on the agency.

d. Managing Risks in Federal Procurement of Artificial Intelligence

This section provides agencies with recommendations for responsible procurement of AI, supplementing an agency's required risk management practices above for rights-impacting AI and safety-impacting AI. In addition to these recommendations and consistent with section 7224(d) of the Advancing American AI Act and Section 10.1(d)(ii) of Executive Order 14110, OMB will also develop an initial means to ensure that Federal contracts for the acquisition of an AI system or service align with the guidance in this memorandum.

i. **Aligning with the Law**. Agencies should ensure that procured AI is consistent with the Constitution and complies with all other applicable laws, regulations, and policies, including those addressing privacy, confidentiality, intellectual property, cybersecurity, human and civil rights, and civil liberties.

ii. **Transparency and Performance Improvement**. Agencies should take steps to ensure transparency and adequate performance for their procured AI, including by:

A. obtaining adequate documentation to assess the AI's capabilities, such as through the use of model, data, and system cards;

[51] *See* OMB M-22-10 and supporting document "Strategies for Reducing Administrative Burden in Public Benefit and Service Programs."

[52] Some uses of AI in these categories, such as the use of biometrics for identity verification, may be subject to requirements in other guidance that would necessitate an option to opt-out, and this memorandum does not replace, supersede, otherwise interfere with any such requirements.

B. obtaining adequate documentation of known limitations of the AI and any guidelines on how the system is intended to be used;
C. obtaining adequate information about the provenance of the data used to train, fine-tune, or operate the AI;
D. regularly evaluating claims made by Federal contractors concerning both the effectiveness of their AI offerings as well as the risk management measures put in place, including by testing the AI in the particular environment where the agency expects to deploy the capability;
E. considering contracting provisions that incentivize the continuous improvement of procured AI; and
F. requiring sufficient post-award monitoring of the AI, where appropriate in the context of the product or service acquired.

iii. **Promoting Competition in Procurement of AI.** Agencies should take appropriate steps to ensure that Federal AI procurement practices promote opportunities for competition among contractors and do not improperly entrench incumbents. Such steps may include promoting interoperability so that, for example, procured AI works across multiple cloud environments, and ensuring that vendors do not inappropriately favor their own products at the expense of competitors' offerings.

iv. **Maximizing the Value of Data for AI**. In contracts for AI products and services, agencies should treat relevant data, as well as improvements to that data—such as cleaning and labeling—as a critical asset for their AI maturity. Agencies should take steps to ensure that their contracts retain for the Government sufficient rights to data and any improvements to that data so as to avoid vendor lock-in and facilitate the Government's continued design, development, testing, and operation of AI. Additionally, agencies should consider contracting provisions that protect Federal information used by vendors in the development and operation of AI products and services for the Federal Government, so that such data is protected from unauthorized disclosure and use and cannot be subsequently used to train or improve the functionality of the vendor's commercial offerings without express permission from the agency.

v. **Overfitting to Known Test Data.** When testing AI using data that its developer may have access to—including test data that the agency has itself shared or released—agencies should ensure, as appropriate, that their AI developers or vendors are not directly relying on the test data to train their AI systems.[53]

vi. **Responsible Procurement of AI for Biometric Identification.** When procuring systems that use AI to identify individuals using biometric identifiers—e.g., faces, irises, fingerprints, or gait—agencies are encouraged to:

A. Assess and address the risks that the data used to train or operate the AI may not be lawfully collected or used, or else may not be sufficiently accurate to support reliable biometric identification. This includes the risks that the biometric information was collected without appropriate consent, was originally collected

[53] For instance, using validation data to train a model could lead the model to learn spurious correlations that make the model appear accurate in tests but harm the real-world performance of the AI system.

for another purpose, embeds unwanted bias, or was collected without validation of the included identities; and

B. Request supporting documentation or test results to validate the accuracy, reliability, and validity of the AI's ability to match identities.

vii. **Responsibly Procuring Generative AI**. Agencies are encouraged to include risk management requirements in contracts for generative AI, and particularly for dual-use foundation models, including:

A. requiring adequate testing and safeguards,

B. requiring results of internal or external testing and evaluation, to include AI red-teaming against risks from generative AI, such as discriminatory, misleading, inflammatory, unsafe, or deceptive outputs;

C. requiring that generative AI models have capabilities, as appropriate and technologically feasible, to reliably label or establish provenance for their content as generated or modified by AI; and

D. incorporating relevant NIST standards, defined pursuant to Sections 4.1(a) and 10.1(d) of Executive Order 14110, as appropriate.

viii. **Assessing for Environmental Efficiency and Sustainability.** When procuring computationally intensive AI services, for example those that rely on dual-use foundation models, agencies should consider the environmental impact of those services, including whether the vendor has implemented methods to improve the efficiency and sustainability of such AI. This should include considering the carbon emissions and resource consumption from supporting data centers.

6. DEFINITIONS

The below definitions apply for the purposes of this memorandum.

Accessibility: The term “accessibility” has the meaning provided in Section 2(e) of Executive Order 14035.

Agency: The term “agency” has the meaning provided in 44 U.S.C. § 3502(1).

Algorithmic Discrimination: The term “algorithmic discrimination” has the meaning provided in Section 10(f) of Executive Order 14091 of February 16, 2023.

Artificial Intelligence (AI): The term “artificial intelligence” has the meaning provided in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019,[54] which states that “the term ‘artificial intelligence’ includes the following”:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

[54] Pub. L. No. 115-232, § 238(g), https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf.

2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

For the purposes of this memorandum, the following technical context should guide interpretation of the definition above:

1. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
2. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.
3. For this definition, no system should be considered too simple to qualify as covered AI due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).
4. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

<u>AI and AI-Enabling Roles:</u> The term “AI and AI-enabling roles” refers to individuals with positions and major duties whose contributions are important for successful and responsible AI outcomes. AI and AI-Enabling Roles include both technical and non-technical roles, such as data scientists, software engineers, data engineers, data governance specialists, statisticians, machine learning engineers, applied scientists, designers, economists, operations researchers, product managers, policy analysts, program managers, behavioral and social scientists, customer experience strategists, human resource specialists, contracting officials, managers, and attorneys.

<u>AI Maturity:</u> The term “AI maturity” refers to a Federal Government organization’s capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with relevant Federal law, regulation, and policy on AI.

<u>AI Model</u>: The term “AI model” has the meaning provided in Section 3(c) of Executive Order 14110.

<u>AI Red-Teaming:</u> The term “AI red-teaming” has the meaning provided for “AI red-teaming” in Section 3(d) of Executive Order 14110.

Applied Research: The term "applied research" refers to original investigation undertaken in order to acquire new knowledge to determine the means by which a specific practical aim or objective may be met.

Automation Bias: The term "automation bias" refers to the propensity for humans to inordinately favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.

Basic Research: The term "basic research" refers to experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts without a specific application towards processes or products in mind.

CFO Act Agency: The term "CFO Act Agency" refers to the agencies identified in 31 U.S.C. § 901(b).

Custom-Developed Code: The term "custom-developed code" has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Customer Experience: The term "customer experience" has the meaning established in Section 3(b) of Executive Order 14058.[55]

Data Asset: The term "data asset" has the meaning provided in 44 U.S.C § 3502.

Dual-Use Foundation Model: The term "dual-use foundation model" has the meaning provided in Section 3(k) of Executive Order 14110.

Equity: The term "equity" has the meaning provided in Section 10(a) of Executive Order 14091.[56]

Federal Information: The term "Federal information" has the meaning provided in OMB Circular A-130.

Generative AI: The term "generative AI" has the meaning provided in Section 3(p) of Executive Order 14110.

Intelligence Community: The term "intelligence community" has the meaning provided in 50 U.S.C. § 3003.

Model Weight: The term "model weight" has the meaning provided in Section 3(u) of Executive Order 14110.

[55] Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government*, https://www.federalregister.gov/documents/2021/12/16/2021-27380/transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government.

[56] Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government,* https://www.govinfo.gov/content/pkg/FR-2023-02-22/pdf/2023-03779.pdf.

National Security System: The term "National Security System" has the meaning provided in 44 U.S.C. § 3552(b)(6).

Open Government Data Asset: The term "open government data asset" has the meaning provided in 44 U.S.C § 3502.

Open Source Software: The term "open source software" has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Rights-Impacting AI:[57] The term "rights-impacting AI" refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect on that individual's or entity's:

1. Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance;
2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or
3. Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services.

Risks from the Use of AI: The term "risks from the use of AI" refers to risks related to efficacy, safety, equity, fairness, transparency, accountability, appropriateness, or lawfulness of a decision or action resulting from the use of AI to inform, influence, decide, or execute that decision or action. This includes such risks regardless of whether:

1. the AI merely informs the decision or action, partially automates it, or fully automates it;
2. there is or is not human oversight for the decision or action;
3. it is or is not easily apparent that a decision or action took place, such as when an AI application performs a background task or silently declines to take an action; or
4. the humans involved in making the decision or action or that are affected by it are or are not aware of how or to what extent the AI influenced or automated the decision or action.

While the particular forms of these risks continue to evolve, at least the following factors can create, contribute to, or exacerbate these risks:

1. AI outputs that are inaccurate or misleading;
2. AI outputs that are unreliable, ineffective, or not robust;
3. AI outputs that are discriminatory or have a discriminatory effect;
4. AI outputs that contribute to actions or decisions resulting in harmful or unsafe outcomes, including AI outputs that lower the barrier for people to take intentional and harmful actions;
5. AI being used for tasks to which it is poorly suited or being inappropriately repurposed in a context for which it was not intended;
6. AI being used in a context in which affected people have a reasonable expectation that a human is or should be primarily responsible for a decision or action; and

[57] Appendix I(2) of this memorandum lists AI applications that are presumed to be rights-impacting.

7. the adversarial evasion or manipulation of AI, such as an entity purposefully inducing AI to misclassify an input.

This definition applies to risks specifically arising from using AI and that affect the outcomes of decisions or actions. It does not include all risks associated with AI, such as risks related to the privacy, security, and confidentiality of the data used to train AI or used as inputs to AI models.

Safety-Impacting AI:[58] The term "safety-impacting AI" refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of:

1. Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms;
2. Climate or environment, including irreversible or significant environmental damage;
3. Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21[59] or any successor directive and the infrastructure for voting and protecting the integrity of elections; or,
4. Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

Significant Modification: The term "significant modification" refers to an update to an AI application or to the conditions or context in which it is used that meaningfully alters the AI's impact on rights or safety, such as through changing its functionality, underlying structure, or performance such that prior evaluations, training, or documentation become misleading to users, overseers, or individuals affected by the system. This includes significantly changing the context, scope, or intended purpose in which the AI is used.

Underserved Communities: The term "underserved communities" has the meaning provided in Section 10(b) of Executive Order 14091.

[58] Appendix I(1) of this memorandum lists AI applications that are presumed to be safety-impacting.

[59] Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, or successor directive, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Appendix I: Purposes for Which AI is Presumed to be Safety-Impacting and Rights-Impacting

OMB has determined that the categories in this appendix in general meet the definition of safety-impacting AI or rights-impacting AI and are automatically *presumed* to be safety-impacting or rights-impacting. The following lists only identify a subset of uses of AI that impact rights and safety, and they do not represent an exhaustive list. Additionally, the presumption that a particular use of AI in the following lists will impact rights or safety can be waived by an agency's CAIO with adequate justification, pursuant to the processes outlined in Section 5.

1. Purposes That Are Presumed to Be Safety-Impacting. A use of AI is presumed to be safety-impacting if it is used or expected to be used, in real-world conditions, to control or significantly influence the outcomes of any of the following agency activities or decisions:

a. Controlling the safety-critical functions within dams, emergency services, electrical grids, the generation or movement of energy, fire safety systems, food safety mechanisms, traffic control systems and other systems controlling physical transit, water and wastewater systems, or nuclear reactors, materials, and waste;
b. Maintaining the integrity of elections and voting infrastructure;
c. Controlling the physical movements of robots or robotic appendages within a workplace, school, housing, transportation, medical, or law enforcement setting;
d. Applying kinetic force; delivering biological or chemical agents; or delivering potentially damaging electromagnetic impulses;
e. Autonomously or semi-autonomously moving vehicles, whether on land, underground, at sea, in the air, or in space;
f. Controlling the transport, safety, design, or development of hazardous chemicals or biological agents;
g. Controlling industrial emissions and environmental impacts;
h. Transporting or managing of industrial waste or other controlled pollutants;
i. Designing, constructing, or testing of industrial equipment, systems, or structures that, if they failed, would pose a significant risk to safety;
j. Carrying out the medically relevant functions of medical devices; providing medical diagnoses; determining medical treatments; providing medical or insurance health-risk assessments; providing drug-addiction risk assessments or determining access to medication; conducting risk assessments for suicide or other violence; detecting or preventing mental-health issues; flagging patients for interventions; allocating care in the context of public insurance; or controlling health-insurance costs and underwriting;
k. Detecting the presence of dangerous weapons or a violent act;
l. Choosing to summon first responders to an emergency;
m. Controlling access to or security of government facilities; or
n. Determining or carrying out enforcement actions pursuant to sanctions, trade restrictions, or other controls on exports, investments, or shipping.

2. Purposes That Are Presumed to Be Rights-Impacting. A use of AI is presumed to be rights-impacting if it is used or expected to be used, in real-world conditions, to control or significantly influence the outcomes of any of the following agency activities or decisions:

a. Blocking, removing, hiding, or limiting the reach of protected speech;
b. In law enforcement contexts, producing risk assessments about individuals; predicting criminal recidivism; predicting criminal offenders; identifying criminal suspects or predicting perpetrators' identities; predicting victims of crime; forecasting crime; detecting gunshots; tracking personal vehicles over time in public spaces, including license plate readers; conducting biometric identification (e.g., iris, facial, fingerprint, or gait matching); sketching faces; reconstructing faces based on genetic information; monitoring social media; monitoring prisons; forensically analyzing criminal evidence; conducting forensic genetics; conducting cyber intrusions in the course of an investigation; conducting physical location-monitoring or tracking of individuals; or making determinations related to sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention;
c. Deciding or providing risk assessments related to immigration, asylum, or detention status; providing immigration-related risk assessments about individuals who intend to travel to, or have already entered, the U.S. or its territories; determining individuals' border access or access to Federal immigration related services through biometrics or through monitoring social media and other online activity; monitoring individuals' physical location for immigration and detention-related purposes; or forecasting the migration activity of individuals;
d. Conducting biometric identification for one-to-many identification in publicly accessible spaces;
e. Detecting or measuring emotions, thought, impairment, or deception in humans;
f. Replicating a person's likeness or voice without express consent;
g. In education contexts, detecting student cheating or plagiarism; influencing admissions processes; monitoring students online or in virtual-reality; projecting student progress or outcomes; recommending disciplinary interventions; determining access to educational resources or programs; determining eligibility for student aid or Federal education; or facilitating surveillance (whether online or in-person);
h. Screening tenants; monitoring tenants in the context of public housing; providing valuations for homes; underwriting mortgages; or determining access to or terms of home insurance;
i. Determining the terms or conditions of employment, including pre-employment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; performing time-on-task tracking; or conducting workplace surveillance or automated personnel management;
j. Carrying out the medically relevant functions of medical devices; providing medical diagnoses; determining medical treatments; providing medical or insurance health-risk assessments; providing drug-addiction risk assessments or determining access to medication; conducting risk assessments for suicide or other violence; detecting or preventing mental-health issues; flagging patients for interventions; allocating care in the context of public insurance; or controlling health-insurance costs and underwriting;

k. Allocating loans; determining financial-system access; credit scoring; determining who is subject to a financial audit; making insurance determinations and risk assessments; determining interest rates; or determining financial penalties (e.g., garnishing wages or withholding tax returns);
l. Making decisions regarding access to, eligibility for, or revocation of critical government resources or services; allowing or denying access—through biometrics or other means (e.g., signature matching)—to IT systems for accessing services for benefits; detecting fraudulent use or attempted use of government services; assigning penalties in the context of government benefits;
m. Translating between languages for the purpose of official communication to an individual where the responses are legally binding; providing live language interpretation or translation, without a competent interpreter or translator present, for an interaction that directly informs an agency decision or action; or
n. Providing recommendations, decisions, or risk assessments about adoption matching, child protective actions, recommending child custody, whether a parent or guardian is suitable to gain or retain custody of a child, or protective actions for senior citizens or disabled persons.

Appendix II: Consolidated Table of Actions

Responsible Entity	Action	Section	Deadline
Each Agency	Designate an agency Chief AI Officer and notify OMB	3(a)(i)	60 days
Each CFO Act Agency	Convene agency AI Governance Board	3(a)(ii)	60 days
Each Agency	Submit to OMB and release publicly an agency plan to achieve consistency with this memorandum or a written determination that the agency does not use and does not anticipate using covered AI	3(a)(iii)	180 days and every two years thereafter until 2036
Each CFO Act Agency	Develop and release publicly an agency strategy for removing barriers to the use of AI and advancing agency AI maturity	4(a)(i)	365 days
Each Agency**	Publicly release an expanded AI use case inventory and report metrics on use cases not included in public inventories	3(a)(iv), 3(a)(v)	Annually
Each Agency*	Share and release AI code, models, and data assets, as appropriate	4(d)	Ongoing
Each Agency*	Stop using any safety-impacting or rights-impacting AI that is not in compliance with Section 5(c) and has not received an extension or waiver	5(a)(i)	December 1, 2024 (with extensions possible)
Each Agency*	Certify the ongoing validity of the waivers and determinations granted under Section 5(c) and 5(b) and publicly release a summary detailing each and its justification	5(a)(ii)	December 1, 2024 and annually thereafter
Each Agency*	Conduct periodic risk reviews of any safety-impacting and rights-impacting AI in use	5(c)(iv)(D)	At least annually and after significant modifications

Each Agency*	Report to OMB any determinations made under Section 5(b) or waivers granted under Section 5(c)	5(b);
		5(c)(iii)
			Ongoing, within 30 days of granting waiver

* Excluding elements of the Intelligence Community.

** Excluding elements of the Intelligence Community. The Department of Defense is exempt from the requirement to inventory individual use cases.

(xxii) the Assistant to the President for Economic Policy;

(xxiii) the Assistant to the President and Domestic Policy Advisor;

(xxiv) the Assistant to the President and Chief of Staff to the Vice President;

(xxv) the Assistant to the President and Director of the Gender Policy Council;

(xxvi) the Chairman of the Council of Economic Advisers;

(xxvii) the National Cyber Director;

(xxviii) the Chairman of the Joint Chiefs of Staff; and

(xxix) the heads of such other agencies, independent regulatory agencies, and executive offices as the Chair may from time to time designate or invite to participate.

(d) The Chair may create and coordinate subgroups consisting of White House AI Council members or their designees, as appropriate.

Sec. 13. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
October 30, 2023.

AFGE Comments on Draft OMB Policy

December 5, 2023

Clare Martorana
U.S. Federal Chief Information Officer
Office of the Federal Chief Information Officer Office of Management and Budget
725 17th St., NW
Washington, DC 20503

Re: OMB-2023-0020, AFGE Comments on *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* Draft Memorandum

Dear Chief Information Officer Martorana:

The American Federation of Government Employees, AFL-CIO, (AFGE) hereby submits its comments to the draft memorandum on *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* prepared by the Office of Management and Budget (AI Memo). *See* Request for Comments on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence Draft Memorandum, 88 Fed. Reg.
75625 (Nov. 3, 2023). AFGE is the largest labor organization representing federal employees. On its own and in conjunction with its affiliated councils and locals, AFGE represents over 750,000 employees in agencies and departments across the federal government and the District of Columbia.

The responsible regulation and safe use of artificial intelligence (AI) by the federal government presents a defining public policy challenge. The Government must balance the need to control and develop outward-facing use cases with its internal administrative and workforce commitments and obligations, while ensuring that necessary safeguards in both areas are able to keep pace with a rapidly changing cyber environment. And it must simultaneously ensure that agency use of AI does not result in discrimination or bias against members of protected classes, including within the federal workforce. It is therefore of the utmost importance that the AI Memo acknowledge that federal employees and the labor organizations that represent them are key stakeholders in the governance, innovation, and risk management of agency use of AI. It is federal workers who are responsible for day-to-day agency operations, and it is these same rank- and-file federal workers who will be chiefly responsible for the implementation and application of agency AI initiatives and programs and who will also, in many instances, feel their effects.

The successful rollout of agency AI initiatives thus hinges on consequential employee and union engagement. *See* Brian DeWyngaert Sr., *Want successful integration of AI at federal agencies? Engage employees through the unions*, GovExec.com (July 19, 2023), https://www.govexec.com/workforce/2023/07/want-successful-integration-ai-federal-agencies- engage-employees-through-unions/388574/.

The fact that federal worker engagement is a critical component of the effective and efficient delivery of high-quality government services is a seminal reason why the Federal Service Labor-

Management Relations Statute (Statute) requires that agencies bargain in good faith with those labor organizations certified as their employees' exclusive representatives on any condition of employment. *See* 5 U.S.C. § 7114; *see also* 5 U.S.C. §§ 7102(2), 7103(a)(12), 7116(a)(5). It is also why the President has directed agency heads to bargain with their associated labor organizations over the numbers, types, and grades of employees assigned to any organizational subdivision, work project, or tour of duty, as well as over the technology, methods, and means of performing work. *See* Exec. Order 14003, § 4, 86 Fed. Reg. 7231 (Jan.
27, 2021); *see also* 5 U.S.C. § 7106(b)(1). It is, after all, the policy of the United States to protect, empower and rebuild the career Federal workforce, and to encourage union organizing and collective bargaining. Exec. Order 14003, § 1; *see also* Exec. Order 14025, § 1, 86 Fed. Reg. 22829 (April 26, 2021); 5 U.S.C. § 7101(a) ("[L]abor organizations and collective bargaining in the civil service are in the public interest.").

Consequently, the AI Memo should elevate the role of federal employee labor organizations with respect to agency use of AI. The AI Memo should, for example, expressly and specifically state that agencies must meet their obligation to bargain with the relevant labor organizations over changes to federal employees' conditions of employment arising from or related to agency use of AI before such changes may go into effect. The Statute requires more than mere consultation or feedback with respect to federal employees' conditions of employment. It requires collective bargaining. The same is true with respect to agencies' compliance with existing collective bargaining agreements. While it may be that AI will, in some ways, pose new and novel challenges for the federal workplace, such challenges do not relieve agencies from complying with their legal and contractual obligations. The obligation to bargain and to abide by agreements reached through collective bargaining is a statutory duty that may not be waived or diminished by an agency merely because a matter is complex or is one of first impression.

The potential novelty of future AI challenges, in fact, only reinforces the need for robust labor-management partnership because joint agency, employee, and union, problem-solving will promote a more durable AI governance framework. For this reason, the AI Memo should include a demonstrated commitment to and understanding of labor-management partnership among the skills, knowledge, training, and expertise, necessary to perform the role of Chief AI Officer (CAIO), and should include coordination and the sharing of workforce-related information (e.g., potential workforce impacts identified by agency AI impact assessments) with employees' exclusive representatives, i.e., labor organizations, as part of the CAIO's responsibilities. The AI Memo also should require that agencies provide labor organizations the opportunity for meaningful representation on agency AI Governance Boards. Plans made in the dark are unlikely to bear fruit. Active union participation in AI Governance Boards, however, will bring agencies the benefit of frontline workers' experience and knowledge when addressing the substantive and logistical issues that may arise from agency regulation and use of AI.

The AI Memo should, moreover, seize the opportunity to promote worker empowerment by directing agencies to prioritize the preservation and/or expansion of federal positions within existing bargaining units or, when necessary, to reorganize in a fashion that provides for continued representation by existing exclusive representatives. In this same vein, the AI Memo should strengthen its direction to agencies that they provide training offerings for federal employees, including opportunities that provide pathways to AI occupations and assist and cultivate employees affected by the application of AI to their work. The AI Memo should direct agencies to develop, and negotiate with the pertinent labor organizations, concrete plans that, at a minimum, offer federal employees appropriate re-skilling or up-skilling opportunities any time it is foreseeable that their positions may be affected by the agency use of AI, and which provide attainable, clear, and equitable, pathways for federal employee advancement.

Lastly, the AI Memo should establish a presumption that work related to the Government's continued design, development, testing, and operation of AI will be insourced whenever doing so is feasible. The Government should, for example, eschew reliance on AI contracts for the creation, regulation, or maintenance of controls over artificial general intelligence or generative AI because these subjects raise issues that are inherently governmental in nature. The growth and retention of a deep, internal federal employee talent pool thus will help ensure the long-term sustainability and success of federal agencies' AI governance, innovation, and risk management.

AFGE thanks OMB for providing it the opportunity to submit these comments. AFGE notes that by submitting these comments, AFGE does not waive any arguments, claims, challenges, or rights that it may have, now or in the future, concerning any aspect of the AI Memo or its application.

Sincerely,
/s/ Andres M. Grajales Andres M. Grajales Deputy General Counsel
American Federation of Government Employees 80 F Street NW
Washington, DC 20001

OPM Memo on Pay Flexibility, Incentive Pay, and Leave and Workforce Flexibility Program for Artificial Intelligence (AI, AI-enabling, and Other Key Technical Employees

February 27, 2024
CPM 2024-06

Memorandum for Heads of Executive Departments and Agencies
From: Kiran A. Ahuja Director

Subject: Pay Flexibility, Incentive Pay, and Leave and Workforce Flexibility Programs for Artificial Intelligence (AI), AI-enabling, and Other Key Technical Employees

On October 30, 2023, the President signed Executive Order (EO) 14110 titled, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence." Section 10 of the EO addresses the advancement of AI across the Federal Government and directs a number of actions to increase AI talent in the Federal Government. Subsection 10.2(d)(iv) requires that the U.S. Office of Personnel Management (OPM):

> (iv) within 120 days of the date of this order, as appropriate and permitted by law, issue guidance for agency application of existing pay flexibilities or incentive pay programs for AI, AI-enabling, and other key technical positions to facilitate appropriate use of current pay incentives.

In support of EO 14110, OPM is issuing the attached guidance for agencies on pay flexibility, incentive pay, and leave and workforce flexibility programs for AI, AI- enabling, and other key technical employees. The guidance summarizes the flexibilities and programs available to agencies to recruit and retain AI and related talent, including information on where to find additional resources. These flexibilities may also be used by agencies to recruit and retain talent more broadly, and may therefore be used for other positions of need within agencies.

Agencies can use most of the flexibilities and authorities summarized in the attached guidance without OPM approval. For the few flexibilities that require OPM approval— special rates, critical pay, and waivers of the recruitment, relocation, and retention incentive payment limits—we stand ready to assist agencies and respond to their requests for enhanced compensation tools.

Questions

Agency headquarters-level human resources offices may contact OPM at paypolicy@opm.gov. Component-level human resources offices must contact their agency headquarters for assistance. Employees must contact their agency human resources office for assistance.

cc: Chief Human Capital Officers
Human Resource Directors

Pay Flexibility, Incentive Pay, and Leave and Workforce Flexibility Programs for Artificial Intelligence (AI), AI-enabling, and Other Key Technical Employees

Agencies have considerable discretionary authority to use a variety of pay flexibility, incentive pay, and leave and workforce flexibility programs to support their recruitment, relocation, and retention efforts for AI, AI-enabling, and other key technical employees. A summary of available flexibilities and programs is provided below with information on where to find additional resources. Most of these flexibilities and authorities can be used without approval from the Office of Personnel Management (OPM).

- Tips:
  - Many of the flexibilities below can be used simultaneously and with other human resources tools to enhance an agency's AI and AI-enabling employee recruitment and retention efforts. For example, an agency may use an OPM-approved direct hire authority to hire a new AI employee, pay the new employee a recruitment incentive, set the new employee's pay above step 1 of their grade using the superior qualifications and special needs pay setting authority, provide service credit towards a higher annual leave accrual rate based non-Federal AI work experience, and provide alternative work schedule and telework options.
  - These flexibilities may also be used by agencies to recruit and retain talent more broadly, and may therefore be used for other positions of need within agencies.

Pay Flexibilities and Incentive Pay Programs

- **Recruitment Incentives** – Agencies may offer newly appointed employees in difficult-to-fill positions up to 25 percent of basic pay multiplied by the number of years in the service agreement (up to 4 years). Information on recruitment incentives can be found on this webpage. (5 U.S.C. 5753 and 5 CFR part 575, subpart A)
  - Tip: An agency may document in its written justification that an AI, AI- enabling, and other key technical position is difficult to fill if OPM has approved the use of a direct-hire authority applicable to the position with no further evidence required.
- **Relocation Incentives** – Agencies may offer current employees who must relocate to difficult-to-fill positions up to 25 percent of basic pay multiplied by the number of years in the service agreement (up to 4 years). Information on relocation

incentives can be found on this webpage. (5 U.S.C. 5753 and 5 CFR part 575, subpart B)

  - Tip: An agency may document in its written justification that an AI, AI- enabling, and other key technical position is difficult to fill if OPM has approved the use of a direct-hire authority applicable to the position with no further evidence required.

- **Retention Incentives** – Agencies may offer highly qualified employees or employees filling a special agency need who are likely to leave the Federal service up to 25 percent of basic pay for an individual or 10 percent for a group. Information on retention incentives can be found on this webpage. (5 U.S.C. 5754 and 5 CFR part 575, subpart C)

  - Tip: An employee is not required to have a non-Federal job offer in hand to qualify for a retention incentive. An agency may determine that an employee is likely to leave the Federal service based on other considerations such as employment trends and labor market factors, the salaries typically paid outside the Federal Government for the employee's skills, and the success of recent recruitment and retention efforts for similar employees and positions.

- **Student Loan Repayment Program** – Agencies may repay Federally insured student loans as a recruitment or retention incentive for candidates or current employees of the agency, up to a maximum of $10,000 for an employee in a calendar year and a total of not more than $60,000 for any one employee. Information on the student loan repayment program can be found on this webpage. (5 U.S.C. 5379 and 5 CFR part 537). (Note: Federal service is also considered qualifying service for the Public Service Loan Forgiveness Program (PSLF), a separate authority from the Student Loan Repayment Program. PSLF forgives the remaining balance on Federal Direct Loans after a Federal student loan borrower has made 120 qualifying payments while working full-time for a qualifying employer. More information can be found on the Department of Education's PSLF website.)

- **Superior Qualifications and Special Needs Pay-Setting Authority** – Agencies may set a new General Schedule (GS) employee's pay above step 1 (up to step 10), because of the employee's superior qualifications or the agency's special need of the candidate's services. Information on this pay-setting authority can be found on this webpage. (5 CFR 531.212)

- **Maximum Payable Rate Rule** – Agencies may set pay at a higher-than-normal GS rate based on a higher rate of pay the employee previously received in another Federal job (not to exceed step 10 of their grade). Information on this pay-setting flexibility can be found on this webpage. (5 CFR 531.221-223)

- **Special Rates** – Agencies may request OPM approval of special rates (higher rates of pay) to address staffing needs for a group or category of employees. Information on special rates can be found on this webpage, including instructions for requesting OPM approval of special rates. (5 U.S.C. 5305 and 5 CFR part 530, subpart C)

- **Critical Position Pay** – Agencies may request that OPM approve critical position pay, in consultation with OMB, so that an agency may fix the rate of basic pay for one or more positions requiring an extremely high level of expertise at a higher rate than would otherwise be payable for the position, up to level I of the Executive Schedule. Information on critical position pay can be found on this webpage, including an OPM request template. (5 U.S.C. 5377 and 5 CFR part 535)

- **Waivers of Recruitment, Relocation, and Retention Incentive Payment Limits** – Agencies may request that OPM approve a waiver of the normal recruitment, relocation, and retention incentive payment limits and provide authority to pay incentives under a higher limit of up to 50 percent based on a critical agency need. Recruitment, relocation, and retention incentive waiver request templates can be found on this webpage. (5 CFR 575.109(c), 575.209(c), and 575.309(e))

Leave and Workforce Flexibilities

- **Creditable Service for Annual Leave Accrual for Non-Federal Work Experience and Experience in the Uniformed Service** – An agency may provide service credit for the purpose of determining the annual leave accrual rate of a new employee or a retired member of the active duty uniformed service under certain conditions. Information on this leave flexibility can be found on this webpage. (5 U.S.C. 2101(1), 5 U.S.C. 6303(e), and 5 CFR 630.205)

- **Extension of the Higher Annual Leave Accrual Rate to SES and SL/ST Equivalent Pay Systems** – Members of the Senior Executive Service (SES) and employees in senior-level (SL) and scientific and professional (ST) positions accrue annual leave at the rate of 1 day (8 hours) per biweekly pay period without regard to their length of service. An agency may request that OPM authorize this same annual leave accrual rate for additional categories of employees that are equivalent to SES and SL/ST pay systems. Information on this leave flexibility can be found here. (5 U.S.C. 6303(f) and 5 CFR 630.301(a) - (d))

- **Alternative Work Schedules** – An agency may establish programs that allow the use of alternative work schedules (AWS) that differ from the 40-hour/5-day traditional workweek. AWS programs enable managers and supervisors to meet their program goals while, at the same time, providing employees more flexibility in scheduling their personal activities (e.g., family and other personal responsibilities, volunteer activities, and educational opportunities). Information on alternative work schedules and other work schedule flexibilities can be found here. (5 U.S.C. 6120–6133 and 5 CFR 610.401–610.408)

- **Telework and Remote Work** – Agencies use telework as a workplace flexibility to meet mission-critical needs of their organization while helping employees balance work and personal responsibilities. Remote work can allow agencies to recruit and retain high-quality

MARCH 06, 2024

Executive Order on Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Sec. 6. Implementation of Labor-Management Forums Throughout the Executive Branch. (a) Executive Order 13812 of September 29, 2017 (Revocation of Executive Order Creating Labor-Management Forums), is hereby revoked.

(b) Each Labor-Management Forum agency, consistent with any guidance issued by OPM, shall:

(i) establish Labor-Management Forums by creating joint labor-management committees or councils at the levels of recognition and other appropriate levels agreed to by the employee union and management, or by adapting existing councils or committees if such groups exist, to help identify problems and propose solutions to better serve the public and agency mission;

(ii) allow employees and their union representatives to have pre-decisional involvement in workplace matters, including consultation on Registered Apprenticeship recommendations and discussions with management for the development of joint solutions to workplace challenges; and

(iii) evaluate and document, in consultation with union representatives and any further guidance provided by OPM, changes in employee satisfaction, manager satisfaction, and organizational performance resulting from the Labor-Management Forums.

(c) Each head of a Labor-Management Forum agency for which there exists one or more exclusive representatives, as defined in 5 U.S.C. 7103(a)(16), shall, in consultation with union representatives, prepare and submit to OPM, within 180 days of the date of this order, a written implementation plan that addresses the requirements of subsection (b) of this section. The Office of Personnel Management shall review each plan within 60 days of receipt and shall determine whether to certify that the plan satisfies the requirements of this order and any further guidance issued by OPM. Upon certification, the head of each Labor-Management Forum agency shall ensure that the certified plan is faithfully executed. Any plan that is determined by OPM to be insufficient shall be returned to the Labor-Management Forum agency with guidance for improvement, and the agency shall resubmit its revised plan to OPM within 30 days of receipt of the original plan from OPM.

Sec. 7. General Provisions. (a) This order supersedes Executive Order 13522 of December 9, 2009 (Creating Labor-Management Forums to Improve Delivery of Government Services).

(b) Nothing in this order shall abrogate any collective bargaining agreements in effect as of the date of this order.

(c) Nothing in this order shall be construed to limit, preclude, or prohibit the head of any executive department or agency from electing to negotiate over any or all of the subjects set forth in 5 U.S.C. 7106(b)(1) in any negotiation.

(d) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(e) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(f) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

March 13, 2024

Memorandum for Heads of Executive Departments and Agencies

From: Kiran A. Ahuja
Director

Subject: Guidance on Implementation of Labor-Management Forums: Executive Order on Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums

Section 1 of the Executive Order (EO) on Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums reinforces the policy of the Biden-Harris Administration to encourage union organizing and collective bargaining. It notes that "[l]abor-management forums, as complements to the existing collective bargaining process, allow managers and employees to collaborate in order to continue to deliver the highest quality goods and services to the American people." It further provides that it is the policy of the Biden-Harris Administration "to establish cooperative and productive labor-management relations throughout the executive branch."

Section 6 of the EO requires implementation of labor-management forums throughout the Executive Branch to be consistent with any guidance provided by OPM. OPM is issuing this guidance to help agencies and unions implement the labor-management forum requirements, including allowing employees and their union representatives to have pre-decisional involvement on workplace matters, as set forth in the EO. While this guidance is not designed to be all-inclusive or to be construed as the "only" approach, we believe it will be helpful to agency and union representatives in establishing a cooperative and productive form of labor-management relations throughout the executive branch. This guidance does not cover matters on scaling and expanding the use of registered apprenticeships discussed elsewhere in the EO.

Revocations

Section 6(a) of the EO revokes EO 13812 of September 29, 2017 (Revocation of Executive Order Creating Labor-Management Forums). EO 13812 was perceived to be an obstacle to the creation of labor-management forums.

Implementation of Labor-Management Forums Through the Executive Branch

In support of the policies of the EO and consistent with the attached OPM guidance, agencies should work with their union representatives and take the following actions at the earliest opportunity:

(1) Establish Labor-Management Forums by creating joint labor-management committees or councils at the levels of recognition. Forums may be established at other appropriate levels agreed to by labor and management;

(2) Allow employees and their union representatives to have pre-decisional involvement in workplace matters, including discussions with management for the development of joint solutions to workplace challenges;

(3) Evaluate and document, in consultation with union representatives and consistent with the attached OPM guidance, changes in employee satisfaction, manager satisfaction, and organizational performance (including organizational health) resulting from Labor-Management Forums; and

(4) Prepare and submit, in consultation with union representatives, within 180 days of the date of the order, a written implementation plan to OPM where there exists one or more exclusive representatives, consistent with the attached OPM guidance.

The attachments provide additional guidance for Federal agencies and unions on the above actions which support the Labor-Management Forum policies of the EO.

Additional Information

Agency headquarters-level human resources offices and national unions may contact OPM at awr@opm.gov with additional questions. Agency field offices and local unions should contact their appropriate headquarters-level agency human resources offices.

cc: Chief Human Capital Officers (CHCOs), Deputy CHCOs, and Human Resources Directors

Attachments:

Appendix A: Creating Labor Management Forums
Appendix B: Additional Guidance on Establishment of Labor-Management Forums
Appendix C: Guidance for LMF Metrics
Appendix D: Timeframes and Key Actions for Implementation of LMF Requirements

Appendix A: Creating Labor Management Forums

Labor Management Forum Requirements

Labor-Management Forums (LMFs) allow managers and employees' union representatives to discuss how Federal Government operations can promote satisfactory labor relations and improve the productivity and effectiveness of the Federal Government.[1] Section 6(b) of the EO provides that each Labor-Management Forum agency[2], consistent with any guidance provided by OPM, shall:

1. establish LMFs[3] by creating joint labor-management committees or councils at the level of recognition and other appropriate levels agreed to by the union and management, to help identify problems and propose solutions to better serve the public and agency mission;[4]

2. allow employees and their union representatives to have pre-decisional involvement in workplace matters, including discussions with management for the development of joint solutions to workplace challenges; and

3. evaluate and document, in consultation with union representatives and consistent with any further guidance provided by the Office of Personnel Management (OPM), changes in employee satisfaction, manager satisfaction, and organizational performance[5] resulting from the LMFs.

Section 6(c) provides that each head of Labor-Management Forum (LMF) agency for which there exists one or more exclusive representatives, as defined in 5 U.S.C. 7103(a)(16), shall, in consultation with union representatives, prepare and submit for approval, within 180 days of the date of the EO, a written implementation plan to OPM. OPM requests each LMF agency plan to:

[1] The EO also requires an interagency working group to convene and issue an initial report to the President with findings and recommendations regarding Registered Apprenticeship programs. This guidance does not address matters related to Registered Apprenticeship programs and is focused on the EO requirements for labor-management forums and use of pre-decisional involvement on workplace matters.
[2] Section 2(g) of the EO defines "Labor-Management Forum agencies" to mean all agencies subject to chapter 71 of title 5, United States Code.
[3] For ease of reading OPM's guidance, all references to labor-management forums, councils, or committees will simply be referred to as LMFs as these terms can be used interchangeably.
[4] Section 7(a) of the EO states "[t]his order supersedes Executive Order 13522 of December 9, 2009 (Creating Labor-Management Forums to Improve Delivery of Government Services)."
[5] Organizational performance includes organizational health.

- describe how the agency will work with the exclusive representatives of its employees to conduct a baseline assessment of the current state of labor-management relations within the agency, including assessment of any outstanding issues regarding implementation of EO 14003 (Protecting the Federal Workforce) and OPM's guidance related to implementation of EO 14025 (Worker Organizing and Empowerment[6], in any bargaining units within the agency;

- report the extent to which the agency has already established LMFs at the levels of recognition and, if agreed to by labor and management, at other appropriate levels, or adapting existing councils or committees if such groups exist;

- address how the agency will evaluate and document, in consultation with union representatives and consistent with any further guidance provided by OPM, changes in employee satisfaction, manager satisfaction, and organizational performance (including organizational health) resulting from the Labor-Management Forums; and

- explain the agency plan for devoting sufficient resources to the implementation of the plan, including sufficient resources to create and operate LMFs.

Next Steps for Agencies and Unions – Creation of Implementation Plans

As noted above, Section 6(c) of the EO requires agencies to prepare and submit, in consultation with union representatives, within 180 days of the date of the EO, a written implementation plan to OPM. The written implementation plan should be a consolidated plan which covers all bargaining units in the Department or agency.[7] The purpose of the implementation plan is to affirm the creation of the LMF(s) and to create a guide for the evolving relationship. The implementation plan serves as a roadmap for the parties as the relationship moves forward. It is not a contractual document between the participants, and it is not intended to modify any of the existing collective bargaining agreements between the parties or for either party to waive their rights under the law.

[6] EO 14003 and EO 14025 are critical components of the Administration's policies supporting collective bargaining, worker organizing and empowerment. To the extent there are outstanding implementation issues, these are ideal issues for labor-management forums to address and should be addressed for successful implementation of LMF requirements.

[7] Some agencies have multiple bargaining units involving different unions. OPM is not requesting implementation plans for each bargaining unit. Agencies and unions may elect to submit plans that provide a framework for all bargaining units in the agency while allowing local management and local unions to establish more comprehensive plans that meet their needs and which do not need to be submitted to OPM.

While OPM is not prescribing a specific format for implementation plans, each plan should clearly answer the following questions:

1. How will the agency work with the exclusive representatives of its employees to conduct a baseline assessment of the current state of labor-management relations within the agency? Where appropriate, please report to the extent the agency has already established LMFs for all exclusive representatives which wish to participate in labor-management forums.

2. What are any outstanding issues regarding implementation of EO 14003, Protecting the Federal Workforce? This includes any outstanding issues on compliance with Section 4 of EO 14003 regarding collective bargaining on matters covered by 5 USC § 7106(b)(1). Please identify agency location, name and local or chapter number of union, and bargaining unit status (BUS) code(s) of union(s) involved.

3. What are any outstanding issues regarding implementation of OPM guidance for EO 14025, Worker Organizing and Empowerment? Please identify agency location, name and local or chapter number of union, and any BUS code(s) of union(s) involved. OPM's guidance for EO 14025 includes:

    Highlighting Bargaining Unit Employee Rights in the Hiring and On-boarding Process | CHCOC – October 20, 2021

    Guidance on Implementation of EO 14025: Highlighting Bargaining Unit Employee Rights to Join a Union and Other Rights | CHCOC – October 20, 2021

    Guidance on Implementation of EO 14025: Highlighting Requirements During Union Organizing | CHCOC – April 12, 2022

    Guidance on Implementation of EO 14025: Highlighting Union Rights to Access and Communicate with Bargaining Unit Employees | CHCOC – April 12, 2022

    Guidance on Implementation of EO 14025: Highlighting Requirement to Timely Process Requests for Payroll Deductions for Labor Organization Dues | CHCOC – April 12, 2022

    Guidance on Implementation of EO 14025: Addressing Whether Non-Bargaining Unit Positions are Correctly Excluded from Bargaining Unit Coverage | CHCOC – January 26, 2023

4. How will the agency work with the exclusive representatives through its LMFs to develop agency or bargaining unit specific metrics to monitor changes in employee satisfaction, manager satisfaction, and organizational performance (including organizational health) resulting from the LMFs?
5. How will the agency devote sufficient resources to the implementation of the plan, including sufficient resources to create and operate LMFs?

Written implementation plans must be submitted to OPM within 180 days of the date of the EO. The EO was issued on March 6, 2024. Since 180 days falls on a federal holiday, agencies should submit their plans to OPM by close of business, Tuesday, September 3, 2024. Plans may be sent to AWR@opm.gov.

Section 6(c) of the EO provides that OPM shall review each implementation plan within 60 days of receipt to determine whether to certify that the plan satisfies all requirements of the EO. Plans that are determined by OPM to be insufficient will be returned to the agency with guidance for improvement and resubmission within 30 days and after consultation with union representatives, unless OPM authorizes an extension of the deadline. Extension requests may be sent to AWR@opm.gov.

Appendix B: Additional Guidance on Establishment of Labor-Management Forums[8]

General Considerations

No two federal agencies are alike, and the same is true of the relationships between agencies and their unions. Each LMF will develop its own goals and adopt its own implementation plan for success. While one size does not fit all when it comes to creating an LMF, the following strategies may assist in successful labor-management cooperative efforts:

Meetings

The participants' first endeavor will be to jointly design the LMF for sustainable success. This will require the development of a shared vision for the future of their relationship and how the LMF will enable them to achieve that desired future state. All participants are best served by refraining from "win-lose" positioning. Instead, they should look for "win-win" opportunities that balance common interests and mutual goals capable of driving agency success.

Provide Top-Down Support Driven by Agency Head and Union Leadership

The success of any LMF depends largely on the visible commitment, endorsement, and involvement of leaders within the agency and the union. Top agency and union leaders should be actively involved and model the behaviors they expect from others. Their participation has to be genuine. Both parties must realize that LMFs are a tool of cultural transformation and results may take some time. But real change may never happen unless top agency and union leaders are visibly and actively leading the way. The support of top leaders sets the stage to change behavior and drive results through the entire organization.

Recognize Labor-Management Forums Are Not Co-Management Arrangements

In creating LMFs, department and agencies must recognize that some managers, union leadership, and employees may disapprove of and resist this effort. Previous attempts at Labor-Management partnerships sometimes have been criticized as "co-management arrangements," typically by individuals who firmly believe that management and unions

[8] This information is based on OPM's prior experiences on supporting agencies and unions in establishing LMFs or equivalents under EO 12871 and EO 13522.

are adversaries. It is critical for the LMF to address these concerns early, with firm resolve and with a clearly articulated value proposition that answers the question, “What’s in it for me?,” for all stakeholders. In this process, management still manages, and unions still represent the interests of bargaining unit employees; however, both parties make a cooperative effort to address mutual interests in solving workplace problems and improving the organization.

Use of Pre-Decisional Involvement in LMFs

Pre-decisional involvement, or PDI, is a key component of the EO. The EO envisions employees and their union representatives as stakeholders whose viewpoints and input should be obtained in a collaborative labor-management engagement process before agency leaders make decisions which impact conditions of employment and which would normally be subject to collective bargaining. PDI topics may include the full range of management initiatives which impact employees in the workplace. While PDI should not be limited to the LMF, the forums may be a way for parties to engage and discuss those topics.

PDI can provide benefits to all parties involved: bargaining unit employees, unions, and management. Bargaining unit employees and their union representatives are provided an opportunity to participate in and have meaningful input into agency decisions concerning a broad spectrum of workplace issues and topics before decisions are made. Past experiences show that a successful PDI can foster employee engagement and reduce the likelihood of disputes between unions and their agency counterparts regarding employment issues, with the goal of reaching better solutions that impact the workplace.

PDI also provides agency decision-makers with an invaluable source of information from employees on the agency’s front line and their union representatives. Agency decision-makers who incorporate this rich set of information into their decision-making model can make better, customer-centric decisions about the delivery of government services to the American people.

PDI complements the collective bargaining process but does not replace it. However, if both parties are pleased with a resolution reached through PDI, further bargaining may not be necessary. This depends on several factors, including the type of issue addressed through PDI and especially the parties’ shared understanding of the relationship between PDI and collective bargaining.

It is imperative that before engaging in PDI, the parties discuss and reach a common understanding of the relationship between PDI and collective bargaining. PDI through an LMF is intended to be a collaborative, interest-based decision-making process, but PDI may also satisfy the obligation to bargain, depending on the circumstances. Determining whether the obligation to bargain has been satisfied is within the jurisdiction of the Federal Labor Relations Authority.

If either party requests, the Statute requires that the parties execute a written document embodying the agreed terms. Use of PDI does not mean an agency must sign a collective bargaining agreement with nonnegotiable provisions.[9] Likewise, use of PDI does not mean that a union waives its collective bargaining rights under 5 USC Chapter 71.

PDI works best when the agency and union use collaborative approaches, such as interest-based problem-solving, including a thorough and detailed discussion of each party's interests. If either union or management representatives have not had experience with collaborative or consensus-based decision-making processes, it is recommended that they engage in joint training. It may also be helpful to obtain the services of a facilitator to guide them through the PDI process.

Ensure the Right People Are Included in the Labor-Management Forum

An LMF is only as good as the mix of its members and the quality of their participation. Its composition sends clear messages about the commitment of the agency and union leadership to the process. LMFs should be developed at the level of recognition within the organization. Both the union and management have common interests and needs that will have to be accommodated in creating effective forums.

LMF members should be willing participants who are energized about working together to achieve results that matter to the agency and its employees. Participants should bring a positive attitude and a willingness to engage in honest, open communication that involves speaking freely and listening actively. In most cases, this process takes time and will require commitment and patience on the part of all LMF members.

[9] PDI is an opportunity for a union to influence a management decision on policy impacting the bargaining unit. Even with matters covered by management rights under 5 U.S.C. 7106, management can still engage unions in substantive discussions about the policy and consider the union's input before making any management decision that involves exercising a management right. Management still retains the right to make the decision but should do so with input from the union. However, collective bargaining agreements are still limited to negotiable matters.

Create a Shared Vision for the LMF

All LMFs should be built around a shared vision for the future of the parties' labor-management relationship and a common understanding of how the LMF will help them achieve results for the Agency and its employees. While the initial catalyst for change is the issuance of the EO, acting simply because the approach has been ordered is not enough.

Agency and union leadership must understand the purpose of the LMF and have confidence that it will yield tangible results. Answering the following questions can help the parties develop that common understanding:

- What is the current state of the agency's labor-management relationship?
- How can the LMF help the agency meet its mission?
- How can the LMF harness the great ideas, creativity, technical expertise, and engagement of the workforce?
- How can the parties create mutual commitment to build a relationship that resolves disputes more constructively?

Available Resources and Training

OPM encourages unions and management to collaborate and utilize the expertise of the Federal Mediation and Conciliation Service (FMCS) and the Federal Labor Relations Authority (FLRA) in establishing labor management forums, committees, or for skills training.

The FLRA's Collaboration and Alternative Dispute Resolution Office (CADRO) is available to provide consultation, guidance, and joint-training for management and union representatives who want interactive assistance with their labor-management forum and PDI initiatives. CADRO also can link parties to other appropriate resources if necessary. FLRA's Office of General Counsel can offer training on parties' rights and obligations under the Federal Service-Labor Management Relations Statute and has released video training on many subjects, including training on labor-management forums found here: Video Training | FLRA.

FMCS is a key provider of training, both basic training on labor-management forums (including at conferences and with the FLRA), as well as training based on a needs assessment of specific parties. FMCS's LMF training can be tailored for new labor-management forums, inactive labor-management forums, and those who want a more productive labor-management forum.

FMCS is available to provide training and facilitation for all aspects of the collective bargaining relationship, including:

- Bargaining training (including collaborative bargaining training);
- Relationship development training (including effective contract administration, effective communications, and repairing broken relationships);
- Collective bargaining mediation; and
- Facilitating a bargaining debrief to improve bargaining for the next round of bargaining, as well as the overall labor-management relationship.

Parties may contact FMCS through its Office of Client Services at clientservices@fmcs.gov. Additional information on FMCS resources can be found here:

- LMC-LMF Partnerships - Federal Mediation and Conciliation Service
- FMCS Partnerships Brochure

OPM's Accountability and Workforce Relations office is available to provide policy and technical guidance to parties as they take steps to implement the Executive Order requirements. Parties may send an email to awr@opm.gov.

Appendix C – Guidance for LMF Metrics

Section 6(b)(iii) of the EO directs agencies to evaluate and document, in consultation with union representatives and consistent with any further guidance provided by OPM, changes in employee satisfaction, manager satisfaction, and organizational performance[10] resulting from the LMFs. LMFs can develop metrics to meet these requirements. OPM recommends that metrics be practical and easily understood. If they require a lot of explanation and definition, then turning data into action becomes more difficult. Examples of possible metrics[11] include, but are not limited to:

1. labor-management satisfaction;
2. productivity gains;
3. cost savings; and
4. other areas as identified by the relevant labor-management forum's participants.

Goal and Metrics Development, Data Collection, and Reporting Mechanisms

LMFs should begin by identifying an issue (or issues) to focus on for improvement and for which it will jointly develop actions or steps to be taken to make these improvements.[12] Once identified, the next steps and actions to be taken on each issue should be to identify the metrics to use, monitor the progress for implementing suggested actions, and assess the impact of those actions.

LMFs should report identified issues, goals, and metrics to their agencies and update their agencies on the data collected at least annually thereafter. Agencies should report annually on the metrics they receive from their LMFs to OPM. Within 60 days of receiving approval of their implementation plan, agencies should report to OPM on the measures that will be included in their baselines. Each year, OPM will request agencies provide agency progress against their metrics.

Labor-Management Satisfaction Suggested Metric

The EO aims to promote satisfactory labor relations. The goal of this suggested metric is to chart changes in labor-management relations resulting from the LMF.

[10] Organizational performance includes organizational health.

[11] These categories are suggested metrics which have been used by parties over the years.

[12] To the extent agencies are already working with unions regarding any goals and strategies which support the President's Management Agenda (PMA), LMFs may wish to consider focusing on any metrics identified for the PMA.

Guidelines

It is noted that both purely statistical information as well as anecdotal evidence concerning the state of labor-management relations is relevant in assessing whether relationships have improved. Accordingly, information reported to OPM may include such anecdotal evidence where the LMF participants agree that it is instructive, and the parties elect to use this metric category.

Descriptive Information

This data may be collected at the forum levels where specific labor-management relations issues are identified and resolved. Such resolution can include collective bargaining agreements and should also include general policy determinations that are developed through the collaborative efforts of labor and management at a forum. Accordingly, this data could be collected for each LMF at all levels where LMFs exist within an agency.

Data could be tracked with respect to each issue on which pre-decisional involvement was provided by or through the LMF, only select issues, or any other issues deemed appropriate. For example, the data could include the following:

1. The issue or issues identified, including the significance of the issue -- i.e., costs, number of employees impacted, impact on mission performance or delivery of services.

2. The date the issue is identified.

3. The date the issue is resolved (if at all).

4. If the issue is resolved, describe the nature of the resolution (i.e., collective bargaining agreement, a resolution, or plan.

5. At what level was the issue resolved (i.e., LMF, bargaining teams, before a third party such as an arbitrator, FLRA, EEOC, or MSPB).

6. If the issue was not resolved, provide an explanation of why the issue was not resolved.

7. If the issue was not resolved, describe the way the issue was addressed (i.e., whether through traditional bargaining, or was third-party assistance necessary).

8. Resources associated with addressing issue (i.e., timeline, money, staff).

Subjective Information

This data may also be collected from a survey provided to both union and management representatives. If the parties elect to do a survey, participants should include those with a role in Employee/ Labor Relations, such as supervisors/managers, HR specialists and attorneys who handle labor and employee relations matters for the agency, and union officials/representatives. Ideal measurements could evaluate:

1. Whether pre-decisional involvement has occurred.
2. Whether labor and management have a productive relationship.
3. Whether information is shared and available to both parties.
4. Whether there is organizational support for labor-management relations.
5. Whether bargaining/negotiations are effective.

In formatting survey questions, areas may include the following: (1) general labor-management interactions; (2) nature of dispute resolution -- i.e., the grievance process; (3) negotiations; and (4) general suggestions for improving labor-management relations. Sample questions in each area are included later in this guidance.

Productivity Gains Suggested Metric

The focus of metrics in this suggested category is evaluating and documenting changes in results achieved, specifically whether the forum is contributing to improved mission achievement, service quality, or cost-effectiveness. In many cases, agencies may have already developed metrics for evaluating mission achievement, service quality, or cost-effectiveness through their strategic plans. The LMF may decide to use existing metrics, as appropriate, or may develop new metrics that are more relevant to the issues being addressed.

Varied Missions, Varied Measures

Selections could be made from the following categories:

1. General or Specific Outcomes
2. Process / Cycle time
3. Error Rate / Quality
4. Public Responsiveness / Problem resolution / Customer Satisfaction
5. Internal Resource Management
6. Revenue Collected
7. Agility
8. Other

Definitions and examples of these metrics include, but are not limited to:

1. **General or specific outcomes** – These metrics include broad deliverables to outside stakeholders that employees and management may collaborate to achieve. Labor and management may find it useful to specify a subset of people or businesses that will be the focus of the forum's attention.

2. **Process / Cycle Time** - These metrics gauge progress streamlining or otherwise improving internal processes to achieve better cycle times.

3. **Error Rate / Quality** – Attention to error rates and other aspects of quality when focusing on improving processes and efficiency, ensures that acceptable quality is not sacrificed for speed or cost reductions.

4. **Public Responsiveness / Problem resolution / Customer Satisfaction** – Every Federal government organizational unit deals with individuals and groups of people outside the organization and addressing their needs can be paramount to organizational success. Establishing public responsiveness metrics to gauge whether government is meeting the needs of outside stakeholders is particularly important for dealing with issues where there is direct contact with customers.

5. **Internal Resource Management** – These measures improve internal agency resource management to serve the needs of internal stakeholders and to improve transactions with suppliers or delivery partners.

6. **Revenue Collected** – These metrics are only applicable where participants are involved in collecting revenue but can be important indicators supporting mission success.

7. **Agility** – These metrics are focused on the ability to make decisions and execute plans and strategies requiring short turn-around collaboration, to quickly implement the agreed-to solution. For example:

    - The number of days it takes to decide on a new telework policy.

    - The number of meetings required to change the procedure for approving annual leave.

While the above categories have common attributes across organizations, some metrics may be specific to the mission of an individual organization. LMFs are encouraged to create relevant specific metrics even if they don't fall into any other categories but are reflective of accomplishing the mission of many participants.

Cost Savings Metric

Finding ways to cut costs while keeping outcomes and service quality high is always important. Each LMF is encouraged to quantify costs to find ways to reduce the cost of effective program and mission delivery practices and increase the return on government investment.

Sample Questions for Assessing the Labor-Management Relationship

In formatting survey questions, we recommend exploring areas that include five areas included below. Sample questions in each area have also been provided and are not meant to be an all-inclusive list of questions or areas to cover.

Possible Work Unit Discussions Questions

Work Unit is defined as your immediate work unit headed by an immediate supervisor. These can be questions about workplace issues between union and management, in a work unit.

In my work unit, within the last six months, union representatives and management have met to discuss workplace matters:

- 0 times
- 1-2 times
- 3-4 times
- 5-6 times
- 7 or more times
- I do not know how often meetings have occurred

The subjects discussed during formal meetings are important to my work unit:

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

Agendas are typically sent out in advance for each formal meeting.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

I am comfortable voicing opinions or asking questions during the meetings.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

Possible General Discussions Questions

General: Possible questions about union and management relations, covering several different areas.

Together labor and management address issues relevant to the organization’s business and mission.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

Labor-Management Forums or Committees can positively impact mission accomplishment.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

I have been provided formal training on collaborative labor-management relations.

- Yes (please provide an approximate date)
- No

Management keeps union representatives aware of potential changes to employees' working conditions.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don't Know

Open communication between union representatives and management officials exists in my organization.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don't Know

A sense of fairness is associated with labor-management dealings.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don't Know

Possible Grievance Process Discussions Questions

The Grievance Process: Possible questions about the negotiated grievance process.

In the last year, how many grievances have

- Been filed in your work unit: ___ (number) -or- I don't know
- Reached the last step in the grievance process: ___ (number) -or- I don't know
- Gone to arbitration: ___ (number) -or- I don't know

In general, both parties work cooperatively during the grievance process.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

The grievance process is an efficient way to resolve conflicts.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

Possible Negotiations Discussions Questions

Negotiations: Questions about perceptions regarding negotiations between labor and management.

Management and union representatives regularly engage in “good faith” negotiations.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

The process for negotiating a collective bargaining agreement is effective.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree
- I Don’t Know

Appendix D – Timeframes and Key Actions for Implementation of LMF Requirements

When	Who	What	Reference
Within 180 days of the date of the EO.	Agency, in consultation with union representatives	Prepare and submit a written implementation plan that addresses the requirements in subsection (b) of Section 6 of the EO.	Section 6(c) of the EO.
Within 60 days of receipt of agency implementation plan	OPM	Review each Labor-Management Forum agency implementation plan and determine whether to certify that the plan satisfies all requirements of the EO and any further guidance provided by OPM.	Section 6(c) of the EO.
Within 30 days of OPM notifying an agency that an implementation plan is insufficient (unless OPM authorizes an extension of the deadline)	Agency, in consultation with union representatives	Considering OPM's guidance for improvement, resubmit revised implementation plan.	OPM's guidance issued pursuant to Sections 6(b) and (c) of the EO.

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO