NSCAI FINAL REPORT RECOMMENDATIONS, DRAFT

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

PART I: DEFENDING AMERICA IN THE AI ERA

Chapter 1 – Emerging Threats in the AI Era
- Create a Joint Interagency Task Force (JIATF) and Operations Center
- Coordinate government-wide challenges to detect and attribute AI-enabled malign information campaigns and to authenticate digital media
- Develop policies that treat data security as national security
- Develop and deploy AI-enabled defenses against cyber attacks
- Create a National AI Assurance Framework
- Create dedicated red teams for adversarial testing
- Increase the profile of biosecurity and biotechnology issues within U.S. national security agencies

Chapter 2 – Foundations of Future Defense
- Build the technical backbone
- Train and educate warfighters
- Accelerate the adoption of existing digital technologies
- Democratize AI development
- Invest in next generation capabilities

Chapter 3 – AI and Warfare
- Promote AI interoperability and the adoption of critical emerging technologies among allies and partners
- Drive organizational reforms through innovative leadership
- Design imaginative warfighting concepts to inform the development of AI-enabled capabilities
- By the end of 2021, establish AI-readiness performance goals
- Set the conditions to continuously out-innovate competitors
- Define a joint warfighting network architecture by the end of 2021
- Invest in priority AI research and development (R&D) areas that could support future military capabilities

Chapter 4 – Autonomous Weapon Systems & Risks Associated with AI-Enabled Warfare
- Clearly and publicly affirm existing U.S. policy that only human beings can authorize employment of nuclear weapons, and seek similar commitments from Russia and China
- Discuss AI's impact on crisis stability in the existing US-Russia Strategic Security Dialogue and create an equivalent dialogue with China
- Work with allies to develop international standards of practice for the development, testing, and use of AI-enabled and autonomous weapon systems
- Pursue technical means to verify compliance with future AI arms control agreements
- Fund research on technical means to prevent proliferation of AI-enabled and autonomous weapon systems

Chapter 5 – AI and the Future of National Intelligence
- Change risk management practices to accelerate new technology adoption
- Empower the IC's science and technology leadership
- Improve coordination and interoperability between the IC and DoD
- Capitalize on AI-enabled analysis of open source and publicly available information
- Prioritize and accelerate collection of scientific and technical intelligence to better understand adversary capabilities and intentions
- To recruit more science and technology experts into the IC, aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC
- Advance and continue to build out a purpose-built IC Information Technology Environment that can fuse intelligence from different domains and sources
- Embrace fused, predictive analysis as the new standard
- Develop innovative human-centric approaches to human-machine teaming

Chapter 6 – Technical Talent in Government
- Create a Digital Corps
- Establish a Civilian National Reserve Digital Corps
- Streamline the hiring process and expand digital talent pipelines
- Establish a United States Digital Service Academy
- Establish new digital career fields
- Expand access to tools, data sets, and infrastructure

Chapter 7 – Establishing Justified Confidence in AI Systems
- Focus more federal R&D investments on advancing AI security and robustness
- Consult interdisciplinary groups of experts to conduct risk assessments, improve documentation practices, and build overall system architectures to limit the worst-case consequences of system failure
- Pursue a sustained, multi-disciplinary initiative through national security research labs to enhance human-AI teaming
- Clarify policies on human roles and functions, develop designs that optimize human-machine interaction, and provide ongoing and organization-wide AI training
- DoD should adopt a sweeping package of testing evaluation processes, methods, and resources for AI systems
- NIST should provide and regularly refresh a set of standards, performance metrics, and tools for qualified confidence in AI models, data, and training environments, and predicted outcomes
- Appoint a full-time, senior-level Responsible AI Lead in each national security agency and each branch of the armed services
- Create a standing body of multi-disciplinary experts in the National AI Initiative Office
- Adapt and extend existing accountability policies to cover the full lifecycle of AI systems and their components
- Establish policies that allow individuals to raise concerns about irresponsible AI development, and institute comprehensive oversight and enforcement practices

Chapter 8 – Upholding Democratic Values
- Invest in and adopt AI tools to enhance oversight and auditing in support of privacy and civil liberties
- Improve public transparency about how the government uses AI
- Develop and test systems with the goal of advancing privacy preservation and fairness
- Strengthen the ability of those impacted by government actions involving AI to seek redress and have due process
- Strengthen oversight mechanisms to address current and evolving concerns

PART II: WINNING THE TECHNOLOGY COMPETITION

Chapter 9 – A Strategy for Competition and Cooperation
- Create a Technology Competitiveness Council
- Develop a National Technology Strategy
- Establish a high-level U.S.-China Comprehensive Science & Technology Dialogue

Chapter 10 – The Talent Competition
- Pass the National Defense Education Act II
- Strengthen AI Talent Through Immigration
- Broaden the scope of "extraordinary" talent to make the O-1 visa more accessible and emphasize AI talent
- Implement and advertise the international entrepreneur rule
- Expand and clarify job portability for highly skilled workers
- Recapture green cards lost to bureaucratic error
- Grant green cards to students graduating with STEM PhDs from accredited American universities
- Double the number of employment based green cards
- Create an entrepreneur visa
- Create an emerging and disruptive technology visa

Chapter 11 – Accelerating AI Innovation
- Scale and coordinate federal AI R&D funding
- Expand access to AI resources through a National AI Research Infrastructure
- Leverage both sides of the public-private partnership
- Tackle some of humanity's biggest challenges

Chapter 12 – Intellectual Property
- Develop and implement national Intellectual Property policies to incentivize, expand, and protect AI and emerging technologies

Chapter 13 – Microelectronics
- Implement the National Microelectronics Strategy
- Revitalize domestic microelectronics fabrication
- Double-down on federally funded microelectronics research

Chapter 14 – Technology Protection
- Clarify U.S. technology protection principles and build regulatory capacity to implement ECRA and FIRRMA
- Require companies to disclose investments in AI and other sensitive technologies to CFIUS
- Utilize targeted export controls on key semiconductor manufacturing equipment
- Align the export control policies of the United States, the Netherlands, and Japan regarding SME
- Utilize targeted end-use export controls and reporting requirements to prevent use of high-end U.S. AI Chips in human rights violations
- Build capacity to protect the integrity of the U.S. research environment
- Coordinate research protection efforts internationally with allies and partners
- Bolster cybersecurity support for research institutions
- Counter foreign talent recruitment programs
- Strengthen visa vetting to limit problematic research collaborations

Chapter 15 – A Favorable International Technology Order
- Develop and implement an International Science and Technology Strategy
- Build an Emerging Technology Coalition
- Launch an International Digital Democracy Initiative (IDDI)
- Implement a comprehensive U.S. national plan to support international technology efforts
- Enhance the United States' position as an international emerging technology research hub
- Reorient U.S. foreign policy and the Department of State for great power competition in the Digital Age

Chapter 16 – Associated Technologies
- Define and prioritize the key emerging technologies that are needed to ensure U.S. national competitiveness
- Prioritize the development of an advanced biotechnology manufacturing ecosystem
- Transition quantum computing basic research to national security applications and incentivize domestic quantum fabrication
- Bolster and accelerate U.S. 5G network deployment through mid-band spectrum sharing
- Incentivize the development of world-class software platforms for robotic and autonomous systems
- Accelerate additive manufacturing production of legacy parts across the Department of Defense
- Develop and domestically manufacture energy storage technologies to meet U.S. market demand by 2030

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

FINAL REPORT: **KEY JUDGMENTS IN THE INTRODUCTION**

WHY DOES AI MATTER?

- AI is ubiquitous in everyday life.
- Deploying and adopting AI remains a hard problem.
- AI tools are diffusing broadly and rapidly.
- AI is changing relationships between humans and machines.

PART I - DEFENDING AMERICA IN THE AI-ERA.

1. AI is the quintessential "dual use" technology—it can be used for civilian and military purposes.
2. We can expect the large-scale proliferation of AI-enabled capabilities.
3. AI-enabled capabilities will be tools of first resort in a new era of conflict.
4. AI will transform all aspects of military affairs.
5. Competitors are actively developing AI concepts and technologies for military use.
6. AI will revolutionize the practice of intelligence.
7. Defending against AI-capable adversaries without employing AI is an invitation to disaster.
8. Compelling logic dictates quick, but careful and responsible AI adoption.
9. There is an emerging consensus on principles for using AI responsibly in the defense and intelligence communities.
10. The U.S. government still operates at human speed not machine speed.

PART II - WINNING THE TECHNOLOGY COMPETITION.

1. China is organized, resourced, and determined to win the technology competition.
2. Advancements in AI are contributing to a broad platform technology competition in e-commerce, search engines, social media, and much else.
3. The AI competition is complicated by deep interconnections.
4. The United States retains advantages in critical areas, but trends are worrisome.
5. The U.S. government must take a hands-on approach to national technology competitiveness.
6. The AI competition will require White House leadership.

AI FOR WHAT ENDS? TECHNOLOGY AND VALUES.

1. The U.S. government should develop and field AI-enabled technologies with adequate transparency, strong oversight, and accountability to protect against misuse.
2. The United States must lead a coalition of democracies.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 1: EMERGING THREATS IN THE AI ERA

The U.S. government is not prepared to defend the United States in the coming AI era. AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state adversaries to exploit vulnerabilities in our open society.

THREAT 1: AI-ENABLED INFORMATION OPERATIONS

- **CREATE A JOINT INTERAGENCY TASK FORCE (JIATF) AND OPERATIONS CENTER**
- **COORDINATE GOVERNMENT-WIDE CHALLENGES TO DETECT AND ATTRIBUTE AI-ENABLED MALIGN INFORMATION CAMPAIGNS AND TO AUTHENTICATE DIGITAL MEDIA.**

THREAT 2: DATA HARVESTING & TARGETING OF INDIVIDUALS

- **DEVELOP POLICIES THAT TREAT DATA SECURITY AS NATIONAL SECURITY IN THREE AREAS:**
  1. The government must ensure that a security development lifecycle approach for its own AI systems is in place
  2. The government should ensure that data privacy and security are priority considerations
  3. National efforts to legislate and regulate data protection and privacy must integrate national security considerations

THREAT 3: ACCELERATED CYBER ATTACKS

- **DEVELOP AND DEPLOY AI-ENABLED DEFENSES AGAINST CYBER ATTACKS. THE GOVERNMENT NEEDS TO:**
  - Purchase the requisite sensors and instrumentation needed to train AI systems
  - Develop more effective AI-enabled cyber defenses with large, instrumented, and realistic testing.
  - Ensure the robustness of these defenses
  - Deploy AI-enabled cyber defenses
  - Accelerate the establishment of a Joint Cyber Planning and Operations Center

THREAT 4: ADVERSARIAL AI

- **CREATE A NATIONAL AI ASSURANCE FRAMEWORK**
- **CREATE DEDICATED RED TEAMS FOR ADVERSARIAL TESTING**

THREAT 5: AI-ENABLED BIOTECHNOLOGIES

- **INCREASE THE PROFILE OF BIOSECURITY AND BIOTECHNOLOGY ISSUES WITHIN U.S. NATIONAL SECURITY AGENCIES**

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 2: **FOUNDATIONS OF FUTURE DEFENSE**

The Department of Defense (DoD) must set an ambitious goal. By 2025, the foundations for widespread integration of AI across DoD must be in place.

BUILD THE TECHNICAL BACKBONE

- Establish a DoD-wide AI Ecosystem

TRAIN AND EDUCATE WARFIGHTERS

- Identify service members who excel at computational thinking during the accession process;
- Invest in upskilling its workforce through self-guided education courses and coding language incentives;
- Teach junior leaders about problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making as part of their pre-commissioning requirements and initial training;
- Integrate emerging and disruptive technology training into professional military education courses; and
- Create emerging technology coded billets and an emerging technology certification program comparable to the joint billet and qualification system.

ACCELERATE THE ADOPTION OF EXISTING DIGITAL TECHNOLOGIES

- Integrate commercial AI to optimize core business processes.
- Network digital innovation initiatives to scale impact.
- Expand use of specialized acquisition pathways and contracting approaches.
- Update the budget and oversight processes.

DEMOCRATIZE AI DEVELOPMENT

- Designate the Joint AI Center (JAIC) as the Department's AI Accelerator.
- Establish software teams at each Combatant Command.

INVEST IN NEXT GENERATION CAPABILITIES

- Fund AI research and development (R&D).
- Retire legacy systems ill-equipped to compete in AI-enabled warfare.
- Produce a technology annex to National Defense Strategy (NDS).

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 3: AI AND WARFARE

Even with the right AI-ready technology foundations in place, the U.S. military will still be at a battlefield disadvantage if it fails to adopt the right concepts and operations to employ AI.

2025: AI-READY DoD

Warfighters enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in training, exercises, and operations. Preparing for an AI-Ready 2025 demands the following actions:

INNOVATIVE LEADERSHIP

- Establish high-level Steering Committee on Emerging Technology.
- Ensure JAIC Director remains a 3-star general or flag officer with significant operational experience who reports directly to Secretary of Defense or Deputy Secretary of Defense.
- Appoint the Under Secretary of Defense for Research and Engineering as the co-chair and chief science advisor to the Joint Requirements Oversight Council.
- Assign an AI Operational Advocate on every Combatant Command staff.

CONTINUOUSLY OUT-INNOVATE

- Set the conditions to continuously out-innovate competitors

ADVANCED TECHNOLOGIES AND R&D

- Define a joint warfighting network architecture by the end of 2021
- Invest in priority AI research and development areas that could support future military capabilities

IMAGINATIVE CONCEPTS

- Design imaginative warfighting concepts to inform the development of AI-enabled capabilities

STRONGER TOGETHER

- Promote AI interoperability and the adoption of critical emerging technologies among allies and partners, including the Five Eyes, the North Atlantic Treaty Organization (NATO), and across the Indo-Pacific.

AI READINESS

- Direct DoD components to assess military AI-readiness through existing readiness management forums and processes.
- Direct the military services to accelerate review of specific skill gaps in AI, in order to inform recruitment and talent management strategies.
- Direct the military services to accelerate use of AI in predictive analytics for maintenance and supply chain to optimize equipment and parts.
- Direct the military services, in coordination with the Defense Logistics Agency and Joint Staff J-4, to prioritize integration of AI into logistics systems wherever possible.
- Integrate AI into major wargames and exercises to promote field-to-learn approaches to technology adoption.
- Incentivize experimentation with AI-enabled applications through the Warfighting Lab Incentive Fund.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 4: AUTONOMOUS WEAPON SYSTEMS & RISKS ASSOCIATED WITH AI-ENABLED WARFARE

The United States must take steps, including with allies and competitors, to mitigate strategic risks posed by AI-enabled and autonomous weapon systems.

	STRATEGIC RISKS OF AI-ENABLED WEAPONS	RECOMMENDATIONS	OBJECTIVES
US ACTIONS	Nation states could allow AI to authorize employment of key strategic weapon systems.	**CLEARLY AND PUBLICLY AFFIRM EXISTING U.S. POLICY THAT ONLY HUMAN BEINGS CAN AUTHORIZE EMPLOYMENT OF NUCLEAR WEAPONS.**	Prevent unintended nuclear conflict due to AI-enabled launch authorization. Obtain similar commitments from Russia & China.
US ACTIONS	Global, unregulated proliferation of AI-enabled weapons.	**FUND TECHNICAL MEANS TO VERIFY COMPLIANCE WITH FUTURE AI ARMS CONTROL AGREEMENTS, AND PREVENT PROLIFERATION OF AI-ENABLED WEAPON SYSTEMS.**	Develop means to prevent proliferation of AI-enabled weapons and potentially shared them with Russia and China
US ACTIONS WITH ALLIES	Poorly designed or improperly utilized AI-enabled weapons could behave unpredictably.	**DEVELOP INTERNATIONAL STANDARDS OF PRACTICE FOR THE DEVELOPMENT AND USE OF AI-ENABLED AND AUTONOMOUS WEAPON SYSTEMS.**	Set international norms guiding responsible development and use of AI-enabled and autonomous weapon systems.
US ACTIONS WITH RUSSIA & CHINA	AI-enabled systems could cause inadvertent conflict escalation.	**DISCUSS AI'S IMPACT ON CRISIS STABILITY IN THE EXISTING U.S.-RUSSIA STRATEGIC SECURITY DIALOGUE AND CREATE AN EQUIVALENT DIALOGUE WITH CHINA.**	Improve understanding of doctrine and develop confidence building measures regarding use of AI-enabled and autonomous weapon systems.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 5: **AI AND THE FUTURE OF NATIONAL INTELLIGENCE**

Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission.

2025: AI-READY INTELLIGENCE

Intelligence professionals enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in each stage of the intelligence cycle. Preparing for an AI-Ready 2025 demands the following actions:

- **CHANGE RISK MANAGEMENT PRACTICES TO ACCELERATE NEW TECHNOLOGY ADOPTION.**
- **EMPOWER THE IC'S SCIENCE AND TECHNOLOGY LEADERSHIP.**
- **IMPROVE COORDINATION AND INTEROPERABILITY BETWEEN THE IC / DOD.**
- **CAPITALIZE ON AI-ENABLED ANALYSIS OF OPEN SOURCE AND PUBLICLY AVAILABLE INFORMATION.**
- **PRIORITIZE AND ACCELERATE COLLECTION OF SCIENTIFIC AND TECHNICAL INTELLIGENCE TO BETTER UNDERSTAND ADVERSARY CAPABILITIES AND INTENTIONS.**
- **TO RECRUIT MORE SCIENCE AND TECHNOLOGY EXPERTS INTO THE IC, PURSUE SECURITY CLEARANCE REFORM FOR THE TOP SECRET LEVEL AND ABOVE, AND ENFORCE SECURITY CLEARANCE RECIPROCITY AMONG MEMBERS OF THE IC.**

2030: AI-ENABLED INTELLIGENCE

The IC should rely on a continuous pipeline of all-domain/all-source intelligence analysis processed through a federated architecture of continually-learning analytic engines. An AI-Enabled 2030 will require:

- **ADVANCE AND CONTINUE TO BUILD OUT A PURPOSE-BUILT IC INFORMATION TECHNOLOGY ENVIRONMENT THAT CAN FUSE INTELLIGENCE FROM DIFFERENT DOMAINS AND SOURCES.**
- **EMBRACE FUSED, PREDICTIVE ANALYSIS AS THE NEW STANDARD.**
- **DEVELOP INNOVATIVE HUMAN-CENTRIC APPROACHES TO HUMAN-MACHINE TEAMING.**

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 6: TECHNICAL TALENT IN GOVERNMENT

The United States government needs digital experts now or it will remain unprepared to buy, build, and use AI and its associated technologies.

ORGANIZE

CREATE AGENCY-SPECIFIC DIGITAL CORPS

Organize the Government's Technical Workforce to:

- Recruit, train, and educate personnel
- Place personnel in and remove from digital workforce billets
- Manage digital careers
- Set standards for digital workforce qualifications

Career Field Examples:
Software Development, Data Science, Artificial Intelligence, DevOps and Site Reliability Engineering, Human-Centered Product Design, Product Management, Security, Data Governance and Use, and Emerging Technologies

RECRUIT

CREATE CIVILIAN NATIONAL RESERVE DIGITAL CORPS

- Modeled after military reserves service commitments and incentive structure
- Members would become civilian special government employees (SGEs) and work at least 38 days a year as short-term advisors, instructors, or developers across the government.

STREAMLINE HIRING PROCESS AND EXPAND PIPELINES

- Create Digital Talent Recruiting Offices Aligned with the Digital Corps
- Grant Exemption from OPM General Schedule Policies for Specific Billets and Position Descriptions
- Expand CyberCorps: Scholarship for Service
- Establish a STEM Corps

BUILD

"The United States Digital Service Academy's mission is to develop, educate, train, and inspire digital technology leaders and innovators and imbue them with the highest ideals of duty, honor, and service to the United States of America in order to prepare them to lead in service to our nation."

ESTABLISH UNITED STATES DIGITAL SERVICE ACADEMY

- Accredited, degree-granting university designed to meet the whole of government's needs for digital expertise in AI and related subjects.
- Independent entity within the United States Government.

EMPLOY

ESTABLISH NEW DIGITAL CAREER FIELDS

- Software Development
- Software Engineering
- Data Science
- Knowledge Management
- Artificial Intelligence
- + Military Digital Career Fields

EXPAND ACCESS TO WORLD-CLASS TOOLS, DATA SETS, & INFRASTRUCTURE

- To perform meaningful work in government, employees within the digital workforce need access to enterprise-level software capabilities at par with those found in the private sector.
- Such as: software engineering tools, access to software libraries, open-source support, and infrastructure for large-scale collaboration

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 7: ESTABLISHING JUSTIFIED CONFIDENCE IN AI SYSTEMS

Artificial intelligence (AI) systems must be developed and fielded with justified confidence. The recommendations cover five issue areas:

ROBUST AND RELIABLE AI

- FOCUS MORE FEDERAL RESEARCH AND DEVELOPMENT (R&D) INVESTMENTS ON ADVANCING AI SECURITY AND ROBUSTNESS.
- CONSULT INTERDISCIPLINARY GROUPS OF EXPERTS TO CONDUCT RISK ASSESSMENTS, IMPROVE DOCUMENTATION PRACTICES, AND BUILD OVERALL SYSTEM ARCHITECTURES TO LIMIT THE WORST-CASE CONSEQUENCES OF SYSTEM FAILURE.

TESTING AND EVALUATION, VERIFICATION, AND VALIDATION (TEVV)

- DOD SHOULD ADOPT A SWEEPING PACKAGE OF TESTING AND EVALUATION PROCESSES, METHODS, AND RESOURCES FOR AI SYSTEMS.
- NIST SHOULD PROVIDE A SET OF STANDARDS, PERFORMANCE METRICS, AND TOOLS FOR QUALIFIED CONFIDENCE IN AI MODELS, DATA, AND TRAINING ENVIRONMENTS, AND PREDICTED OUTCOMES.

HUMAN-AI INTERACTION AND TEAMING

- PURSUE A SUSTAINED, MULTI-DISCIPLINARY INITIATIVE THROUGH NATIONAL SECURITY RESEARCH LABS TO ENHANCE HUMAN-AI TEAMING.
- CLARIFY POLICIES ON HUMAN ROLES AND FUNCTIONS, DEVELOP DESIGNS THAT OPTIMIZE HUMAN-MACHINE INTERACTION, AND PROVIDE ONGOING AND ORGANIZATION-WIDE AI TRAINING.

LEADERSHIP

- APPOINT A FULL-TIME, SENIOR-LEVEL RESPONSIBLE AI LEAD IN EACH NATIONAL SECURITY AGENCY AND EACH BRANCH OF THE ARMED SERVICES.
- CREATE A STANDING BODY OF MULTI-DISCIPLINARY EXPERTS IN THE NATIONAL AI INITIATIVE OFFICE.

ACCOUNTABILITY AND GOVERNANCE

- ADAPT AND EXTEND EXISTING ACCOUNTABILITY POLICIES TO COVER THE FULL LIFECYCLE OF AI SYSTEMS AND THEIR COMPONENTS.
- ESTABLISH POLICIES THAT ALLOW INDIVIDUALS TO RAISE CONCERNS ABOUT IRRESPONSIBLE AI DEVELOPMENT, AND INSTITUTE COMPREHENSIVE OVERSIGHT AND ENFORCEMENT PRACTICES.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 8: UPHOLDING DEMOCRATIC VALUES: PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS IN USES OF AI FOR NATIONAL SECURITY

With new models of techno-authoritarian governance gaining traction abroad, the United States must continue to serve as a beacon of democratic values.

INVEST IN AND ADOPT AI TOOLS TO ENHANCE OVERSIGHT AND AUDITING IN SUPPORT OF PRIVACY AND CIVIL LIBERTIES.

IMPROVE PUBLIC TRANSPARENCY ABOUT HOW THE GOVERNMENT USES AI.

DEVELOP AND TEST SYSTEMS WITH THE GOAL OF ADVANCING PRIVACY PRESERVATION AND FAIRNESS.

- Assess risks in the design, development, and testing of AI systems.
- Identify an office, committee, or team in each agency that can conduct a pre-deployment review of AI technologies that will impact privacy, civil liberties, and civil rights.
- Establish third-party testing centers for national security-related AI systems that could impact U.S. persons.

STRENGTHEN THE ABILITY OF THOSE IMPACTED BY GOVERNMENT ACTIONS INVOLVING AI TO SEEK REDRESS AND HAVE DUE PROCESS.

- Review DHS and FBI policies and practices that may impact due process and the ability to seek redress.
- Issue Attorney General guidance on AI and due process.

STRENGTHEN OVERSIGHT MECHANISMS TO ADDRESS CURRENT AND EVOLVING CONCERNS.

- Establish a task force to assess the privacy and civil liberties implications of AI and emerging technologies.
- Strengthen the ability of the Privacy and Civil Liberties Oversight Board to provide meaningful oversight and advice on AI use for national security.
- Empower DHS Offices of Privacy and Civil Rights and Civil Liberties.
- Require stronger coordination and alignment among federal oversight and audit organizations.

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 9: **A STRATEGY FOR COMPETITION AND COOPERATION**

The Commission is urging a government-led process to restore a more balanced equilibrium between government, industry, and academia that ensures a diverse research environment, competitive economy, and the sustainment of a research agenda that supports the needs of the nation.

CREATE A TECHNOLOGY COMPETITIVENESS COUNCIL

VICE PRESIDENT

+

ASSISTANT TO THE PRESIDENT FOR TECH COMPETITIVENESS

EOP LEADERS AND CABINET SECRETARIES

- Reconcile Security, Economic, and Scientific Priorities; and
- Elevate Technology Policy Concerns from Technical to Strategic

DEVELOP A NATIONAL TECHNOLOGY STRATEGY

The Strategy should build upon the following pillars:

I. **WINNING THE AI TALENT COMPETITION**

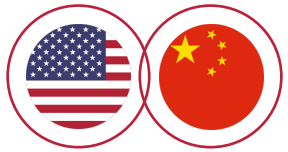
II. **PROMOTING AMERICAN AI INNOVATION**

III. **PROTECTING US AI ADVANTAGES**

IV. **LEADING A FAVORABLE INTERNATIONAL AI ORDER**

ESTABLISH A HIGH-LEVEL US-CHINA COMPREHENSIVE SCIENCE & TECHNOLOGY DIALOGUE (CSTD)

- Identify targeted areas of cooperation on emerging technologies
- Provide a forum to air a discrete set of concerns around specific uses of emerging technologies



NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 10: THE TALENT COMPETITION

The United States is in a global competition for scarce artificial intelligence (AI) and science, technology, engineering, and mathematics (STEM) talent. The United States needs to invest in all AI talent pipelines in order to remain at the forefront of AI now and into the future.

PASS NATIONAL DEFENSE EDUCATION ACT II

- NDEA II would focus on funding students acquiring digital skills, like mathematics, computer science, information science, data science, and statistics.

STRENGTHEN AI TALENT THROUGH IMMIGRATION

- **BROADEN THE SCOPE OF "EXTRAORDINARY" TALENT TO MAKE THE O-1 VISA MORE ACCESSIBLE AND EMPHASIZE AI TALENT.**
- **IMPLEMENT AND ADVERTISE THE INTERNATIONAL ENTREPRENEUR RULE.**
- **EXPAND AND CLARIFY JOB PORTABILITY FOR HIGHLY SKILLED WORKERS.**
- **RECAPTURE GREEN CARDS LOST TO BUREAUCRATIC ERROR.**
- **GRANT GREEN CARDS TO STUDENTS GRADUATING WITH STEM PHDS FROM ACCREDITED AMERICAN UNIVERSITIES.**
- **DOUBLE THE NUMBER OF EMPLOYMENT BASED GREEN CARDS.**
- **CREATE AN ENTREPRENEUR VISA.**
- **CREATE AN EMERGING AND DISRUPTIVE TECHNOLOGY VISA.**

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 11: ACCELERATING AI INNOVATION

To remain the world's leader in AI the U.S. Government must renew its commitment to investing in America's national strength—innovation. This will require building incentives and making substantial new investments in AI research and development (R&D).

SCALE AND COORDINATE FEDERAL AI R&D FUNDING

- Establish a National Technology Foundation (NTF)
- Increate federal funding for AI R&D at compounding levels, doubling annually to reach $32 billion per year by Fiscal Year 2026
- Prioritize funding for key areas of AI R&D
- Triple the number of National AI Research Institutes
- Invest in talent that will transform the field

EXPAND ACCESS TO AI RESOURCES THROUGH A NATIONAL AI RESEARCH INFRASTRUCTURE

- A National AI Research Resource (NAIRR)
- A set of domain-specific AI R&D test beds
- Pipelines for the curation, hosting, and maintenance of complex data sets
- An open knowledge network
- A Multilateral AI Research Institute

LEVERAGE BOTH SIDES OF THE PUBLIC-PRIVATE PARTNERSHIP

- Create markets for AI and other strategic technologies
- Form a network of regional innovation clusters focused on strategic emerging technologies
- The private sector should privately fund an AI competitiveness consortium

Tackle Some of Humanity's Biggest Challenges

Such as: enabling long term quality of life, revolutionizing education and life-long learning, transforming energy management, and disaster response

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 12: **INTELLECTUAL PROPERTY**

China is both leveraging and exploiting intellectual property (IP) policies as a critical tool within its national strategies for emerging technologies. The United States has failed to similarly recognize the importance of IP in securing its own national security, economic interests, and technology competitiveness.

DEVELOP AND IMPLEMENT NATIONAL INTELLECTUAL PROPERTY POLICIES TO INCENTIVIZE, EXPAND, AND PROTECT AI AND EMERGING TECHNOLOGIES.

- The President should issue an **Executive Order to recognize IP as a national priority** and require the development of a comprehensive plan to further national security, economic and technology competitiveness strategies.
- The Executive Order should **direct the Vice President, as Chair of the Technology Competitiveness Council (TCC),** or otherwise as Chair of an interagency task force, **to oversee this effort**.
- The **Secretary of Commerce**, in coordination with the Under Secretary for Intellectual Property and **Director of the United States Patent and Trademark Office to develop proposals to reform and establish new IP policies and regimes as needed.**
- The Executive Order should direct the TCC or Vice President to assess which IP policies, regimes, and reform proposals from the Secretary of Commerce should be **elevated for implementation and integration** as part of **national security, economic interests, and technology competitiveness strategies.**

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 13: MICROELECTRONICS

U.S. Leadership in Microelectronics is Critical to Overall U.S. Leadership in AI

GOAL: STAY TWO GENERATIONS AHEAD OF CHINA IN STATE-OF-THE-ART MICROELECTRONICS AND MAINTAIN SOURCES OF CUTTING-EDGE MICROELECTRONICS FABRICATION IN THE U.S. BY FOCUSING ACTION ALONG THREE FRONTS:

IMPLEMENT THE NATIONAL MICROELECTRONICS STRATEGY

- To Coordinate Semiconductor Policy, Funding, and Incentives with the Executive Branch and Externally with Industry and Academia

REVITALIZE DOMESTIC MICROELECTRONICS FABRICATION

- Incentivize Domestic State-of-the Art Merchant Fabrication Through Refundable Investment Tax Credits

DOUBLE DOWN ON FEDERALLY FUNDED MICROELECTRONICS RESEARCH

- Double Down on Federal Funding to Lead the Next Generation of Microelectronics

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 14: **TECHNOLOGY PROTECTION**

America's ability to out-innovate competitors is the dominant component of any U.S. strategy for technology leadership. Promoting research, entrepreneurship, and talent development remain the key ingredients of success.

MODERNIZING EXPORT CONTROLS AND INVESTMENT SCREENING

- CLARIFY U.S. TECHNOLOGY PROTECTION PRINCIPLES AND BUILD REGULATORY CAPACITY TO IMPLEMENT ECRA AND FIRRMA
- REQUIRE COMPANIES TO DISCLOSE INVESTMENTS IN AI AND OTHER SENSITIVE TECHNOLOGIES TO CFIUS
- UTILIZE TARGETED EXPORT CONTROLS ON KEY SEMICONDUCTOR MANUFACTURING EQUIPMENT (SME)
- ALIGN THE EXPORT CONTROL POLICIES OF THE UNITED STATES, THE NETHERLANDS, AND JAPAN REGARDING SME
- UTILIZE TARGETED END-USE EXPORT CONTROLS AND REPORTING REQUIREMENTS TO PREVENT USE OF HIGH-END AI CHIPS IN HUMAN RIGHTS VIOLATIONS

STRENGTHENING RESEARCH PROTECTION

- BUILD CAPACITY TO PROTECT THE INTEGRITY OF THE U.S. RESEARCH ENVIRONMENT
- COORDINATE RESEARCH PROTECTION EFFORTS INTERNATIONALLY WITH ALLIES AND PARTNERS
- BOLSTER CYBERSECURITY SUPPORT FOR RESEARCH INSTITUTIONS
- COUNTER FOREIGN TALENT RECRUITMENT PROGRAMS
- STRENGTHEN VISA VETTING TO LIMIT PROBLEMATIC RESEARCH COLLABORATIONS

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 15: **A FAVORABLE INTERNATIONAL TECHNOLOGY ORDER**

The U.S. must work with allies and partners for AI innovation and adoption that advances the international rules-based order, protects free and open societies, and unleashes economic prosperity.

Direct an interagency task force to **DEVELOP AND IMPLEMENT AN INTERNATIONAL SCIENCE &TECHNOLOGY STRATEGY** to coordinate emerging tech policies government-wide & with allies & partners through four initiatives:

- **BUILD A EMERGING TECHNOLOGY COALITION** to organize around seven critical areas to advance the development and use of democratically-aligned and trusted AI, emerging technologies, and digital infrastructure
- **LAUNCH INTERNATIONAL DIGITAL DEMOCRACY INITIATIVE (IDDI)** to align international digital assistance efforts for AI and associated technologies
- **IMPLEMENT A COORDINATED U.S. NATIONAL PLAN** for IDDI efforts (shaping technical standards, foreign aid, development finance, and export controls)
- **ENHANCE THE US POSITION AS AN INTERNATIONAL SCIENCE & TECHNOLOGY RESEARCH HUB** through 1) partnerships with U.S. National AI Research Institutes & multilateral initiatives, 2) a NSF-run Multilateral AI Research Institute, and 3) international talent exchanges

REORIENT U.S. FOREIGN POLICY & THE DEPARTMENT OF STATE FOR TECH DIPLOMACY

- Establish a **DEPUTY SECRETARY FOR MANAGEMENT AND RESOURCES (D/MR)** to lead on tech diplomacy
- Prioritize tech diplomacy through **CSET BUREAU**, formal presence in Silicon Valley and foreign tech hubs, FSI training modules
- **INCREASE APPROPRIATIONS** for tech-focused diplomatic corps and programming
- Reorganize around permanent **UNDER SECRETARY FOR SCIENCE, RESEARCH, AND TECHNOLOGY (Q)**

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

CHAPTER 16: **ASSOCIATED TECHNOLOGIES**

The United States must view its efforts to lead in AI through the broader lens of competition across a range of emerging technologies, and, therefore, also support a comprehensive strategy to sustain U.S. leadership in key associated technologies.

STEP ONE:

DEFINE AND PRIORITIZE THE KEY EMERGING TECHNOLOGIES THAT ARE NEEDED TO ENSURE U.S. NATIONAL COMPETITIVENESS.

STEP TWO:

ACTIONS TO PROMOTE TECHNOLOGIES AND PLATFORMS ESSENTIAL TO US LEADERSHIP IN NATIONAL SECURITY

BIOTECHNOLOGY

- PRIORITIZE THE DEVELOPMENT OF AN ADVANCED BIOTECHNOLOGY MANUFACTURING ECOSYSTEM

QUANTUM COMPUTING

- TRANSITION QUANTUM COMPUTING BASIC RESEARCH TO NATIONAL SECURITY APPLICATIONS AND INCENTIVIZE DOMESTIC QUANTUM FABRICATION

5G AND ADVANCED NETWORKING

- BOLSTER AND ACCELERATE U.S. 5G NETWORK DEPLOYMENT THROUGH MID-BAND SPECTRUM SHARING

AUTONOMY AND ROBOTICS

- INCENTIVIZE THE DEVELOPMENT OF WORLD-CLASS SOFTWARE PLATFORMS FOR ROBOTIC AND AUTONOMOUS SYSTEMS

ADVANCED & ADDITIVE MANUFACTURING

- ACCELERATE ADDITIVE MANUFACTURING PRODUCTION OF LEGACY PARTS ACROSS THE DEPARTMENT OF DEFENSE

ENERGY SYSTEMS

- DEVELOP AND DOMESTICALLY MANUFACTURE ENERGY STORAGE TECHNOLOGIES TO MEET U.S. MARKET DEMAND BY 2030