# Campaign for an AI Ready Force

## Executive Summary

The Department of Defense (DoD) Artificial Intelligence (AI) Strategy recognizes that AI is "poised to transform every industry, and is expected to impact every corner of the Department, spanning operations, training, sustainment, force protection, recruiting, healthcare, and many others."[1] AI is a general-purpose technology; it helps many systems become more capable, precise, and versatile.

The Department is beginning to grapple with the changes it needs to make to adapt to this new technology, notably establishing the Joint AI Center (JAIC), and launching a series of new task forces and initiatives at each Service[2] and at DARPA[3]. However, the Defense Innovation Board (DIB) contends that insufficient attention has been paid to what approaches are necessary to modernize the workforce itself[4], and the access to data, compute resources, training, and other techniques the force will need to be successful on a battlefield increasingly reshaped by advances in AI. We propose the term "AI Readiness" to capture the notion of how well-poised the Department is to seize opportunities and respond to threats in this emergent area. To correct this -- and to do so urgently -- will require a campaign level of focus, investment, and prioritization. This recommendation is intended to offer a recommendation on how to design and execute such a campaign.

## Background

The arc of AI development across the Department will fundamentally mirror (and be dependent on) DoD's ability to build and acquire basic, modern software faster, cheaper, and with better design and architecture. By "basic" we mean software that is explicitly and finitely programmed by human beings, rather than machines. The Defense Innovation Board's Software Acquisition and Practices (SWAP) Study discusses this in depth.[5]

Modern software practices are foundational to any applied AI project. At the same time, AI is different than other software applications. AI does not come out of development as a finished program; it must be deployed in real contexts to improve over time. It is not a capability that can be developed in a lab or acquired from industry; rather, it represents a dense network of dependencies and linkages: data, modern cloud storage and compute, domain knowledge, hardware and software engineering disciplines, new testing regimes, new concepts of operation, many personnel and organizational adaptations, and ultimately changes to workflows, which in turn will require policy and process changes. There are also important ethical and normative considerations in the development and adoption of AI, which the Board has addressed in a separate report.[6]

[1] DoD AI Strategy, p. 5 https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[2] Noted examples: the USAF MIT AI Task Force, the USA CMU AI Task Force, and USN DWO

[3] AI Next

[4] This document focuses on the DoD workforce not already engaged in fundamental AI research, in which DoD has been investing for decades.

[5] https://innovation.defense.gov/software/

[6] The report, "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense" is available at www.innovation.defense.gov/ai.

Consequently, as DoD Components (Services, OSD) progress toward the adoption and deployment of AI, technology will likely *not* be the hardest challenge. The biggest challenges will instead center around people and organization.

Leaders will need to answer a panoply of questions: How do we determine what types of problems are suitable for AI applications, and which kinds are not well-suited to avoid misapplication of the tools beyond their designed capabilities? How do we reshape our structures and processes to optimize data collection, management, curation, sharing, and analysis? How do we use both DoD-owned data and best-in-class commercial data, labeling, and curation? How do we translate AI capabilities into real mission impact, ensuring that the outputs of the tools are useful to decision makers and warfighters? How do we get leaders to understand and trust AI outputs?

Taking full advantage of the potential of AI to deliver positive mission impact requires a whole ecosystem and a transformational shift in how DoD organizes, makes decisions, and competes with adversaries. DoD leaders must accord proper emphasis not only to the development of the technology, but also to the *readiness* of the total force to receive and deploy it.

## Defining An AI Ready Force

An AI Ready Force is a force that has the capability and capacity to understand, design, develop, test, evaluate, deliver, sustain, and scale AI in support of DoD missions. To apply AI effectively and at scale, four pillars of an AI Ready Force must align: **people, data, technological infrastructure,** and **organizational design.**

### People

An effective AI-ready workforce has a range of technical and non-technical workers and leaders, working in multidisciplinary teams. The National Security Commission on AI (NSCAI) has proposed an AI workforce model that describes both the worker archetypes and capabilities a national security organization needs to be ready to apply AI to its mission. This is a valuable model for DoD leaders to assess needs across the force, and it poses important questions that DoD Components will need to answer regarding force composition and training.

DoD needs broad access to many kinds of talent, to include experts outside of government. Even the top technology companies in Silicon Valley struggle to hire and retain AI talent. Consequently, DoD will need to blend recruiting with training and upskilling its workforce. The Department will have to learn to balance internal and external capability and capacity, and collaborate with academic and industry partners.

### Data

Vast amounts of useful data in the right formats and systems are a core component of what enable applications to make positive mission impact.  DoD must treat data as a strategic asset.

### Technological Infrastructure

The application of AI in any context requires sufficient tools and infrastructure. Basic technical requirements must be met before algorithms can be put to use; often, the prevalence of legacy systems is a major barrier to adoption. People need access to industry-standard software, sufficient compute and storage, authorizations to operate, sufficiently open architectures, and secure networks and learning environments. Enterprise cloud is the only way to make data accessible, affordable, and secure across the Department.[7]

Organizational Design

DoD must learn how to organize and deploy its people and technology to produce effective outcomes consistently and at scale. Organizational structures need to adopt iterative loops for data collection, application updates, and inputs for human decision-making. Policies need to enable application development iteratively and at speed with security and oversight inline, rather than serially. Incentives need to encourage leaders to take managed risks and push through bureaucratic inertia to deliver capability.

## A *Campaign* for an AI Ready Force

As described in the DoD AI Strategy, the Department should iteratively develop a comprehensive approach to transforming its operations and maintaining its strategic advantage in the field of AI. Like industry, DoD will need to learn not only through research, but also *by doing*, and must do so expeditiously. Adversaries are moving forward with urgency and so must we.

There is no top-down, linear approach for creating an AI Ready Force. DoD senior leaders need to think critically and independently about sequencing their initiatives because of differences in mission application. Recruiting or training an AI-ready workforce will be ineffective absent an enabling environment (data, technological infrastructure, and organizational design). At the same time, an AI-ready workforce is needed to influence key decisions when building enabling environments (the continuous maintenance and modernization of these development environments is itself its own distinct sub-discipline). So where to start and how to accelerate?

DoD Components should pursue a three-phase campaign plan to develop AI Ready Forces. This effort requires sustained attention and direction from senior leaders continuously setting expectations and incentives, driving progress, and holding people accountable. Rather than a linear plan that makes unrealistic projections, we embrace uncertainty and propose an iterative and adaptive planning cycle where the discoveries from each phase informs the decisions in the next.

### Phase 1: Learn and Set Conditions

DoD Components are all currently in Phase 1. The goal at this stage is to better understand how the four pillars (people, data, technological infrastructure, and organizational design) will come together to achieve positive mission impact consistently and at scale.

The Department is not starting from scratch. There are already established pathfinder pilots and initiatives in every Service and OSD. **More pilots may not be necessary or feasible given limited**

[7] The JAIC's Joint Common Foundation (JCF) represents an effort to build this common infrastructure. The success of this effort is a prerequisite of wider AI adoption.

**capital and human resources.** If Component leaders decide that more pilots are necessary, then DIB recommends they follow Recommendations #1 and #2 as a guide.

- AI Readiness Assessment Teams

  **Recommendation #1: Before initiating any new AI pathfinder pilots or initiatives, Component leaders should deploy AI Readiness Assessment Teams (AI-RATs) to examine potential focus areas and assess people, data, technological infrastructure, and organizational design readiness levels.**[8]

  The goal is to quickly assess what problem sets are suitable for AI applications and which are the most promising for pilots. Assessments should take no longer than 4-6 weeks. Team composition, at a minimum, should include data scientists, machine learning algorithm specialists, domain experts, and design specialists. Service Labs, UARCs, FFRDCs, and university and industry partners can offer important insights and technical expertise. The JAIC should oversee the development of an assessment scorecard to enable this process and encourage common rubrics that can translate between Components, when feasible.

- Pathfinder Pilots and Initiatives

  **Recommendation #2: Service Secretaries should, as deemed necessary, task the most appropriate senior agent to assign or identify pilot initiatives based on AI-RAT readiness assessments.**[9]

  Each pathfinder pilot or initiative should "learn by doing":

  - Make positive mission impact by building usable products
  - Capture best practices; experiment with workflows and processes
  - Identify people, data, technological infrastructure, and organizational design barriers

  Pathfinder teams should be of similar composition to AI-RATs, with greater involvement of domain experts and leaders in the host office or unit. Senior leaders overseeing the pilots will ensure

[8] A large complex organization without a long history in applied AI, such as DoD, must demonstrate proof of concept to mollify bureaucratic concerns that AI is too new and therefore too risky to embrace fully. Components should consider first deploying mature AI systems in low-risk environments, as this approach is likely to yield more favorable results and help DoD personnel learn how to manage and build on successful applied AI projects. This is one of the main reasons why the Joint AI Center's first projects focus on intelligence, surveillance, and reconnaissance (ISR); humanitarian assistance and disaster relief; and predictive maintenance. Each of these mission areas involve machine learning or computer vision techniques that have proven to be successful in non-DoD contexts and can be applied to DoD missions relatively smoothly. In addition, if AI in these cases "fails," the potential life or death ramifications are markedly lower than in higher-risk (i.e. combat) environments. Starting with these types of projects and learning from them not only informs Components' future work on applying less-mature AI to higher-risk DoD-specific situations, but also builds trust among commanders that AI will help them make better decisions.

[9] These pilots may be already existing projects such as National Mission Initiatives or Component Mission Initiatives.

necessary resources, waivers, and exceptions are available to enable success. Each pilot should be reviewed for renewal or cancellation after six months to ensure progress and accountability.

- Consolidated Lessons Learned

  **Recommendation #3: The JAIC, as DoD's AI Center of Excellence, should set up an online central community hub for all DoD AI programs to collaborate and share lessons learned.**

  DoD must intentionally learn from existing efforts and use a rigorous framework to translate that knowledge to remove barriers and reinforce positive developments. AI pathfinders will face many challenges, both technical and organizational, which they should document. These observations should be shared across the Department in the form of case studies. Components can make what adjustments and changes they can at their level, but changes requiring higher-level decisions will be consolidated by the JAIC to be addressed through appropriate mechanisms.

  The collection of AI lessons should ultimately be formalized, similar to the JCS Joint Lessons Learned Information System to continue to provide value over time.[10] Case studies demonstrating value to DoD can be used to build trust and demand.

- Talent Management

  **Recommendation #4: Establish an OSD Functional Community Manager for AI.**

  DoD's AI Strategy calls for the Department to cultivate a leading AI-ready workforce and to move quickly to operationalize its strategic guidance. The Department needs to ensure the alignment of DoD Component efforts with enterprise-level mandates and investments. DoD needs to assign an OSD Functional Community Manager to oversee the direction and development of the AI-ready workforce.

  **Recommendation #5: The Department should write an AI-ready workforce strategic plan, as it has done for the cyber workforce.[11]**

  Early on, DoD Components will not know their full personnel needs. The pathfinders will experiment and develop best practices for recruiting, hiring, training, and deploying teams. The Department should develop a comprehensive strategic workforce planning capability that baselines current workforce capability against desired future mission state, and then identifies and deploys appropriate strategies to close competency gaps, either through upskilling or external augmentation.

- Broad AI Education

  **Recommendation #6: The Secretary of Defense should develop a strategy for broad, multi-tier AI education across the Department and hold DoD Components accountable for its implementation.**

[10] https://www.jcs.mil/Doctrine/Joint-Lessons-Learned/

[11] The DoD Cyber Workforce plan is described in DoD Directive 8140.01: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001_2015_dodd.pdf

Shifting to an AI Ready Force will be challenging, as with any organizational change. Successfully managing change requires buy-in at all levels; understanding the changes and perceiving their value are critical contributors. A DoD-wide effort is needed to inculcate AI literacy at a level appropriate for each audience. There are broad and persistent misconceptions of what AI is and is not, and what AI can and cannot do. Foundational to using AI tools wisely will be teaching DoD leaders and personnel to understand the difference between well-structured, complicated problems in which AI will help us detect and act upon that structure, and complex/wicked problems - especially those sensitive to highly contingent social contexts and subjective value assessments - that inherently defy formal decomposition and quantitative analysis.

AI education will necessarily encompass related enabling technologies and practices such as cloud, data science, and modern software development. Just as critical will be AI ethics and risk management, given the central importance of ongoing research in and debates around AI safety, security, and resilience. Training in these areas for leaders at all levels will help set the necessary conditions to scale AI across the Department responsibly. DoD should expand immediate access to private vendors and universities that offer a host of technology training programs ranging from free to in-depth courses.[12] However, scaling basic technology training, and setting the use of these tools within specific DoD mission contexts, will require internal course development at the full gamut of DoD education institutions (service academies, National Defense University, etc.).

## Phase 2: Transition and Institutionalize

DoD Components have begun institutionalizing organizational changes in all four pillars, but have more road ahead of them than behind them. The discoveries and insights from Phase 1 will inform the decisions necessary in Phase 2. (For this reason, this paper does not include recommendations for Phase 2 and 3.) This sequencing also gives Components a longer runway to build sufficient expertise and infrastructure to accelerate progress.

- Create Talent Pipelines

  Each Component at this stage should be able to deploy a comprehensive AI-ready workforce strategy that sets clear guidance for personnel needs. Components should have informed estimates for the numbers, roles, and team composition, as well as how to recruit, hire, and train its AI-ready workforce. This analysis will inform the creation of talent pipelines (active duty, Reserve, and civilian career paths) and supporting training curriculums.

[12] The Air Force's Digital University is a new offering that will provide Airmen with best in class digital training from the same providers that Silicon Valley firms use to train their own talent. This investment will be key to upskilling our workforce and identifying latent talent in emerging skill areas such as DevSecOps, data science, and artificial intelligence. Further, we will use it as an amplifier to our computer language initiative to assess skills and aptitude and package courses into capability badges that will be eligible for bonus pay and considered for placements in the future.

- Address Organizational and Technical Barriers

  At this stage, sufficient pathfinder programs have been run to clearly identify existing barriers (legal, structural, procedural, data, technological, and organizational) and what actions are needed (informal guidance at the operational level, new DoD-wide policies, Congress changing laws, etc.). Components should be able to make significant progress in these areas and incorporating changes into standard operations.

- Expand AI Applications

  Phase 2 will see Components moving beyond isolated pathfinder programs into solutions that can scale to meet multiple mission needs and realize efficiencies through sharing common infrastructure, labeled data and data schemas, algorithms, software tooling, etc. Each Component has unique mission sets, but not unique technology components, as some applications will scale across the enterprise. The time and effort required to apply AI to new missions are significantly reduced. Data-driven decision-making starts becoming the expectation, rather than the exception. Leaders will becoming increasingly confident that AI programs can provide real value.

## Phase 3: Hone and Advance

DoD Components in this phase will demonstrate the capability and capacity to apply AI to new and existing missions. However, an AI Ready Force is never “done.” AI applications need to be monitored daily, be it data validity or algorithm retraining. Mature AI organizations seek continuous improvement and broader AI applications.

Achieving competitive advantage will require more than applying AI to our existing mission objectives and information workflows. AI will open the possibility for new concepts of operations for how we develop and deploy people and technology. Our current conception of how to train and fight will have to adapt to a future environment in which AI systems are abundant and military competition occurs at machine speed. DoD Components will need to creatively re-think potential strategies and use their AI pathfinder programs to experiment.

# The National Security Commission on AI (NSCAI)
# AI Workforce Model

The AI Workforce Model was developed by the NSCAI in partnership with the Defense Innovation Board and the Joint Artificial Intelligence Center. Their collaboration on the model does not extend to the remainder of the report. The material is based on more than 30 briefings with experts from AI-first companies, traditional companies that have successfully integrated AI, consulting groups, AI organizations within the government, and human resource and force structure experts within the government. The model and explanatory note also include information from AI and organizational theory discussed in business and academic literature.

## Table: AI Workforce Model for Federal Government[13]

| Build Consensus | | | Questions for Departments | |
|---|---|---|---|---|
| **WORKER ARCHETYPES** | **OUTPUT** | **CAPABILITIES (ETHICS THROUGHOUT)** | **TRAINING, EDUCATION, AND RECRUITMENT** | **ORGANIZATIONAL NEEDS AND COMPOSITION** |
| **AI EXPERT** | Leads the ethical design, development, and deployment of AI-driven technologies; oversees test and evaluation (verification and validation) to determine technology readiness; helps maintain and leverage supporting data architecture; translates requirements into capabilities; translates technical topics for senior leaders | Expert in data science, machine learning (e.g., deep learning), AI lifecycle, applied ethics and one or more of the following: natural language processing, computer vision, robotics, human-computer interfaces; human centered systems engineering; algorithmic and computational theory | How will the national security community train or recruit and integrate AI experts? | How many AI experts does the national security workforce need? Where should they be? Should they be uniformed, civilian, or contractors? |
| **AI DEVELOPER** | Data selection and preprocessing; model selection, training, and validation; partnership with domain knowledge experts and end users; discovery of local opportunities | Computational statistics and data science; programming (e.g. Python or R); model development using an ML library | Who trains developers for the national security workforce? When will they be identified and trained? | How many developers does the national security workforce need? Should they be uniformed, civilian, contractors, and/or contracted companies? |
| **DEPLOYMENT SPECIALIST** | Infrastructure installation and maintenance, review input/output sent by end-users, additions to training data sets, rough examination of training data sets, training/testing existing models, deployment | Hardware/software installation and maintenance, training data management, model verification/validation, algorithm deployment, data cleansing | Education equivalent to a technical certification offered by a military program or vocational training | How many AI technicians does the national security workforce need? Where should they be? |
| **END USER** | Daily business augmented/enabled by AI | Use of systems and apps | Normal systems training | Ubiquitous |
| **NON-TECHNICAL TACTICAL LEADER** | Gathers tactical requirements to guide the development of new AI-enabled capabilities, oversees deployment to ensure tactical requirements are met; partners with technicians, data engineers, and AI experts; leads normal | Tactical domain implementation expert, basic data collection and management, basic understanding of AI decision making within the context of use and the sources of failures and errors, ethics applied to | How will the national security community train and educate tactical leaders? How much do they need to know? | How many tactical leaders should the national security enterprise have? |

[13] Table developed by Commission staff.

| | | | | |
|---|---|---|---|---|
| | operations | tactical use | | |
| **NON-TECHNICAL STRATEGIC LEADER** | Oversees the creation of strategic and enterprise objectives, considers the ethics of new capabilities, oversees deployment and scaling, partnership with experts, developers, and tactical leaders; career management | Basics and ethics of AI lifecycle, strategic and enterprise expertise, tactical domain management, software development processes | When and where will leaders learn about AI? How much do they need to know? | How will leaders incentivize AI competence? How many leaders need to be competent, and at what point in their careers? |
| **SUPPORT ROLES** | Acquisition and contracting of AI hardware and software, services, and identification of commercial opportunities; legal support; legislative affairs, human resources, etc. | Understanding of software purchasing, data boundaries/limitations and rights; funding requirements; and compute purchases, identification of skill and qualifications of AI practitioners; legal and ethical aspects of development and deployment | When and where will support experts learn about AI? How much do they need to know? | What parts of the support workforce needs to learn about AI demands? |

Adopting a common workforce model will help the Department of Defense (DoD) approach AI workforce development with a common set of concepts, vocabulary, and understanding of the types of questions it needs to answer. This model describes different types of AI workers, their outputs, skills, training and education, and composition and disposition in the larger workforce. The model is meant to serve as a tool to guide the DoD's understanding of workforce needs, not as a set of recommendations for career fields.

The most important takeaway from this model is that building an AI workforce will require much more than highly educated, deep technical experts. The DoD must also develop non-technical leaders, deployment specialists, and end-users to effectively employ AI solutions across the force.

Ideally, the first three columns will be endorsed by consensus throughout the DoD and U.S. government:

- *Column 1: Worker Archetypes*. The model has seven worker archetypes that should be represented in an AI workforce.
- *Column 2: Output*. The output column describes what each category of worker will contribute.
- *Column 3: Capabilities*. The capabilities column lists critical, required knowledge and abilities.

The last two columns offer guiding questions for which each department and agency will likely have different answers based on different enterprise strategies and needs:

- *Column 4: Training/Education/Recruitment?* The education/training/recruitment column asks how the government will develop each type of worker.
- *Column 5: Organizational needs and composition?* The far right column, organizational needs and composition, asks how many of each type of worker the government will need, where they will be located within departments and agencies, and what percentage of them

will be uniformed, civilian, or contractors that work alongside government counterparts, or contracted companies that deliver a service.

### AI Worker Archetypes

Below, the archetypes shown in the model graphic are explained in more detail, including a non-exhaustive list of sub-archetypes with an example persona.

#### Technical Roles

- **AI experts** will lead the ethical design, development, and deployment of AI-driven technologies; translate requirements into capabilities; and help inform senior leaders. The greatest difference between AI developers and AI experts will be experts' ability to oversee testing and evaluation, an area that AI developer training may not support adequately enough to sufficiently minimize risk. AI experts are expected to have the educational, work, and research experience equivalent to a PhD.
    - Sub-archetypes: AI research engineer, AI software and systems architect, AI machine learning software engineer, cloud computing application architect, solution architect, machine learning engineer, human-centered systems engineer
    - Example job illustration:
        - AI research engineers focus on research and development of technologies that enable and advance semi and fully autonomous systems. They serve as algorithm experts with up-to-date knowledge of modern AI research and may be involved in the inception of ideas and drive the development cycles from research to testing of prototypes for a major project or component of a major project.
        - AI solution architects identify and collect data sources, analyze and extract key data and information, and evaluate and monitor data quality to meet the organization's information system needs and requirements.

- **AI Developers** will be data focused. They will be responsible for data cleaning, feature extraction and selection, and analysis; model training and tuning; partnerships with domain knowledge experts and end users; and the discovery of local opportunities for exploitation. Developers require less training and education than AI experts, and will have training, education, and/or experience that is roughly equivalent to an associates or bachelors degree; and that includes relevant ethics and bias mitigation in data processing and model training. Because they require less training than experts, there is more potential for the government to hire or internally train developers and to have them more widespread across the workforce. This allows the U.S. government to expand the pool of AI talent it selects and trains, placing less reliance on a small number of universities and private sector companies whose relationship with the national security enterprise may not always be relied upon.
    - Sub-archetypes: data engineer, data analyst, data administrator, software engineer.
    - Example job illustration:

        - Data engineers deliver full-stack data solutions across the entire data processing pipeline and rely on systems engineering principles to implement solutions that span the data lifecycle to collect, ingest, process, store, persist, access, and deliver data at scale and at speed. They have knowledge of local, distributed, and cloud-based technologies; data virtualization and smart caching; and all security and authentication mechanisms required to protect data.

- **Deployment Specialists** will be responsible for the installation and maintenance of the hardware/software that collects and processes data, the regular management of end user inputs and outputs, and management of data sets.  They will be the most common point of contact with technical expertise for end users.  They are strongly analogous to today's mechanics and IT specialists and technicians.
    - Sub-archetypes: AI hardware engineer, AI systems engineer.
    - Example job illustration:
        - AI hardware/software engineers serve as hardware experts for autonomous systems and work with other experts to provide the next generation of hardware/software solutions, including and not limited to sensing computer storage as well as controls and systems safety.  They support teams with the integration of hardware with software and systems, human-machine interface tests, and preparations of autonomous systems for certification and deployment.

<u>**Enablers**</u>

- **End users** will use AI-enabled systems during normal operations.  Their use of AI will strongly resemble the use of currently available software in that it will require some system specific training, but, with the exception of some positions that manage data, little to no AI specific expertise.  Most if not all members of the federal government will be end users.
    - Sub-archetypes: tracked vehicle mechanic, all-source intelligence analyst, F-35 pilot.

- **Non-technical tactical leaders** will serve as domain knowledge experts that help create the tactical requirements for AI systems, ensure the effective and ethical employment of AI systems, and partner with developers and experts.  Tactical leaders already exist in today's organization, such as the military's officer corps.  To become part of an effective AI workforce, they should be trained to understand the basics of data collection and management, AI decision making, and AI specific ethics.
    - Sub-archetypes: Battalion/squadron commander, program manager, senior intelligence analyst.

- **Non-technical strategic leaders** will oversee the creation of strategic and enterprise objectives, the deployment and scaling of new systems, and manage the careers of developers and experts.  All organizations need to train and certify their strategic leaders in areas such as the basics and ethics of the AI lifecycle and software development processes, in order to be able to interpret and trust output from AI-enabled decision support systems.

    - Sub-archetypes: Deputy Assistant Secretary of Defense, U.S. Central Command Commander, J7, Deputy Director of National Intelligence for Mission Integration.

- **Support roles** is the broadest category on the workforce model, and includes the support functions that are necessary to support AI development and employment. These include, but are not limited to acquisition officers who understand how to identify and purchase viable or modifiable commercial solutions and contracting officers who can negotiate service and development contracts that address traditionally troubled topics like data rights; human resource officers who understand how to leverage hiring authorities to quickly and less painfully hire talented developers and experts and the skills and qualifications of AI practitioners; legislative affairs personnel need to be able to explain AI funding requirements to members of Congress and their staff; and legal professionals need to understand the legal and ethical aspects of the entire AI development and deployment process.
    - Sub-archetypes: human resource specialist (classification/recruitment & placement), legislative fellow, staff judge advocate.