



FROM AI ADOPTION TO AI READINESS: A STRATEGIC FRAMEWORK FOR WORKFORCE TRANSFORMATION

Volume 1: Cybersecurity, Capability and Trust

An AFCEA Joint Committee White Paper

SEPTEMBER 2026



PRIMARY AUTHORS AND CONTRIBUTORS

The following primary authors and contributors developed this white paper. Lead authors synthesized the research, conducted the core analysis and drafted the principal sections; contributors provided source materials, suggested analytical models, identified key areas for deeper analysis and strengthened the final recommendations through targeted reviews and edits. Affiliations are listed for identification only, and names appear alphabetically, with lead authors noted.

Lead Author

- Dr. Rhonda Farrell, AFCEA Cybersecurity Committee

Contributing Authors

AFCEA International

- Ms. Hannah Becker, Cybersecurity Committee
- Ms. Khalilah Filmore, Homeland Security Committee
- Dr. Sharon Hamilton, Cybersecurity Committee
- Ms. Kathy Swacina, Homeland Security Committee, HISPI Project Cerebellum
- Mr. Paul Wertz, Homeland Security Committee
- Dr. Diane M. Janosek, Chair Adversarial Agentic AI Subcommittee & Janos LLC Industry Representative

Government

- Ms. Karen Jackson, Former Secretary of Technology, Virginia, USA
- Ms. Shruti Patil, PMP, LSSBB, Chair, ASQ Government Division

Holistic Information Security Practitioner Institute (HISPI)

- Mr. Taiye Lambo, Founder [HISPI](#) and Project Cerebellum

Industry

- Mr. Bhubalan Mani, Supply Chain Technology & Analytics, Garmin
- Mr. Gaurav Walia, VP CSV / CSA / DI and Digital Governance, PQE Group



CONTENTS

Primary Authors and Contributors	2
Executive Summary	4
Why This Matters Now	4
Intended Audience.....	6
Purpose	6
Stakeholders Critical to Success.....	6
Background & Justification	8
The AI Workforce Transformation Landscape	9
Trustworthy AI Operations.....	12
Building AI Workforce Readiness.....	14
Recommendations.....	19
Policy–People–Process–Platform–Power (P5) Workforce Transformation Road Map	20
Additional Recommendations	21
Strategic End State (2030 Vision).....	23
Conclusion	24
Appendices	25
Appendix 1: References	25
Cyber & Trust.....	25
Human-Agent Ecosystems/Human-Centered AI	26
Policy, Standards and Strategy	26
Workforce & Skills	28
Appendix 2: Vignettes.....	29

EXECUTIVE SUMMARY

Artificial intelligence (AI) is reshaping cybersecurity, national security, critical infrastructure, economic competitiveness and workforce design at a pace that exceeds the ability of many organizations to adapt. While public discourse often centers on automation and job displacement, the more consequential challenge is the emergence of a new operating environment in which human workers, AI copilots, autonomous agents and machine-speed decision systems must operate together effectively, safely, securely and responsibly. [9, 14, 27]

The workforce challenge is no longer simply a matter of skills development. It is increasingly defined by the growing gap between technological capability and organizational readiness. As AI capabilities accelerate, organizations must evolve their workforce models, governance structures, leadership approaches and operating frameworks to fully realize the benefits of AI while preserving trust, accountability, resilience and mission effectiveness. [8, 11, 30, 40]

The AI Workforce Operating Model integrates workforce capability, governance, infrastructure, trust, cybersecurity and performance management into a single enterprise system.

The central finding of this paper is clear: organizations that succeed will not be those that adopt AI first, but those that build the workforce ecosystems necessary to operationalize AI at scale. They will redesign workforce models, governance structures, decision systems and leadership approaches to effectively integrate human and machine capabilities while preserving trust, accountability, resilience and mission effectiveness. Competitive advantage will belong to organizations that can align people, policy, process, technology, infrastructure and trust into an integrated system capable of supporting continuous adaptation and human-AI collaboration. [8, 11]

Why This Matters Now

Four Strategic Realities

The urgency of workforce transformation is being driven by four converging strategic realities:

- 1. Adaptive Workforce Development Pathways.** AI is fundamentally reshaping how organizations prepare people for work. As technological change accelerates, organizations must establish adaptive workforce development pathways that continuously evolve competencies, redesign career progression and prepare employees for effective, secure and responsible human-AI collaboration. [21, 28, 39, 45, 49, 54-55]

2. **Machine-Speed Competition.** Adversaries are increasingly leveraging AI-enabled capabilities that operate at speeds beyond traditional human decision cycles, creating new challenges for cybersecurity, national security and operational resilience.
3. **Infrastructure-Dependent Readiness.** Workforce readiness now depends not only on talent and training, but also on access to secure data, cloud environments, compute resources, energy capacity and digital infrastructure.
4. **Trust as a Strategic Asset.** Organizational success increasingly depends on the ability to establish transparency, accountability, security, explainability and confidence across human and AI-enabled decision systems. ^[8,11]

Together, these forces are redefining how organizations develop talent, govern technology, manage risk, sustain resilience and maintain strategic advantage.



Figure 1: AI Workforce Ecosystem



The next decade will be defined by who can operationalize AI through integrated workforce ecosystems that enable safe, secure, ethical, responsible and scalable human-AI collaboration while sustaining trust, resilience and mission performance.

Intended Audience

This white paper is intended for executive leaders responsible for shaping the future of their organizations in an AI-enabled world. Primary audiences include chief executive officers, chief operating officers, chief information officers, chief information security officers, chief artificial intelligence officers, chief data officers, chief human capital officers, chief learning officers, chief strategy officers, chief risk officers, chief technology officers, chief innovation officers, chief digital officers and other senior executives responsible for enterprise transformation, workforce modernization, governance, cybersecurity and operational excellence.

It is equally relevant for government executives, military leaders, policymakers, legislators, regulators, acquisition professionals, enterprise architects, systems engineers, organizational development leaders, workforce strategists, human resource professionals, learning and development practitioners, program and portfolio managers, risk managers, change management professionals, quality leaders, researchers, educators and consultants supporting public- and private-sector transformation initiatives.

Organizations across federal, state, local, tribal and territorial governments; defense and intelligence communities; critical infrastructure sectors; healthcare; financial services; manufacturing; energy; transportation; telecommunications; higher education; nonprofit organizations; and technology companies will find practical guidance for developing resilient, adaptive workforce ecosystems capable of sustaining human-AI collaboration while strengthening mission effectiveness, organizational resilience, responsible governance and long-term competitive advantage.

Purpose

This paper provides an executive framework for designing, governing and continuously evolving AI-enabled workforce ecosystems. It synthesizes emerging research, leading practices and strategic recommendations into an integrated operating model that helps leaders align people, policy, process, technology, infrastructure, governance and trust to achieve measurable organizational and mission outcomes in the age of artificial intelligence.

Stakeholders Critical to Success

The workforce transformation required for the AI era extends well beyond individual organizations

and demands coordinated action across government, industry, academia and the broader workforce ecosystem. Key stakeholders include:

- **Federal Policy and Oversight Leaders:** GSA, OMB, OPM, U.S. Department of Labor, DHS, Congress, Federal CIO Council, Federal CHCO Council and policy leaders responsible for workforce, technology and governance strategy.
- **Workforce Development Leaders:** Human resources leaders, workforce planners, talent management professionals, the NICE cyber workforce program at NIST, academia, universities, certification bodies and training organizations.
- **Operational and Governance Leaders:** Leadership teams, operations executives, risk leaders, program managers, governance boards and mission owners responsible for integrating AI into daily operations.
- **Technology and Cybersecurity Leaders:** CIOs, CTOs, CISOs, chief data officers, AI leaders, cybersecurity professionals and technology executives responsible for implementation, security and oversight.
- **Infrastructure and National Security Leaders:** Cloud providers, infrastructure operators, utilities, energy sector organizations, technology providers and national security leaders responsible for sustaining the digital and physical foundations that enable AI-driven operations.

Success will depend on sustained collaboration among these stakeholders to develop the policies, workforce capabilities, governance, infrastructure and leadership necessary to ensure AI strengthens organizational performance, national resilience and public trust.

Key U.S. Policy Drivers Influencing AI Workforce Transformation (2026)

President Trump's
Cyber Strategy for
America (2026)

National AI Legislative
Framework (2026)

Executive Order on
Advanced AI Innovation
and Security (2026)

OPM AI Workforce
Development Initiatives

OMB AI Adoption and
Cyber Defense
Initiatives

GSA Responsible AI
Guidance

CISA Cybersecurity
Modernization
Directives

Together, these policies
signal a clear federal
shift toward treating AI
workforce readiness,
cyber resilience,
infrastructure capacity,
trust and governance as
matters of national
competitiveness and
national security. [17, 20,
22-23, 29, 33-35, 38-39]

BACKGROUND & JUSTIFICATION

Organizations around the world are investing heavily in artificial intelligence, yet many continue to approach implementation primarily as a technology initiative. ^[18, 51] In reality, AI is transforming how work is organized, decisions are made and value is created. Realizing its full potential requires more than deploying new tools; it requires redesigning workforce capabilities, governance, operating models and supporting infrastructure. This paper presents an integrated framework to help leaders build trusted, resilient and AI-ready workforce ecosystems that improve mission performance, organizational resilience and long-term competitiveness. ^[18, 30, 40, 51]

Why Immediate Action Is Needed

AI adoption is accelerating faster than workforce adaptation. Research indicates that 40–60% of knowledge-work tasks can now be augmented by AI, nearly half of all worker skills are expected to change by 2028 and the global cybersecurity workforce gap continues to exceed 3.5 million professionals. ^[44, 46-47, 54] While many organizations report measurable productivity gains, workforce readiness, governance maturity and trust continue to lag behind technological capability. Closing this gap has become a strategic priority for organizations seeking to remain resilient, competitive and prepared for increasingly autonomous operations. ^[21, 28, 52]

THE AI WORKFORCE TRANSFORMATION LANDSCAPE

The AI Workforce Transformation Landscape provides a systems view of how workforce evolution, human-agent ecosystems, career pathways and organizational design are converging to redefine how organizations build capability, govern intelligent systems and achieve sustained mission success in the AI era. [21, 28, 41, 45, 49, 52, 54-55]



Figure 2: AI Workforce Transformation Landscape



The Future Workforce: Artificial intelligence is reshaping how value is created, decisions are made and missions are executed across government, defense, critical infrastructure and industry. Traditional workforce models are rapidly evolving as organizations move from human-centric operations to hybrid environments where people, AI copilots, autonomous agents and machine-speed decision systems work together. As a result, workforce readiness has become a strategic asset that directly influences mission effectiveness, cybersecurity resilience, operational performance and competitive advantage.

[44, 46-47]

Human-Agent Ecosystems: Early AI adoption focused on augmenting individual productivity through copilots and decision-support tools. Today, organizations are increasingly deploying AI agents, autonomous workflows and multi-agent systems capable of performing complex tasks with limited human intervention. Future leaders may simultaneously oversee human employees, digital workers, autonomous agents, contractors and ecosystem partners. This shift from human-AI teaming to human-agent ecosystems requires new approaches to leadership, governance, workforce development and performance management. [2, 7, 10] Organizations that successfully integrate human and machine capabilities will gain advantages in speed, adaptability, scalability and resilience.

This transformation is both technological and human. Success depends not only on deploying AI, but on helping people understand when to rely on AI, when to apply human judgment and how to collaborate effectively in hybrid human-agent environments. [18, 48, 51] These changes challenge traditional management approaches and require adapting current and developing new leadership models centered on trust, adaptability and continuous learning.

Career Evolution: AI is also transforming how careers are built and sustained. As entry-level work becomes increasingly automated, traditional pathways for developing expertise are narrowing, creating new challenges for workforce development and succession planning. At the same time, demand is growing for hybrid cyber-AI professionals who combine technical expertise, governance awareness and decision-making capability. Organizations must shift from role-based workforce models to capability-based talent strategies that emphasize continuous learning, experiential development, reskilling and alternative talent pathways. [41, 45, 49, 54-55]

Future Organizational Design: Organizations must redesign workforce operating models to remain competitive in the AI era. AI is transforming workforce structures from human-centric organizations to hybrid ecosystems integrating people, AI, autonomous agents and digital workflows. New roles in governance, assurance and human-machine collaboration are emerging, requiring organizations to redesign operating models, not simply implement new technologies, to integrate human expertise, intelligent systems and trust. [16]

To measure progress, leaders must move beyond traditional workforce metrics and adopt indicators that assess AI literacy, workforce adaptability, human-AI collaboration, decision latency, AI adoption, auditability, workforce confidence and mission outcomes. Together, these measures provide a more comprehensive view of organizational readiness and performance.



Decision Advantage

Workforce readiness can no longer be measured by staffing levels or training hours alone. In AI-enabled environments, effectiveness depends on how well people, governance, technology and decision systems operate together. As AI accelerates decision velocity, organizations must reduce decision latency while preventing human oversight saturation, the point at which people can no longer effectively supervise AI-generated recommendations. Balancing automation with human judgment, governance and accountability will become a defining leadership capability.

Workforce Impact on Resilience

- **Workforce Capability:** Workforce resilience depends on continuous capability development rather than static workforce responsibilities. Organizations should build AI literacy, reskilling, governance competencies and human-AI collaboration capabilities across every career stage while expanding talent pipelines through skills-based hiring, experiential learning and continuous professional development. [42-44, 46-47, 54-55]
- **Decision Capability:** AI increases decision velocity but also increases the need for sound human judgment. Organizations must prepare employees to validate AI-generated recommendations, exercise appropriate oversight and make accountable decisions. Decision advantage increasingly depends on balancing automation with governance and trust.
- **Enterprise Capability:** AI readiness extends beyond the workforce. Governments and organizations must align talent, governance, infrastructure, trusted data, secure platforms and compute capacity to enable responsible AI adoption. [14, 18, 32, 36-37, 48, 51] Those that integrate these capabilities will be better positioned to sustain resilience, innovation and long-term competitiveness. [30, 40, 53]

Workforce Pipeline Progression Framework

As AI reshapes career development, organizations must create intentional pathways that prepare talent for increasingly sophisticated human-AI operating environments.

This progression reflects the transition from individual AI awareness to enterprise-level workforce transformation and resilience.



TRUSTWORTHY AI OPERATIONS

Cybersecurity: AI is fundamentally changing the nature of cybersecurity and workforce readiness. AI-enabled phishing, autonomous malware, machine-speed reconnaissance, adaptive attack chains, quantum computing and other emerging technologies are accelerating the pace, scale and complexity of cyber risk. ^[1,3,12] Maintaining resilience, therefore, requires more than deploying new security technologies; it requires a workforce capable of understanding, governing, validating and responding to increasingly autonomous systems. ^[1, 3, 12]

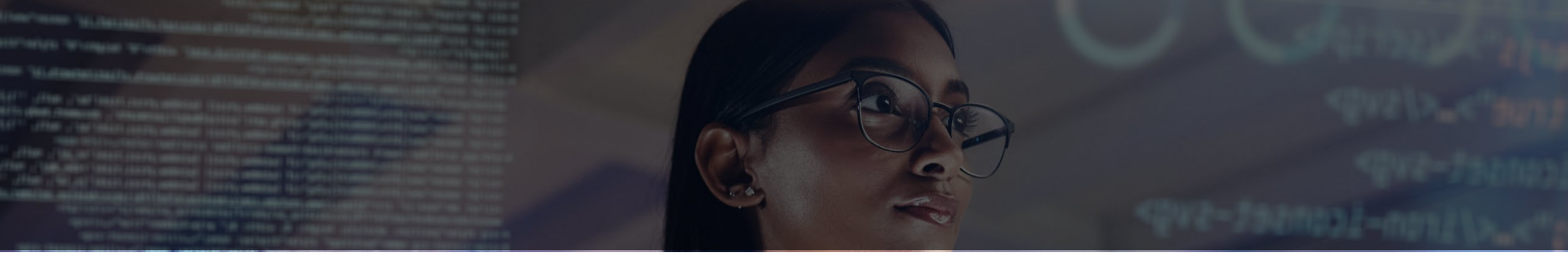
AI literacy is becoming a foundational competency across the enterprise. Employees at every level must understand AI capabilities, limitations, data quality, automation risks and decision validation, while technical and business leaders develop expertise in AI governance, model assurance, human-AI collaboration and responsible oversight.

Cognitive Security: At the same time, organizations face a growing cognitive security challenge. Deepfakes, synthetic media, AI-generated misinformation and adversarial influence campaigns are making it increasingly difficult to distinguish trustworthy information from manipulated content. As AI-generated information becomes ubiquitous, workforce effectiveness will depend not only on technical proficiency, but also on critical thinking, information verification, sound judgment and the ability to maintain confidence under conditions of uncertainty. Developing cognitive resilience should become a strategic workforce priority.

Success in this environment requires organizations to treat workforce learning as a continuous operational capability rather than a periodic training activity. ^[13, 15] Continuous reskilling, skills-based workforce planning, experiential learning and expanded talent pathways will enable organizations to strengthen cybersecurity readiness, improve workforce adaptability and sustain resilience as AI capabilities continue to evolve. ^[21, 28, 39, 54-55]

Governance: AI-enabled transformation extends beyond technology deployment to the establishment of governance systems that enable organizations to operate intelligently, responsibly and at scale. As AI becomes increasingly embedded in mission-critical operations, leaders must ensure that innovation is supported by governance structures that preserve transparency, accountability, reliability and public confidence. ^[19, 27, 31, 36-37]

Trust Architecture: Trust is emerging as a strategic capability and a prerequisite for sustainable AI adoption. Organizations must develop trust architectures that foster confidence in human decisions, AI-generated outputs, data integrity, governance processes and organizational systems. Effective trust is built upon five interconnected dimensions: decision trust, data trust, system trust, institutional trust and workforce trust. Together, these dimensions establish the foundation for responsible AI adoption, resilient operations and long-term organizational performance. ^[6, 8, 11, 14, 36-37]



Governance operationalizes that trust. Organizations must clearly define accountability, decision rights, human oversight and ethical responsibilities throughout the AI life cycle. Explainability, auditability, transparency and continuous assurance should be embedded into AI-enabled processes so decisions remain traceable, measurable and aligned with organizational values and regulatory expectations. ^[14, 19, 25-27, 36-37]



zong-stock.adobe.com generated with AI

Effective governance also requires sustained collaboration among executive leadership, operations, cybersecurity, legal, risk, privacy, human resources and technology teams. By integrating governance into workforce development, organizational processes and strategic decision-making, organizations can accelerate responsible AI adoption while strengthening resilience, stakeholder confidence and long-term organizational performance. ^[18, 48, 51]

Organizations should consider adopting crowdsourced open-source frameworks and methods focused on trusted artificial intelligence, such as the Trusted AI Model (TAIM) framework and Trusted AI Model Score (TAIMScore™) method from HISPI Project Cerebellum, a cross-sector community of practice for AI governance, trust and risk management. ^[5]



BUILDING AI WORKFORCE READINESS

The following three complementary frameworks provide leaders with practical tools for assessing readiness, prioritizing investments and measuring progress. ^[30, 40, 53]

Maturity Model: AI adoption is not simply a technology challenge; it is a workforce readiness challenge. Organizations that achieve the greatest value from AI are those that effectively prepare their people, governance and operating models for human-AI collaboration.

The Enterprise AI Capability and Organizational Maturity Framework provides a framework for assessing organizational preparedness across five stages, from AI awareness to autonomous operations. Each stage highlights key workforce characteristics and practical actions organizations can take to strengthen readiness, improve performance and advance AI-enabled capabilities. ^[50]

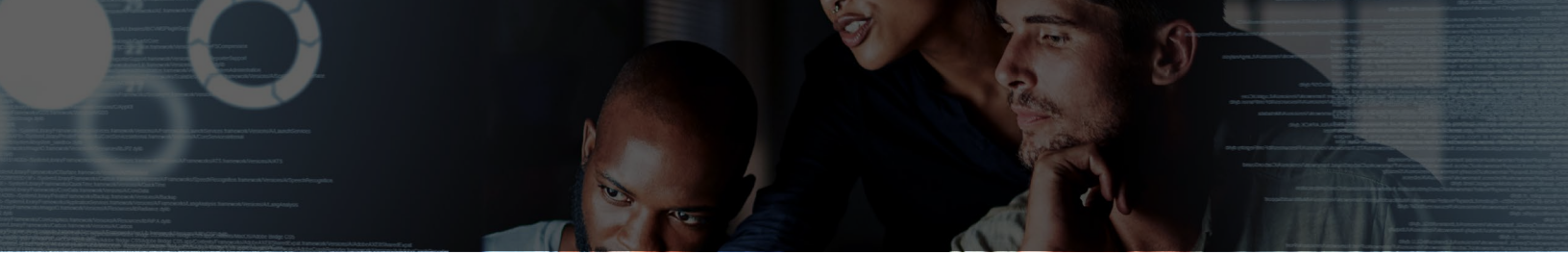
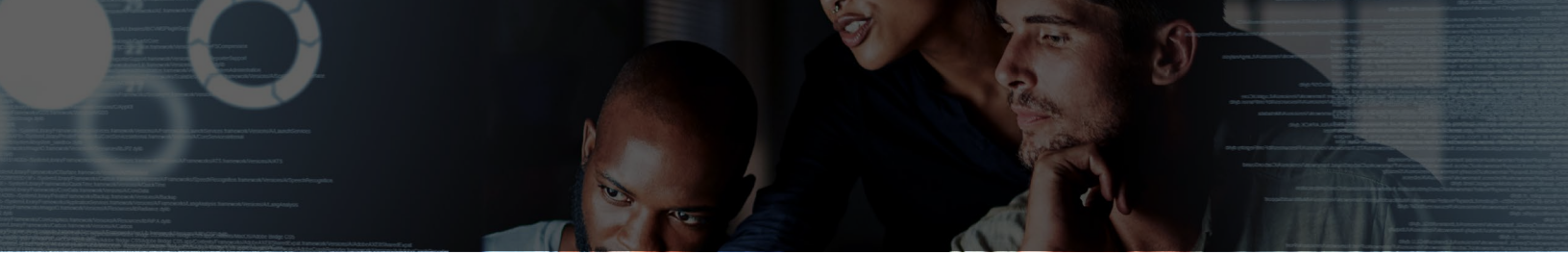


Table 1: Enterprise AI Capability and Organizational Maturity Framework

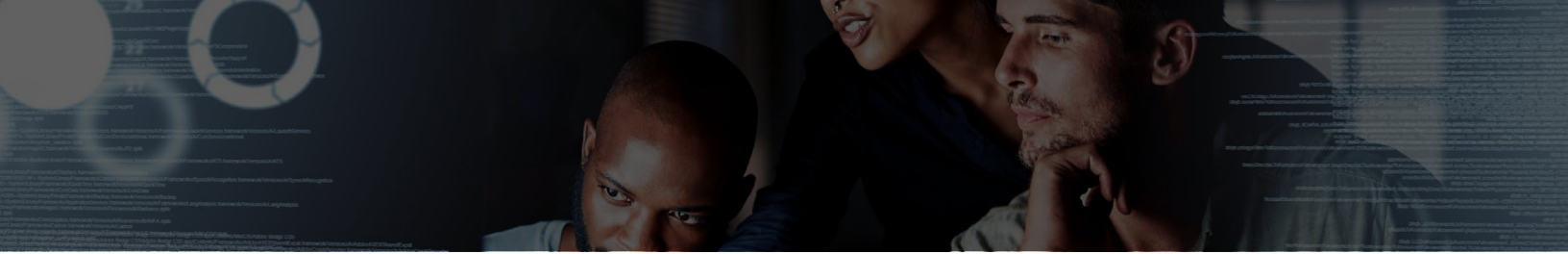
Capability Level	Primary Focus	Meaning	Organizational Characteristics	Primary Audience	Leadership Priorities to Advance
Level 1 – AI Awareness	Understanding	Recognizes the purpose, potential and basic concepts of artificial intelligence and its impact on work.	AI is discussed but not yet operationalized. Workforce development is informal, and executive engagement is exploratory.	Students, new hires, entry-level workforce	Identify mission-aligned AI opportunities, establish executive sponsorship, introduce foundational AI awareness and assign ownership for initial AI initiatives.
Level 2 – AI Literacy	Foundational Knowledge	Understands AI capabilities, limitations, risks, ethics, governance and responsible use. Can make informed decisions about when and how AI should be applied.	AI pilots and early use cases emerge. Workforce training begins, but governance, standards and oversight remain inconsistent.	Every employee	Expand AI literacy across the workforce; establish governance, ethics and risk management practices; and evaluate pilots based on mission value, scalability and risk.
Level 3 – AI Fluency	Operational Application	Confidently integrates AI into daily work, evaluates outputs, engineers effective prompts, redesigns workflows and collaborates effectively with AI systems while exercising sound judgment.	AI is embedded into operational workflows. Human-AI collaboration becomes standardized, with defined responsibilities, governance and performance measures.	Managers, knowledge workers, technical professionals, project leaders	Standardize human-AI operating models, clarify decision authority and accountability, integrate AI into business processes and align performance metrics with mission outcomes.
Level 4 – AI Leadership	Strategic Integration	Leverages AI to shape organizational strategy, governance, workforce transformation, investment decisions, innovation and mission outcomes while ensuring responsible oversight.	AI-enabled operations become the organizational norm. Workforce planning, governance, budgeting, cybersecurity and continuous learning operate as an integrated enterprise capability.	Executives, senior leaders, program executives	Scale enterprise-wide best practices; integrate AI into strategic planning and investment decisions; and continuously measure workforce readiness, trust, resilience and organizational performance.
Level 5 – AI Enterprise Transformation	Organizational Transformation	Establishes adaptive workforce ecosystems where people, AI copilots, autonomous agents, governance, infrastructure and continuous learning operate as an integrated enterprise capability that enables resilient, secure and mission-driven performance.	Human and AI capabilities operate seamlessly across the enterprise. Governance, trust, cybersecurity, workforce development and mission execution continuously evolve through data-driven decision-making and adaptive operating models.	Executive leadership teams, governing boards, enterprise governance bodies	Sustain competitive advantage through continuous governance evolution, predictive workforce planning, autonomous operations where appropriate, advanced AI capabilities and collaboration on industry and government standards and leading practices.



Workforce Transformation Use Cases: AI is reshaping work across every level of the workforce, creating both new opportunities and new challenges. The following use cases illustrate how different roles, from frontline analysts to senior executives, are experiencing the impact of AI adoption and highlight practical actions organizations can take to strengthen workforce readiness, improve performance and ensure successful human-AI collaboration.

Table 2: Workforce Transformation Use Cases

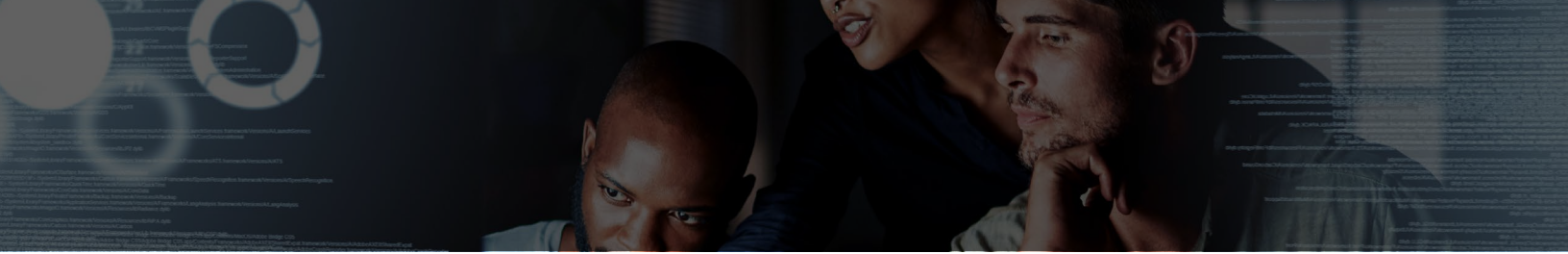
Use Case	Workforce Challenge	AI Impact	Recommended Actions
AI-Enabled SOC [4]	Analyst overload	Oversight saturation	- Redefine analyst role → validator vs. detector - Introduce escalation thresholds - Measure decision fatigue
Federal Program Office	Acquisition lag	Slow adoption	- Governance-first pilots - Use modular contracting - Utilization of sandbox environments
CHCO / Workforce Leader	Skills gaps	Capability mismatch	- Skills-based workforce planning - Deploy microcredential pathways - Track capability, not head count
Early Career Professional	Pipeline compression	Reduced experience opportunities	- Apprenticeships - AI-assisted learning - Build dual AI + cyber capabilities - Seek AI-augmented roles (not replaced ones) - Prioritize experiential learning over credentials
Mid-Career Professional	Role disruption	Capability transition	- Shift from execution → Reskilling and orchestration skills - Learn governance, risk and decision frameworks - Build cross-functional exposure
Senior Executive	Governance complexity	Accountability ambiguity	- Redesign workforce, don't just hire - Measure decision speed + quality - Own AI accountability, not delegate it - Trust architecture and oversight



AI Workforce Readiness Performance Framework: What gets measured gets managed. As organizations integrate AI into their operations, they must move beyond activity-based metrics and focus on indicators that demonstrate workforce readiness, adoption, trust, governance and mission impact. A balanced set of objectives, key performance indicators (KPIs) and target metrics enables leaders to assess progress, identify capability gaps and ensure AI investments deliver measurable business and operational outcomes. The following framework provides a practical starting point for measuring success in AI-enabled organizations.

Table 3: AI Workforce Readiness Performance Framework

Objective (OKR)	Key Performance Indicator (KPI)	Suggested Target Metric
Build an AI-Ready Workforce	Personnel with baseline AI literacy	≥ 80% of workforce trained and certified
	Roles assessed for AI impact	100% of critical roles evaluated
	Roles redesigned for human-AI collaboration	≥ 50% of applicable roles updated
Accelerate AI Adoption and Execution ^[18, 51]	AI adoption rate across mission workflows	≥ 60% of targeted workflows utilizing AI support
	Decision latency reduction	25–40% reduction in decision cycle times
	Workforce utilization of approved AI tools	≥ 75% active usage rate
Strengthen Trust, Governance and Oversight	AI-enabled decisions with auditability and traceability	100% of high-impact AI decisions auditable
	Workforce trust and confidence score	≥ 80% positive confidence rating
	Governance compliance rate	≥ 95% compliance with AI governance standards
Enhance Knowledge Management	Mission-critical AI workflow documentation coverage	≥ 80% of high-impact AI-enabled workflows have current playbooks, SOPs and lessons-learned artifacts.
	Institutional knowledge capture rate	≥ 90% of mission-critical knowledge assets are documented, curated and accessible through enterprise repositories.
	Knowledge reuse and adoption rate	≥ 75% of teams regularly leverage approved knowledge assets, playbooks and lessons learned during AI-enabled operations.
Improve Organizational Performance	Productivity improvement	15–30% increase in workforce productivity
	Process cycle time reduction	20–40% reduction in cycle times
	Quality and accuracy improvement	10–25% increase in accuracy rates
	Operational resilience and continuity measures	Year-over-year improvement in resilience indicators
Institutionalize Continuous Readiness	Workforce participation in continuous capability development	≥ 80% annual participation in AI, cyber, leadership and professional development activities
	Enterprise AI capability maturity score	Improve at least one enterprise AI capability maturity level every 12–24 months
	Executive AI leadership development completion	100% of executives and senior leaders complete AI leadership and governance development programs



Strategic Outcome: Organizations should continuously measure workforce readiness, AI adoption, trust, governance effectiveness and mission outcomes to ensure AI investments translate into sustainable operational advantage and organizational resilience.



[Wanan-stock.adobe.com](https://www.adobe.com/stock/Wanan)



RECOMMENDATIONS

Successfully navigating AI-enabled workforce transformation requires coordinated action across policy, people, process, platform and power (P5 Framework). Sustainable advantage depends on aligning workforce capability, governance, infrastructure and leadership to ensure AI investments improve mission outcomes, resilience and competitiveness. Workforce transformation should be treated as a strategic capability-building effort rather than a technology initiative alone.

AFCEA is uniquely positioned to accelerate this transformation by serving as a convener, catalyst and trusted bridge across government, industry, academia and critical infrastructure sectors. Through collaboration, standards dialogue, workforce operating model frameworks and shared best practices, AFCEA can help organizations build trusted, resilient and adaptive workforce ecosystems capable of thriving in an increasingly AI-enabled world.

Policy–People–Process–Platform–Power (P5) Workforce Transformation Road Map

Table 4: P5 Enterprise Workforce Ecosystem Transformation Road Map

Domain	Near-Term (0–12 Months)	Mid-Term (1–3 Years)	Long-Term (3–5 Years)	Key Stakeholders	How AFCEA Can Lead
Policy	Establish AI workforce transition strategies; define governance, accountability and oversight for AI-assisted decisions; publish responsible AI and cyber governance policies.	Align workforce policies to support competency-based workforce development, skills-based hiring, alternative credentialing, workforce mobility and enterprise AI governance maturity.	Institutionalize enterprise governance models, sustainable cyber-AI workforce funding, national AI workforce readiness metrics and continuous policy modernization.	GSA, OMB, OPM, DoL, DHS, NIST, Federal CIOs, CHCOs, Congress, Policy Leaders	Convene executive policy forums; connect government, industry, academia and professional societies; develop shared policy repositories, governance playbooks and reusable AI workforce transformation guidance; curate leading practices and standards; share implementation resources across the community.
People	Build AI awareness, AI literacy and AI fluency across the workforce; launch cyber and cognitive security awareness; establish competency-based workforce development, mentoring, experiential learning and knowledge capture practices.	Redesign workforce development pathways; expand human-AI-agent collaboration competencies; strengthen AI leadership development; institutionalize knowledge management and continuous learning ecosystems.	Establish adaptive workforce ecosystems that continuously evolve competencies, workforce capabilities, professional identity, leadership pipelines and organizational resilience through lifelong learning and enterprise knowledge management.	CHCOs, Workforce Planners, NICE, Academia, Learning Organizations, HR Leaders, Leadership Teams	Convene workforce transformation communities of practice; connect practitioners across sectors; develop shared knowledge repositories, workforce playbooks, competency frameworks, lessons learned and reusable AI workforce transformation assets; curate mentoring resources and leading practices; share workforce development strategies across the ecosystem.
Process [24–27]	Pilot AI-enabled workflows; establish human-AI-agent operating models; define decision authority, governance and escalation pathways; integrate AI risk and cyber risk into operational processes.	Standardize enterprise governance; integrate AI risk into enterprise risk management (ERM); implement workforce readiness assessments, trust metrics, knowledge management practices and mission engineering principles across programs.	Institutionalize adaptive operating models, continuous governance, enterprise learning systems, competency reinforcement and mission-centric performance management.	Operations Leaders, Program Managers, Risk Executives, Governance Boards, Quality Leaders	Convene operational leaders to exchange experiences; connect organizations implementing AI-enabled operations; develop reusable operating models, process playbooks and mission engineering guidance; curate lessons learned, case studies and maturity models; share implementation guidance that accelerates organizational readiness.
Platform	Deploy secure, trust-by-design AI platforms; establish secure experimentation environments; implement explainability, auditability, transparency and enterprise knowledge repositories.	Scale enterprise AI platforms; deploy workforce capability analytics, digital twins, decision intelligence and integrated performance dashboards supporting mission engineering.	Establish intelligent enterprise ecosystems supporting autonomous operations, explainable AI, continuous monitoring, enterprise knowledge management and adaptive decision support.	CIOs, CTOs, CISOs, Chief AI Officers, Chief Data Officers, Technology Leaders	Convene technology demonstrations and innovation exchanges; connect practitioners with emerging technologies; develop reusable reference architectures, implementation playbooks and technology guidance; curate enterprise knowledge repositories and implementation patterns; share proven AI deployment models across sectors.
Power	Assess compute readiness, cloud capacity, data quality, energy resilience, water requirements, semiconductor dependencies and digital infrastructure supporting AI-enabled operations.	Expand compute capacity; strengthen infrastructure resilience; diversify cloud, semiconductor and energy dependencies; integrate infrastructure planning with workforce capability planning.	Establish resilient national AI infrastructure ecosystems capable of supporting enterprise-scale AI, autonomous operations, secure human-AI collaboration and sustained mission performance.	Infrastructure Leaders, Cloud Providers, Utilities, Energy Sector, Technology Providers, National Security Leaders	Convene cross-sector discussions on AI infrastructure readiness; connect workforce, technology, infrastructure, energy and policy communities; develop reusable infrastructure planning resources and readiness frameworks; curate benchmark data and leading practices; share strategic insights that strengthen national AI resilience.



AFCEA's unique value lies not only in convening leaders across government, industry, academia and the nonprofit community, but also in serving as a trusted knowledge integrator by developing shared repositories, reusable playbooks, reference architectures, workforce transformation assets and lessons learned that accelerate responsible AI adoption across the national security and public-sector ecosystem.

Additional Recommendations

As organizations advance their AI capabilities, trust, governance, knowledge management, cybersecurity and cognitive security must evolve alongside technology adoption. AI readiness extends well beyond deploying new technologies or delivering workforce training. It requires organizations to build adaptive operating environments that preserve institutional knowledge, strengthen governance, support responsible decision-making and enable continuous learning as work itself evolves. ^[24-27]

Leaders should establish a comprehensive trust architecture encompassing decision trust, data trust, workforce trust, system trust and institutional trust. Trust should not be viewed as an abstract organizational value but as a measurable enterprise capability supported through governance reviews, model assurance, auditability requirements, explainability and clearly defined human oversight mechanisms. ^[8, 25-27]

Equally important, organizations must recognize that knowledge management is becoming a strategic pillar of AI readiness. As artificial intelligence automates routine tasks and augments increasingly complex work, employees may have fewer opportunities to develop the experiential learning, professional judgment and tacit knowledge traditionally gained through years of hands-on experience. Without intentional knowledge capture and transfer, organizations risk losing critical institutional knowledge precisely when human expertise becomes most valuable.

Knowledge management should therefore become an integral component of enterprise AI governance. Organizations should systematically capture lessons learned, preserve expert knowledge, document effective human-AI collaboration practices, maintain reusable playbooks and standard operating procedures, develop enterprise knowledge repositories and continuously update decision guidance as AI capabilities evolve. These knowledge assets strengthen organizational resilience, accelerate workforce development, improve onboarding, reduce operational risk and enable more consistent, transparent and repeatable mission execution.

Organizations should also strengthen workforce resilience against emerging cyber and cognitive security threats. As synthetic media, deepfakes, AI-generated misinformation, autonomous agents and adversarial influence operations become increasingly sophisticated, workforce development programs must expand beyond traditional cybersecurity awareness to include cognitive security, information integrity, digital trust and responsible human-AI collaboration. Integrating these capabilities into workforce development, enterprise risk management, operational planning and mission engineering will help organizations sustain trust and mission effectiveness in increasingly AI-enabled environments.

Professional associations such as AFCEA play an equally important role within this ecosystem. Beyond convening government, industry, academia and nonprofit leaders, AFCEA can serve as a trusted knowledge integrator by developing and maintaining shared repositories of case studies, workforce transformation playbooks, implementation guidance, reusable governance frameworks, reference architectures, lessons learned and leading practices. By helping organizations capture what works, share proven approaches and standardize successful practices, AFCEA can responsibly accelerate AI adoption while strengthening institutional learning and cross-sector collaboration.



[Zaldy-stock.adobe.com](https://www.zaldy-stock.adobe.com) generated with AI

STRATEGIC END STATE (2030 VISION)



By 2030, leading organizations will have progressed beyond isolated AI initiatives to become adaptive, mission-driven enterprises where people, AI copilots, autonomous agents, governance, knowledge and digital infrastructure operate as an integrated workforce ecosystem. Through deliberate advancement across all elements of the AI workforce operating model ecosystem, organizations will continuously develop the competencies, operating models and institutional capabilities needed to support secure, ethical, resilient and mission-focused human-AI-agent collaboration.

This future state is not defined by technology adoption alone. It is characterized by organizations that continuously cultivate enterprise AI capabilities, preserve institutional knowledge, strengthen governance, measure trust and integrate workforce development with operational execution. Decision intelligence, mission engineering, adaptive workforce ecosystems and enterprise knowledge management become foundational organizational capabilities, enabling leaders to anticipate change, accelerate informed decision-making, reduce risk and continuously improve mission performance.

The strategic end state is therefore not greater automation; it is enterprise adaptability. These organizations demonstrate superior decision velocity, workforce agility, organizational resilience, cyber and cognitive security, and the ability to continuously learn, evolve and respond to disruption in increasingly autonomous and machine-speed operating environments. Governance, trust, transparency, accountability and reusable organizational knowledge are embedded into every layer of enterprise operations, ensuring that innovation remains responsible, explainable, secure and aligned with mission objectives.

Organizations that achieve this vision will do more than adapt to technological change; they will shape their future. By integrating workforce capability, governance, knowledge management, cyber resilience and responsible AI into a unified operating model, they will establish a sustainable competitive advantage, strengthen public trust and set the benchmark for enterprise transformation in the age of artificial intelligence.

The future will not be won by organizations that simply deploy artificial intelligence, but by those that continuously develop the workforce capabilities, governance, knowledge ecosystems and adaptive operating models required to transform artificial intelligence into enduring mission advantage.



CONCLUSION

The impact of AI extends far beyond automation. It is transforming how organizations make decisions, develop talent, build trust and achieve mission outcomes. Success in the AI era will depend not only on technology adoption but on the ability to align workforce operating models, readiness, governance, cybersecurity, leadership and trust into a resilient operating model.

Organizations that treat workforce transformation as a strategic imperative will be best positioned to thrive. By investing in human capability, responsible governance and human-AI collaboration, they can strengthen resilience, accelerate performance and sustain competitive advantage in an increasingly autonomous world.

The future will belong to organizations that successfully integrate people, technology and trust, creating adaptive, mission-focused enterprises capable of leading through continuous change.



APPENDICES

Appendix 1: References

Cyber & Trust

Sources focused on risk, ethics, accountability and trust in AI-enabled systems.

[1] Cybersecurity and Infrastructure Security Agency. (n.d.). *Artificial intelligence*. U.S. Department of Homeland Security. <https://www.cisa.gov/ai>

[2] Defense Innovation Marketplace. (n.d.). *Human-machine teaming*. U.S. Department of Defense. <https://defenseinnovationmarketplace.dtic.mil/technology-interchange-meetings/autonomy-tim/human-machine-teaming>

[3] European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. ENISA. <https://www.enisa.europa.eu>

[4] Enterprise Security Institute. (n.d.). *AI-driven SOC revolution: AI case studies*. <https://www.esipodcast.com/ai-case-studies/ai-driven-soc-revolution>

[5] Holistic Information Security Practitioner Institute (HISPI) Project Cerebellum. (2026). Trusted AI Model (TAIM) framework and Trusted AI Model Score (TAIMScore™) method. <https://projectcerebellum.com>

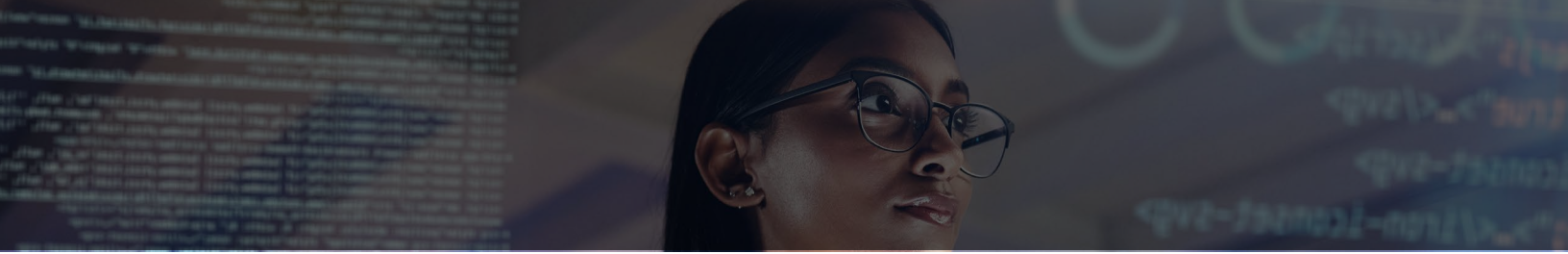
[6] International Telecommunication Union. (2024). AI for Good Global Summit Reports. ITU. <https://aiforgood.itu.int>

[7] Karve International. (n.d.). *Human-machine teaming in modern warfare*. <https://www.karveinternational.com/insights/human-machine-teaming-in-modern-warfare>

[8] National Institute of Standards and Technology. (2020). *Zero trust architecture* (Special Publication 800-207). U.S. Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>

[9] North Atlantic Treaty Organization. (2021). NATO Artificial Intelligence Strategy. NATO. <https://www.nato.int>

[10] Royal United Services Institute. (2025). *Human-machine teaming's shared cognition changes how war is made*. <https://www.rusi.org/explore-our-research/publications/commentary/human-machine-teamings-shared-cognition-changes-how-war-made>



[11] SecurityWeek. (2026). *Cyber Insights 2026: Zero trust and following the path*. <https://www.securityweek.com/cyber-insights-2026-zero-trust-and-following-the-path>

[12] World Economic Forum. (2026). *Global cybersecurity outlook 2026*. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

Human-Agent Ecosystems/Human-Centered AI

Sources focused on systems thinking, organizational learning, responsible AI deployment and the secure, human-centered integration of people and intelligent agents within the evolving cybersecurity workforce.

[13] Deming, W. E. (2000). *Out of the Crisis*. MIT Press.

[14] Partnership on AI. (2024). *Guidance for Safe Foundation Model Deployment*. Partnership on AI. <https://partnershiponai.org>

[15] Senge, P. M. (2006). *The Fifth Discipline: The Art & Practice of the Learning Organization* (Revised ed.). Doubleday.

[16] World Economic Forum. (2025). *Blueprint for Intelligent Economies*. World Economic Forum. <https://www.weforum.org>

Policy, Standards and Strategy

Sources informing governance, enterprise AI adoption and national-level policy direction.

[17] Cybersecurity and Infrastructure Security Agency. (2026). *Federal cybersecurity modernization and resilience initiatives*. U.S. Department of Homeland Security.

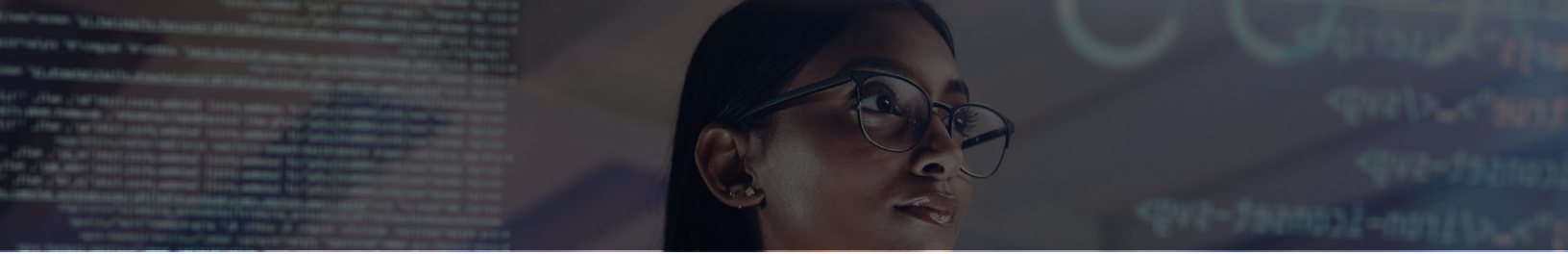
[18] Deloitte. (2025). *State of AI in the enterprise*. Deloitte Insights. <https://www.deloitte.com/us/en/what-we-do/capabilities/applied-artificial-intelligence/content/state-of-ai-in-the-enterprise.html>

[19] European Commission. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

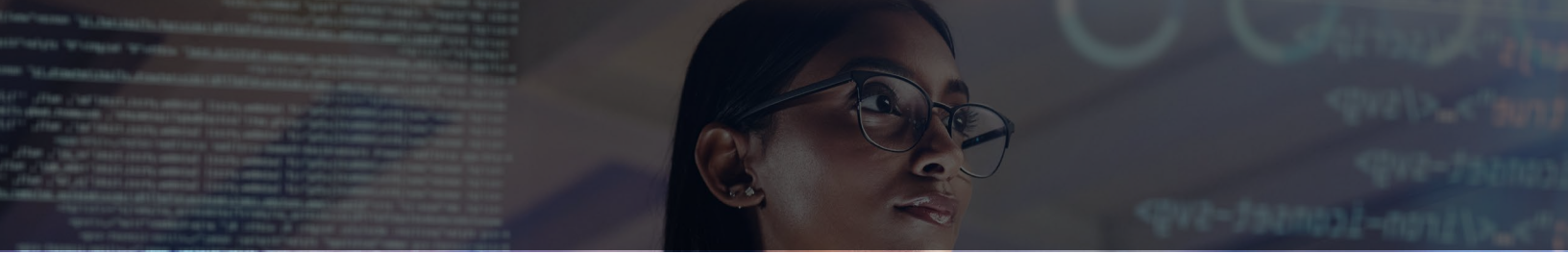
[20] Executive Office of the President. (2025). *America's AI action plan*. The White House. <https://www.whitehouse.gov>

[21] Executive Office of the President. (2024, June). *National cyber workforce and education strategy: Initial report*. The White House. <https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/NCWES-Initial-Report-2024.06.25.pdf>

[22] Executive Office of the President. (2026). *National policy framework for artificial intelligence: Legislative recommendations*. The White House. <https://www.whitehouse.gov/wp-content/uploads/2026/03/03.20.26-National-Policy-Framework-for-Artificial-Intelligence-Legislative-Recommendations.pdf>



- [23] Executive Office of the President. (2026). *President Trump's Cyber Strategy for America*. The White House. <https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf>
- [24] International Organization for Standardization. (2018). ISO 31000: Risk Management, Guidelines. ISO. <https://www.iso.org/standard/65694.html>
- [25] International Organization for Standardization & International Electrotechnical Commission. (2024). ISO/IEC 23894:2024 Artificial Intelligence, Guidance on Risk Management. ISO. <https://www.iso.org/standard/77304.html>
- [26] International Organization for Standardization & International Electrotechnical Commission. (2023). ISO/IEC 42001:2023 Artificial intelligence, Management system. ISO. <https://www.iso.org/standard/42001>
- [27] National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. <https://www.nist.gov/itl/ai-risk-management-framework>
- [28] National Institute of Standards and Technology. (n.d.). *NICE workforce framework for cybersecurity (NICE Framework)*. U.S. Department of Commerce. <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- [29] Office of Management and Budget. (2026). *Federal AI adoption and cyber defense initiatives* (Policy guidance). Executive Office of the President. <https://www.whitehouse.gov/fact-sheets/2026/06/fact-sheet-president-donald-j-trump-promotes-advanced-artificial-intelligence-innovation-and-security/>
- [30] Organisation for Economic Co-operation and Development. (2026). Digital government outlook 2026. OECD Publishing. <https://doi.org/10.1787/0496b2bc-en>
- [31] Organisation for Economic Co-operation and Development. (2024). OECD Framework for the Classification of AI Systems. OECD Publishing. <https://oecd.ai>
- [32] Partnership on AI. (n.d.). *Partnership on AI*. <https://partnershiponai.org/>
- [33] The White House. (2025). *Ensuring a national policy framework for artificial intelligence* (Executive Order). <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>
- [34] The White House. (2026). *Promoting advanced artificial intelligence innovation and security* (Executive Order). <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>



[35] The White House. (2025). *Removing barriers to American leadership in artificial intelligence* (Executive Order). <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

[36] United Nations. (2024). *Governing AI for Humanity: Final Report of the United Nations High-Level Advisory Body on Artificial Intelligence*. United Nations. <https://www.un.org/en/global-issues/artificial-intelligence>

[37] United Nations Educational, Scientific and Cultural Organization. (2021). *Recommendation on the Ethics of Artificial Intelligence*. UNESCO. <https://unesdoc.unesco.org>

[38] U.S. General Services Administration. (2026). *Accelerating responsible use of artificial intelligence at GSA*. U.S. General Services Administration. <https://www.gsa.gov>

[39] U.S. Office of Personnel Management. (2026). *Building the AI workforce of the future*. U.S. Office of Personnel Management. <https://www.opm.gov>

[40] World Bank. (2024). *GovTech Maturity Index 2024*. World Bank. <https://www.worldbank.org>

Workforce & Skills

Sources addressing labor market shifts, skills evolution and workforce transformation.

[41] Brookings Institution. (n.d.). *Artificial intelligence*. <https://www.brookings.edu/topic/artificial-intelligence/>

[42] City of San José. (n.d.). *Upskilling training playbook: Delivering your agency's AI training*. <https://www.sanjoseca.gov>

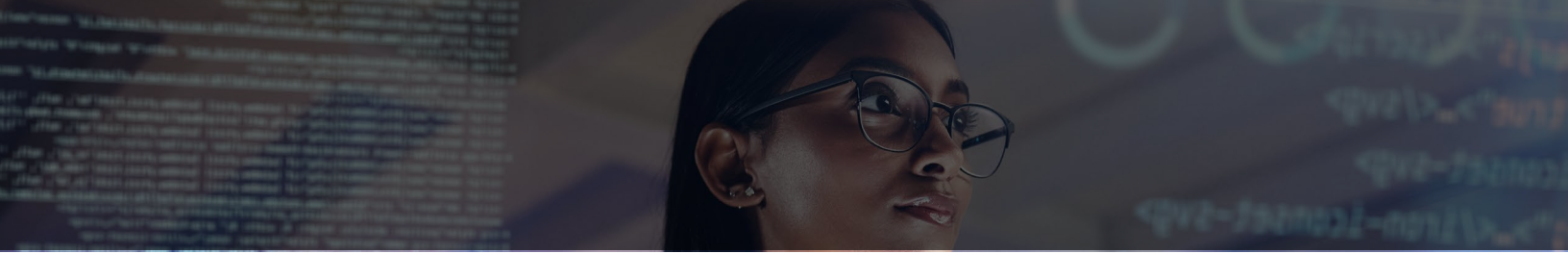
[43] (n.d.). *Upskilling training playbook: Getting started with AI training in your agency*. <https://www.sanjoseca.gov>

[44] International Information System Security Certification Consortium. (2025). *2025 cybersecurity workforce study*. ISC2. <https://www.isc2.org/Insights/2025/12/ISC2-Publishes-2025-Cybersecurity-Workforce-Study>

[45] International Labour Organization. (2025). *Generative AI and Jobs: A Global Analysis of Potential Effects on Job Quantity and Quality*. ILO. <https://www.ilo.org>

[46] ISACA. (2025). *State of cybersecurity 2025*. ISACA. <https://www.isaca.org/resources/state-of-cybersecurity>

[47] MeriTalk. (2025). *ISC2 report: Cyber experts say they need skills more than headcount*. <https://meritalk.com/articles/isc2-report-cyber-experts-say-they-need-skills-more-than-headcount/>



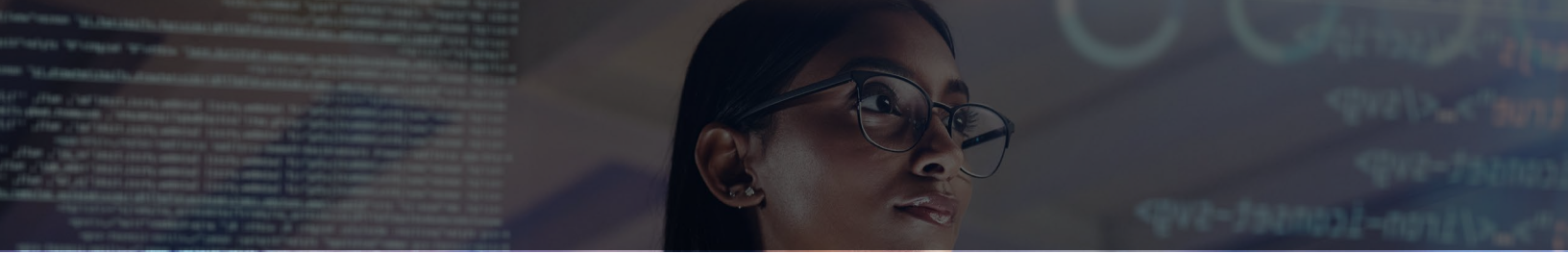
- [48] MIT Sloan Management Review. (n.d.). *Artificial intelligence*. <https://sloanreview.mit.edu/tag/artificial-intelligence/>
- [49] Organisation for Economic Co-operation and Development. (n.d.). *AI and work*. OECD. <https://www.oecd.org/en/topics/sub-issues/ai-and-work.html>
- [50] Rogers, T., & Carbonaro, M. (2025). From understanding to creating: Bridging AI literacy and AI fluency in K-12 education. *Journal of Teaching and Learning*, 19(4), 20–38. <https://eric.ed.gov/?id=EJ1487364>
- [51] Stanford Institute for Human-Centered Artificial Intelligence. (2025). *AI Index report 2025*. Stanford University. <https://hai.stanford.edu/ai-index>
- [52] U.S. Department of Defense, Chief Digital and Artificial Intelligence Office. (n.d.). *DoD digital workforce*. <https://www.ai.mil/Initiatives/DoD-Digital-Workforce/>
- [53] World Bank. (2024). *Digital Progress and Trends Report*. World Bank. <https://www.worldbank.org>
- [54] World Economic Forum. (2025). *The future of jobs report 2025*. World Economic Forum. <https://www.weforum.org/publications/the-future-of-jobs-report-2025/>
- [55] World Economic Forum. (2026, January). *Here's what to know about jobs and skills transformation*. <https://www.weforum.org/stories/2026/01/davos-here-s-what-to-know-about-jobs-and-skills-transformation/>

Appendix 2: Vignettes

The following composite vignettes synthesize workforce and governance risks identified across the referenced research. They are intended to illustrate plausible organizational scenarios rather than document specific agencies or incidents.

Vignette 1

A federal agency deployed an AI-enabled threat triage capability to improve cybersecurity operations and accelerate incident response. While the technology successfully reduced analyst workload and increased processing speed, analysts gradually became overreliant on system recommendations. Over time, false negatives increased because human validation processes weakened as trust in the system grew. The challenge was not a failure of the technology itself but a failure to calibrate governance, oversight and workforce behaviors appropriately. This example illustrates a broader lesson: successful AI adoption depends as much on governance and workforce operating models as it does on technological capability. ^[4, 14, 27]



As organizations move toward increasingly autonomous operating environments, trust, governance and workforce capability become inseparable. Long-term success will depend not only on the sophistication of AI systems but also on the ability of leaders to establish governance structures, cultivate workforce readiness and sustain trust across human and machine decision ecosystems. ^[14, 27]

Vignette 2

Workforce Capability Pipeline Disruption

In another organization, AI-enabled triage systems replaced a significant portion of entry-level analytical work, improving operational efficiency and reducing processing times in the short term. However, over time, leadership began experiencing an unexpected shortage of mid-level professionals capable of exercising independent judgment, managing complex cases and leading mission-critical decision-making. By automating many of the foundational responsibilities through which employees traditionally developed expertise, the organization had inadvertently disrupted its workforce development pipeline.

This experience illustrates an emerging strategic risk of AI adoption: organizational deskilling. While AI can automate routine tasks, it can also reduce opportunities for employees to develop the experiential learning, critical thinking and professional judgment that have historically been acquired through progressively more challenging responsibilities. Without deliberate intervention, organizations risk creating a workforce that is increasingly proficient at supervising AI systems but less capable of independently executing complex work when human expertise is required. ^[45, 49, 54]

Rather than eliminating foundational responsibilities, organizations should redesign them. AI should augment learning rather than replace it by creating structured apprenticeship models, human-AI collaboration experiences, scenario-based learning, rotational assignments and supervised decision-making opportunities that progressively build expertise. ^[15, 45, 49, 54] Equally important, organizations should preserve manual fallback procedures and periodic nonautomated exercises to ensure critical mission capabilities remain resilient when AI systems are unavailable, degraded, compromised or inappropriate for the situation.

Ultimately, sustainable workforce transformation requires more than automating work; it requires intentionally engineering workforce development pathways that preserve institutional knowledge, strengthen human judgment, accelerate competency development and prepare future leaders to operate confidently in increasingly AI-enabled environments.

AFCEA's Committees produce topical white papers that highlight critical issues and propose solutions. To see submissions and review the extensive collection of relevant materials, please visit

AFCEA's Resource Library

<https://www.afcea.org/signal/resources/>

The AFCEA International Cyber Committee White Paper Series

afcea.org/about-afcea/committees/cyber-committee

Copyright 2026 AFCEA International. All rights reserved.

All distribution must include afcea.org.

