SYM-AM-24-117

Excerpt from the Proceedings

of the

Twenty-First Annual Acquisition Research Symposium

Acquisition Research:
Creating Synergy for Informed Change

May 8–9, 2024

Published: April 30, 2024

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Unlock the Hidden Secrets of AI Transformation on the Workforce

Symantha “Sam” Loflin—has an MS in program management and a certification in advanced acquisition studies from the Naval Postgraduate School (NPS), where she was a contributor to the 18th, 19th, and 20th Annual NPS Acquisition Research Symposium. She also holds a BS in finance from the University of Houston. Loflin is a Case Manager and Researcher at Tanner and Associates. She has more than 20 years of acquisition experience supporting DCMA, the DoD, NASA, and the military services. She recently served as an acquisition program manager on the Coronavirus Task Force that focused on building the industrial base for personal protective equipment. Loflin’s career began at NASA, supporting the Space Shuttle, ISS, and the Constellation Programs in Houston. [symanthaloflin@gmail.com]

Abstract

The author has written this paper to defend and strengthen the use of governmental risk mitigation measures that prevent divergence, ensure safety, and highlight the possibilities of future growth in workforce skills. The purpose of the investigation is to discover and disclose of the impact of artificial intelligence (AI) and cyberspace on the nation and global human population and workforce. The analysis of the research revealed the key results related to the current and future measures that the United States government, military services, the country, and the world, endorse to secure and protect consumers and the workforce, while promoting innovation from the use of safe AI and cyberspace. Each year, the federal government increases the funding of developmental contracts as a measure to “Protect Sea, Air, and Space” (White House, 2022b). These efforts aim to protect U.S. interests in developing technologies, creating economic opportunities, and enabling climate surveillance, and to responsibly oversee the space environment. The government is working with allies and industrial base partners in advancing and developing new technologies with trusted artificial intelligence and secure internet to create prosperity and economic security. Industry and the United States government’s ability to engage the right people, processes, and tools at the right time is essential to effective program management policy and control (Hite, 2010. p. 23).

Research Issues

How will the United States defend, protect, and safely navigate the workforce throughout the emerging technology of artificial intelligence and the risk of cyber-attacks? Are the AI secrets really hidden or is there so much information on the web that unless it touches us we do not see it?

Research Results Statement

The results are clear and convincing that it takes a whole-of-nation and global approach to defend and protect the workforce to achieve and enhance economic growth and protect national security. The conformality of legal and regulatory procedures is necessary to protect human rights and safely use AI and protect against cyber vulnerabilities and cyber-attacks is essential to strengthen the future of workforce jobs. Investing in our workforce effectively and efficiently increases economic growth in the production of good, services, and materials in the United States that meet Federal procurement needs. On January 29, 2024, the White House published *Fact Sheet: Biden-Harris Administration Announces Key AI Actions Following President Biden’s Landmark Executive Order* (White House, 2024).

Recommendations

1. Provide public service announcements on the measures the U.S. government has taken to educate the American public and the workforce on the safe and secure AI and cybersecurity (White House, 2024). Research shows that subject matter knowledge increases

the likelihood of successful problem resolutions "experiential learning offers a way to ensure we are imparting not just rote learning and certifications but providing our people the knowledge, skills, and experience to effectively control the efforts we charge them to lead" (Pickar, 2020). Human capabilities lead to improved preventative measures. 2. Enhance government oversight of statutory and regulatory policies, standards, and procedures to safeguard and preserve the rights of the workforce. 3. Create a consortium for enhanced collaboration. (See the *Evidence-Based Policymaking Act of 2018 (Evidence Act)* (The Evidence Act, 2019).)[1] See also learning agendas:

> According to Office of Management and Budget (OMB) guidance for implementing the Evidence Act, a learning agenda is to define and prioritize relevant questions and identify strategies for building evidence to answer them. In developing a learning agenda, an agency should involve key leaders and stakeholders, to help (1) meet their evidence needs for decision-making and (2) coordinate evidence-building activities across the agency. (GAO, 2019)

Introduction

The United States government, humans, companies, the nation, and the world's ability to develop the workforce and engage the right people, processes, and tools at the right time is challenging. Education and communication for humans to safely use AI technology and prevent cyber-attacks and guard against vulnerabilities are essential to be effective and efficient. To ensure the rights of humans there must be accountability through government oversight of AI and cybersecurity laws, regulations, standards, guidance, and policy. These measures will provide the capabilities required to maximize the innovations of the workforce and support proper stewardship of taxpayer dollars.

> *Biden-Harris Administration's National Security Strategy*,
>
> By enhancing our industrial capacity, investing in our people, and strengthening our democracy, we will have strengthened the foundation of our economy, bolstered our national resilience, enhanced our credibility on the world stage, and ensured our competitive advantages. (White House, 2022)

In the March 2017 issue of the *ScienceDirect Engineering Journal*, the Research Intelligent Manufacturing-Review issued the publication, "Intelligent Manufacturing in the Context of Industry 4.0: A Review Industry," and provided the research results that provide an understanding of intelligent manufacturing in Industry 4.0. "Our next generation of Industry—Industry 4.0—holds the promise of increased flexibility in manufacturing, along with mass customization, better quality, and improved productivity" (Zhong et al., 2017). Additionally, the results showed that some technologies have AI, including cyber-physical systems that allows learning with manufacturing systems. In Industry 4.0, the expected colloborations between humans and machines will enable humans to be more efficient and effective with decision making (Zhong et al., 2017). Even though in Industry 4.0, AI and an IT infracture provide the

[1] The Evidence Act adopts as its definition of evidence "information produced as a result of statistical activities conducted for a statistical purpose." It adopts as its definition of statistical purpose "the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups and includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support" those actions. Pub. L. No. 115-435, § 101(a)(1); 44 U.S.C. § 3561(6), (12). OMB's June 2019 update to Cir. No. A-11 contains these definitions. The guidance also states that in the context of improving organizational and agency performance, "evidence" can be viewed more broadly, in line with OMB's definition.

workforce with improved efficiency, reliability, and human involvement, there are inherent risks of cyber attacks and cybersecurity must be a top priority for humans, companies, the nation, and the world.

June 23, 2009—United States Cyber Command (USCYBERCOM)

It is important to note that Dr. Robert M. Gates, in his book *Duty* (2014, p. 300), emphasized the urgency to direct the establishment of the United States Cyber Command (USCYBERCOM). On June 23, 2009 Gates's memorandum also stipulated that the Under Secretary for Policy would develop a new national cybersecurity strategy (p. 1). The nation and military operations dependance on cyberspace continues to increase, along with the threats and exposures. The cyber risk of exposing required technical warfighting capabilities across the globe is a matter of national security. Gates's highest mission priority was realized with the establishment and successful accomplishments of the USCYBERCOM. The command is now almost 14 years old and the nation's unified combatant command operates globally to ensure the United States and its allies have freedom of action in cyberspace while defending against the same adversaries. Additionally, as shown on the command website, "This is our code. As the nation's first line of defense in cyberspace, we operate at the speed, relevance, and scale necessary to win" (United States Cyber Command, n.d.). Mr. Gates notable book cover and quote about the importance of knowledge are shown in Figure 1.

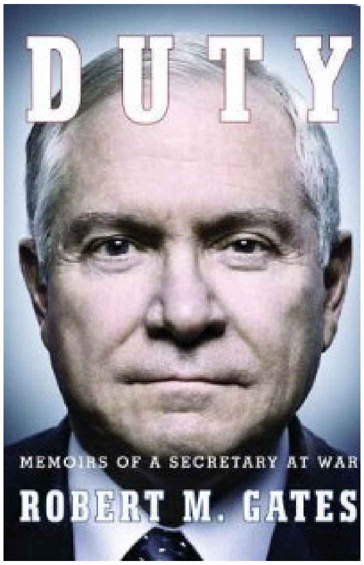


Figure 1. Cover of Robert M. Gates Book,
Duty: Memoirs of a Secretary at War
(Gates, 2014)

"What I know concerns me. What I don't know concerns me even more.
What people aren't telling me worries me the most" (Gates, 2014).

National Institute of Standards and Technology (NIST)—Industry 4.0—Cybersecurity

On October 26, 2023, Katie Rapp a writer/editor for the National Institute of Standards and Technology's (NIST's) Manufacturing Extension Partnership, published "Infographic—Integrating Cybersecurity with Industry 4.0: What it Means for Manufacturing" (Rapp, 2023, p. 1). She asked the questions and provides her research answers,

> Did you know that manufacturing is now the most targeted industry for cyber attacks? The average cost of a data breach for a small business is $105,000. Can your firm absorb that cost? Can you risk the down time and the damage that a data breach would cause your business? (Rapp, 2023)

The NIST has a blog that is a series on cybersecurity and Industry 4.0. On May 11, 2022, Pat Toth, a 30 year cybersecurity guidance document professional at the NIST, posted "Cybersecurity and Industry 4.0—What You Need to Know" (infographic is shown in Figure 2 (Toth, 2022). She provided a thorough background of Industry 4.0 and the relationship of the *NIST Special Publication 1500-201, Framework for Cyber-Physical Systems: Volume 1* (Giffor, 2017) that is intended to document external viewpoints/artifacts (use cases with activities and artifacts for certification and regulatory compliance testing) in the application of the CPS Framework from industry, academia, and government. Note: The reports do not represent official NIST positions.

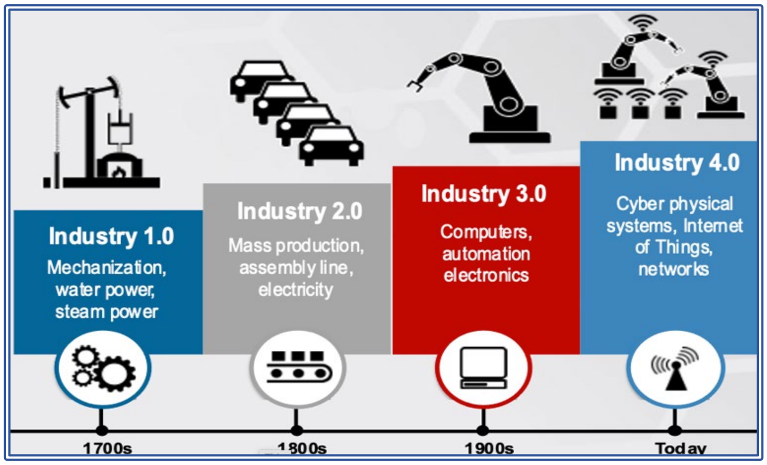

Industry 1.0
Mechanization, water power, steam power
Industry 2.0
Mass production, assembly line, electricity
Industry 3.0
Computers, automation electronics
Industry 4.0
Cyber physical systems, Internet of Things, networks
1700s
1800s
1900s
Today

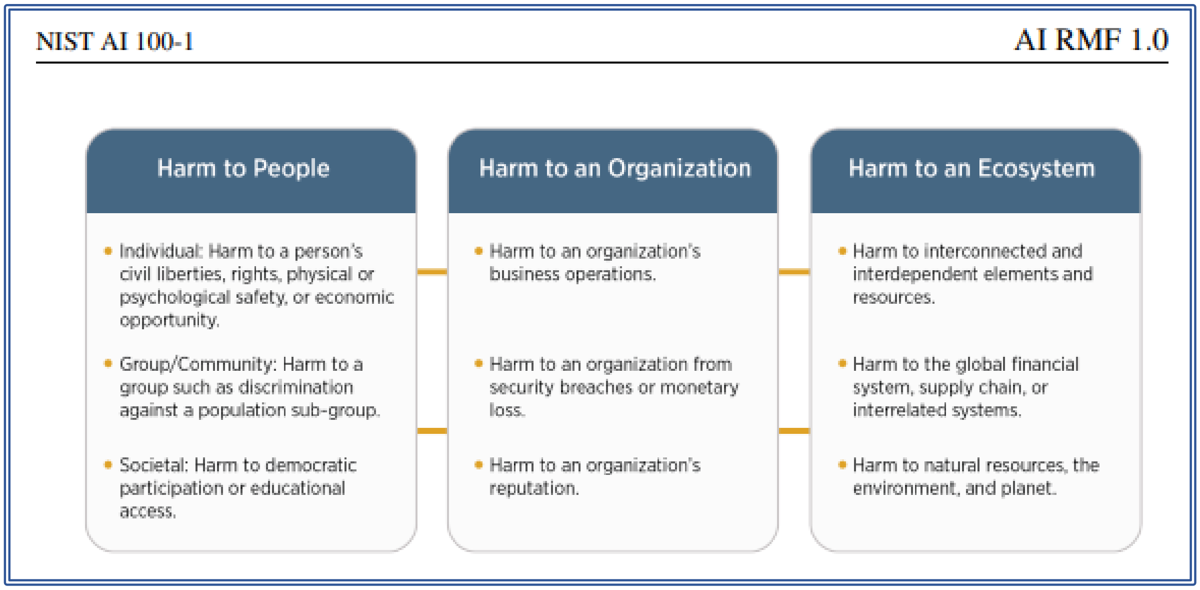
Figure 2. NIST Industrial Revolutions—Cybersecurity and Industry 4.0—What You Need to Know (Toth, 2022)

The cybersecurity and Industry 4.0 blog provides the "Need to Know" on Cyber-Physical Systems (CPS). Cobots are engineered interacting networks between cyber-physical systems and the networks of physical and computational components. The systems are providing new functionalities in many domains including our quality of life, smart manufacturing, defense, and homeland security. Cobots (used to perform some manufacturing tasks) are rapidly being adopted by manufacturers to assist humans in a shared share workspace and requires ongoing safety risk assessments.

Additionally, Internet of Things (IoT) and Big Data, as well as Cloud Manufacturing have transformed resources and capabilities that improve production and provide a safer and higher quality manufacturing life cycle. However, hackers, cybercriminals, and industry competors pose extreme cyber risk. Cyber risk assessments are essential prior to the introduction of new technology. Industry 4.0 brings robotic and automation effeciencies to manufacturing, as well as the risk cyber vunerabilities.

January 26, 2023, AI Risk Management Framework (NIST AI 100-1)

The world must be vigilant in creating safe and trustworthy AI systems with ongoing surveillance to ensure compliance. Safe AI systems contribute to human efficiencies when used in manufacturing through automation and robotics. The NIST published examples of the documented harms of AI systems in Figure 3 (NIST, 2023a).



NIST AI 100-1

AI RMF 1.0

Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

Figure 3. NIST AI 100-1, Harms from AI systems (NIST, 2023a)

January 26, 2023, AI Risk Management Framework (RMF)

Ideally, the life cycle stages of the AI area teams include actions from a diverse team in AI risk management, operations, plan and design function, as well as all stakeholders that exists through the AI system life cycle. The teams share ideas, develop, deploy, test, and evaluate to identify, analyze, track, and manage-prioritize current and emerging risk. The risk are mitigated and preventive measures are integrated. The AI RMF life cycle shows the stages of the AI system actors in planning and design as an integral part of the risk management efforts as shown in Figure 4.

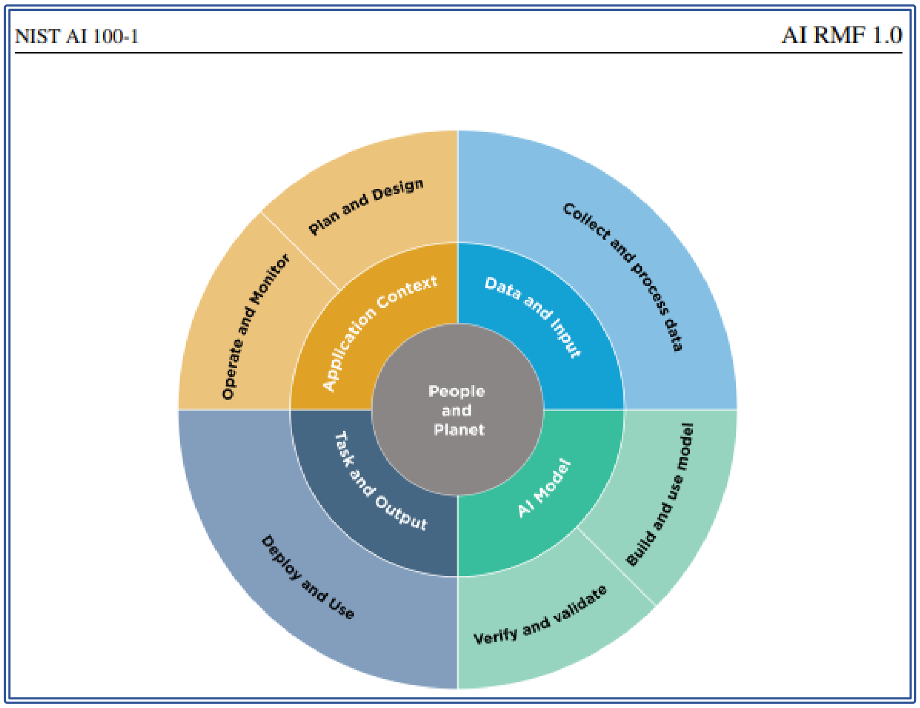
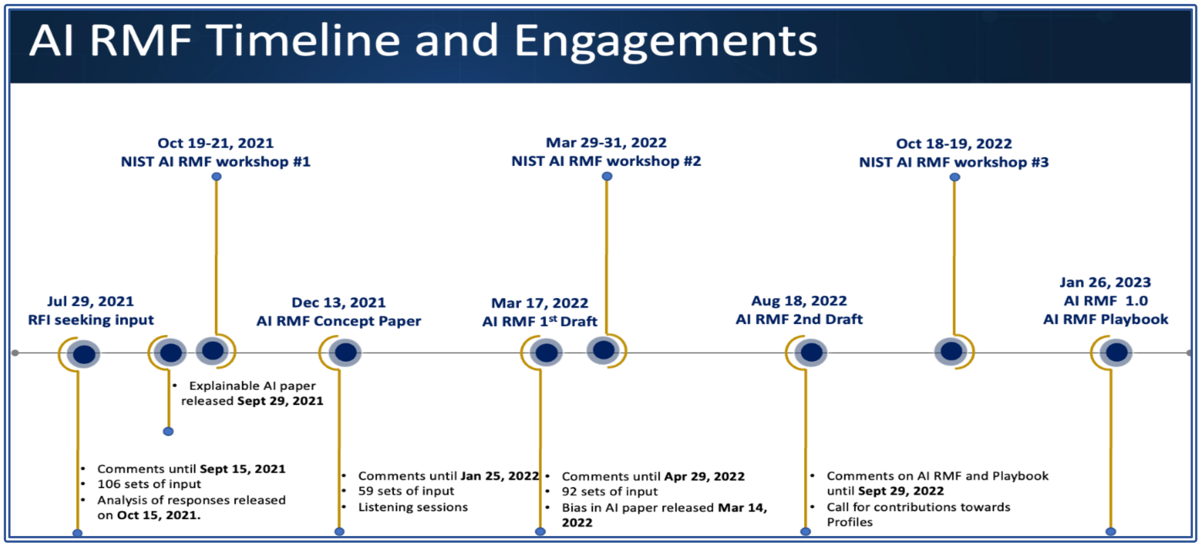


Figure 4. Life Cycle and Key Dimensions of an AI System (Organization for the Economic Cooperation and Development [OCED], 2022)

March 30, 2023, Trustworthy & Responsible AI Resource Center

The center was established by the NIST Trustworthy & Responsible Artificial Intelligence Center (AIRC; NIST n.d.). The AIRC was developed to provide AI actors in the "development and deployment of trustworthy and responsible AI technologies" (NIST, 2023). The center offers numerous resources (e.g., NIST AI RMF 1.0, Playbook, Training, etc.). The AI RMF Timeline and Engagements shows a that the establishment of the AI RMF from its July 29, 2021 inception to publication of the AI RMF 1.0 and the Playbook on July 26, 2023, took more than 30 months (Figure 5).



AI RMF Timeline and Engagements

Jul 29, 2021
RFI seeking input

- Comments until **Sept 15, 2021**
- 106 sets of input
- Analysis of responses released on **Oct 15, 2021.**

- Explainable AI paper released **Sept 29, 2021**

Oct 19-21, 2021
NIST AI RMF workshop #1

Dec 13, 2021
AI RMF Concept Paper

- Comments until **Jan 25, 2022**
- 59 sets of input
- Listening sessions

Mar 17, 2022
AI RMF 1st Draft

- Comments until **Apr 29, 2022**
- 92 sets of input
- Bias in AI paper released **Mar 14, 2022**

Mar 29-31, 2022
NIST AI RMF workshop #2

Aug 18, 2022
AI RMF 2nd Draft

- Comments on AI RMF and Playbook until **Sept 29, 2022**
- Call for contributions towards Profiles

Oct 18-19, 2022
NIST AI RMF workshop #3

Jan 26, 2023
AI RMF 1.0
AI RMF Playbook

Figure 5. AI Risk Management Framework Timeline and Engagements (NIST, 2023)

Table 1 Shows examples of some of the notable government measures related to AI.

Table 1. Notable Government Measures Related to AI

United States Government Measures ~Artificial Intelligence (AI)~
United States Department of State
January 1, 2021, *National Artificial Intelligence Initiative Act of 2020 (NAIIA)*, became law. H.R.6216 - 116th Congress (2019-2020): National Artificial Intelligence Initiative Act of 2020 | Congress.gov | Library of Congress
April 28, 2022, Declaration for the Future of the Internet.
CDAO CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE **OSD Bias Bounty** **Presented by** CONDUCTOR AI bugcrowd January 29–March 11, 2024 (closed), AI Bias Testing Office of Secretary of Defense. (2024, January 29–March 11). OSD Bias Bounty. https://osdbiasbounty.com/sign-in?callbackUrl=https%3A%2F%2Fosdbiasbounty.com%2Fsign-in
THE WHITE HOUSE WASHINGTON
October 4, 2022, What is the Blueprint for an AI Bill of Rights? Relationship to Existing Law and Policy, **E.O. 13960, 13985, and** **Fair Information Practice Principles (FIIPs)** https://www.whitehouse.gov/ostp/ai-bill-of-rights/what-is-the-blueprint-for-an-ai-bill-of-rights/ and https://www.whitehouse.gov/ostp/ai-bill-of-rights/relationship-to-existing-law-and-policy/
October 30, 2023, AI Bill of Rights on Safe, Secure, and Trustworthy Artificial Intelligence **Executive Order 14110** Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**.** https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

May 2023, World Economic Forum, Future of Jobs Report 2023—Industry 4.0

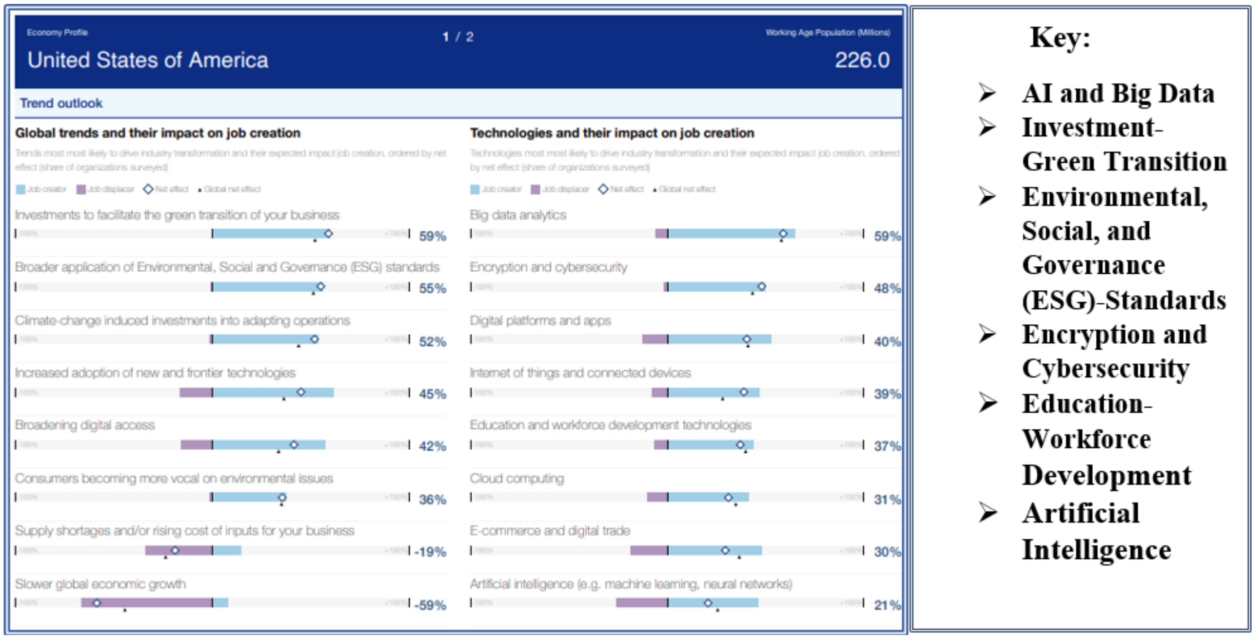
The World Economic Forum was established in 2014 and its first edition report was published in 2016 (World Economic Forum, 2023). The forum serves a significant purpose by collaborating with governments from around the globe and public-private sectors as an international organization to create surveys that are distributed to employees. The survey results provide insight over the next five years for analysis and employer planning into the future of jobs and skills under the **Forth Industrial Revolution—Industry 4.0**.

The 2023–2027 survey included 44 survey questions in 12 languages with data collection between November 2022 and February 2023. The survey was administrated by participating companies for future of jobs and skills projections in the November 2023 through February 2027 timeframe. The data was collected by 830 companies with a collective 11.3 million workers in 45 world region economies and 22 country acknowledgements. The results provide the private- and public-sector leaders with insight into the future of jobs and skills needed to be successful in providing a better work future for all. The World Economic Forum, Future of Jobs Insight Report 2023 cover is shown in Figure 6.

Figure 6. World Economic Forum, Future of Jobs Report (World Economic Forum, 2023)

United States of America Job Creation/Displacer Outlook 2023–2027

The World Economic Forum determined that age 25 and older is the working age population. The major focus was on the economy and global five-year business transformation for trends and technologies and the impact as a job creator, displacer, net effect, and global net effect. The Future of Jobs 2023 Insight Report calculated 226 million people of the working age in the United States. The economic profile for the United States of America shows the key impacts in job creation in Figure 7. The largest impact globally is in skills (cognitive and self-efficacy), reskilling (AI and big data analytical and creative thinking), and training funding (org. and free training) as shown in Figure 8.



Economy Profile

1 / 2

Working Age Population (Millions)

United States of America 226.0

Trend outlook

Global trends and their impact on job creation

Trends most most likely to drive industry transformation and their expected impact job creation, ordered by net effect (share of organizations surveyed)

Investments to facilitate the green transition of your business	59%
Broader application of Environmental, Social and Governance (ESG) standards	55%
Climate-change induced investments into adapting operations	52%
Increased adoption of new and frontier technologies	45%
Broadening digital access	42%
Consumers becoming more vocal on environmental issues	36%
Supply shortages and/or rising cost of inputs for your business	-19%
Slower global economic growth	-59%

Technologies and their impact on job creation

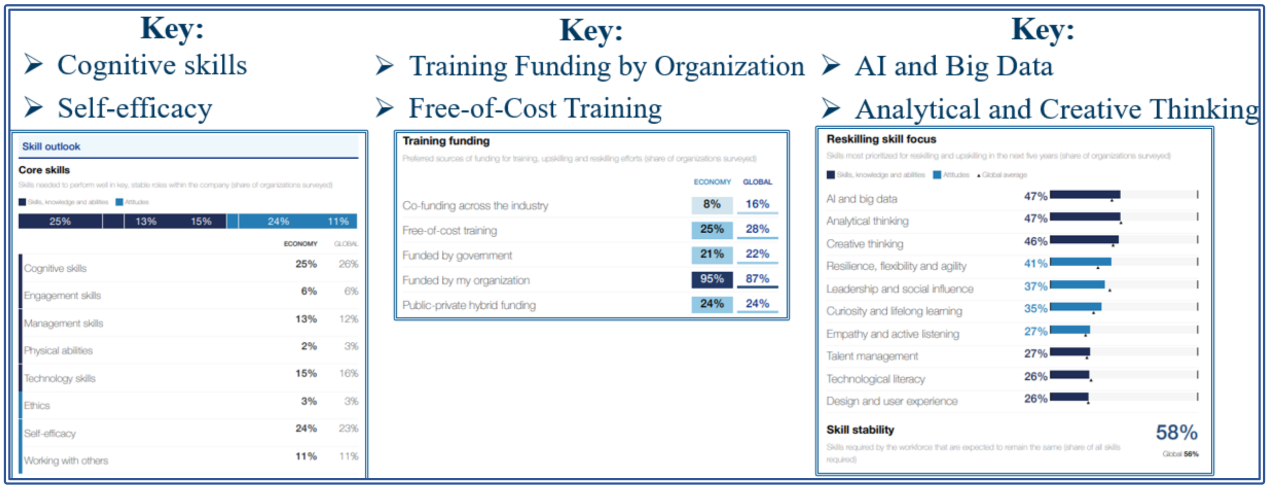
Technologies most most likely to drive industry transformation and their expected impact job creation, ordered by net effect (share of organizations surveyed)

Big data analytics	59%
Encryption and cybersecurity	48%
Digital platforms and apps	40%
Internet of things and connected devices	39%
Education and workforce development technologies	37%
Cloud computing	31%
E-commerce and digital trade	30%
Artificial intelligence (e.g. machine learning, neural networks)	21%

Key:

- ➢ AI and Big Data
- ➢ Investment-Green Transition
- ➢ Environmental, Social, and Governance (ESG)-Standards
- ➢ Encryption and Cybersecurity
- ➢ Education-Workforce Development
- ➢ Artificial Intelligence

Figure 7. Economic Profile for the United States of America



Key:

- ➢ Cognitive skills
- ➢ Self-efficacy

Skill outlook

Core skills

Skills needed to perform well in key, stable roles within the company (share of organizations surveyed)

	ECONOMY	GLOBAL
Cognitive skills	25%	26%
Engagement skills	6%	6%
Management skills	13%	12%
Physical abilities	2%	3%
Technology skills	15%	16%
Ethics	3%	3%
Self-efficacy	24%	23%
Working with others	11%	11%

Key:

- ➢ Training Funding by Organization
- ➢ Free-of-Cost Training

Training funding

Preferred sources of funding for training, upskilling and reskilling efforts (share of organizations surveyed)

	ECONOMY	GLOBAL
Co-funding across the industry	8%	16%
Free-of-cost training	25%	28%
Funded by government	21%	22%
Funded by my organization	95%	87%
Public-private hybrid funding	24%	24%

Key:

- ➢ AI and Big Data
- ➢ Analytical and Creative Thinking

Reskilling skill focus

Skills most prioritized for reskilling and upskilling in the next five years (share of organizations surveyed)

AI and big data	47%
Analytical thinking	47%
Creative thinking	46%
Resilience, flexibility and agility	41%
Leadership and social influence	37%
Curiosity and lifelong learning	35%
Empathy and active listening	27%
Talent management	27%
Technological literacy	26%
Design and user experience	26%

Skill stability 58%

Skills required by the workforce that are expected to remain the same (share of all skills required)

Global 56%

Figure 8. Economy and Global Skills-Reskilling-Training

ARTIFICIAL INTELLIGENCE

Addendum to the NPS Strategic Plan 2018–2023

> "Humanity is at the edge of a revolution driven by artificial intelligence ... This revolution is unstoppable. Attempts to halt it would cede the future to that element of humanity more courageous in facing the implications of its own inventiveness. Instead, we should accept that AI is bound to become increasingly sophisticated and ubiquitous, and ask ourselves: How will its evolution affect human perception, cognition and interaction? What will be its impact on our culture and, in the end, our history?"
>
> -Henry Kissinger, Eric Schmidt and Daniel Huttenlocher
> The Atlantic • August 2019

Figure 9. ***Artificial Intelligence. An Addendum to the Strategic Plan*** **(Naval Postgraduate School, 2019, p. 2)**

References

Bias Bounty. (n.d.). https://osdbiasbounty.com/

Bureau of Labor Statistics. (2024 January 23). *News release*. U.S. Department of Labor. https://www.bls.gov/news.release/pdf/union2.pdf

COPILOT. (n.d.). Microsoft. https://copilot.microsoft.com/

The Evidence Act, Pub. L. No. 115-435, 132 Stat. 5529 (Jan. 14, 2019). https://www.congress.gov/bill/115th-congress/house-bill/4174/text

Federal Register. (2020, December 3). *Promoting the use of trustworthy artificial intelligence in the federal government* (Executive order 13960).

Gates, R. M. (2009, June 23). *Establishment of a subordinate unified U.S. cyber command under U.S. strategic command for military cyberspace operations* [Memorandum]. Department of Defense. https://nsarchive.gwu.edu/document/21425-document-29

Gates, R. M. (2014). *Duty: Memoirs of a secretary at war*. Alfred A. Knopf. https://www.google.com/books/edition/Duty/lYzZAAAAQBAJ?hl=en&gbpv=1&bsq=What%20I%20know%20concerns%20me

Giffor, E. (2017). *Framework for cyber-physical systems* [Special Publication 1500-201]. Department of Commerce. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.1500-201

Government Accountability Office. (2019, December). *Report to congressional requestors. Evidence-based policymaking. Selected agencies coordinate activities, but could enhance collaboration*. https://www.gao.gov/products/gao-20-119

Government Accountability Office. (2023, December). *Artificial intelligence agencies have begun implementation but need to complete key requirements* (GAO-24-105980). https://www.gao.gov/assets/d24105980.pdf

Hite, R. C. (2010, August). *Organizational transformation: A framework for assessing and improving enterprise architecture management (version 2.0)* (GAO-10-846G). Government Accountability Office. https://www.gao.gov/assets/gao-10-846g.pdf

Homeland Security. (2008, December 29). *Fair information practice principles (FIPPs).* https://www.dhs.gov/sites/default/files/2024-01/Fair%20Information%20Principles_12_2008.pdf

Foundations for Evidence-Base Policymaking Act of 2018, Pub. L. No. 115–435 (2018). https://www.congress.gov/bill/115th-congress/house-bill/4174/text

International Association of Machinists and Aerospace Workers (IAMAW). (1888). https://www.goiam.org/

International Brotherhood of Teamsters (IBT). (1903). https://teamster.org/

Kehoe, A. (2022, May 21). *Navy ships swarmed by drones, not UFOs, defense officials confirm*. The Warzone. https://www.twz.com/navy-ships-swarmed-by-drones-not-ufos-defense-officials-confirm

Kennedy, B., Tyson, A., & Saks, E. (2023, February 15). *Public awareness of artificial intelligence in everyday activities*. Pew Research Center. https://www.pewresearch.org/science/2023/02/15/public-awareness-of-artificial-intelligence-in-everyday-activities/

Kobielus, J. (2020, July 10). *Robotics: How crisis is accelerating automation*. Information Week. https://www.leadershipreview.net/robotics-how-crisis-is-accelerating-automation/

Livescience. (2014, August 25). *Timeline of artificial intelligence*. https://www.livescience.com/47544-history-of-a-i-artificial-intelligence-infographic.html

Lynch, S. (2023, April 3). *2023 State of AI in 14 charts*. Stanford University. https://hai.stanford.edu/news/2023-state-ai-14-charts

National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Cong. (2020). https://www.congress.gov/bill/116th-congress/house-bill/6216/text

National Institute of Standards and Technology (NIST). (2023a, January 26). *AI risk management framework (RFM).* https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

National Institute Standards and Technology (NIST). (2023b, March 30). Trustworthy & responsible AI resource center. https://airc.nist.gov/Home

National Institute of Standards and Technology (NIST). (2023c, March 30). *AI RMF timeline.* https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development

National Institute of Standards and Technology (NIST). (n.d.). *Crosswalk document list*. https://airc.nist.gov/home

Naval Postgraduate School. (2019, August 15). *Artificial intelligence. An addendum to the strategic plan.* https://nps.edu/documents/115153495/115155926/AI_StratPlan_Addendum_WEB-FINAL.pdf/ed7ddfbf-49c1-4a3e-b3ca-67d04775e799?t=1568929349000

Office of Secretary of Defense. (2024). *OSD bias bounty*. https://osdbiasbounty.com/sign-in?callbackUrl=https%3A%2F%2Fosdbiasbounty.com%2Fsign-in

Organization for the Economic Cooperation and Development (OCED). (2022, February 22). *OECD framework for the classification of AI systems*. https://www.oecd-ilibrary.org/science-and-technology/oecd-framework-for-the-classification-of-ai-systems_cb6d9eca-en

Pickar, C. (2020). *Learning from experience: Acquisition professional education for this century* (SYM-AM-20-070). Naval Postgraduate School, Acquisition Research Symposium. nps.edu

Rapp, K. (2023, October 26). Infographic—Integrating cybersecurity with industry 4.0: What it means for manufacturing. National Institute of Standards and Technology. https://www.nist.gov/blogs/manufacturing-innovation-blog/infographic-integrating-cybersecurity-industry-40-what-it-means

Raymond, N. (2024, January 29). *Lawyers voice opposition to 5th Circuit's proposed AI rule*. https://www.reuters.com/legal/transactional/lawyers-voice-opposition-5th-circuits-proposed-ai-rule-2024-01-29/

Rogoway, T. (2024a, February 5). Drone warfare's terrifying AI-enabled next step is imminent. *The Warzone.* https://www.twz.com/news-features/drone-warfares-terrifying-ai-enabled-next-step-is-imminent

Rogoway, T. (2024b, April 4). The compelling case for arming U.S. navy warships with drone swarms. *The Warzone.* https://www.twz.com/sea/the-compelling-case-for-arming-u-s-navy-warships-with-drone-swarms

Service Employees International Union (SEIU). (1921). https://www.seiu.org/about?fdonav

Sheffi, Y. (2023, September 15). The UAW and other unions must focus more on AI and automation in their negotiations. *Harvard Business Review.* https://hbr.org/2023/09/the-uaw-and-other-unions-must-focus-more-on-ai-and-automation-in-their-negotiations

The Federal Privacy Council. (n.d.). *Fair information practice principles (FIPPs), roles in federal privacy, the Privacy Act of 1974, privacy impact assessments.* https://www.fpc.gov/learn-about-federal-privacy-program/

The Internet in Real–Time. (2024, February 15). https://visual.ly/community/Infographics/how/internet-real-time

Thomson Reuters. (n.d.-a). AI infographic. https://tax.thomsonreuters.com/content/dam/ewp-m/documents/tax/en/pdf/infographics/7-things-professionals-need-to-know-about-ai-tr840725.pdf

Thomson Reuters. (n.d.-b). AI infographic. https://www.thomsonreuters.com/en/artificial-intelligence.html

Toth, P. (2022, May 11). *Cybersecurity and industry 4.0—What you need to know*. National Institute of Standards and Technology (NIST). https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-and-industry-40-what-you-need-know

United Auto Workers (UAW). (1935). https://uaw.org/about/

United Nations. (n.d.). *Member States*. https://www.un.org/en/about-us/member-states.

United States Cyber Command (USCYBERCOM). (n.d.). *This is our code*. https://www.cybercom.mil/

United States Cyber Command (USCYBERCOM). (2009, June 23). https://www.cybercom.mil/About/History/

United States Department of Justice Overview of the Privacy Act of 1974, 2020 Edition. Overview of the Privacy Act of 1974. https://www.justice.gov/Overview_2020/dl?inline

United States Department of Labor. (2023, September 1). *Worker organizing resource and knowledge center.* https://www.workcenter.gov/

United States Department of Labor Blog. (2023, November 14). *Worker organizing resource and knowledge center.* https://blog.dol.gov/2023/11/14/find-collective-bargaining-resources-at-the-work-center

United States Department of State. (2021, January 1). *National artificial intelligence initiative act of 2020 (NAIIA)*. https://www.state.gov/artificial-intelligence/

United States Department of State. (2022, April 28). *Declaration for the future of the internet*. https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf

United Steelworkers (USW). (1942, May 22). https://www.usw.org/union

White House. (2021, January 20). *Advancing racial equity and support for underserved* (Executive order 13985). https://www.govinfo.gov/content/pkg/DCPD-202100054/pdf/DCPD-202100054.pdf

White House. (2021, January 25). *Executive order 14005, section 4(a): Ensuring the future is made in all of America by all of America's workers.* https://www.whitehouse.gov/briefingroom/presidential-actions/2021/01/25/executive-order-on-ensuring-the-future-is-made-in-allof-america-by-all-of-americas-workers/

White House. (2022a, October 4). *Blueprint for an AI bill of rights*. Office of Science and Technology Policy. https://www.whitehouse.gov/ostp/

White House. (2022b, October 12). *Biden-Harris administration's national security strategy*. https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

White House. (2023a, February 16). *Executive order on further advancing racial equity and support for underserved communities through the federal government*. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

White House. (2023b, September 1). *Fact sheet: Ahead of labor day, Biden-Harris administration announces new actions to empower workers—Building on the president's historic support for workers and unions*. https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/01/fact-sheet-ahead-of-labor-day-biden-harris-administration-announces-new-actions-to-empower-workers-building-on-the-presidents-historic-support-for-workers-and-unions/

White House. (2023c, October 30). *Blueprint for an AI bill of rights*. https://www.whitehouse.gov/ostp/ai-bill-of-rights/

White House. (2023d, October 30). *Fact sheet: President Biden issues executive order on safe, secure, and trustworthy artificial intelligence* (Executive order 14110). https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

White House. (2024, January 29). *Fact Sheet: Biden-Harris administration announces key AI actions following President Biden's landmark executive order*. https://www.whitehouse.gov/briefing-room/statements-releases/2024/01/29/fact-sheet-biden-harris-administration-announces-key-ai-actions-following-president-bidens-landmark-executive-order/

World Economic Forum. (2023, May). *Future of jobs report 2023*. https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf

Young, S. D. (2024, March 28). *Memorandum for the heads of executive departments and agencies: Advancing governance, innovation, and risk management for agency use of artificial intelligence* (M-24-10). Office of Management and Budget. M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf (whitehouse.gov)

Zhong, R. Y., Xu, X., Klotz, E., & Newman, S. T. (2017). Intelligent manufacturing in the context of industry 4.0: a review. *Engineering*, *3*(5), 616–630. https://www.sciencedirect.com/science/article/pii/S2095809917307130

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net