AI ACTION PLAN INPUT: ACHIEVING READINESS THROUGH A COMMUNITY-DRIVEN FRAMEWORK

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit association dedicated to advancing collaborative, public-private-academic approaches to intelligence and national security priorities. Through the application of industry expertise, leading-edge academic research, and commercial best practices, INSA seeks to make the Intelligence and National Security Community more effective and efficient. Our 175+ member organizations and 4,000+ individual and associate members include senior executives and intelligence experts in the public, private, and academic sectors.

INSA is pleased to provide the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO) our perspectives and input to the nation's AI Action Plan. As an organization, INSA is in a unique position representing 175+ public/private organizations that have ongoing interest and activities with regards to our Intelligence Agencies, Labs and Departments providing critical technology in support of the country's national security. Based on collective input and interactions across the community our input focuses on a plan that operationalizes three critical innovation pillars. Building on INSA's 2024 workforce transformation findings[1] and 2023 cyber partnership white papers[2], this roadmap demonstrates how our member ecosystem – spanning across large national security strategists and small, emerging technology firms - can accelerate implementation through existing collaboration frameworks.

Our recommendations focus on:

- Rigor and thoughtfulness in assessment and inventory of capabilities with an emphasis on interoperability.
- Investment in national-level skills development and enhancement.
- Increased prioritization on public-private partnerships focused on IP generation and innovation through a scalable commercialization framework.

[1] https://www.insaonline.org/detail-pages/news/2024/10/29/insf-future-of-the-ic-workforce-technology-and-talent-transformation
[2] https://www.insaonline.org/detail-pages/news/2023/12/04/new-video-highlighting-the-importance-of-osint

1. National Model Inventory & Interoperability Ecosystem

1.1 An Inventory and Assessment Process

The collective experience over the past several years has demonstrated the gaps in assessing, documenting and sharing the inventory of tools, models and integrated capabilities in use or available. A concerted effort must be taken to bring together a wide swath of data, normalizing where possible against standardized data collection such as Model Cards, and making these data available across key sectors and across public and vetted private industry entities.

1.2 Federated Model Registry Architecture

A unified national registry must adopt a *modular architecture* to enable decentralized governance while maintaining interoperability. Drawing lessons from the Department of Energy's National Laboratory system, regional nodes could operate under shared standards while tailoring implementations to sector-specific needs—healthcare models at NIH-funded facilities, defense systems at DoD testbeds, and civil infrastructure tools at NSF AI Institutes. Each node would enforce standardized metadata requirements, including training data lineage tracked via blockchain (leveraging prototypes from the FDA's DSCSA pharmaceutical traceability system) and ethical risk assessments using frameworks like the NIST AI RMF 1.0. API-first design principles would mandate OpenAPI standards compliance. In order to effectively develop an ecosystem that is modular yet responsive to unique needs of any one agency or industry, international standards and approaches to interoperate model standards need to be developed fundamentally built upon the concept of decentralization.

Implementation could prioritize phased adoption: initially at innovation accelerators and funded R&D centers (FFRDCs), followed by incentives tied to federal contracting preferences. Mirroring the CHIPS Act's success, companies achieving 90% model card completeness and API availability could qualify for accelerated SBIR/STTR grant reviews, while defense contractors might receive priority consideration in RFPs for Joint All-Domain Command and Control (JADC2) programs.

2. Dynamic Skills Ecosystem Development

2.1 National Skills Topography Mapping

A skills mapping initiative would combine traditional workforce analytics with emergent competency tracking. Competency mapping in AI needs to assess math and software development skills as well as promoter and coaching skills. Mapping skills is paramount to assessing opportunities to reskill and advance our workforce and should be done utilizing AI in conjunction with traditional hard and soft skills analysis. Expert concentration could be identified through machine learning analysis of data such as patent filings, academic citations and degrees, and industry collaboration patterns. Advocate networks might be mapped using natural language processing (NLP) applied to conference proceedings and policy white papers, and identifying key influencers and research leaders. Competency benchmarks could tier skills from foundational (e.g., Python for data analysis) to advanced (e.g., adversarial ML techniques), validated against existing and emergent standards. To identify risk-takers, the system could analyze startups, grant and SBIR proposals and innovation-oriented projects such as Defense Innovation Unit (DIU) project portfolios and the broader startup landscape for patterns of exploratory R&D, creating a “risk propensity index” to assess entities (individuals and companies) modeled after DARPA’s Heilmeier Catechism evaluation framework.

2.2 Next-Gen Training Infrastructure

AI MakerSpaces would blend physical and virtual environments, with regional hubs co-located with major academic institutions taking inspiration from NSA’s Centers for Excellence approach. Physical locations might feature quantum computing testbeds (for example using DOE’s Oak Ridge infrastructure) and robotics labs (adapting NASA’s Swarmathon platform[3]), while virtual environments could offer pre-configured Jupyter notebooks with accessible sample data such as US Census Bureau microdata, NOAA climate datasets or FDA drug shortage data. Curriculum could emphasize creative problem-solving through challenge-based learning—for example, having high school or college teams optimize wildfire prediction models develop supply chain resilience algorithms with an emphasis on develop new models or techniques that have not been explored yet. Continuous assessment could employ adaptive testing engines like the Army’s Machine Learning Certainty & Competence Framework[4], providing real-time skill gap analysis to educators and employers. The goal of such centers should be focus on coalescing, creating and making available a range of training aimed at “leveling-up” our collective ability to use, develop, enhance or partner with any class of AI algorithms while understanding and managing risk.

[3] https://swarmathon.cs.unm.edu/
[4] https://github.com/ACI-ICSARL/CandC_Framework

3. Adaptive Consortium Network

A collaborative approach needs to be designed to foster public-private institutions charted to advance the collective growth of IP and trade secret across AI.

3.1 Consortium Design Principles

Public-private consortia must balance agility with accountability. Member-driven collaboration leveraging organizations such as INSA could enable collaboration and collective prioritization of R&D objectives. In order to compete against pacing threats, we recommend to AI consortia to adhere to three major objectives:

1. Foster and support increased invention and patents
2. Develop and publish findings based on AI experimentation and independent testing
3. Manage community-based vetted subject matter experts (SMEs)

To foster experimentation, consortia might establish “sandbox” environments paired with synthetic data and sample operational data. Risk assessment would integrate red-teaming methodologies from cybersecurity (MITRE ATT&CK framework) with ethical AI evaluation tools, creating standardized playbooks for adversarial testing. Services and resources could be provided through these consortia consisting of experts and lawyers to provide tactical assistance with development of materials to support the patent application process. Developing the processes, governance and funding mechanisms to support a community and consortia-driven ecosystem with a fundamental charter to grow the national patent and trade secret basis is fundamental to keeping up with and surpassing PRC. Matchmaking across a collection of experts can foster faster reduction to practice and enable rapid use of new technology as quickly as possible.

3.2 Red Team Exchange Program

A national red team corps, modeled after the FBI’s Cyber Action Teams[5], could conduct biannual stress tests of critical AI systems. Defense-focused teams might challenge operational systems such as JADC2 decision-support algorithms using tactics observed in Ukraine’s electronic warfare operations, while civilian teams could probe hospital predictive staffing models against synthetic pandemic scenarios. Evaluations could employ crowdsourced scoring, adapting the “Hack the Pentagon” methodology[6], with monetary bounties scaled using the Department of the Treasury’s software vulnerability severity framework.

[5] https://www.fbi.gov/news/stories/meet-the-cyber-action-team
[6] https://hackthepentagon.mil/

3.3 Licensing and Commercialization Playbook

Also leveraging the consortia, the Federal Government can develop licensing pathways that can provide a beneficial mechanism for government and commercial interests. Several organizations ranging from DARPA to National Labs have commercialization strategies.[7] However these activities are underutilized and do not provide sustained strategic value. Under the AI Action Plan, a novel AI-focused commercialization framework could be developed and deployed that allows for rapid development of capabilities under federal funding and with Government Purpose Rights (GPR) allowing for royalty escrow, and providing commercial license grants to companies to deploy capabilities in commercial markets. Selected consortia would focus on developing the commercialization pathways and incentive mechanisms (to include tax credits) to meet security and governance needs to protect national security while advancing capabilities.

[7] https://www.energy.gov/eere/solar/technology-commercialization-fund