

V.3 DRAFT

FINAL REPORT –

BLUEPRINTS FOR ACTION

PART I

National Security Commission on Artificial Intelligence

Table of Contents

Chapter 1: Emerging Threats in the AI Era	3
Combating Malign Information Operations Enabled by AI	3
Preparing for AI-Enabled Cyber Conflict	10
Chapter 2: Foundations of Future Defense	21
Chapter 3 - AI and Warfare	61
Chapter 5: AI and the Future of National Intelligence	74
Chapter 6: Technical Talent in Government	83
Chapter 7: Establishing Justified Confidence in AI Systems	105
Chapter 8: Upholding Democratic Values: Privacy, Civil Liberties, and Civil Rights in Uses of AI for National Security	120

The following Blueprints for Action cover Part I of NSCAI’s Final Report. Part I, “Defending America in the AI Era,” (Chapters 1-8) outlines what the United States must do to defend against the spectrum of AI-related threats from state and non-state actors, and recommends how the U.S. government can responsibly use AI technologies to protect the American people and our interests. These Blueprints for Action complement the Commission’s Final Report and mirror its organizational structure.

Building upon the top-line recommendations in the Commission’s Final Report, the Blueprints for Action serve as more detailed roadmaps for Executive and Legislative branch actions to retain America’s AI leadership position. The Blueprints for Action identify who should take a particular action—Congress, the White House, or an executive branch department or agency. The Commission provides estimated increases in funding or appropriations as part of its recommendations. All recommendations that include funding figures should be considered estimates for consideration by Congress and/or the Executive Branch.

**Chapter 1: Emerging Threats in the AI Era
Blueprint for Action
Combating Malign Information Operations Enabled by AI**

The use of AI to produce, manipulate, and promote malign information marks a disruptive evolution in the use of information as a tool of statecraft, a weapon of war, and a threat to democracy.¹ The following recommendations represent a strategic, organizational, and operational framework that the U.S. government should adopt to adequately defend and counter malign information operations in the AI era, including by employing AI-enabled technologies.

Recommendation: A National Strategy for the Global Information Domain

Expanding upon the principles of information statecraft outlined in the 2017 National Security Strategy,² the President should issue a new national strategy for the global information domain that more fulsomely addresses how AI and associated technologies are defining new fronts in this area. The strategy should:

- Acknowledge that the network-connected world is dissolving barriers between societies.
- Prioritize the global information domain as an arena for competition.
- Detail how adversarial state and non-state actors are attempting to define and control the global information domain in order to shape global opinion and achieve strategic advantage.
- Account for the critical role of AI-enabled malign information in achieving these goals.
- Designate malign information operations as a national security threat with its own set of priority actions to defend, counter, and compete against them.
- As necessary, update critical infrastructure designations and require relevant departments and agencies to update sector-specific plans to reflect emerging technologies.
- Establish organizational structures for U.S. national security agencies to defend, counter, and compete against the threat.

¹ For the purposes of this section, “malign information” includes both disinformation—false information or intentionally misleading facts communicated with the intent to deceive—and misinformation—false information not necessarily meant to deceive. See Daniel Fried & Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council at n.1 (Feb. 2018); https://www.atlanticcouncil.org/wp-content/uploads/2018/03/Democratic_Defense_Against_Disinformation_FINAL.pdf. For a broader discussion, see Laura Rosenberger, *Making Cyberspace Safe for Democracy*, Foreign Affairs (May/June 2020), www.foreignaffairs.com/articles/china/2020-04-13/making-cyberspace-safe-democracy. For a study of how AI might be used to counter disinformation, see William Marcellino, et al., *Human-machine Detection of Online-based Malign Information*, RAND Europe (2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA500/RRA519-1/RAND_RRA519-1.pdf.

² *National Security Strategy of the United States*, The White House at 34 (Dec. 18, 2017), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf>.

Action for the President:

- Issue a supplemental National Strategy for the Global Information Domain.

Action for Congress:

- Congress should direct the Executive Branch to transmit a National Strategy for the Global Information Domain that categorizes the global information domain as an arena of competition vital to the national security of the United States.

Organizational Framework

The proliferation of malign information has exposed an Achilles heel in the U.S. national security apparatus. Previous major reorganizations could not foresee contemporary digital technology and society's profound dependence upon it. They could not anticipate the use of ICT platforms and tools, bots, and AI-enabled technologies to spread false information. They do not account for the role that the commercial sector and civil society play in defending against malign information, and enabling its spread. Individual agencies such as the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) have stretched their mandates to confront the threat. They rely on narrow sets of outdated tools, and are hampered by cultures shaped by the Cold War and counter-terrorism paradigms.

Recommendation: Create a Joint Interagency Task Force (JIATF) and Operations Center.

Action for the President:

- **Direct creation of a JIATF and operations center to lead and integrate government efforts to counter foreign-sourced malign information in real time.**
 - The Presidential action should direct the Secretaries of State, Defense, Justice, and Homeland Security, as well as the Director of National Intelligence, to create a JIATF and stand-up an operations center to counter foreign-sourced malign information.
 - The JIATF should integrate efforts of key offices, bureaus, and divisions within each of these agencies, as well as the broader intelligence community (IC) and law enforcement establishment.
 - The JIATF should have the responsibility to survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns.

DRAFT NSCAI DOCUMENT

- The JIATF should draw on existing authorities to create an operations center with modern, AI-enabled digital tools and expert staff to expose, attribute, and respond effectively.
- The Presidential action should also direct these officials, as part of the JIATF, to create a mechanism to share and exchange critical information with key companies in the private sector that run internet and social media platforms where malign information proliferates.

Action for the Secretaries of State, Defense, Justice, and Homeland Security and the Director of National Intelligence:

- **Establish the JIATF and Operations Center.**
 - These agency heads should direct immediate development of a plan to create the JIATF and operations center with a focus on identifying those offices, bureaus, and divisions within their agencies and the broader IC and law enforcement establishment that are essential to the mission of countering foreign-sourced malign information.
 - As part of this effort, the JIATF should leverage the authority provided by Congress in the FY 2020 NDAA to stand-up a Foreign Malign Influence Response Center within ODNI.³
 - Components that will be critical to the JIATF include, among others, the Central Intelligence Agency's Open Source Enterprise and the National Counterintelligence and Security Center.⁴ Leadership will need to ensure involvement of relevant components from the FBI, the National Security Agency, across the Department of Defense, and the Global Engagement Center (GEC) at the Department of State.
 - The JIATF would lead and integrate existing and new national strategic efforts against foreign malign information operations by providing analysis, sharing information with government and commercial partners, and driving whole-of-government *action*, subject to Presidential direction, to advance U.S. information objectives.
 - The Commission proposes that the operations center component of the JIATF be modeled on the National Counterterrorism Center (NCTC), as a proven model for providing real-time situational awareness of and response to evolving national security threats.

³ Pub. L. 116-92, The National Defense Authorization Act for Fiscal Year 2020, 133 Stat. 1198, 2129-30 (2019).

⁴ *National Counterintelligence and Security Center*, Office of the Director of National Intelligence (last accessed Feb. 8, 2020), <https://www.dni.gov/index.php/ncsc-home>.

DRAFT NSCAI DOCUMENT

- To exchange information and coordinate with internet and social media platforms on malign information threats, the Commission proposes creation of an associated industry consortium that includes an information sharing and analysis center (ISAC). The consortium, supplemented by the ISAC, would allow the JIATF to exchange information with industry, monitor malign information across ICT platforms, and improve U.S. government response to malign information threats. In developing the ICT consortium and ISAC, JIATF should look to the Global Internet Forum to Counter Terrorism as a model.⁵

Action for the Director of National Intelligence:

- **Appoint a Malign Information Threat Executive (MITE) to lead the JIATF.**
 - In July 2019, ODNI created the Election Threat Executive position responsible for coordinating across the IC on issues related to election security.⁶ The threat of foreign malign information operations demands that this position be elevated, renamed, and expanded beyond the subject of elections.
 - The MITE role should also serve a liaison function between the White House/National Security Council and the JIATF to ensure alignment and responsiveness to the national security strategy.

Action for Congress:

- **Appropriate \$30 million per year to support the operations of the JIATF.**

Operational Framework

Efforts by the U.S. Government and private sector to counter terrorist propaganda offer a potential roadmap for how the United States can go on the offensive to counter and compete against malign information. The creation of the Global Coalition to Defeat the Islamic State of Iraq and Syria (ISIS) has shown how a burden sharing model can be deployed to successfully counter and defeat a shared threat.⁷ The United States and its allies will only succeed if they can develop and deploy personnel as well as an advanced set of tools to assist in their effort to counter and compete against malign information operations. Efforts need to be made to encourage innovation as well as harness commercially available technologies to go on the offensive.

Recommendation: The Department of State should lead a global effort to counter disinformation.

⁵ About, Global Internet Forum to Counter Terrorism (last accessed Oct. 2, 2020), <https://www.gifct.org/about/>.

⁶ Press Release, *Director of National Intelligence Daniel R. Coats Establishes Intelligence Community Election Threats Executive*, Office of the Director of National Intelligence, (July 19, 2019), www.dni.gov/index.php/newsroom/press-releases/item/2023-director-of-national-intelligence-daniel-r-coats-establishes-intelligence-community-election-threats-executive.

⁷ Brett McGurk, *America Should Build an International Coalition Now*, The Atlantic (Mar. 29, 2020), <https://www.theatlantic.com/ideas/archive/2020/03/america-should-build-international-coalition-now/608983/>.

Action for the President:

- **Designate the Under Secretary of Public Diplomacy and Public Affairs at the Department of State to lead the international fight against malign information operations.**

Action for the Department of State:

- **Build an International Task Force to Counter and Compete Against Disinformation.** Modeled after the Global Coalition to Defeat ISIS, the Department of State should build a similar task force to counter malign information. The International Task Force to Counter and Compete Against Disinformation should be led by the Department of State's Under Secretary for Public Diplomacy and Public Affairs, with the GEC coordinating its daily activities.⁸ The task force will be in charge of directing, leading, synchronizing, integrating, and coordinating efforts by allies to recognize, understand, expose, and counter foreign state and non-state propaganda and malign information efforts. The GEC should leverage the work of the Technology Engagement Team (TET) to share and test technologies to detect and disrupt the creation, manipulation, and dissemination of malign information from state and non-state actors. *See also the Chapter 15 Blueprint for Action for more detail on creating a task force as part of the Emerging Technology Coalition proposed by the Commission.*

Recommendation: The Defense Advanced Research Projects Agency (DARPA) should coordinate multiple research programs to detect, attribute, and disrupt AI-enabled malign information campaigns and to authenticate the provenance of digital media.

The government should sponsor research to develop technologies to detect, attribute, and disrupt malign influence operations, including influence campaigns, psychological operations on social media platforms, and manipulated and synthetic media. In parallel the government should develop alternative technologies to authenticate the provenance of digital media and head off the risk that other approaches will not be successful. These efforts should be led by DARPA.

Action for Congress:

- **Appropriate \$60 to 80 million in additional funding for DARPA to sponsor multiple research projects to develop technologies to detect, attribute, and disrupt malign influence operations that rely on AI-generated content, and to develop alternative technologies to authenticate the provenance of digital media.**⁹ DARPA has existing authority to fund such research with the scope outlined in this recommendation but will require dedicated appropriations to carry out the effort and a security review of the best innovation vehicles to sponsor the research.

⁸ Though this overall Blueprint for Action uses the term malign information to broaden beyond disinformation to include misinformation, it will likely be easier to organize a task force around countering disinformation.

⁹ Funding level should depend upon the number of programs DARPA has the capacity to execute in this area.

Action for DARPA:

- **Sponsor further research as described above using innovation vehicles, such as challenge competitions, or any other deemed necessary by DARPA to develop and transition these technologies to accountable agencies and departments for maximum employment.**

Recommendation: Executive Branch departments and agencies should utilize Other Transaction Authorities (OTAs), creative investing, and the Small Business Innovation Research (SBIR) program to deploy capital to companies that offer technical solutions that will assist the United States Government in identifying, countering, and defending against malign information operations.

The U.S. Government has an array of mechanisms that are not currently leveraged to deploy capital to companies that create strategic technology to unleash AI, machine learning (ML), and associated technologies in this counter-information operations fight.¹⁰

Action for all U.S. departments and agencies:

- **Explore the use of the SBIR program and OTAs to acquire technology solutions that will assist the United States Government in identifying, countering, and defending against malign information operations.**

¹⁰ These could be SBIRs, OTAs, or other modern vehicles with minimal red tape. Recently published reports on countering malign influence have issued wide-ranging recommendations including: deploying special operations forces to areas “vulnerable to political warfare,” building “rapid-reaction information cells to track and counter” malign influence operations, and promoting civil society to “combine the values of accurate media with engagement skills and an understanding of how propagandists prey on polarization, inflaming divides.” These recommendations are already being put into action by Special Operations Command in Africa, using commercially available services to combat and attribute malign information operations about COVID-19 and other issues on the continent. The General Services Administration has awarded IST Research a Phase III SBIR contract to “support operations in the information environment for the special operations and Federal Government community.” Additionally, the U.S. Air Force and U.S. Special Operations Command have contracted with Primer to “automatically identify and assess suspected disinformation” using ML technology. See David Ronfeldt & John Arquilla, *Whose Story Wins: Rise of the Noosphere, Noopolitik, and Information Age Statecraft*, RAND at 72 (July 2020), https://www.rand.org/content/dam/rand/pubs/perspectives/PEA200/PEA237-1/RAND_PEA237-1.pdf (citing or quoting other experts or reports); Dave Nyczepir, *SOCOM Looks to Combat Disinformation in Africa on New Governmentwide Contract*, FedScoop (July 27, 2020), <https://www.fedscoop.com/socofrica-disinformation-ist-research/>; *IST Research Awarded Five-year, \$66 Million GSA Contract*, IST Research (July 23, 2020), <http://www.globenewswire.com/news-release/2020/07/23/2066650/0/en/IST-Research-Awarded-Five-year-66-Million-GSA-Contract.html>; *SOCOM and US Air Force Enlist Primer to Combat Disinformation*, Cision PR Newswire (Oct. 1, 2020), <https://www.prnewswire.com/news-releases/socom-and-us-air-force-enlist-primer-to-combat-disinformation-301143716.html>.

[BLANK PAGE]

DRAFT

**Chapter 1: Emerging Threats in the AI Era
Blueprint for Action
Preparing for AI-Enabled Cyber Conflict**

The United States must prepare for both the present and future threat of increasingly automated and AI-enabled cyber conflict. The expanding threats of mutating malware and AI-powered tools are combining with traditional cyber threats to automate, optimize, and ultimately transform the precision, speed, stealth, scale, and effectiveness of cyber-attack and espionage campaigns.¹¹ To defend the U.S. from current and future cyber threats, we must move to develop AI-enabled cyber defenses and to mitigate proliferating cyber vulnerabilities.

Section 1: Developing AI-enabled defenses against cyber attacks

Recommendation: Develop and deploy machine-speed threat detection and mitigation.

Detecting and reacting to unknown threats on a network is difficult, but not impossible for self-learning AI systems that have been trained to differentiate between normal and anomalous network behavior.¹² To address deficiencies highlighted by the SolarWinds attack, autonomous defenses are needed to defend the U.S. Government's systems.

Actions for the Department of Homeland Security and Department of Defense:

- **Expand machine speed threat information sharing, behavior-based anomaly detection, and cyber threat mitigation to all government networks containing sensitive information and critical functions.**
 - DHS must improve the National Cybersecurity Protection System (NCPS) while DoD must also accelerate its efforts to harness AI-enabled cyber defenses and sensors. At a minimum, the objective of these new defenses should be to flag or potentially block never-before-seen connections and communications missed by currently deployed intrusion detection and prevention technologies such as EINSTEIN.¹³ To fully take advantage of new capabilities, these defenses should

¹¹ Nicholas Duran, et al., *2018 Webroot Threat Report*, Webroot (2018), https://www-cdn.webroot.com/9315/2354/6488/2018-Webroot-Threat-Report_US-ONLINE.pdf; Gary J. Saavedra, et al., *A Review of Machine Learning Applications in Fuzzing*, arXiv (Oct. 9, 2019), <https://arxiv.org/pdf/1906.11133.pdf>; Isao Takaesu, *Machine Learning Security: DeepExploit*, GitHub (Aug. 29, 2019), https://github.com/13o-bbr-bbq/machine_learning_security/tree/master/DeepExploit; Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, Wall Street Journal (Aug. 30, 2019), <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>; *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine (2019), <https://doi.org/10.17226/25488>; Ben Buchanan, et al., *Automating Cyber Attacks*, Center for Security and Emerging Technology (Nov. 2020), <https://cset.georgetown.edu/research/automating-cyber-attacks/>; Nektaria Kaloudi & Jingyue Li, *The AI-Based Cyber Threat Landscape*, ACM Computing Surveys at 1-34 (Feb. 2020), <https://dl.acm.org/doi/abs/10.1145/3372823>; Dakota Cary & Daniel Cebul, *Destructive Cyber Operations and Machine Learning*, Center for Security and Emerging Technology at 5-23 (Nov. 2020), <https://cset.georgetown.edu/research/destructive-cyber-operations-and-machine-learning/>.

¹² Max Heinemeyer, *Dissecting the SolarWinds Hack without the Use of Signatures*, Darktrace (Jan. 7, 2021), www.darktrace.com/en/blog/dissecting-the-solar-winds-hack-without-the-use-of-signatures/.

¹³ See *EINSTEIN*, U.S. Cybersecurity and Infrastructure Security Agency (last accessed Feb. 8, 2021), <https://www.cisa.gov/einstein>.

DRAFT NSCAI DOCUMENT

also aim to accelerate recovery from cyber-attack by automatically generating courses of action for federal agencies to assure secure continuity of operations. These defenses should assist recognition of insider threats as well as externally launched attacks, and use machine speed information sharing to prepare other public and private networks to defend themselves against detected threats.

- DoD and DHS must also assess and mitigate security risks posed by introducing and enhancing threat detection systems. These systems will require precautions against their elevated system access being used to deliver malware or abused by other cyber threats. AI enabled system components designed to mitigate new and unknown threats likewise will need defenses against adversarial techniques.
- To minimize cost overruns in altering a multi-billion dollar project, DHS should reprogram \$10 million to investigate the best means to accelerate and set up AI-enabled threat detection systems. This study would be tasked to look for synergies with existing intrusion detection software and infrastructure, seek to address any remaining key deficiencies found by GAO in the National Cybersecurity Protection System, and to develop a final budget proposal for Congress.¹⁴ This study likewise should aim to address how previous intrusion detection systems failed to detect the SolarWinds cyber-attack.

Recommendation: Execute large, instrumented, and realistic tests to gather data and train AI-enabled cyber defenses.

AI-enabled cyber defenses require training to recognize potential threats, and sensors to detect them. By experimenting with larger networks in realistic conditions, the United States can train more robust AI-enabled cyber defense capabilities.

Action for Congress:

- **Fund the Defense Advanced Research Projects Agency (DARPA) to sponsor additional secure, instrumented, and realistic research on AI-enabled cyber defenses.**
 - DARPA funding should be increased by \$20 million, to be divided between a security review, and other programmatic costs for the additional research. DARPA should be left free to determine the structure of further research, with an innovation vehicle such as a challenge competition or any other that DARPA deems necessary.
- **Expand the National Institute of Standards and Technology AI testbed program.**

¹⁴ Gregory C. Wilshusen, *DHS Needs to Enhance Efforts to Improve and Promote the Security of Federal and Private-Sector Networks*. Government Accountability Office, (Apr. 24, 2018), www.gao.gov/assets/700/691439.pdf. See also *Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System*, Government Accountability Office (Jan. 28, 2016), <https://www.gao.gov/assets/680/674829.pdf>.

DRAFT NSCAI DOCUMENT

- For FY 2021 NIST requested a \$25 million increase, for measurement tools and testbeds to accelerate the development and adoption of interoperable, secure, and reliable AI technologies.¹⁵ Since then, NIST has been authorized for \$64 million in additional AI R&D responsibilities including AI testbeds. To ensure NIST can meet its new responsibilities in addition to its prior ones, Congress should meet NIST's authorized funding increase for AI R&D.

Actions for DARPA:

- **Structure and standardize an innovation vehicle, such as a challenge competition, or any other DARPA deems necessary, to increase insight about options for new AI-enabled cyber defenses.**
 - DARPA should aim to encourage the prototyping of new means of AI-enabled cyber defense and test the efficacy of these defenses against intelligent opponents and AI-enabled cyber threats. DARPA should structure new research to broaden insight on the importance of real-life factors such as cyber-attack externalities, differences in risk tolerance between threat actors, and differences in network infrastructure between defenders.¹⁶
- **Bring broader fields of expertise to bear for cyber defense research.**
 - Cyber expertise is not the only expertise relevant to cybersecurity and the efficacy of cyber operations.¹⁷ The new research should involve experts from other fields such as economics, game theory, and behavioral psychology to improve scoring metrics, improve the human components of cyber strategy, and propagate insight further within government. With these improved metrics and insights, future investments can be more directly aligned with mission assurance.
- **Conduct a security review to determine the rules and bounds of new cyber research initiatives.**
 - DARPA must conduct a thorough security review about the second order effects of sponsoring research with public facing results and without strong information security measures, to mitigate against potential adversaries acquiring information that can be weaponized against us. International competition in this area is getting so intense that the organization must consider using a vetted closed challenge competition or initiative as opposed to an open-challenge competition format.

¹⁵ *President's FY 2021 Budget Request to Congress for the National Institute of Standards and Technology*, National Institute of Standards and Technology (2020), www.nist.gov/system/files/documents/2020/02/11/FY2021-NIST-Budget-Book.pdf.

¹⁶ *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 17-19 (2019), <https://doi.org/10.17226/25488>.

¹⁷ *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 12-19, 69 (2019), <https://doi.org/10.17226/25488>.

Actions for NIST:

- **Expand the NIST AI testbed program to generate data for AI-enabled cyber defenses in differing IT infrastructure environments.**
 - Larger scale testing is necessary to generate the data required for AI-enabled cyber defenses. By scaling testbeds within NIST, there will be the opportunity to generate this data, and to evaluate the performance of varying network architectures at strengthening network security.
 - Training data often reflects a broad sampling of common scenarios and does not itself necessarily convey the costs of different types of compromises without further labelling.¹⁸ *NIST should create optimized data sets for training cyber defenses to minimize expected costs of network disruption, compromise, and damage* rather than merely trying to identify cyber threats and vulnerabilities with high accuracy. To develop these data sets, NIST will need to hire or contract multidisciplinary talent to develop better metrics.

Recommendation: Ensure the robustness of AI-cyber defenses.

To make AI-based cyber defenses stronger, their supporting supply chains and data must be defended, while the algorithms themselves must be protected from malware, trained against adversarial techniques, and red teamed to the point of failure. *This approach can be found in the Chapter 7 Blueprint for Action.*

Section 2: Ensuring resilience against AI-enabled cyber attacks

Many of the defenses required to protect against AI-enabled cyber threats are also required to defend against less advanced cyber threats. To provide this protection, the Commission endorses specific Cyberspace Solarium Commission’s recommendations which are instrumental in enhancing U.S. defenses against AI-enabled cyber threats.¹⁹

Recommendation: Improve incentives for information and cyber security.

AI cannot defend inherently indefensible digital infrastructure against escalating offensive AI-enabled cyber capabilities. Even if vulnerabilities are known and easily patchable, that is no guarantee that they will be closed without a further impetus to action. Similarly, while new instrumented digital infrastructure is required to accelerate AI-enabled cyber defenses, those that build it must be careful to ensure new vulnerabilities don’t outweigh the benefits of these defenses. In both cases, incentives must be realigned in the public and private sector to assure gaps are closed and new infrastructure is secure.

¹⁸ *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop*, National Academies of Sciences, Engineering, and Medicine at 15 (2019), <https://doi.org/10.17226/25488>.

¹⁹ *Report*, U.S. Cyberspace Solarium Commission (Mar. 2020), <https://www.solarium.gov/report>. [hereinafter CSC Report]

Action for Congress:

- **Establish liability for final goods assemblers for damage stemming from incidents that exploit known and unpatched vulnerabilities, incentivize reporting, and amend the Sarbanes-Oxley Act to include cybersecurity reporting requirements.**²⁰
 - The Cyberspace Solarium Commission made recommendations to incentivize timely vulnerability patching. In addition to these recommendations, companies should be incentivized to improve their cybersecurity and participate in new vulnerability disclosure programs via selectively reducing legal liability and product recalls for companies that can mitigate and patch controlled vulnerabilities within a limited, but rule defined time period. The overall structure of liability reform should aim to minimize perverse incentives to avoid liability by concealing failure. Grid, critical infrastructure, and medical device companies should be the primary targets for improvement.
 - To harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies, Congress should amend the Sarbanes-Oxley Act to explicitly account for cybersecurity.²¹

Action for the Executive Branch

- **Incentivize information technology security through Federal Acquisition Regulations and Federal Information Security Management Act authorities.**²²
 - Zero trust networking and robust code should become key priorities for government contracts related to information technology, and especially for contracts related to AI. Contractors should not be paid more for additional lines of code when adding them generates new vulnerabilities without additional functionality. Code should be subjected to AI-enabled vulnerability review.
- **Task CISA to develop an IT infrastructure “Cash for Clunkers” incentive plan, to submit to Congress for FY 2022.**
 - This program would support the replacement of vulnerable outdated equipment with modern alternatives through targeted federal subsidies. CISA should coordinate the effort by setting the program’s strategy, prioritizing devices and critical digital infrastructure for replacement, and determining subsidy levels for the systems to be replaced. CISA must develop the plan so as to minimize perverse incentive to acquire vulnerable infrastructure before the plan is funded,

²⁰ This recommendation modifies an existing Cyberspace Solarium Commission recommendation in order to reduce the risk of creating perverse incentives to avoid enforcement. See recommendation 4.2 and 4.4.4, CSC Report at 76, 83.

²¹ See recommendation 4.4.4, CSC Report at 83.

²² See recommendation 4.4.3, CSC Report at 82.

and once the plan is developed, Congress must implement it as quickly as possible to reduce perverse incentives for companies to hold out on replacing vulnerable devices and infrastructure in the meantime.

Section 3: Disrupting adversary AI-enabled cyber-attacks and capabilities

Recommendation: Develop additional, impactful non-kinetic options to respond to adversarial cyber and information operations.

Modern information operations have enormous overlap with cyber operations. As AI-enabled cyber capabilities spread in the presence of wide-open societal vulnerabilities, the United States needs to have additional tools to counter proliferating threat actors, and to establish deterrence in the cyber and information domains.

Action for Congress:

- **Expedite the establishment of the Bureau of Cyberspace Security and Emerging Technologies (CSET) within the U.S. Department of State.**
 - The CSET Bureau will be essential for strengthening norms in cyberspace, engaging other countries on information technology standards, assisting allied cyber defense, and improving international cyber law enforcement.
Recommendations to expedite the Bureau's build out and ensure that it has a clear mandate to coordinate strategy on the full range of emerging technology issues, in addition to critical cybersecurity needs, can be found in the Chapter 15 Blueprint for Action.
- **Strengthen the U.S. Government's ability to take down botnets by enacting Section 4 of the International Cybercrime Prevention Act.**
 - Botnets are already a present threat and may become more powerful with advances in AI, not just directly spreading malware, but harvesting both computational power and data to put toward further offensive training in ways that were not previously possible. "To enable the U.S. government to better work with private industry and international partners, Congress, in consultation with the Department of Justice, should enact Section 4 of the International Cybercrime Prevention Act. This legislation would provide broader authority to disrupt all types of illegal botnets, not just those used in fraud."²³

Actions for Cyber Command, the Department of Homeland Security, the Federal Bureau of Investigation, and the National Security Agency

- **Expand current cyber threat inoculation initiatives.**

²³ See recommendation 4.5.3, CSC Report at 87.

- “Machine speed information sharing is a key piece of enabling AI-cyber defenses. To contribute to the readiness of U.S. defense and critical infrastructure, efforts should be made to accelerate sharing of the most recent malicious code captured in the wild through appropriate interagency channels, including through a Joint Collaborative Environment. U.S. Cyber Command should ensure and accelerate coordination with DHS, the FBI, NSA, and stakeholders in the private sector in the release of threat information, particularly with owners and operators of systemically important critical infrastructure.”²⁴

Section 4: Coordinating and Strategizing a Response

Recommendation: Reform the U.S. Government’s strategy, structure, organization, and authorities for handling AI-enabled cyber threats.

The U.S. must organize and align authorities to fully implement the cyber security mission and fully capitalize on machine speed information sharing defenses. Technology alone isn’t enough: cyber threat intelligence, joint planning, and response must be integrated into the same organization to keep pace with AI cyber threats.

Actions for the Executive Branch:

- **Issue an updated National Cyber Strategy with the following components.**
 - First, the strategy should build on the layered deterrence framework put forward by the Cyberspace Solarium Commission with a focus on making the framework more robust against the ways AI will transform cyber conflict.²⁵
 - To support the strategy, the Department of Defense, in partnership with the Department of State and the IC, should also develop a multitiered signaling strategy and promulgate a declaratory policy that addresses the use of AI in cyber operations.²⁶
 - Second, to inform the strategy, the Department of Homeland Security should run a study to develop regulatory recommendations for the most cost-effective means of defending digital devices and infrastructure. This study should investigate, but not be limited to:
 - Standards requiring critical private and public sector networks to keep their data encrypted at rest and in transit
 - Multi-factor authentication requirements for critical private and public sector networks

²⁴ See recommendation 6.1.2, CSC Report at 114.

²⁵ See recommendation 1.1, CSC Report at 32.

²⁶ See recommendation 1.1.1 and 1.1.2, CSC Report at 32.

- Air gapping requirements for select sensitive, but still unclassified networks
 - Analog defenses for cyber physical infrastructure to prevent the most lethal failures regardless of how much network access cyber attackers gain, or how advanced their methods of attack become
 - Federated machine learning techniques that lower espionage and privacy risk via enabling data to be partitioned or remain decentralized
 - Specialized, narrow purpose computation hardware which can't be repurposed by malware for attacks
 - Ways to harness AI to lock down and constrain hardware toward its intended purpose on vulnerable networks that can't yet be patched or replaced
 - Ways to use cloud computing and virtual machines to reduce vulnerability of AI and cyber systems to advanced persistent threats
- **Accelerate the establishment of a Joint Cyber Planning and Operations Center, modeled after the National Counterterrorism Center.**²⁷
 - This planning office under the Cybersecurity and Infrastructure Security Agency is necessary to coordinate cybersecurity planning and readiness across the federal government and between public and private sectors. To properly stand-up such a collaborative environment, the Executive Branch must submit to Congress a list of authorities and data sharing issues that will require additional authorities or funding.
 - **Develop and implement an information and communications technology industrial base strategy.**²⁸
 - This strategy must increase support to supply chain risk management efforts, and provide better defense to the hardware supply chains, data, and algorithms that compose the “AI stack.”

Action for Congress:

- **Establish a Bureau of Cyber Statistics to inform both cyber defense policy and AI-enabled cyber defenses.**²⁹

²⁷ See recommendation 5.4, CSC Report at 87.

²⁸ See recommendation 4.6, CSC Report at 88.

²⁹ See recommendation 4.3, CSC Report at 78.

- Large accurate datasets with relevant data are especially useful for training AI-enabled cyber defenses that minimize the costs of cyber-attacks and false alarms, rather than just the number of attacks and false alarms. To that end, “Congress should establish a Bureau of Cyber Statistics, within the Department of Commerce, or another department or agency, that would act as the government statistical agency that collects, processes, analyzes, and disseminates essential statistical data on cybersecurity, cyber incidents, and the cyber ecosystem to the American public, Congress, other federal agencies, state and local governments, and the private sector.”³⁰

Recommendation: Coordinate with the Private Sector to Increase Resilience Against AI-Enabled Cyber Attacks.

Action for Congress:

- **Create or Designate Critical Technology Security Centers.**³¹
 - Congress should direct and appropriate funding for the Department of Homeland Security, in partnership with the Department of Commerce, Department of Energy, Office of the Director of National Intelligence, and Department of Defense, to competitively select, designate, and fund up to three Critical Technology Security Centers.
 - These Centers would be designed to centralize efforts directed toward evaluating and testing the security of devices and technologies that underpin our networks and critical infrastructure.
 - At least one Center should be dedicated to testing the security of connected control systems and devices used in critical infrastructure sectors. The Center would manage the continuous red-teaming entities proposed in Chapter 11 of this report.
- **Authorize, establish, and fund a joint collaborative environment for sharing and fusing threat information.**³²
 - Sharing and fusing threat information is an instrumental step in improving the speed and capability of potential AI-enabled cyber defenses.³³ Congress will need to ensure different executive branch agencies have the proper authorities required to bring their data together in support of these efforts.

³⁰ CSC Report, 78.

³¹ See recommendation 4.1.1, CSC Report at 75.

³² See recommendation 5.2, CSC Report at 101.

³³ The President’s National Infrastructure Advisory Council detailed a similar recommendation to make cyber intelligence more actionable. *Transforming the U.S. Cyber Threat Partnership*, President’s National Infrastructure Advisory Council at 8 (Dec. 12, 2019), <https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf>.

- To support this effort, “Congress should establish a “Joint Collaborative Environment”, a common, cloud-based environment in which the federal government’s unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis—to the greatest extent possible.”³⁴

DRAFT

³⁴ CSC Report at 102

[BLANK PAGE]

DRAFT

Chapter 2: Foundations of Future Defense Blueprint for Action

The Department of Defense (DoD) lags far behind the commercial sector in integrating new and disruptive technologies such as Artificial Intelligence (AI) into its operations. Technical, bureaucratic, and cultural challenges must be overcome to adopt AI to maintain the U.S. military advantage. By 2025, the Department of Defense must put in place the foundations for widespread AI adoption, by: 1) Building the technical backbone; 2) Training and educating warfighters; 3) Accelerating adoption of existing digital technologies; 4) Democratizing development of AI; and 4) Investing in next-generation capabilities. To the maximum extent possible, these efforts should be coordinated with the intelligence community and other partners across the national security community.³⁵

Recommendation: Drive Change through Top-Down Leadership.

Maintaining the defense advantage in an AI-enabled future will require top-down leadership to overcome organizational barriers and create strategic change. Critically, civilian and military leaders across the DoD and the Intelligence Community must coordinate more closely, aligning priorities, resources, and policies to speed technology adoption and research breakthroughs.

Action for the Department of Defense and the Office of the Director of National Intelligence:

- **Establish a Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence,**³⁶
 - The Secretary of Defense and Director of National Intelligence should issue a directive immediately establishing the senior oversight committee listed above.
 - The Steering Committee on Emerging Technology provides a forum to drive change, focus, and action on emerging technology that otherwise would not be prioritized. It will enhance intelligence analysis related to emerging technology; connect strategic vision to organizational change; focus concept and capability development on emerging threats; guide defense investments that ensure America's strategic advantage against near-peer competitors; and provide the

³⁵ See Chapter 9 of this report and its associated Blueprint for Action for a recommendation to establish a Technology Competitiveness Council that could serve as a body for this kind of strategic-level coordination.

³⁶ The Commission acknowledges section 236 of the FY 2021 National Defense Authorization Act, which permits the Secretary of Defense to establish a steering committee on emerging technology and national security threats composed of the the Deputy Secretary of Defense; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for Intelligence and Security; the Under Secretary of Defense for Research and Engineering; the Under Secretary of Defense for Personnel and Readiness; the Under Secretary of Defense for Acquisition and Sustainment; the Chief Information Officer; and such other officials of the Department of Defense as the Secretary determines appropriate. However, the structure described in section 236 does not include leadership from the Intelligence Community and will thus not drive the intended action. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021), <https://docs.house.gov/billsthisweek/20201207/CRPT-116hrpt617.pdf>.

authority to drive technology adoption and application by the Department.

- **Assign the tri-chair Steering Committee on Emerging Technology responsibility for overseeing the development of a Technology Annex to the next National Defense Strategy³⁷**

Action for Congress:

- **In the National Defense Authorization Act (NDAA) for Fiscal Year 2022, establish a Steering Committee on Emerging Technology and National Security Threats and designate that it be tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence.**

Recommendation: Build the Technical Backbone

Integration of AI into DoD operations requires urgent investment in a modern digital ecosystem that will enable ubiquitous development and fielding at all levels—from the headquarters to the tactical edge. It is most essential to establish a technical foundation that: 1) provides access to leading cloud technologies and services for scalable computing; 2) enables the sharing of data, software, and capabilities through well-documented and hardened application programming interfaces (API) with proper access controls; and 3) gives all DoD developers and scientists access to the tools and resources they need to drive new AI capabilities. This should be realized through a federated approach, building on existing resources and pathfinder efforts.³⁸

The key elements that comprise the envisioned AI digital ecosystem are:

- *Contributors and Users.* A diverse, distributed network that includes development teams working at the tactical edge and at headquarters levels; private sector partners contributing trained models and applications; academic researchers working on open challenge problems; researchers working within a DoD lab; or international allies or partners co-developing interoperable AI capabilities.
- *Common Interfaces.* A service-oriented architecture where resources at each level of the stack are accessed and maintained through common application programming interfaces based on industry-standard protocols.

³⁷ This action is mirrored in the Chapter 3 and Chapter 5 Blueprints for Action.

³⁸ The DoD's Joint AI Center (JAIC) is building a joint common foundation (JCF) that aims to provide policies and tools that support an enterprise cloud-enabled AI environment. See *About the JAIC*, JAIC (last accessed Feb. 2, 2021), <https://www.ai.mil/about.html>. Other Digital ecosystem pathfinders include, but are not limited to, the Air Force's PlatformOne, Kessel Run, Space CAMP, Black Pearl, CReATE, ADVANA, and the Army Futures Command Software Factory.

DRAFT NSCAI DOCUMENT

- *Authentication.* Enhancing both the sharing and the safeguarding of resources through a uniform policy and practice for managing authoritative, shared user attributes across classification levels to control who will build, use, or share AI building blocks.³⁹
- *Applications.* Discoverable and accessible AI solutions ready for fielding through provisioned platform environments.⁴⁰
- *Platforms.* Environments that support development, testing, fielding, and continuous updating of applications to diverse sets of contributors and users.⁴¹ These platforms include workflows and processes supporting the DevSecOps⁴² lifecycle, MLOps⁴³ for machine learning pipelines, and digital engineering.⁴⁴
- *Software.* Federated software architecture⁴⁵ linking distributed repositories hosted across the Department by mission components, their software factories, and service labs, making software discoverable through a catalog.⁴⁶ Includes AI algorithms, data analysis tools, and tools supporting TEVV⁴⁷ as well as processes and tools to support continuous Authorization to Operate (ATO) frameworks and reciprocity.⁴⁸
- *Data.* Federated and secured data architecture linking distributed repositories across the department hosted by mission components, service labs, and enterprise programs, making

³⁹ See DoD Digital Modernization Strategy, U.S. Department of Defense at 30, 42-43 (Jul. 12, 2019), <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF> (describing how the DoD plans to deploy an end-to-end identity, credential, and access management infrastructure). This is an essential function that must be implemented in an interoperable way across the national security-wide digital AI R&D ecosystem. DoD plans include a goal to “Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation.” Id. at 30.

⁴⁰ Implemented as applications as a service (AaaS).

⁴¹ Implemented as platforms as a service (PaaS).

⁴² The digital ecosystem should incorporate DevSecOps processes and tools laid out in the DoD Enterprise DevSecOps Reference Design. See DoD Enterprise DevSecOps Reference Design, U.S. Department of Defense (Aug. 12, 2019), https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf. For more information see *Understanding the Differences Between Agile & DevSecOps - from a Business Perspective*, GSA (last accessed Jan. 1, 2021), <https://tech.gsa.gov/guides/understanding-differences-agile-devsecops/> (“DevSecOps improves the lead time and frequency of delivery outcomes through enhanced engineering practices; promoting a more cohesive collaboration between Development, Security, and Operations teams as they work towards continuous integration and delivery.”).

⁴³ For a short primer on MLOps, see *2021 Technology Spotlight - The Emergence of MLOps*, Booz Allen Hamilton (2021), https://www.boozallen.com/content/dam/boozallen_site/dig/pdf/white_paper/the-emergence-of-mlops.pdf.

⁴⁴ Notably, the Office of the Under Secretary of Defense for Research & Engineering (OUSD(R&E)) in 2020 outlined a similar vision for an enterprise-wide, shared digital ecosystem to implement the Department’s Digital Engineering Strategy and accelerate broad adoption of model-based system engineering. See Andrew Monje, *Future Direction of Model-Based Engineering Across the Department of Defense*, U.S. Department of Defense (Jan. 27, 2020), <https://ac.cto.mil/wp-content/uploads/2020/05/RAMS-Monje-27Jan2020-Future.pdf>.

⁴⁵ A common software delivery platform used by industry and academia based on the features of Git (<https://git-scm.com>), GitHub (<https://github.com>), and GitLab (<https://about.gitlab.com>).

⁴⁶ Implemented as software as a service (SaaS).

⁴⁷ See Chapter 7 of this report. See also Issue 2: Recommendation 6: Expedite the development of tools to create tailored AI test beds supported by both virtual and blended environments, in *Second Quarter Recommendations*, NSCAI at 14 (July 2020), <https://www.nscai.gov/previous-reports/>.

⁴⁸ See Issue 1 - Recommendation 1: Create an AI software repository to support AI R&D, *Second Quarter Recommendations*, NSCAI at 3 (July 2020), <https://www.nscai.gov/previous-reports/>; see also Issue 1 - Recommendation 2: Promote ATO reciprocity as the default practice within and among programs, Services, and other DoD agencies to enable sharing of software platforms, components, infrastructure, and data for rapid deployment of new capabilities, in *Second Quarter Recommendations*, NSCAI at 5 (July 2020), <https://www.nscai.gov/previous-reports/>.

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

data discoverable through a catalog.⁴⁹ With appropriate access controls, this will facilitate finding, accessing, and moving desired data across the Department⁵⁰ including datasets, associated data models, and trained AI models along with supporting documentation.⁵¹

- *Hardware Infrastructure.* Networking and communications backbone to transport ecosystem resources, particularly data, and provide seamless access and interchange between cloud computing and storage services.

To accelerate the process of building on existing resources and pathfinder efforts, and to increase interoperability in the short-term, DoD should determine a governance structure and develop necessary policies and guidance, draft a reference design, and make the technical investments in the network and in platform environments. Implemented correctly, the digital ecosystem will ensure force-multiplying common access and interoperability. The Blueprint for Action framework outlined below marries top-down coordination and direction with bottom-up mission implementation to realize an enterprise-wide ecosystem in a manner that does not slow or stymie innovation, but rather incorporates new capabilities at the speed of innovation and mission requirements.

Actions for the Department of Defense:

- **Establish Digital Ecosystem Leadership and Governance.**
 - The Secretary of Defense should direct the establishment of an enterprise-wide digital ecosystem to support capability development to maintain the technological superiority of the United States military.
 - To ensure senior leader oversight and sustained resourcing, the Secretary should assign the Steering Committee on Emerging Technology with the responsibility to oversee the implementation and sustainment of the ecosystem.
 - The Secretary should assign the DoD Chief Information Officer (CIO) as the Executive Agent responsible for the ecosystem design, development, and operation.
 - The Steering Committee on Emerging Technology, coordinating with the DoD CIO, DoD Comptroller, Cost Assessment and Program Evaluation, and appropriate acquisition and programming representatives from the military services, should produce a funding plan⁵² for the ecosystem within 90 days of the Secretary's direction.

⁴⁹ Implemented as data as a service (DaaS). See Issue 1 - Recommendation 3: Create a DoD-wide AI data catalog to enable data discovery for AI R&D, *Second Quarter Recommendations*, NSCAI at 7 (July 2020), <https://www.nscai.gov/previous-reports/>.

⁵⁰ The data services and resources provided by the digital ecosystem should support the DoD Data Strategy. See *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept 30, 2020), <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

⁵¹ See the Appendix on Key Considerations for Responsible Development & Fielding of AI and Chapter 7 of this report for additional details on AI documentation.

⁵² As part of the funding plan the Department should consider proposing expansion of the pilot for consumption-based solutions outlined in Section 834 of the FY 2021 NDAA to extend across the stack of managed services that compose the digital

DRAFT NSCAI DOCUMENT

- DoD CIO should form and chair an enduring digital ecosystem implementation working group⁵³ to establish and maintain an open architecture, an evolving reference design, governance structure, and processes to include management and authorization for ecosystem functions and growth. The Steering Committee on Emerging Technology will ensure strategic direction and coordination and pathfinder organizations will provide bottom-up and mission-oriented implementation.⁵⁴
 - The working group should report to the Steering Committee on Emerging Technology, add members when appropriate, and include representatives from:⁵⁵
 - The Office of the DoD Chief Data Officer (CDO).
 - Component CIOs and CDOs.
 - The Joint Artificial Intelligence Center (JAIC).
 - The Office of the Under Secretary of Defense for Research & Engineering (OUSD(R&E)).
 - The Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)).
 - The Office of the Under Secretary of Defense for Intelligence & Security (OUSD(I&S)).
 - Service Acquisition Executives.
 - The Office of the Director of Operational Test and Evaluation (DOT&E).
 - The Director of the Defense Advanced Research Projects Agency (DARPA).
 - Digital ecosystem pathfinders, including but not limited to the Air Force's PlatformOne, Kessel Run, Space CAMP, the Navy's Black Pearl, the Army's CReATE, ADVANA, and the Army Futures Command Software Factory.⁵⁶

ecosystem. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

⁵³ DoD CIO should determine the appropriate structure for such a working group and may decide to leverage or federate existing cross-functional working groups such as those for the DoD Enterprise DevSecOps Initiative or Enterprise Infrastructure. Similarly, DoD CIO should work with pathfinder organizations to determine whether they should be incorporated as part of the governance working group or broken out as a separate community from which to draw best practices.

⁵⁴ For example, contributions to the digital ecosystem would come from AI delivery teams at the combatant command headquarters level, and from forward-deployed teams, as they leverage the ecosystem for agile development of AI-driven capabilities.

⁵⁵ The list included is intended as a general outline of key stakeholders; it is not exhaustive.

⁵⁶ In recent years the Department has made promising initial steps to establish managed services constructs for platforms, cloud infrastructure, and software development. For example, the Air Force's CloudOne and PlatformOne as well as multiple in-house software factories such as Kessel Run and Space CAMP (<https://software.af.mil/software-factories> and <https://software.af.mil/dsop/services/>); the Navy's Black Pearl (<https://blackpearl.us/>); and the Army's Coding Repository and Transformation Environment (CReATE) and new software factory at Army Futures Command. Further, the Office of the Secretary of Defense has built a data management platform, ADVANA, with the goal to establish it as the single authoritative source for audit and business data analytics. See Written Statement for the Record of David L. Norquist, Deputy Secretary of Defense before the U.S. Senate Armed Services Committee Subcommittee on Readiness at 6 (Nov. 20, 2019), https://www.armed-services.senate.gov/imo/media/doc/Norquist_11-20-19.pdf.

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

- **Develop and Mandate Participation in a Digital Ecosystem Governed by an Open Architecture and Reference Design.**
 - Within 12 months of the Secretary’s direction to establish the ecosystem, the DoD CIO should work with the implementation working group to develop and publish an open, interoperable architecture⁵⁷ built on common interfaces based on industry-standard protocols along with an evolving reference design..⁵⁸
 - The open architecture and reference design should be owned by the DoD CIO and reviewed quarterly and updated through the working group.
 - An unclassified version of the open architecture and reference design should be published publicly for commercial capability providers.
 - The Secretary of Defense should issue a memorandum that requires all new joint and service programs participate in the digital ecosystem and adhere to the open architecture.⁵⁹ This should include a requirement that all existing programs develop a plan to participate and become interoperable with the digital ecosystem wherever possible by 2025.
 - Through the Joint Requirements Oversight Council (JROC), the Vice Chairman of the Joint Chiefs of Staff (VCJCS) and USD(R&E)⁶⁰ should ensure that all joint and service programs designed to meet joint capability needs adhere to the digital ecosystem open architecture.
 - The DoD CDO, acting in coordination with the DoD Data Council, should ensure that the Data Strategy Implementation Plans developed by each Component under the DoD Data Strategy adhere to the digital ecosystem open architecture.⁶¹
 - The USD(A&S) should update the guidance governing the formatting requirements for deliverable data in contracts to be well documented,⁶² “non-proprietary formats designed for interoperability.”⁶³
 - The Steering Committee on Emerging Technology should lead an effort with the Intelligence Community (IC) to assess additional ways to accelerate implementation and leverage the digital ecosystem, including designating service

⁵⁷ The digital ecosystem’s open architecture should be developed with consideration of existing warfighting architectures. For example, the Joint Warfighting Network Architecture recommended in Chapter 3 of this report.

⁵⁸ The open architecture should: 1) define a common set of well-documented common interfaces for the ecosystem’s key components and building blocks; 2) support and integrate the work of existing pathfinders up and down the ecosystem technology stack; and 3) incorporate the process elements of the DoD DevSecOps Reference Design Version 1.0 12 August 2019, data authorizations, and continuous software ATO reciprocity.

⁵⁹ The CIO should include guidance along with the open architecture describing what categories of systems are to be adherent and which may be exempt.

⁶⁰ NSCAI recommends that USD(R&E) be appointed co-chair and chief science advisor to the Joint Requirements Oversight Council (JROC) for Joint and cross-domain capabilities. See also *Interim Report and Third Quarter Recommendations*, NSCAI at 70 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

⁶¹ The Executive Summary that accompanies the DoD Data Strategy states that each Component will develop “measurable Data Strategy Implementation Plans, overseen by the CDO and DoD Data Council.” See *Executive Summary: DoD Data Strategy*, U.S. Department of Defense (Sept 30, 2020), <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

⁶² For example, ensuring contract Data Item Descriptions (DIDs) include the use of application programming interfaces as the data transfer medium. See the Appendix on Key Considerations for Responsible Development & Fielding of AI and Chapter 7 of this report for additional details on AI documentation.

⁶³ Memorandum from Deputy Secretary of Defense, *Actions to Enhance and Accelerate Enterprise Data Management*, U.S. Department of Defense at 1 (Dec. 10, 2020).

providers to proliferate applications across the enterprise and make them available for integration into complex mission solutions.⁶⁴ Wherever possible, the digital ecosystem's open architecture should leverage and interoperate with proven solutions from the IC such as the Information Technology Environment recommended in Chapter 5 of this report.

- **Establish a Strategic Data Node.**

- The DoD CDO should make it a priority to create a linked, large-scale, cloud-based data repository (i.e., a node within the digital ecosystem) adherent to the data service interfaces specified in the ecosystem's open architecture. This would be a critical step to enable distributed development efforts by providing AI development teams secure access to authoritative data from diverse mission sets and functional areas and serve as a prototype for the digital ecosystem reference design.⁶⁵
 - The CDO should create this strategic data node by integrating digital ecosystem interoperability into the DoD ADVANA system⁶⁶ and prioritize construction of enterprise datasets as recommended below.

- **Expand the Network and Communications Backbone to the Digital Ecosystem.**

- The Department should fully fund its network and communications modernization effort as outlined in the DoD Digital Modernization Strategy,⁶⁷ require the DoD CIO to factor this into their list of highest priorities, and hold the DoD CIO accountable for expediting critical upgrades.

- **Create a Marketplace to Promote Democratization of AI Building Blocks.**

- The DoD CIO, in accordance with the digital ecosystem governance and reference design addressed above, should create an AI marketplace for strategic exchanges of the essential AI building blocks.⁶⁸ The marketplace should include:

⁶⁴ As an example, the Steering Committee on Emerging Technology could consider designating the Defense Logistics Agency (DLA) as an enterprise service provider for logistics applications and associated services. These applications would be made available within the ecosystem for reuse and integration. Similarly, upon publication of the reference design, the Committee could explore working with the Intelligence Community to designate and integrate Intelligence Community application service providers (e.g., the National Geospatial Agency for GEOINT application services).

⁶⁵ The repository would support implementation of the DoD Data Strategy; the Strategy's guiding principles include "data is a strategic asset" and "enterprise-wide data access and availability." See *DoD Data Strategy*, U.S. Department of Defense at 3-4 (Sept. 30, 2020), <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

⁶⁶ See "Advana" *Defense Analytics Platform – Department of Defense*, ACT-IAC (June 16, 2020), <https://www.youtube.com/watch?v=BIQ31B9Hv44>.

⁶⁷ The digital ecosystem rides on the capacity of DoD's underlying network and communication backbone to provide rapid, on-demand access to the essential AI building blocks. The DoD Digital Modernization Strategy calls out the need to modernize the Department's primary networks, the warfighter's communication connectivity, and coalition networks—highlighting the need to upgrade the optical network transport, routers, switches, and satellite gateways. See *DoD Digital Modernization Strategy*, U.S. Department of Defense at 20-21, 35, 37 (July 12, 2019), <https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF>.

⁶⁸ Components of which are already underway as a result of the JAIC's Joint Common Foundation initiative.

DRAFT NSCAI DOCUMENT

- SoftEx – GitLab-like⁶⁹ software repository system⁷⁰ hosting AI algorithms, testing, evaluation, verification, and validation (TEVV) tools,⁷¹ hardened AI software stacks, etc.
 - DataEx – a federated data repository system⁷² of AI-ready data sets, documentation, and associated data models.⁷³
 - ModelEx – a federated repository system of trained models⁷⁴ generated from various types of AI approaches and techniques, including statistical machine learning.⁷⁵
 - CloudEx – a cloud-agnostic, networked marketplace for pre-negotiated computing and storage services from a pool of vetted cloud providers.⁷⁶
 - Trusted partners (inside and outside government) should be able to develop solutions and products within secured environments of the ecosystem, offering monetized access to users.⁷⁷
- **Develop Prototypical Platform Environments within the Digital Ecosystem.**
 - The DoD CIO should work closely with the digital ecosystem pathfinder community to build a set of tailorable development environments for training AI systems using: data-driven statistical machine learning; the latest simulation and modeling capabilities to support reinforcement learning (e.g., digital twinning within an accurate world model); and complementary TEVV services.⁷⁸

⁶⁹ A common software delivery platform used by industry and academia based on the features of Git (<https://git-scm.com>), GitHub (<https://github.com>), and GitLab (<https://about.gitlab.com>).

⁷⁰ See Issue 1 - Recommendation 1: Create an AI software repository to support AI R&D, in *Second Quarter Recommendations*, NSCAI at 3 (July 2020), <https://www.nscai.gov/previous-reports/>.

⁷¹ See Chapter 7 of this report. Also see Issue 2 - Recommendation 6: Expedite the development of tools to create tailored AI test beds supported by both virtual and blended environments, in *Second Quarter Recommendations*, NSCAI at 14 (July 2020), <https://www.nscai.gov/previous-reports/>.

⁷² A federated repository system uses a federated directory that ties distributed repositories together as a virtual whole. See Issue 1 - Recommendation 3: Create a DoD-wide AI data catalog to enable data discoverability for AI R&D, in *Second Quarter Recommendations*, NSCAI at 7 (July 2020), <https://www.nscai.gov/previous-reports/>.

⁷³ This would be supported by the prototype centralized data repository recommended above and hinges on implementation of the new DoD Data Strategy, which details the goals to make DoD data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. *DoD Data Strategy*, U.S. Department of Defense at 6 (Sept. 30, 2020), <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

⁷⁴ Trained AI models are a special class of data, and the same federated repository system solution used for DataEx can also be used to support ModelEx.

⁷⁵ Another type of anticipated trained AI model is digital twins as modeling and simulation platforms such as the Army's One World Terrain advance to support training digital twins through reinforcement learning. For more on One World Terrain, see *One World Terrain: A Pillar of the Army's Synthetic Training Environment*, USCICT (Aug. 2, 2019), <https://www.youtube.com/watch?v=K50eL1wU4ic>.

⁷⁶ DoD users can choose services off a multi-cloud provider schedule paying as you go for computing resources and uploading/storing the government's data. To facilitate seamless migration of data and software from one platform to another, the DoD should negotiate contracts with providers that appropriately limit expenses related to data egress and migration.

⁷⁷ Internally-developed software solutions and data sets could be contributed for use across the DoD (to address common challenges and capability needs) with built-in incentives for contributors through awarded cloud credits when products are contributed and used. Limited public-facing elements could be brokered on the National AI Research Resource. See Issue 2 - Recommendation 3: Launch a Task Force Study and Pilot Program to Establish a National AI Research Resource, in *First Quarter Recommendations*, NSCAI at 12 (Mar. 2020), <https://www.nscai.gov/previous-reports/>.

⁷⁸ See Chapter 7 of this report.

DRAFT NSCAI DOCUMENT

- The DoD CIO should work closely with the digital ecosystem pathfinder community to implement a set of prototypical platform environments⁷⁹ that support development, testing, fielding, and continuous update of AI-powered applications for diverse categories of contributors and users.⁸⁰

Action for Congress:

- **Prioritize funding for the Department’s digital ecosystem and associated activities.**
 - The Armed Services Committees should use the FY 2022 NDAA to direct the Department to develop a resourcing plan for the digital ecosystem that establishes, sustains, and incentivizes use of its various components as enterprise-wide, enduring resources.
 - The Committees should also authorize the obligation of funds to begin work on the ecosystem.

Recommendation: Train and Educate Warfighters

Warfighters need the following capabilities to effectively build and use AI-enabled systems:

- **Data-informed decision-making:** Data-informed decision-making uses data to generate insights and act on them. Data-driven organizations often make decisions more quickly, at lower levels in the organization, and with a stronger empirical foundation than organizations that rely primarily on intuitive or experience-based decision-making.⁸¹
- **Computational thinking:** Service members need to better understand how to use information processing agents to perform beneficial calculations that could not be done quickly or efficiently by a human, rather than just representing human thinking in a digital format.
- **Maker culture:** Service members of all ranks and occupations need regular contact with AI-enabled machines, and should be able and encouraged to experiment with and participate in the development of new tools.
- **Human-machine teaming:** Military leaders need to understand how to effectively provide input to machines, interpret machine outputs, and critically, when to trust or not trust machine outputs.⁸²

⁷⁹ These platform environments should have ATO reciprocity for the building blocks they provision, including incorporating DevSecOps development stacks.

⁸⁰ Digital ecosystem contributors and users include embedded development teams working at the tactical edge (see below Recommendation: Embed AI development capabilities in support of operations); private sector partners contributing trained models; academic researchers working on open challenge problems; researchers working within a DoD lab; or international partners co-developing interoperable AI capabilities.

⁸¹ Becky Frankiewicz & Tomas Chamorro-Premuzic, *Digital Transformation Is About Talent, Not Technology*, Harvard Business Review (May 6, 2020), <https://hbr.org/2020/05/digital-transformation-is-about-talent-not-technology>.

⁸² As recommended in Chapter 7 of this report, national security departments and agencies should provide ongoing training to help the workforce better interact, collaborate with, and be supported by AI systems—including understanding AI tools.

- **Organizational transformation:** Leaders need to understand when and how to integrate AI-related tasks into their organization’s priorities, allocate resources needed to build and maintain the AI stack, oversee the deployment and scaling of new systems, and how to effectively interact with and support the careers of their technical experts.

Component 1: Integrate Digital Skill Sets and Computational Thinking into Military Junior Leader Education.

Military junior leaders need to understand enough about AI to manage and operate AI-enabled organizations responsibly and effectively. Commanding and leading AI-driven systems and humans are very different fields. Leadership is even more complex in organizations that combine human and AI elements. The below skill sets will equip junior leaders with the fundamental skills needed.

Problem Definition and Curation. Military leaders need to understand problem curation, or the process of discovering the causal mechanisms that lead to problems, associated issues, stakeholders, and potential minimum viable products.⁸³ Poor problem definition and curation can lead to projects that attempt to solve the incorrect problem, wasting significant amounts of time and money. This is particularly true for AI. Not all problems can be solved using the type of probabilistic reasoning performed by many algorithms, or with limited data sets. Also, many problems with potential AI solutions can be solved with much easier, less resource intensive techniques. Military leaders that understand problem curation will be better able to identify problems with potential AI solutions, and, just as importantly, problems that AI will not help solve. This would not only help with the use of AI but would also make junior leaders generally more productive.

A Conceptual Understanding of the AI Stack. The AI stack is a model that “provides a streamlined approach to visualize, plan, and prioritize strategic investments in commercial technologies and transformational research to leverage and continuously advance AI across operational domains, and achieve asymmetric capability through human augmentation and autonomous systems.”⁸⁴ A conceptual understanding of the AI stack would reinforce the importance of building structural solutions to data collection, management, curation, installation of sensors, and other underappreciated topics and reduce attempts to add AI at the end of a project. It will also help military leaders better understand what part of their adversaries’ AI to target to degrade its effectiveness.

Data Collection and Management. Junior leaders need to understand how to collect and manage data and to use systems that do the same in a manner that prepares it for exploitation, and to operate in an environment where adversaries are doing the same. They also need to understand the causes, effects, and ethical implications of data bias. Training junior leaders to

⁸³ Steve Blank & Pete Newell, *What Your Innovation Process Should Look Like*, Harvard Business Review (Sept. 11, 2017), <https://hbr.org/2017/09/what-your-innovation-process-should-look-like>.

⁸⁴ Andrew Moore, et al., *The AI Stack: A Blueprint for Developing and Deploying Artificial Intelligence*, Proc. SPIE 10635 (May 4, 2018), <https://doi.org/10.1117/12.2309483>. For a graphical depiction of the AI stack, see *About*, Carnegie Mellon University Artificial Intelligence (last accessed Jan. 1, 2021), <https://ai.cs.cmu.edu/about>.

collect and manage data with the same degree of responsibility and expertise that they use for medical care and equipment maintenance would accelerate the government's ability to create AI solutions, and to employ data-informed decision-making.

Understanding Probabilistic Reasoning and Data Visualization. Junior leaders need to know enough about probabilistic reasoning and data visualization to understand the outputs of their AI systems and their implications for a particular situation or environment. This is critically linked to understanding when to trust and not trust a system's outputs, and other aspects of commanding and leading AI-driven systems. Notably, this does not require leaders to perform computational statistics, just to understand their output, a much less demanding task.

Data-informed Decision-making. To make data-informed decisions, leaders need to understand system thinking and critical thinking. System thinking combines all of the above to create an empirical but incomplete understanding of factors influencing a decision, and how both their system affects their AI and how their decision will affect their system. Critical thinking will help leaders understand the limits of AI, and the limits of data-informed decision-making processes that are based on imperfect information. This report references data-informed rather than data-driven decision-making because military leaders should never be bound by the imperfect information in front of them. Their critical thinking, judgement, and intuitive understanding of both their system and their environment will always have a critical role to play, even as it is informed by decision-making aids.

Action for Congress:

- **Require the military services to integrate digital skills and computational thinking into pre-commissioning and entry-level training.**
 - The Armed Services Committees should use the National Defense Authorization Act for Fiscal Year 2022 (FY 2022 NDAA) to require the military services to integrate understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making into existing, pre-commissioning or entry-level training for junior officers and training for non-commissioned officers within one year of the passage of the legislation.

Action for the Military Services:

- **Integrate digital skills and computational thinking into pre-commissioning and entry-level training.**
 - The military services need to integrate understanding problem curation, the AI lifecycle, data collection and management, probabilistic reasoning and data visualization, and data-informed decision-making into pre-commissioning or entry-level training for junior officers and training for both junior and senior non-commissioned officers. The military services can accomplish this by creating new

modules or courses, or by integrating this training into existing training and education for commissioned and non-commissioned officers. Whenever possible, this training should include the use of existing AI-enabled systems and tools.

Component 2: Integrate Emerging and Disruptive Technologies into Service-level Professional Military Education.

While it is critical that military junior leaders better understand digital technology, military leaders must also understand how technology will affect warfare, their role in their organization, and how they should integrate new technology, both as they increase in rank and responsibility and as technology changes.

Action for Congress:

- **Require the military services to integrate emerging and disruptive technologies into service-level Professional Military Education.**
 - The Armed Services Committees should use the FY 2022 NDAA to direct the DoD to require emerging and disruptive technologies courses for officers within one year. The Armed Services Committees should also require the DoD to develop a training plan that incrementally builds the necessary skills in its officer corps.

Action for the Military Services:

- **Integrate emerging and disruptive technologies into service-level Professional Military Education.**
 - Course materials should address AI and other militarily significant emerging technologies, as identified by the military services and the USD(R&E), in coordination with the national laboratories, federally funded research and development centers (FFRDCs), and university affiliated research centers (UARCs).
 - Course materials should include an introduction to the latest technology, the benefits and challenges of adapting new technologies, how organizations successfully and unsuccessfully adopt these technologies, and ethical issues surrounding the uses of emerging technologies, including the impact of biases in these technologies.
 - As officers progress in rank, such courses should increasingly build the knowledge base, vocabulary, and skills necessary to better understand new threats/challenges, develop operational and organizational concepts, and incorporate technology into operations and operational support.
 - Military services should establish a mechanism that audits these courses annually to ensure that emerging technologies have been properly identified, and that the

nomenclature, lexicon, definitions, and course content matches changes in emerging technologies.

Component 3: Create Emerging and Disruptive Technology Coded Billets in the Department of Defense.

It is crucial that the DoD incentivize and increase the skill needed to introduce and field emerging and disruptive technologies within the military officer corps. The joint qualification process can serve as a model. The DoD already designates that certain, critical billets must be filled by Joint Qualified Officers⁸⁵ and different levels of joint qualification.⁸⁶ To do this, the DoD should create emerging and disruptive technology designated billets for officers that require an emerging and disruptive technology qualification prior to assignment and a process for military leaders to become emerging and disruptive technology qualified. Emerging and disruptive technology qualified officers would add value in a number of areas for the services, including: 1) assisting with acquisition of emerging technology, 2) helping integrate technology into field units, 3) developing organizational and operational concepts, and 4) developing training and education plans.

Action for Congress:

- **Require the Department of Defense to create emerging and disruptive technology critical billets that must be filled by emerging technology certified leaders.**

Actions for the Department of Defense:

- **Create billets that require officers to become emerging and disruptive technology certified before serving in the positions.**
 - The Office of the USD(R&E) should define emerging and disruptive technologies.
 - These include but are not limited to positions that develop military doctrine and/or operating concepts; positions within Force Structure, Resources, and Assessment directorates; positions within Force Development directorates; and leadership positions at the operational and tactical levels within the military services.
- **Create a process for officers to become emerging and disruptive technology certified.**
 - The process to become emerging tech certified would resemble the joint qualification system.

⁸⁵ Pub. L. 109-364, John Warner National Defense Authorization Act for Fiscal Year 2007, 109th Cong. (2006).

⁸⁶ *DoD Instruction 1300.19: DOD Joint Officer Management Program*, U.S. Department of Defense at 14 (Apr. 3, 2018), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/130019p.pdf?ver=2018-04-03-114842-923>.

- Officers should become emerging technology qualified by serving in emerging technology focused fellowships,⁸⁷ emerging technology focused talent exchanges, emerging technology focused positions within government, and completing educational courses focused on emerging technologies.

Recommendation: Accelerate Adoption of Existing Digital Technologies

The Department must have an integrated approach to AI and other emerging technologies that ensures the U.S. military can continuously identify, source, field, and update capabilities faster than our competitors. This requires more targeted investment in dual-use technologies, ensuring system adaptability through a more agile budget and oversight process, and streamlining the acquisition process to shed those rules and regulations whose benefits are outweighed by the burdens imposed on the system. Critically, the Defense Acquisition System must shift away from a one-size-fits-all approach to measuring value from the acquisition process. Adherence to cost, schedule, and performance baselines is rarely a proxy for value delivered, but is particularly unsuited for measuring and incentivizing the iterative approaches inherent in AI and other software-based digital technologies. Unless the requirements, budgeting, and acquisition processes are aligned to permit faster and more targeted execution, the U.S. will fail to stay ahead of potential adversaries.

Component 1: Adopt Proven Commercial AI Applications for Core Business Processes.

Commercial AI applications for business processes can generate labor and cost savings, speed administrative actions, and inform decision-making with superior insights. To realize these benefits, DoD should initiate the digital transformation of its core administrative functions.

Efforts to apply business AI depend on the availability of clean, organized data. Significant resources are required to access, clean, and label enterprise data from the range of legacy business platforms.

DoD should create opportunities for bottom-up identification of AI use cases by incentivizing DoD organizations to deploy proven commercial applications tailored to their specific mission needs. Promising categories of commercial AI include: 1) knowledge management applications such as intelligent search tools that index, retrieve, and display an agency's digital information, as well as collective intelligence and coaching tools that accumulate and exchange tacit knowledge across an agency's workforce; 2) AI-enabled tools that analyze business information to identify patterns, develop insights, and inform decision-making, and; 3) Robotic Process Automation (RPA) tools including desktop assistants, bots, and other personal productivity applications that automate individual office functions.

Actions for the Department of Defense:

⁸⁷ See Chapter 2 of this report and this associated Blueprint for Action's section below about leveraging public-private talent exchanges to infuse technical expertise into the acquisition corps for NSCAI's recommendation to create a technology fellows program to support development of a technology annex to the National Defense Strategy; there are numerous extant fellowships across the DoD involving emerging technologies.

- **Prioritize construction of enterprise data sets across core DoD business administration areas.**⁸⁸
 - The Deputy Secretary of Defense should:
 - Assign the DoD Chief Data Officer (CDO) responsibility for working with institutional stakeholders to develop enterprise datasets for human resources, budget & finance, acquisition, logistics, retail, real estate, and health care.
 - Place special priority on the CDO building an enterprise dataset that supports portfolio management of investments in emerging technologies, spanning budget requests, acquisition, contracting, and invoicing.⁸⁹
 - Assign the JAIC to support the DoD CDO in developing new methods for generating higher quality data for each core business administration area at the point of origin. This would include applying data tags that allow AI-enabled cross domain analyses.⁹⁰ As part of this effort, the JAIC should also look to develop or procure AI tools that continuously extract tagged information for analysis from enterprise data sets.
 - Ensure sufficient funding is included as part of the FY 2023 budget request to provide data engineering services.
 - The Secretary of Defense should issue a department-wide directive mandating the review and streamlining of policies and regulations wherever possible to increase and accelerate data sharing across agencies, with proper protections, building on the JAIC's Gamechanger AI prototype to analyze and modernize the framework within which data access rules are enforced.
- **Launch a department-wide initiative to incentivize rapid deployment of commercial AI solutions for business functions.**
 - The Deputy Secretary of Defense should assign the JAIC, in its role as the Department's AI accelerator,⁹¹ to administer allocation of matching funds, monitor and assess results, and disseminate best practices and lessons learned for the deployment of AI solutions for knowledge management, business analytics,

⁸⁸ This action aligns with the recommendation to establish a strategic data node within the digital ecosystem discussed earlier in this Blueprint and with the DoD Data Strategy, which lists Senior Leader Decision Support and Business Analytics as initial areas of focus. See *DoD Data Strategy*, U.S. Department of Defense at 11 (Sept. 30, 2020), <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF>.

⁸⁹ Notably, this recommendation is aligned with Section 836 of the FY 2021 National Defense Authorization Act, which directs the Secretary of Defense to develop and integrate advanced digital data management and analytics capabilities that integrate all aspects of the defense acquisition system; facilitate the management and analysis of all relevant data; enable the use of such data to inform further development, acquisition, management and oversight of such systems, including portfolio management; and include software capabilities to collect, transport, organize, manage, make available, and analyze relevant data throughout the life cycle of defense acquisition programs." The section further requires capability demonstrations and revised policies to promote the use of digital management and analytics capabilities by March 15, 2022. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

⁹⁰ For example, critical human resource variables such as performance and retention are likely related to budget variables (pay), health care variables (accessibility and quality of care) and even real estate variables (housing). These relationships will become transparent and quantifiable when data tagging supports cross domain analyses.

⁹¹ See discussion below for details on the responsibilities envisioned for JAIC as the Department's AI Accelerator.

DRAFT NSCAI DOCUMENT

- and RPA across the Department, defense agencies, Services, and Combatant Commands.⁹²
- The Secretary of Defense should issue a DoD directive mandating added flexibility and/or streamlining of policies and regulations wherever possible to increase and accelerate acquisition and deployment of commercial AI software, building on the JAIC's Gamechanger AI prototype to analyze and modernize the existing rules framework.⁹³
 - The Deputy Secretary of Defense should establish a \$100 million fund under the management of the JAIC to accelerate procurement and integration of commercial AI solutions for business applications. This would be used to provide matching incentive funds for agencies contracting with commercial AI vendors with approved solutions. The Deputy Secretary should also:
 - Consider leveraging the defense-wide review process detailed below to identify and reprogram sufficient funds to stand up this fund by the beginning of FY 2022.
 - Ensure sufficient funding is included as part of the FY 2023 budget request to sustain the fund.

Action for Congress:

- **Congress should provide \$125 million as part of the FY 2023 defense appropriations act for developing enterprise-wide datasets and \$100 million for the fund to accelerate procurement and integration of commercial AI solutions for DoD business functions.**

Component 2: Network Digital Innovation Initiatives to Scale Impact.

Too often the Department's enthusiasm for innovation comes at the expense of impact and scale. Dozens of innovation offices across the Department and Services develop, transfer, and apply cutting-edge technology for national security uses.⁹⁴ However, many of the initiatives that are focused on bridging the gap with the technology sector, to include AFWERX, NavalX, Army Applications Laboratory (AAL), and the Defense Innovation Unit (DIU), operate in silos and are

⁹² For example, DIU is currently pursuing a number of AI projects to optimize business processes in the DoD—ranging from using AI-driven Robotic Process Automation to reduce labor costs for the Army Comptroller, to improving Air Force readiness with AI-driven predictive maintenance, to leveraging AI-constructed knowledge graphs to rapidly identify supply chain risks. See *JAIC Partners with DIU on AI/ML Models to Resolve Complex Financial Errors*, JAIC (Oct. 1, 2020), https://www.ai.mil/blog_10_01_20-jaic_partners_with_diu_on_aiml_models_to_resolve_complex_financial_errors.html; *U.S. Defense Department Awards C3.ai \$95M Contract Vehicle to Improve Aircraft Readiness Using AI*, Business Wire (Jan. 15, 2020), <https://www.businesswire.com/news/home/20200115005413/en/US-Defense-Department-Awards-C3.ai-95M-Contract-Vehicle-to-Improve-Aircraft-Readiness-Using-AI>; *Accrete.AI Accelerates Growth and Product Adoption with Defense Innovation Unit Contract*, Accrete.ai (Apr. 23, 2020), <https://blog.accrete.ai/newsroom/accrete.ai-wins-million-dollar-contract-with-the-defense-innovation-unit>.

⁹³ This should include an evaluation of existing policies and regulations on contract data rights, data format, data definitions, and data environments to accelerate application of commercial AI for acquisition, management, and oversight and maximize insights derived.

⁹⁴ For a glimpse into the DoD's innovation ecosystem, see *Tap the Innovation Ecosystem*, MITRE: Acquisition in the Digital Age, (last accessed January 25, 2020), <https://aida.mitre.org/demystifying-dod/innovation-ecosystem/>; *Understanding the DoD Innovation Ecosystem*, MITRE: Bridging Innovation (last accessed Jan. 25, 2020), <https://bridge.mitre.org/visualization/>.

limited in their ability to scale. These pockets of successful bottom-up innovation have achieved some promising results, but disparate activities cannot translate to strategic change without top-down leadership to synchronize efforts and overcome organizational barriers.⁹⁵ The Department should “network” programs that work to source cutting edge technology solutions under the banner of “digital innovation initiatives” to execute a “go to market strategy” for digital technology that is supported at the highest levels of the Department.

Actions for the Department of Defense:

- **Designate an Executive Agent to coordinate the Department’s digital innovation initiatives.**
 - The Secretary of Defense should designate USD(R&E) as Executive Agent for the Department’s digital innovation initiatives⁹⁶ and direct that USD(R&E) coordinate closely with USD(A&S), DoD CIO, and DoD CDO to carry out the responsibilities associated with this role.⁹⁷
 - As Executive Agent, USD(R&E) should facilitate access to resources, provide strategic guidance, and offer other forms of institutional support to enable innovation organizations to execute their current mandates more effectively, without infringing on autonomy or inhibiting bottom-up experimentation.⁹⁸ USD(R&E) should work with the DoD CIO and CDO as well as other institutional stakeholders as appropriate, to:
 - Develop a common digital platform for digital innovation initiatives to share data and best-practices, track ongoing projects, connect with DoD program offices, and identify other means of collaboration.
 - Harness business AI tools to eliminate stovepipes and gain shared understanding of the digital innovation community, including investments and customers.⁹⁹
 - Implement other reporting requirements for the digital innovation initiatives as necessary, so long as they are lightweight and automated to the maximum extent possible.

⁹⁵ See *Interim Report*, NSCAI at 31 (Nov. 2019), <https://www.nscai.gov/previous-reports/>.

⁹⁶ The term “digital innovation initiatives” is used here to describe the various entities across the Office of the Secretary of Defense and the military services, such as the Defense Innovation Unit (DIU), AFWERX, NavalX, and Army Applications Laboratory (AAL), that are focused on bridging the gap with the commercial technology section—especially startups and non-traditional vendors—and accelerating the delivery of best-of-breed technology solutions.

⁹⁷ As the Department’s Chief Technology Officer, USD(R&E) has both the authority and mandate to coordinate discrete efforts across OSD and the military services to accelerate the adoption of digital technology and expand the national security innovation base (NSIB). However, USD(R&E) must ensure close coordination with USD(A&S) and, in the case of IT and information systems, DoD CIO, to improve the transition of solutions emerging from these organizations into operational systems.

⁹⁸ As the Chief Technology Officer of the DoD, USD(R&E) has a “mission to advance technology and innovation.” Additionally, USD(R&E) is responsible for “advis[ing] the Secretary of Defense on all matters related to research; engineering; manufacturing; developmental test & evaluation; and technology development, innovation, and protection activities and programs in the DoD and occurring internationally [as well as] establishing priorities across those matters to ensure conformance with Secretary of Defense policy and guidance.” For a full list of USD(R&E)’s responsibilities and functions, see *DoDD Directive 5137.02: Under Secretary Of Defense For Research And Engineering (USD(R&E))*, U.S. Department of Defense (Jan 4, 2021), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/513702p.pdf?ver=2020-07-15-124712-047>. [hereinafter DoDD 5137.02]

⁹⁹ Also informed by the JAIC, and made accessible through the digital ecosystem.

DRAFT NSCAI DOCUMENT

- **Develop a “go-to-market” strategy for digital technology.**
 - USD(R&E) and USD(A&S) should issue a joint memo outlining a “go-to-market” strategy for digital technology to guide innovation organizations to pursue common objectives,¹⁰⁰ based on the Technology Annex described below. This approach would coordinate efforts for effect and reduce duplication of effort, while preserving room for trial and experimentation with unexpected technologies or applications that could inform new operational concepts.¹⁰¹
 - The Department should back this strategy with significant resources and top-down support, highlighting procurement and development best practices for digital technology¹⁰² and, where appropriate, increasing the procurement budgets of innovation organizations or for other DoD entities to which innovation organizations will hand-off successful prototypes for production.
 - As described further in Chapter 11 of this report, DoD should set a target of increasing its contracts for digital solutions with technology firms from \$500 million to at least \$2 billion over five years and fund digital innovation initiatives appropriately to meet this goal.
 - USD(R&E) should conduct annual investment portfolio reviews of digital innovation initiatives to assess alignment with strategy and report findings to the Steering Committee on Emerging Technology.

- **Optimize operations to enable transition and scaling of AI solutions.**
 - USD(R&E), in partnership with USD(A&S), should assist innovation organizations in providing contracted vendors access and resources to build, deploy, and assure AI solutions often and at scale.¹⁰³ In developing vendor contracts and planning customer journeys, digital innovation initiatives should consider the methods and means to:

¹⁰⁰ While clearly delineating responsibilities and reducing duplication of effort.

¹⁰¹ As described in Chapter 3 of this report, there should be a push-pull relationship between innovative technologies and concepts such that the Technology Annex informs, but does not limit, the scope of activity. Digital Innovation Initiatives will likely continue to have responsibilities outside of this go-to-market strategy, for example the acceleration of commercial AI applications for core business processes.

¹⁰² For example, DIU leverages Other Transaction Authority (OTA) and the Commercial Solutions Opening process to “test, field, and scale commercial technology in less than 24 months.” The Air Force’s AFWERX, in partnership with Air Force Research Lab (AFRL) and DIU’s National Security Innovation Network (NSIN), has pioneered new approaches to Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) funding to “increase the efficiency, effectiveness, and transition rate” of the program. See *Annual Report 2019*, Defense Innovation Unit at 4 (2019), https://assets.ctfassets.net/3nanhbfr0pc/ZF9fhsMe6jtX15APMLalI/cd088a59b91857c5146676e879a615bd/DIU_2019_Annual_Report.pdf; *SBIR Open Topics*, U.S. Air Force AFWERX (last accessed Jan. 1, 2021), <https://www.afwerx.af.mil/sbir.html>.

¹⁰³ Many of the processes and technical roadblocks faced by traditional and non-traditional vendors that slow critical efforts to build and integrate AI systems will be greatly diminished by the implementation of a digital ecosystem, as described above. However, until then, top-down support at the highest levels of leadership will be essential to empower digital innovation initiatives. Per DoDD 5137.02, part of USD(R&E)’s functions include working in conjunction with the Under Secretary of Defense for Acquisition & Sustainment (USD(A&S)) to identify, evaluate, and promote opportunities to reduce barriers to entry for commercial technologies and non-traditional defense partners; and leading initiatives to engage non-traditional suppliers of technology. See DoDD 5137.02.

DRAFT NSCAI DOCUMENT

- Ensure that data access and data security requirements are included in contracts for AI systems that depend on data for training or operations. Provide consistent access to end users as part of AI development processes and throughout the lifecycle of the AI algorithm; and capture in contract terms.
- Include AI testing and evaluation consideration as part of every development agreement.
- Dedicate people and processes to onboard nontraditional vendors, migrate them onto the right networks and sandbox environments, and assist them in securing authorization to operate (ATO)¹⁰⁴
- Connect prototype contract recipients with DoD customers early in the technology development process and match program dollars with additional funding (SBIR, dedicated scaling funds, etc.) wherever possible.¹⁰⁵
- Identify new opportunities for defense primes to team with non-traditional firms to adopt AI capabilities more quickly across existing platforms.¹⁰⁶
- USD(R&E) should work with USD(A&S) to develop common reporting requirements to measure the impact of digital innovation initiatives, building off of ongoing efforts at DIU.¹⁰⁷ Collection of this data should be automated to the maximum extent possible and communicated routinely to Congressional defense committees. Reporting should consider:
 - **Expansion of NSIB:** Number of awards made to companies with no previous DoD experience and percentage of these that receive follow-on contacts; or number of companies that receive recurring government revenue for first-time and funding stability over consecutive quarters.

¹⁰⁴ Where appropriate, efforts should leverage expertise from FFRDCs and UARCs.

¹⁰⁵ Prototyping contracts provide non-recurring engineering dollars to companies for early-stage technologies and projects “to evaluate and inform [their] feasibility or usefulness.” Often these dollars come from dedicated funds, such as the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs and DIU’s internal prototyping budget; and are distributed by organizations like DIU outside of the acquisition lifecycle domains, including DoD programs of record (PoR). Companies executing promising projects through these mechanisms often exhaust prototype funding and are unable to secure sustainable follow-on contracts (i.e. with a clear path toward integration into a PoR) because they cannot identify a customer or the customer’s funding is already committed. AFWERX improved transition in its SBIR program by achieving buy-in from potential customers through matching program funds. See Recommendation 7: Strengthen Return on SBIR Investments in *Interim Report and Third Quarter Recommendations*, NSCAI (October 2020), <https://www.nscai.gov/previous-reports/>; Prototyping Guidebook, U.S. Department of Defense at 36 (Nov. 2019), <https://www.dau.edu/tools/Lists/DAUTools/Attachments/329/DoD%20Prototyping%20Guidebook.%20v2.0.pdf>.

¹⁰⁶ For example, at least one F-22 and F-35 aircraft designated as AI testbeds could incentivize existing contractors and non-traditional firms to work together and better align their incentives to field new mission capabilities. Such an initiative would build on initial efforts to integrate agile software development into F-22 modernization programs. See Craig Ulsh, *Software Acquisition and Practices (SWAP) Study: Vignettes*, DoD Defense Innovation Board at 6 (Jan. 10, 2019), https://media.defense.gov/2019/Mar/07/2002097482/-1/-1/0/SWAP_STUDY_VIGNETTES.PDF.

¹⁰⁷ The 2019 National Defense Authorization Act identified metrics for DIU to report, such as: the number and types of transitions by the Unit to the military departments or fielded to the warfighter.; and the impact of the Unit’s initiatives, outreach, and investments on Department of Defense access to technology leaders and technology not otherwise accessible to the Department, including the number of non-traditional defense contractors with Department of Defense contracts or other transactions resulting directly from the Unit’s initiatives, investments, or outreach; the number of traditional defense contractors with contracts or other transactions resulting directly from the Unit’s initiatives; and the number of innovations delivered into the hands of the warfighter.” See Pub. L. 115-232, sec. 244, John S. McCain National Defense Authorization Act for Fiscal Year 2019, 115th Cong. (2018); Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

DRAFT NSCAI DOCUMENT

- **Rate of Transition:** Number of companies that receive follow-on production contracts.
- **Rate of Scaling:** Number of prototype contract recipients that reach \$10, \$50, \$100, \$500 million, and \$1 billion in total DoD contracts annually.
- **Reach of Products:** Number of users¹⁰⁸ that are benefiting from the product in one year, three years, 10 years, etc.
- **User Experience:** User feedback on the product (scale 1-10).
- **Company Acquisition Process Experience:** Company feedback on the new acquisition process (scale 1-10).
- **Operational/Enterprise Impact:** Actual or projected operational or fiscal return on investment (e.g. initiative addressed an operational gap; innovative RPA reduced production time or manhours X.X%).

Component 3: Expand Use of Specialized Acquisition Pathways and Contracting Approaches.

AI technologies are incompatible with the lengthy, linear processes typical of traditional DoD capabilities acquisition.¹⁰⁹ Recent policy reforms such as the rollout of the Adaptive Acquisition Framework¹¹⁰ and associated resources—such as the Contracting Cone¹¹¹—are positive steps to move the Department away from a “one-size-fits-all” approach to acquisition. However, use of the specialized pathways and authorities¹¹² within the Framework is inconsistent and disincentivized.¹¹³ The traditional acquisition process remains the default for most acquisition

¹⁰⁸ This metric should be appropriately scoped such that consideration is given to products or solutions that lend themselves to enterprise licensing agreements and prioritize measures that indicate the level of cross-service, cross-unit proliferation of a solution.

¹⁰⁹ A 2019 study conducted by the Defense Innovation Board Defense reached similar conclusions with regard to software acquisitions generally, stating “the current approach to software development is broken and is a leading source of risk to DoD; it takes too long, is too expensive, and exposes warfighters to unacceptable risk by delaying their access to tools they need to ensure mission success.” *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, DoD Defense Innovation Board at i (May 2019), <https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF>.

¹¹⁰ The Adaptive Acquisition Framework promotes use of tailored acquisition approaches based on the needed capability. It includes six guiding pathways for acquiring capabilities that Milestone Decision Authorities (MDAs), other Decision Authorities (DAs), and Program Managers (PMs) can “tailor, combine, and transition between”: Urgent Capability Acquisition, Middle Tier of Acquisition, Major Capability Acquisition, Software Acquisition, Defense Business Systems, and Acquisition of Services. See *Adaptive Acquisition Framework Pathways*, Defense Acquisition University, (last accessed Dec. 26, 2020), <https://aaf.dau.edu/aaf/aaf-pathways/>. The Software Acquisition Pathway was developed based on a recommendation from the Defense Innovation Board in the 2019 Software Study. See *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, DoD Defense Innovation Board at 37, S2 (May 2019), <https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF>.

¹¹¹ The Contracting Cone outlines all FAR and Non-FAR contract strategies. *Contracting Cone*, Defense Acquisition University (last accessed Dec. 20, 2020), <https://aaf.dau.edu/aaf/contracting-cone/>.

¹¹² Specialized pathways include approaches captured within the Department’s Adaptive Acquisition Framework such as the Middle Tier of Acquisition and Software Acquisition, that are exempted from certain requirements within the Defense Acquisition System.

¹¹³ In January 2020, former Under Secretary of Defense for Policy Michele Flournoy cited concern over inadequate training and incentives for acquisition professionals to make full use of authorities provided by Congress. She noted “pockets of [acquisition] excellence” in Special Operations Command and the Air Force, but argued the larger acquisition corps “is not using the authorities effectively, consistently, and at scale.” See Testimony of The Honorable Michele A. Flournoy, former Undersecretary of Defense for Policy before the U.S. House of Representatives Armed Services Committee, *Hearing on DoD’s Role in Competing with China* at 6 (Jan. 15, 2020), <https://armedservices.house.gov/cache/files/4/4/44fbef3d-138c-4a0a-b3a9-2f05c898578f/0E4943A5BFAEDA465D485A166FABCF5F.20200115-hasc-michele-flournoy-statement-vfinal.pdf>.

professionals—many of whom are neither incentivized nor properly equipped to make use of the full resources at their disposal through the Framework.

To accelerate delivery of AI-enabled technologies to the warfighter and increase their operational relevance, DoD must build the capacity to use the full breadth of acquisition pathways and contracting approaches.¹¹⁴ Acquisition professionals must have a sufficient understanding of digital and emerging technologies in order to thoughtfully apply these tools. Given the speed of advancements in AI and other software-based technologies, this requires a shift to a continuous learning mindset and a different approach to training for acquisition professionals in which the target metric for success is not course completion, but rather the ability to apply what is learned and impact mission outcomes. DoD should coordinate acquisition workforce training initiatives relative to digital and emerging technologies ongoing across the Department and continuously assess acquisition workforce capability needs. Importantly, the DoD must also ensure acquisition personnel have common access to available digital technology courses and best practices as well as a community of experts that illustrate how specialized authorities can be used to deliver best of breed technologies.

Actions for the Department of Defense:

- **Accelerate training of acquisition professionals and senior leaders on the AAF, Contracting Cone, and Digital Technologies.**
 - The Secretary of Defense should develop a set of best practices in the use of new acquisition pathways¹¹⁵ and direct USD(A&S) and Component Acquisition Executives to train the right acquisition professionals and DoD senior leaders and executives on the Adaptive Acquisition Framework (AAF), the Contracting Cone, and best practices for the use of these flexibilities, within one year.
 - USD(A&S) should also work closely with USD(R&E), the Joint Artificial Intelligence Center, the Service Acquisition Executives, and the Component Acquisition Executives to implement a coordinated approach to training acquisition professionals and senior leaders on cross functional specialties relative to emerging technologies. The approach should amplify and harmonize ongoing workforce training efforts¹¹⁶ related to AI, data analytics, software, and digital

¹¹⁴ Including Federal Acquisition Regulation (FAR)-based approaches and non-FAR based approaches as outlined in the Defense Acquisition University's Contracting Cone. See *Contracting Cone*, Defense Acquisition University (last accessed Dec. 20, 2020), <https://aaf.dau.edu/aaf/contracting-cone/>.

¹¹⁵ Such as the middle-tier of acquisition and the software acquisition pathway.

¹¹⁶ For example, efforts associated with section 230 of the Fiscal Year 2020 NDAA on talent management of digital expertise and software professionals; section 256 on an education strategy for Artificial Intelligence; and section 862 of the FY 2020 NDAA on software development and software acquisition training and management programs. In support of the implementation of Section 862, USD(A&S) is developing a pilot software acquisition training program that aims to better enable the “creation and execution of acquisition strategies and contracts that support the speed of technology and change” by providing students with the foundations of digital technologies through evolutionary content in context of the Defense Acquisition System. *Digital DNA: Software Acquisition Training Pilot*, U.S. Department of Defense at 1 (on file with the Commission); see also *Report to Congress on FY20 NDAA Section 862(b)(1)(B) Software Development and Software Acquisition Training and Management Programs*, U.S. Department of Defense at Appendix H (Jan. 2021), https://www.hci.mil/docs/Policy/FY20_NDAASec862ReportToCongress_DoDSoftwDevSoftwAcqTngMgt_Jan2021.pdf.

DRAFT NSCAI DOCUMENT

engineering and look to leverage training or courses that can be procured off-the-shelf or as a service.

- **Leverage public-private talent exchanges to infuse technical expertise into the acquisition corps.**¹¹⁷
 - The Secretary of Defense should direct that acquisition professionals are considered among the highest priority to participate in public-private talent exchanges.¹¹⁸
- **Establish enterprise learning platforms, course catalogs, and knowledge management tools for acquisition personnel and make them available Department-wide.**¹¹⁹
 - USD(A&S) should invest in and scale appropriate learning platforms, course catalogs, and knowledge management tools and create incentives for their use by FY 2022. These resources should catalog available training¹²⁰ and best practices¹²¹ and make relevant experts and specialists discoverable for acquisition professionals Department-wide.
- **Continuously assess existing acquisition workforce capabilities and evolve training for acquisition professionals.**
 - The Secretary of Defense should direct that USD(A&S) work with the Service Acquisition Executives, Component Acquisition Executives, USD(R&E), and the JAIC to ensure curricula and approach to training¹²² for acquisition professionals is consistently and appropriately updated to support the Technology Annex to the National Defense Strategy, as described below.

¹¹⁷ This should be coordinated appropriately with the relevant legal and ethics officials to avoid any potential conflicts of interest.

¹¹⁸ Section 1102 of the FY 2021 National Defense Authorization Act directs the Secretary of Defense to provide briefings to the defense authorization committees on implementation of public-private exchange programs and recommendations for statutory changes to improve their use and effectiveness. Section 1102 also directs the Secretary to take steps to ensure the exchange program is applied to the defense modernization priorities—including AI. While USD(R&E)’s modernization directors are responsible for “unifying and advancing the Department’s investments and capabilities [in their areas], and ensur[ing] the transition of technologies into operational use,” the Department’s acquisition professionals will be the personnel ultimately responsible for operationalizing the modernization priorities. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021); see also *Modernization Priorities*, U.S. Department of Defense, USD(R&E), (last accessed Dec. 28, 2020), <https://www.cto.mil/modernization-priorities/>.

¹¹⁹ The DoD has already begun to make progress in these areas. For example, the Advanced Distributed Learning (ADL) Initiative under the Office of the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), which originated in the 1990s, is a DoD-wide program for modernizing DoD training/education, including the use of learning technologies and platforms, and support for content sharing, collaboration, and interoperability. ADL is currently pursuing an Enterprise Course Catalog to federate disparate or decentralized catalogs across the organization, aggregating the content into a single, Defense-wide portal. See *Enterprise Course Catalog (ECC)*, Advanced Distributed Learning Initiative (last accessed Feb. 12, 2021), <https://adlnet.gov/projects/ecc/>.

¹²⁰ Including DoD-specific training as well as relevant commercial, and open-source training.

¹²¹ Examples could include draft acquisition strategy documents for programs planning to use the middle tier or software acquisition pathways; model contracting language for AI technologies, etc.

¹²² Including on new or innovative acquisition approaches and best practices as well as new or emerging digital technologies and technical approaches (e.g., digital engineering, MLOps, etc.).

Action for Congress:

- **Authorize the use of a rapid contracting mechanism for the software acquisition pathway.**
 - The Armed Services Committees should direct the Secretary of Defense to develop a rapid contracting mechanism to support the AAF’s software acquisition pathway.¹²³ The mechanism should include:
 - A value-based price evaluation model.
 - An independent, non-advocate cost estimate developed in parallel with engineering and leveraging agile cost estimation best practices.
 - Performance metrics intended to measure value that can be automatically generated by users and shared as requested by DoD officials and congressional defense committees.

Component 4: Modernize the Budget and Oversight Processes for Digital Technologies.

The DoD’s budget process requires that funds be requested two years in advance of their execution and focuses planning within the five-year Future Years Defense Plan (FYDP). Resources are allocated to program elements (PEs) that are defined at the system level¹²⁴ and based upon cost build ups for pre-determined and highly specified system requirements.¹²⁵ In

¹²³ This recommendation echoes a recommendation made by the Defense Innovation Board (DIB) in a 2019 study on software acquisition and practices within the Department of Defense. The DIB called for a new acquisition pathway for software that would prioritize continuous integration and delivery of working software in a secure manner, with continuous oversight from automated analytics. The DIB provided draft legislative language in the body of the report for consideration by the DoD and Armed Services Committees in implementing this recommendation. The draft legislative text indicated the need for a rapid contracting mechanism to be established as part of the software pathway. Although the creation of a software acquisition pathway was directed by section 800 of the FY 2020 NDAA and the Department has since issued a formal policy on the pathway, the rapid contracting mechanism remains unimplemented. See *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, DoD Defense Innovation Board at S58 (May 2019), <https://media.defense.gov/2019/May/01/2002126689/-1/-1/0/SWAP%20COMPLETE%20REPORT.PDF>; Pub. L. 116-92, National Defense Authorization Act for Fiscal Year 2020; *DoD Instruction 5000.87: Operation of the Software Acquisition Pathway*, U.S. Department of Defense (Oct. 2, 2020), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500087p.PDF?ver=virAfQj4v_LgN1JxpB_dpA%3D%3D.

¹²⁴ Using system-level program elements incentivizes programs to build “full stack” with each subcomponent and enabling technology being built and procured individually as part of the broader program makeup. This reduces risk. In recent years enabling services such as PlatformOne have reemerged, but it is difficult to justify base operating budgets for these organizations because they are not tied to discrete outputs. See Eric Lofgren, *The DoD Budget Process: the Next Frontier of Acquisition Reform*, George Mason University Center for Government Contracting (July 9, 2020), https://business.gmu.edu/images/GovCon/White_Papers/The_DoD_Budget_Process.pdf.

¹²⁵ JCIDS and the PPBE process are tightly linked. Military needs drive the development of new programs to deliver capability. Traditionally derived from concepts of operations, these needs are the basis against which the Department evaluates, costs, and ultimately pursues a solution. If the Department determines that a material solution is necessary, the need will be decomposed into requirements that prescribe the design, specification, and function of the system intended to deliver the capability. Once validated, these requirements drive the DoD’s budget. Id. at 5.

DRAFT NSCAI DOCUMENT

addition, the life cycle-phased appropriation categories¹²⁶ that govern the DoD budget structure run counter to the iterative process inherent to AI and other software-based technologies.¹²⁷

This construct creates a paradigm unfriendly to the speed, adaptation, risk-taking, and joint force cohesion necessary to compete in an AI-enabled threat environment. Senior leaders champion the need to experiment¹²⁸ and “fail fast,” but the budget process prevents the allocation of funds without a justification clearly tied to program objectives. At the same time, the DoD requirements process—responsible for formulating the basis of those program objectives—assumes a linear and sequential relationship between requirements and technology.¹²⁹

To adapt faster than our adversaries, DoD must have a requirements and budget process that: 1) prioritizes joint force capabilities and aligns resources accordingly; 2) enables experimentation, iteration, and continuous development—especially for AI and digital technologies where persistent user feedback is critical; and 3) balances speed, scale, and risk depending on the technology or capability being delivered.

Implementation of the large-scale institutional changes required to achieve this vision will take time and equal commitment from both DoD and Congress. In the near-term, DoD and Congressional leaders should focus on generating mutual trust by establishing pilot programs to demonstrate the impact of reforms to the budget and requirements process relative to AI. The inclusion of support for the Department’s Budget Activity 8 pilot program in the FY 2021 defense authorization and appropriations acts represents positive progress to this effect.¹³⁰

¹²⁶ Commonly known as “colors of money,” DoD funds are appropriated into the following categories, each with its own allowable uses per law: Research, Development, Test & Evaluation (RDT&E) dollars, Procurement dollars, Operations & Maintenance (O&M), and Sustainment dollars.

¹²⁷ The distinction between research and development funds and operating funds disincentivizes the cycle of continuous development and integration necessary to derive value from AI and software-based applications. Within the RDT&E appropriation alone, separate funding for research, development, prototyping, and fielding assumes a slow linear progression from lab to field pre-defined system requirements that allow for little to no user feedback. Once fielded, appropriations law governing the use of O&M funds challenges upgrades to digital systems.

¹²⁸ Congressional testimony from former Under Secretary of Defense for Policy Michele Flournoy highlights the centrality of experimentation to developing new concepts and capabilities at the speed required to outpace our competitors. See Testimony of The Honorable Michele A. Flournoy, former Undersecretary of Defense for Policy before the U.S. House of Representatives Armed Services Committee, *Hearing on DoD’s Role in Competing with China* at 8 (Jan., 15, 2020), <https://armedservices.house.gov/cache/files/4/4/44fbef3d-138c-4a0a-b3a9-2f05c898578f/0E4943A5BFAEDA465D485A166FABCF5F.20200115-hasc-michele-flournoy-statement-vfinal.pdf>.

¹²⁹ Requirements are developed that drive technological development, and prototyping and experimentation occurs as a means to refine requirements and manage risk. This incentivizes integration of incremental technologies into programs of record rather than disruptive or rapidly changing user-centered technologies, such as AI; and limits the ability of program managers to respond to any fast-paced change in technology later in the life of the program. See Pete Modigliani et al., *Modernizing DoD Requirements: Enabling Speed, Agility, and Innovation*, The MITRE Center for Technology and National Security (Mar 2020), <https://www.mitre.org/sites/default/files/publications/pr-19-03715-2-modernizing-dod-requirements-enabling-speed-agility-and-innovation.pdf>.

¹³⁰ The budget activity 8 (BA 8) pilot seeks to overcome the barrier that DoD spending categories pose to the development and sustainment of digital technologies. The Office of the Under Secretary of Defense for Acquisition and Sustainment and the Office of the Under Secretary of Defense for Comptroller selected nine programs to begin to pilot the BA 8 for Fiscal Year 2021. Defense appropriators approved eight of the nine programs and BA 8 is being established for each Service and Defense-wide under the Research, Development, Test, & Evaluation appropriation and enable two-year funding. See H.R. 133, Consolidated Appropriations Act, 2021, 116th Cong. (2020), <https://docs.house.gov/billsthisweek/20201221/BILLS-116RCP68-JES-DIVISION-C.pdf?source=email> (joint explanatory statement at 118).

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

Below are recommended steps that DoD and Congress should take immediately and over the longer-term to create a modern budget and requirements process that supports the application of AI at speed and scale.

Immediate actions for the Department of Defense:

- **Reorient the Joint Requirements Oversight Council (JROC) process to focus on Joint and Cross-Domain Capability.**
 - The Chairman of the Joint Chiefs of Staff should appoint the USD(R&E) Co-Chair and Chief Science Advisor of the JROC.¹³¹
 - The Chairman of the Joint Chiefs of Staff should direct that the JROC charter be updated to reflect USD(R&E) as Co-Chair and Chief Science Advisor with responsibility for:
 - Delivering technology assessments and trend reports that inform JROC deliberations on future military requirements; and
 - Validating the technical feasibility of requirements developed by the services and ensuring they comply with the reference design for the digital ecosystem recommended above.
- **Make supplemental funding available to drive operational prototyping, scale, and transition of AI technologies.**
 - The Secretary of Defense should establish a dedicated AI fund as a pilot under the management of USD(R&E) to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies that align with applications identified in the Technology Annex as described below. In doing so, the Secretary of Defense should direct:
 - Inclusion of approximately \$200 million for the fund in the FY 2022 budget request.
 - USD(R&E), in collaboration with the JAIC and the military services, should establish clear metrics for success and a time horizon upon which to stand up additional similar funds for specific technologies or capabilities.
- **Accelerate efforts¹³² to implement a portfolio management approach for requirements and budget.**

¹³¹ Appointing USD(R&E) Co-Chair and Chief Science Advisor to the JROC would help push forward efforts to reform requirements generation and validation. Serving as the system architect for joint and cross-domain solutions, USD(R&E) would advocate for more flexible system design and specifications such as modular open systems architecture and standard, well-documented application programming interfaces (APIs). See See Tab 2 - Part I Recommendation 2 in *Interim Report and Third Quarter Recommendations*, NSCAI at 42 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

¹³² Section 809 of the FY 2021 NDAA directs the Secretary of Defense and the Director for Extramural Innovation and Research Activities to “conduct an assessment of the processes for developing and approving capability requirements for the acquisition programs of the Department of Defense and each military department” and submit reports to the defense authorization committees. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021). Section 809 further stipulates that, as part of the assessment, both officials must evaluate the “extent to which

DRAFT NSCAI DOCUMENT

- The Deputy Secretary of Defense should produce a proposal for consideration in the FY 2022 defense authorization and appropriation bills to establish a pilot to test a portfolio management approach for requirements and budgeting for at least one joint capability area, such as Command and Control, in FY 2023.¹³³ The proposal should:
 - Establish a reasonable ceiling value for the portfolio.
 - Consider consolidation of program elements and the creation of a Program Executive Office or other organizational entity empowered to resource and oversee programs designed to meet the joint capability need.
 - Request reprogramming authority to drive a “fail fast” mentality, promote experimentation and early prototyping, and quickly integrate new capabilities.
 - Provide recommendations on adjusted reporting guidance and justification documents, including metrics and mechanisms¹³⁴, that will allow Congress to conduct appropriate approval and oversight.
- The Deputy Secretary of Defense should also produce a separate proposal to establish a pilot to test mission-focused budgeting and appropriations (e.g., a Mission Element). The proposal should be developed in coordination with a Combatant Command and organized around a high priority operational challenge as identified by the Joint Staff. It should:
 - Consider more flexible funding mechanisms, including reprogramming authorities, applied across existing, relevant Service programs to promote digital modernization and integration of AI technologies, interoperability, and new development or prototyping efforts for the specific operational challenge.
 - Provide recommendations on adjusted reporting guidance, and justification documents, including metrics and mechanisms, that will allow Congress to conduct appropriate approval and oversight.

Immediate Actions for Congress:

- **Direct the Secretary of Defense to establish the dedicated AI fund.**

portfolio management techniques are used in the process for development capability requirements to coordinate decisions and avoid duplication of capabilities across acquisition programs.” Id. The Joint Explanatory Statement accompanying the provision indicates that the Department shall consider the recommendations made in the MITRE Corporation’s *Modernizing the Requirements Process: Enabling Speed, Agility, and Innovation* as part of the directed assessment. Recommendations include the establishment of enterprise-level requirements or “Warfighter Essential Requirements” for capabilities to ensure acquisition programs are closely aligned to warfighter needs, drive systems of systems approaches and reduce redundancies between and among services and domains; and enable budget and requirements tradeoffs through a portfolio management approach. The authors also recommend different management approaches for requirements based on the attributes of the system being developed. See Pete Modigliani, et al., *Modernizing the Requirements Process: Enabling Speed, Agility, and Innovation*, MITRE (Mar. 2020), <https://www.mitre.org/sites/default/files/publications/pr-19-03715-2-modernizing-dod-requirements-enabling-speed-agility-and-innovation.pdf>.

¹³³ A formal legislative proposal may not be required. DoD retains discretion in the structure and objectives of annual budget proposals. However, approval from Congress and the Office of Management and Budget is required.

¹³⁴ Such as dashboards and digital engineering artifacts.

DRAFT NSCAI DOCUMENT

- Congress should include a provision in the FY 2022 National Defense Authorization Act directing the establishment of an AI fund under USD(R&E) and appropriate at least \$200 million to support it as a pilot.¹³⁵
- **Support the continuation of the Budget Activity 8 pilot program in FY 2022 and direct the Department to add an S&T project to the pilot programs.**
 - Congress should continue to support the DoD software and digital technologies pilot program designed to allow for flexibility in funding the full lifecycle of development, procurement, deployment, assurance, modifications, and continuous improvement for digital technologies.¹³⁶
 - Congress should support DoD expanding the pilot in Fiscal Year 2022 to include a program that explicitly supports an S&T development effort in order to effectively test the impact of the single funding mechanism for the entirety of the AI lifecycle, including early-stage research and development.

Longer term actions for the Department of Defense and Congress:

- **Establish a single appropriation and budget structure for software and digital technologies by FY 2023.**
 - Congress should build on the BA8 pilot and establish a single appropriation for software and digital technologies that is exempt from the traditional programming or planning process and can be used as a single source of funding for the full lifecycle of capability delivery and continuous engineering.
 - The Department and Congress should collaborate to develop and implement a budget structure and transparent oversight process for the new software and

¹³⁵ USD(R&E) should work closely with the JAIC, the Joint Staff, and the military services to identify specific programs and mission areas ripe for potential application of AI technologies, with particular attention to near-term warfighter needs from the Combatant Commands, and use the fund to accelerate efforts in those areas. Establishment of this fund would need to be accompanied with transfer authority such that USD(R&E) could transfer resources to the relevant entities to conduct these activities.

¹³⁶ This is being led by the DoD Office of the Under Secretary of Defense for Comptroller (OUSD C) and Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD A&S), based on the findings and recommendations of the Defense Innovation Board's Software Acquisition and Practices Study. *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, DoD Defense Innovation Board (May 2019), https://media.defense.gov/2019/Apr/30/2002124828/-1/-1/0/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINAL.SWAP.REPORT.PDF. Jeff Boleng, Special Assistant for Software Acquisition to the Under Secretary of Defense for Acquisition and Sustainment, publicly stated the goal of the pilot as "simplifying the budget process, increasing the visibility, accountability of the funding." Billy Mitchell, *DOD has OMB Support for Special Software-only Appropriations Pilots*, FedScoop (Sept. 10, 2019), <https://www.fedscoop.com/dod-omb-support-special-software-appropriations-pilots/>. In public remarks made March 3, 2020, Undersecretary of Defense for Acquisition and Sustainment, Ellen Lord, underscored the significance of the pilot, asserting "we will begin to see results almost instantaneously, because the administrative burden of making sure you are charging the right development number, the right production number, the right sustainment number, slows things down." Jared Serbu, *Pentagon Teeing Up Nine Programs to Test New 'Color of Money' for Software Development*, Federal News Network (Mar. 4, 2020), <https://federalnewsnetwork.com/acquisition/2020/03/pentagon-teeing-up-nine-programs-to-test-new-color-of-money-for-software-development/>; *West 2020: 3 March 2020 Morning Keynote with The Honorable Ellen Lord*, WEST Conference (Mar. 3, 2020), <https://www.youtube.com/watch?v=VG1qjyMhtok&list=PLFZb4znIHwx0TcsirmyYD6k5BAYxDRwU0&index=6&t=0s>.

digital technology appropriation that enables agile development of AI technologies and capability portfolio management.¹³⁷

- **Identify and implement successful portfolio- and mission-based budgeting constructs at scale across DoD.**
 - The Department and Congress should look to BA 8 as an example of how to apply a similar approach to monitoring and scaling portfolio- and mission-based budgeting. Based on metrics and oversight of the pilots over an appropriate timeline, DoD and Congress should determine what approaches to implement more broadly.

Recommendation: Democratize AI Development

An AI-enabled threat environment requires our forces to be able to develop and deploy solutions nearly as quickly as threats arise. However, our forces frequently lack the infrastructure, tools, talent, and support to solve their challenges locally and with modern technology.¹³⁸ The JAIC cannot develop and proliferate AI applications for every user group or mission area within the DoD. To accelerate adoption of AI, the Department must create the technical infrastructure and organizational structures that pair top-down strategy with bottom-up development.

Component 1: Leverage the JAIC as the Department's AI Accelerator.

The JAIC should serve as the Department's "AI accelerator" and central node for AI-related information. In this role, the JAIC would maintain critical situational awareness of AI stacks across the Department (i.e., options, including applications, available within the digital ecosystem that mission owners can leverage to enable local development efforts) and provide the expertise and resources necessary to enable distributed development efforts.

Actions for the Department of Defense:

- **Designate the JAIC as the Department's AI Accelerator.**
 - The Deputy Secretary of Defense should issue a memorandum¹³⁹ designating the role of JAIC as the DoD enterprise's AI accelerator with responsibility for:
 - Developing tailorable AI applications to address high-level, cross-domain challenges and shared problems and making them available through the digital ecosystem as enablers for software teams across the enterprise.

¹³⁷ For example: budget activities within the appropriation could be aligned to a DoD Component; program elements or budget lines under the budget activities would align to joint capabilities (e.g., Joint Command and Control) and then further decomposed into projects (i.e., key systems, investments, and supporting activities).

¹³⁸ Often, technology that has been in use in the commercial sector for years.

¹³⁹ Section 232 of the National Defense Authorization Act for FY 2021 designates the JAIC as a direct report to the Deputy Secretary of Defense, adds to the JAIC's responsibilities the "acquisition and development of mature artificial intelligence technologies in support of defense missions," and directs the Secretary of Defense to clarify the roles and responsibilities of various DoD Components relative to the "research, development, prototyping, testing, procurement of, requirements for, and operational use of artificial intelligence technologies." See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

DRAFT NSCAI DOCUMENT

- Administering a matching fund to incentivize integration of commercial AI solutions for business functions across the Department.
- Collecting best practices (including best-of-breed AI applications) from industry, academia, and across the enterprise and making them accessible for the broader DoD developer community.¹⁴⁰
- Providing AI subject matter expertise and assistance to DoD Components to inform strategy, policy, and technical approaches. This would include:
 - Participating as a member of the Steering Committee on Emerging Technology.
 - Contributing to the development of a reference design for the DoD AI digital ecosystem and associated governance policies.¹⁴¹
 - Advising on integrating the appropriate governance frameworks for responsible use of AI into policies and procedures.¹⁴²
 - Advising on TEVV policies and capabilities for AI.
 - In coordination with the Under Secretary of Defense for Policy, serving as the Department’s lead for AI-related international engagement.
- Developing a common AI TEVV framework,¹⁴³ in coordination with DOT&E and any other appropriate stakeholders, that integrates testing as a continuous part of requirements specification, development, deployment, training, and maintenance and includes run-time monitoring of operational behavior.¹⁴⁴
- Identifying, procuring, and orchestrating AI development tools and making them available through the digital ecosystem software exchange (SoftEx)¹⁴⁵ described above to enable distributed development efforts.¹⁴⁶

¹⁴⁰ Best practices could include user-centered approaches such as problem discovery, which could be captured and shared via a modern, queryable knowledge management system; or algorithms or models added to the JAIC’s repository within the digital ecosystem.

¹⁴¹ For example, identity-based user authentication and access controls; definition of common standard interfaces and documentation requirements; and accreditation and ATO reciprocity. See full list above.

¹⁴² For example, working with the Office of the Under Secretary of Defense, the Defense Contract Management Agency, Service Acquisition Executives, and other relevant parties responsible for acquisition and procurement activities to develop model contract language that incorporates the standards and practices outlined in NSCAI’s *Key Considerations for Responsible Development & Fielding of AI*. These would apply both to systems developed by DoD, as well as those that are acquired (including Commercial off-the-shelf systems or those developed by contractors). See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 6 (July 22, 2020), <https://www.nsc.ai.gov/previous-reports/>.

¹⁴³ More details for a TEVV framework can be found in Chapter 7 of this report.

¹⁴⁴ AI applications are extremely diverse and thereby necessitate a wide range of testing methods. Establishing common approaches to tailoring appropriate processes and tools to the type of AI application at hand will support the ability of DoD components to embrace and scale AI solutions by shortening the testing cycle and making test results interpretable and comparable across the Department. Given the diversity of use cases, the framework would not embody a one size fits all approach, but rather provide core capabilities and guidance adaptable across application areas. For a full discussion on this framework, and required resourcing, see Chapter 7 of this report.

¹⁴⁵ Depending on the current state of the implementation of the digital ecosystem, this shared access could be accomplished through the federated system of distributed software repositories—whether the JAIC’s software repository or one managed by a DoD component that originally developed or licensed the software tool.

¹⁴⁶ Including tools for TEVV. This effort should also determine what AI development tools are already available across the Department (e.g., where commercial software licenses already exist) and, leveraging the acquisition authority granted in the FY 2021 NDAA, procuring leading-edge AI development tools with licensing terms to support enterprise-wide usage. Reasonable consideration should be given for the maturity of the product/tool and likelihood of enterprise use. Section 808 of the FY 2021 National Defense Authorization Act grants the Director of the Joint Artificial Intelligence Center acquisition authority up to

DRAFT NSCAI DOCUMENT

- Making available enterprise-wide contracting vehicles (e.g., Blanket Ordering or Purchase Agreements) for talent¹⁴⁷ and AI technical services¹⁴⁸ and continuously onboarding new companies.¹⁴⁹
 - Coordinating with USD(R&E) on AI-related elements of the go-to-market strategy discussed above.
 - Integrating with nation-wide initiatives within other agencies and departments, as directed by the President.
- **Build technical support capability.**
 - The JAIC should grow and train a staff of resident experts¹⁵⁰ that can provide support to users across the enterprise akin to an “AI help desk,” to include providing technical and policy consultation and advice; implementing solutions for small problems; and facilitating connections of support (for larger problems).¹⁵¹

Component 2: Embed AI development capabilities in support of operations.

The Department must ensure operators are paired with technologists at every echelon. Doing so will institutionalize user-centered, agile development, improve the speed and operational relevance of solutions delivered, and build trust and confidence in AI-enabled systems. Implementation of the actions below will create a networked support structure to enable bottom-up AI development extending from the tactical edge to the JAIC.¹⁵²

Actions for the Department of Defense:

- **Establish integrated AI delivery teams at every Combatant Command (CCMD).**
 - The Secretary of Defense should direct each Combatant Commander to stand up an AI delivery team dedicated to developing and deploying AI applications to support operational units.¹⁵³
 - Teams should be staffed with the appropriate talent to manage the full lifecycle of AI solutions, including in disciplines such as data science, AI testing and model

\$75,000,000 out of the funds made available in Fiscal Years 2021-2015 to enter into new contracts. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

¹⁴⁷ Such as data scientists, AI and software engineers, infrastructure engineers, product managers, and other key positions.

¹⁴⁸ Including full stack development, engineering, testing, integration, etc for AI applications and systems.

¹⁴⁹ To reduce barriers to entry, the Department could also consider pairing the Blanket Ordering Agreement or Blanket Purchasing Agreement with a Broad Agency Announcement or Commercial Solutions Open solicitation procedure.

¹⁵⁰ This should include a diverse cross-section of expertise that at a minimum includes engineering (i.e., data science and AI solutions), AI digital ecosystem architecture, AI software experts, product managers; and acquisition, legal, policy experts as well as domain experts.

¹⁵¹ This could also involve JAIC representatives embedded at Combatant Command headquarters where appropriate and feasible.

¹⁵² Of note, the NSCAI Interim Report Appendix 3: Workforce Model’s recommendations are designed to support this model, with AI experts and developers serving at hubs, developers serving in spokes, and deployment specialist training helping domain experts maintain data sets and software and better partner with experts and developers. *Interim Report*, NSCAI at 61 (Nov. 2019), <https://www.nscai.gov/previous-reports/>.

¹⁵³ CCMDs have specific operational needs that routinely outpace centralized development approaches. Modern battlefield dynamics require that each commander have the ability to tailor the character of his or her war to out-adapt the adversary.

training, software engineering, product management, and full stack development.¹⁵⁴ AI Delivery teams should be responsible for:¹⁵⁵

- Finding, tailoring, and fielding applications from the digital ecosystem (e.g., those developed by other CCMDs, Service software factories, or the JAIC).
 - Developing additional sustainable mission applications as needed.
 - Contributing new and tailored applications to the digital ecosystem for use across the CCMD(s) to meet common challenges.
- **Integrate forward-deployed development teams with operational units.**
 - Each Combatant Commander should develop and implement a plan for the integration of forward-deployed development teams to act as the local customer interface for the AI delivery team with each operational unit.¹⁵⁶ Forward-deployed development teams should:
 - Work side-by-side with warfighters to identify problems and opportunities that could be met with AI applications.
 - Leverage the digital ecosystem to provision development environments and tools to produce “quick wins” to improve capabilities and generate efficiencies.¹⁵⁷

Recommendation: Invest in Next Generation Capabilities

The DoD must have an enduring process that clearly identifies, prioritizes, resources, and tracks¹⁵⁸ critical technologies over multiple time horizons. This will drive an investment strategy that pursues technology applications that close key capability gaps and optimize current operational concepts, and simultaneously makes bets on disruptive technologies to enable transformative capabilities and operational concepts over the long term.

Component 1: Increase investments in Science & Technology (S&T) and AI R&D.

¹⁵⁴ To stand up these teams quickly, the CCMDs could leverage the enterprise contracting vehicles through the JAIC to access a pre-vetted pool of talent with AI engineering, data science, and product management competencies. If local contracting vehicles are used, contract provisions should require that all development efforts are interoperable and leverage the digital ecosystem.

¹⁵⁵ In this way, the AI delivery teams will contribute to a growing resource of shared data and software within the digital ecosystem by consuming ecosystem services, developing and fielding tailored AI capabilities, and integrating them into sustainable projects available for use across the department.

¹⁵⁶ As an example, both Army Futures Command (AFC) and Army Special Operations Command (USASOC) use a model known as “tactical data teams.” This model brings AI/ML expertise forward to the field in the form of 3 to 6 person teams to build AI solutions for real-time operational problems. Executed by a small business, Striveworks, under contract with AFC and USASOC, they are currently supporting efforts in Central Command and Indo-Pacific Command Areas of Responsibility.

¹⁵⁷ These are similar interactions with the digital ecosystem as those taken by the delivery teams at Combatant Command HQ, only the forward-deployed development team will be consuming digital ecosystem services locally on their provisioned mobile platform. Collocation of the developers with operators will drive real-time experimentation and shorten application feedback loops.

¹⁵⁸ DoD lacks reliable budget data to track its investments in AI and other critical technologies; a weakness that should be addressed at the source with AI applications that assist humans in generating program descriptions and other budget artifacts.

DRAFT NSCAI DOCUMENT

NSCAI analysis of DoD's RDT&E budget found that from 2013 to 2021, annual spending on core AI research projects approximately tripled from \$490 million to \$1.4 billion.¹⁵⁹ Over half of this core AI spending comes from the Office of the Secretary of Defense, concentrated in funding for DARPA, the JAIC, the Algorithmic Warfare Cross-Functional Team (Project Maven), and the Next Generation Information and Communication Technology (5G) project. During this period, broader research incorporating small elements of AI nearly doubled, from \$7.8 billion to over \$13.7 billion annually.

To compete and win in AI-enabled warfare, the propagation of technology from core AI research to broad AI applications must expand drastically.¹⁶⁰ Across the board, increases in all lines of AI research¹⁶¹ are called for, with particularly large increases in research funding required to advance key areas, such as developing methods for human-machine teaming and deploying trusted AI applications through rigorous methods for TEVV.

Action for the Department of Defense:

- **Commit to building budgets that invest at least 3.4 percent¹⁶² of the annual DoD budget in S&T and allocate at least \$8 billion for research and development of core AI.**
 - Particular focus should go towards strengthening the AI research budgets at organizations where AI expertise is centered, such as DARPA, the Office of Naval Research, the Air Force Office of Scientific Research, the Army Research Office, and the Service Laboratories.

Action for Congress:

- **Support DoD budget requests for amplified funding of AI R&D and AI-related initiatives.**

Component 2: Retire Legacy Systems Ill-Equipped to Compete in AI-Enabled Warfare.

In the face of new budget realities, the Department must undergo an aggressive portfolio rebalance to ensure sustained room in its budget for emerging technologies like AI.¹⁶³ This will require DoD to make hard decisions on where to divest, and identify opportunities and timelines to upgrade or phase out legacy systems, as it continues to invest in new systems. However, the

¹⁵⁹ The Commission defines Core AI as investments where most of the effort is in core AI research disciplines such as machine learning/deep learning; collaborative behavior; computer vision; human-machine teaming; automated reason; robotic autonomy; automated data fusion and self-healing networks.

¹⁶⁰ For a full discussion of how AI will change warfare, see Chapter 3 of this report.

¹⁶¹ For a list of priority AI R&D research areas, see Chapter 3 of this report

¹⁶² The Defense Science Board has recommended the level of 3.4% to mirror best practices in the private sector multiple times. *Department of Defense Research, Development, Test, and Evaluation (RDT&E): Appropriations Structure*, Congressional Research Service at 12 (Oct. 7, 2020), <https://fas.org/sgp/crs/natsec/R44711.pdf>.

¹⁶³ While defense budgets are projected to flatten or decline in the coming years, the threat environment will only increase in complexity. To meet these new realities we must create more room in the budget while simultaneously increasing the lethality of our forces. By retiring legacy systems and investing more in emerging technologies and, over the longer-term, portfolios of attritable systems, DoD can pursue these needs in tandem, boosting the composability and adaptability of our military forces.

Department must also approach new systems differently. Rather than continuing to build large, monolithic platforms while competitors invest heavily in attritable systems, the DoD should focus on speed. DoD should drive investments into rapid prototyping and modular system design to develop and field new capabilities at a rate that allows U.S. forces to continuously out-adapt the adversary.

Actions for the Department of Defense:

- **Institutionalize an enduring defense-wide review and decision-making process,¹⁶⁴ prioritized to the threat, to divest of legacy systems.**
 - The Secretary of Defense should direct the Service Secretaries, USD(A&S), the Defense Agencies, and DoD Field Activities to evaluate the relevance and resiliency of all platforms and systems against emergent threats and ruthlessly divest from systems and platforms deemed too costly or ineffective to equip with AI or make compatible with AI-enabled systems and architectures.¹⁶⁵
 - The Service Secretaries and USD(A&S), in comparing the risk/reward tradeoffs between new versus old technologies and operating concepts, should leverage AI technologies as decision support tools.
 - The Director of the Office of Cost Assessment and Program Analysis (CAPE) should enforce decisions to divest or reduce funding through the program review process.
 - The Service Secretaries and USD(A&S) should explore options for updating legacy systems with leading-edge technologies to buy time for required long-term modernization projects.
- **Evaluate AI alternatives prior to funding new major defense acquisition programs.**

¹⁶⁴ Former Secretary of Defense Mark Esper pioneered his “night-court” budgeting process as Army Secretary (2017-2019) and later applied it Department-wide. He “took a hard look at legacy department programs and cut a number of them, refocusing funds on efforts to challenge China and Russia.” As Army Secretary, he “helped guide those restructurings through Congress, and the process, which found around \$25 billion in savings, has garnered largely positive reviews.” Aaron Mehta & Joe Gould, *Night Court Comes to the Pentagon*, Defense News (Aug. 28, 2019), <https://www.defensenews.com/pentagon/2019/08/28/night-court-comes-to-the-pentagon/>. According to the Pentagon’s press release detailing the highlights of the FY 2021 budget proposal, the process applied defense-wide generated \$5.7 billion in FY 2021 savings, \$0.2 Billion in Working Capital Fund efficiencies, and another \$2.1Billion in activities and functions realigned to the Services. Press Release, The Office of the Under Secretary of Defense for Comptroller, *DoD Releases FY 2021 Budget Proposal*, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Press_Release.pdf.

¹⁶⁵ This echoes a recommendation made by the Future of Defense Task Force. The Task Force recommended that “Congress commission the RAND Corporation (or similar entity) and the Government Accountability Office to study legacy platforms within the Department of Defense and determine their relevance and resiliency to emerging threats over the next 50 years.” The Task Force further recommended that upon completion of the studies “a panel should be convened, comprising Congress, DoD, and representatives from the industrial base to make recommendations on which platforms should be retired, replaced, or recapitalized.” *Future of Defense Task Force Report 2020*, House Armed Services Committee at 8 (Sept. 23, 2020), https://armedservices.house.gov/cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/424EB2008281A3C79BA8C7EA71890AE9_future-of-defense-task-force-report.pdf.

DRAFT NSCAI DOCUMENT

- The Secretary of Defense should issue a memorandum directing that all new major defense acquisition programs must conduct a thorough evaluation of AI alternatives as part of their analysis of alternatives prior to funding for major defense acquisition programs.¹⁶⁶
- USD(R&E) and the JAIC should provide support to program offices conducting such analysis by providing subject matter expertise informed by technology scouting and an awareness of the capabilities in the R&D pipelines across the S&T enterprise.

Action for Congress:

- **The Congressional defense committees should support the Department’s hard decisions when presented with evidence that divestment or defunding can enable a more competitive force posture.**

Component 3: Create an integrated technical intelligence program¹⁶⁷ and a supporting community of practice.

To effectively leverage scientific and technological breakthroughs for competitive advantage, DoD must have a sophisticated technical intelligence program that monitors developments as they progress from basic research to prototype to fielded capabilities, understanding the R&D roadmaps of the private sector wherever possible. This intelligence must be global in scale, monitoring emerging technologies in near real time, especially in the rapidly evolving field of AI. The intelligence must be actionable, informing prioritization of resourcing and providing decision makers the ability to continuously update technology roadmaps for our national security agencies.

Such a technical intelligence program should provide inputs to the Department’s Technology Annex¹⁶⁸ in three main areas: (1) an understanding of the current and future threat capabilities in the R&D, production, and sustainment pipelines of our adversaries; (2) an understanding of the current and future friendly capabilities in the R&D, production, and sustainment pipelines of the U.S. government and allied partners; and (3) an understanding of emerging military and dual use technologies worldwide available for integration into national security capabilities.¹⁶⁹

Actions for the Department of Defense:

- **Transform the Strategic Intelligence Analysis Cell.**
 - USD(R&E) should reconceive the Strategic Intelligence Analysis Cell (SIAC)¹⁷⁰ as a robust analytic hub that marshals DoD, IC, and other technology scouting

¹⁶⁶ As noted in the discussion above on building a technical backbone, new programs should also adhere to the digital ecosystem reference design.

¹⁶⁷ See *Interim Report and Third Quarter Recommendations*, NSCAI at 66 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

¹⁶⁸ The purpose and proposed contents of such a Technology Annex are discussed below.

¹⁶⁹ See recommendations for the IC to increase S&T expertise and intelligence collection in Chapter 5 of this report.

¹⁷⁰ In its response to the 2017 NDAA provision creating USD(R&E), the DoD specified that the new organization would organize around three major themes. The first was a SIAC that would “focus on understanding the enemy’s capabilities and vulnerabilities,

DRAFT NSCAI DOCUMENT

- capabilities for strategic effect.¹⁷¹ The SIAC Director should report directly to the USD(R&E).
- SIAC should convene an interagency technology scouting community of practice from the service laboratories, OSD (including DARPA and DIU), innovation initiatives within the military services (such as AFWERX, and AAL), the Departments of Energy and Homeland Security, university affiliated research centers, federally-funded research and development centers, combatant commands, and international security partners. This community of practice should:
 - Establish a federated approach to provide USD(R&E) with inputs to produce and continuously update the Technology Annex.
 - Conduct analytic exchanges and wargames to assess future technology scenarios and include AI to the maximum extent possible.¹⁷²
 - Develop rigorous technology forecasting capabilities, leveraging best practices from academia and the private sector.
 - Engage with industry and update requirements for technology scouting tools and data.
 - In order to leverage private industry more effectively, SIAC should maintain knowledge of private market investments relevant to the technologies and capabilities outlined in the Technology Annex.
 - In order to locate existing DoD capability gaps and potential solutions, SIAC must receive technical details at all levels of classification on current programs of record from OSD(A&S) and the armed service's acquisition executives, as well as technical details on RDT&E programs from OSD(R&E) and the technology scouting community of practice described above.
 - SIAC should establish a technology fellows' program, inviting organizations in the technology scouting community to nominate personnel for short term (three to twelve month) assignments with SIAC where they would work side-by-side with SIAC analysts. This program should:
 - Build interdisciplinary teams of technologists and warfighters to conduct in depth investigations of emerging technologies, initiating direct contacts with academia and industry in addition to passive data collection.
 - Circulate personnel through the tech fellows' program into key roles in experimentation and concept development activities across OSD and the military services.

conducting analysis on our own U.S. capabilities, tracking technology trends across the globe and assessing potential/emerging threats and/or future opportunities that warrant action, that merit investment.” However, since the establishment of USD(R&E), the SIAC has been downgraded from a direct report to the Under Secretary and largely focused on examining threat technologies for OSD customers. See *Report to Congress, Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization*, U.S. Department of Defense at 8 (Aug. 2017), <https://dod.defense.gov/Portals/1/Documents/pubs/Section-901-FY-2017-NDAA-Report.pdf> [hereinafter 2017 AT&L Reorganization Plan].

¹⁷¹ USD(R&E) has the mandate and authority to perform this function. See DoDD 5137.02 at 5-6.

¹⁷² This is consistent with a recommendation made in Chapter 3 of this report that the DoD should integrate AI-enabled applications into all major Joint and Service exercises and, as appropriate, into other existing exercises, wargames, experiments, and table-top exercises. This recommendation first appeared in NSCAI's *Second Quarter Recommendations*. See *Second Quarter Recommendations*, NSCAI at 27 (July 2020), <https://www.nscai.gov/previous-reports/>.

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

- Develop personnel with greater understanding of emerging technologies across the national security community.
- Leverage hiring authorities from the Public-Private Talent Exchange Program and the Intergovernmental Personnel Act to include fellows from industry, academia, and other government agencies to enhance access to non-DoD research and perspectives.¹⁷³
- SIAC should acquire or develop research tools for use by the technology scouting community of practice, including AI-enabled analysis of large commercial databases, classified threat intelligence, and the technology investment portfolios of the United States Government and its allies.

Actions for Congress:

- **Congress should appropriate an additional \$10 million to USD(R&E)'s budget for the technology fellows' program and AI-enabled technology scouting tools and data.**

Component 4: Develop a Technology Annex to the National Defense Strategy.

To identify where and how to direct scarce resources, the DoD should formulate its investment strategy as a classified Technology Annex to the National Defense Strategy (NDS) produced by the Department's Chief Technology Officer, USD(R&E). The Annex should: 1) identify emerging technologies and applications required to solve the operational challenges outlined in the NDS; and 2) outline a clear plan for pursuing these technologies and applications. This plan should account for existing technologies, including dual-use commercial technologies, and drive rapid integration of these technologies to close near-term capability gaps.¹⁷⁴ The plan should also help inform the agenda for DARPA and the DoD labs, by identifying disruptive technology elements and applications that warrant longer-term, exploratory investments. Finally, the plan must take into account industry's comparative advantage in available R&D capital and include a consistent and transparent approach to messaging defense technology priorities to build and broaden the industrial base.¹⁷⁵

Actions for the Department of Defense:

- **Develop a Technology Annex to the National Defense Strategy.**
 - The Secretary of Defense, with support from the Director of National Intelligence, should issue a memo directing the Steering Committee on Emerging Technology to oversee the development of a comprehensive classified technology annex as a

¹⁷³ This would also directly support objectives of Section 1102 of the FY 2021 NDAA with respect to utilization of public-private talent exchanges. Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

¹⁷⁴ For example, via the go-to-market strategy outlined above.

¹⁷⁵ An unclassified version of the strategy must be communicated externally, to where the bulk of the AI talent resides. Shifting to a more integrated and transparent communication of priorities would enable Defense primes and non-trationals to plan and invest more to help meet DoD R&D needs. See Tab 1 - Issue 3: Expanding Industry's Role in DoD's AI R&D to Develop Next-Gen Capabilities, in *Interim Report and Third Quarter Recommendations*, NSCAI at 48 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

DRAFT NSCAI DOCUMENT

component of the next NDS and assign USD(R&E) as the Executive Agent responsible for producing the Technology Annex.

- The Technology Annex should identify emerging technologies and applications that are critical to enabling specific capabilities for solving the operational challenges outlined in the NDS.
- The Steering Committee on Emerging Technology described above should ensure that the Technology Annex sets clear guidance that drives prioritization and resourcing, while allowing enough flexibility for subordinate organizations to implement that guidance as best suits their mission. At a minimum, the Technology Annex should include:
 - Identified intelligence support requirements, including how the Intelligence Community (IC) analyzes the global environment and monitors technological advancements, adversarial capability development, and emerging threats.
 - Identified functional requirements and technical capabilities necessary to enable concepts that address each challenge.
 - A prioritized, time-phased plan for developing or acquiring such technical capabilities, that takes into account R&D timelines, a strategy for public private partnerships, and a strategy for connecting researchers to end users for early prototyping, experimentation, and iteration.
 - This should include roadmaps for designing, developing, fielding, and sustaining the technologies and applications to address the operational challenges outlined in the NDS.
 - These roadmaps should account for and leverage existing commercial-off-the-shelf/dual-use technologies and identify areas where defense-specific solutions are needed.
 - The roadmaps should use quantitative technological forecasting methods developed in academia and industry to identify disruptive technologies.
 - Identified additional or revised acquisition policies and workforce training requirements to enable DoD personnel to identify, procure, integrate, and operate the technologies necessary to address the operational challenges.
 - A prioritized, time-phased plan for integrating technology into existing DoD exercises that support the NDS.
 - Identified infrastructure requirements for developing and deploying technical capabilities, including data, compute, storage, and network needs; a resourced and prioritized plan for establishing such infrastructure; and an analysis of TEVV requirements to support prototyping and experimentation and a resourced plan to implement them.
 - Identified joint capability and interoperability requirements and a resourced and prioritized plan for implementation.
 - Consideration of human factor elements associated with priority technical capabilities, including user interface, human-machine teaming, and workflow integration.

DRAFT NSCAI DOCUMENT

- Consideration of interoperability with allies and partners, including areas for sharing of data, tools, and operational concepts.
 - Flexibility to adapt and iterate annex implementation at the speed of technological advancement.
- **Steward Implementation of the Technology Annex in Coordination with the Intelligence Community.**
 - The Secretary of Defense should direct the Steering Committee on Emerging Technology to steward implementation of the Technology Annex, to include coordination with the Intelligence Community; and establish a reporting structure and metrics to monitor the implementation of each technology roadmap to ensure each effort is resourced properly and progressing sufficiently.
 - The Steering Committee on Emerging Technology should ensure common technical requirements are developed to align with the digital ecosystem’s open architecture and are adhered to for the acquisition of emerging technologies identified in the Technology Annex. The standards should be coordinated across DoD and the IC.¹⁷⁶
 - The Steering Committee should conduct (at least) an annual review of the Annex and ensure that guidance, policy, and implementation evolve at the pace of technological change.

Component 5: Clearly communicate defense technology priorities to industry.

DoD must leverage industry’s comparative advantage in available R&D capital as part of its investment strategy. To do so effectively, the Department must adopt a consistent and transparent approach to messaging defense technology priorities that enables Defense primes and non-traditionals to plan and invest more to help meet DoD R&D needs, and further supports the Department’s efforts to attract venture-backed companies.

Action for the Department of Defense:

- **Publish unclassified emerging technology R&D objectives to support the Technology Annex to the National Defense Strategy.**
 - The Secretary of Defense should direct USD(R&E) to produce unclassified emerging technology R&D objectives and publish these objectives publicly. The objectives should represent an unclassified component of the Technology Annex,¹⁷⁷ and be regularly updated as living documents.
 - The R&D objectives should be tied to subsets or components of priority

¹⁷⁶ This could be done via the reference design for the digital ecosystem outlined above. As stated above, adherence to the reference design should be driven top-down via a memorandum from the Secretary of Defense and enforced through the Joint Requirements Oversight Council (JROC).

¹⁷⁷ In the *Second Quarter Recommendations*, the NSCAI emphasized that a Technology Annex to the NDS should be more than a simple list of technologies. The annex should identify emerging technologies and applications that are critical to enabling specific capabilities for solving the operational challenges outlined in the strategy. See *Second Quarter Recommendations*, NSCAI at 24 (July 2020), <https://www.nscai.gov/previous-reports/>.

DRAFT NSCAI DOCUMENT

technologies and applications on which the government envisions the private sector playing a major role in building future capabilities.¹⁷⁸ They should be communicated with an appropriate level of detail to provide current defense companies guidance to steer their internal R&D investments, communicate to startups interested in working with the government where future opportunities lie, and signal to venture capitalists where future DoD funding might flow.

- USD(R&E) should incorporate these objectives into the go-to-market strategy, coordinating digital innovation initiatives to act as surrogates to amplify this communication, and where appropriate, execute these priorities.
- The Secretary of Defense should direct the Steering Committee on Emerging Technology to develop an appropriate approach to monitor industry independent R&D investments to gauge effectiveness of these efforts. This should be coordinated with the DoD Office of General Counsel and relevant industry associations.
- OUSD(R&E) should leverage public-private exchange programs, as well as internal technical expertise from entities like DARPA and the interagency technology scouting community, to bring both technical expertise and commercial proficiency to the effort.¹⁷⁹

¹⁷⁸ For example, under microelectronics this might include advancing AI multi-chip packages, development of quantifiable assurance, 3D chip stacking, photonics, carbon nanotubes, Gallium Nitride transistors, domain-specific hardware architecture, electronic design automation, and cryogenic computing. As recommended by NSCAI in our *First Quarter Recommendations*. See *First Quarter Recommendations*, NSCAI at 51 (Mar. 2020), <https://www.nscai.gov/previous-reports/>.

¹⁷⁹ OUSD(R&E) could leverage existing Intergovernmental Personnel Act authorities as well as the pilot Public-Private Talent Exchange Program. See *Department Of Defense Public-Private Talent Exchange (PPTE) Program: Questions/Answers*, DoD Defense Civilian Personnel Advisory Service, (Aug. 23, 2018), https://www.dcpas.osd.mil/Content/Documents/PPTEQuestions_Answers23Aug2018.pdf; Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021) (directing that the Department of Defense establish public-private exchange programs to support the defense modernization priorities).

[BLANK PAGE]

DRAFT

Chapter 3 - AI and Warfare Blueprint for Action

If U.S. forces are not organized, trained, and equipped for a new warfighting paradigm that is emerging because of artificial intelligence (AI) and other emerging technologies, they will be outmatched and paralyzed by the complexity of the future battlefield.

This Blueprint for Action includes five top line recommendations to achieve military AI readiness and prepare our forces for the future: (1) Drive organizational reforms through top-down leadership, (2) Develop innovative warfighting concepts, (3) Establish AI-readiness performance goals,, (4) Develop and fund advanced technologies and R&D, and (5) Promote AI interoperability and the adoption of critical emerging technologies among U.S. allies and partners.

Recommendation: Drive organizational reforms through top-down leadership.

Continuously out-innovating the competition requires strong commitment from the top civilian and military leaders directing the rapid development and adoption of innovative and disruptive approaches to warfare through top-down governance and oversight processes.

Action for the Department of Defense and the Office of the Director of National Intelligence:

- **Establish a Steering Committee on Emerging Technology, tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence,¹⁸⁰**
 - The Secretary of Defense and Director of National Intelligence should issue a directive immediately establishing the senior oversight committee described above.
 - The Steering Committee on Emerging Technology provides a forum to drive change, focus, and action on emerging technology that otherwise would not be prioritized. It will enhance intelligence analysis related to emerging technology; connect strategic vision to organizational change; focus concept and capability development on emerging threats; guide defense investments that ensure America’s strategic advantage against near-peer competitors; and provide the authority to drive technology adoption and application by the Department.

¹⁸⁰ The Commission acknowledges section 236 of the FY 2021 National Defense Authorization Act, which permits the Secretary of Defense to establish a steering committee on emerging technology and national security threats composed of the the Deputy Secretary of Defense; the Vice Chairman of the Joint Chiefs of Staff; the Under Secretary of Defense for Intelligence and Security; the Under Secretary of Defense for Research and Engineering; the Under Secretary of Defense for Personnel and Readiness; the Under Secretary of Defense for Acquisition and Sustainment; the Chief Information Officer; and such other officials of the Department of Defense as the Secretary determines appropriate. However, the structure described in section 236 does not include leadership from the Intelligence Community and will thus not drive the intended action. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021), <https://docs.house.gov/billsthisweek/20201207/CRPT-116hrpt617.pdf>.

- **Assign the tri-chair Steering Committee on Emerging Technology responsibility for overseeing the development of a Technology Annex to the next National Defense Strategy**¹⁸¹

Actions for the Department of Defense:

- **Ensure all future JAIC Directors are a three-star general or flag officer with significant operational experience who reports directly to the Deputy Secretary of Defense;**¹⁸²
 - Three-star leadership allows the JAIC to engage with the services at a senior rank and within their command structure. Operational experience enables the Director to understand how AI can serve operational requirements and better communicate with the services as to how AI meets capability needs.
- **Appoint Under Secretary of Defense for Research and Engineering (USD(R&E)) as the co-chair and chief science advisor to the Joint Requirements Oversight Council.**¹⁸³
 - To accelerate AI and other emerging technologies for competitive advantage, USD(R&E) must play a central role in connecting technological advancements in research and development to joint operational requirements.

Action for Congress:

- **In the Defense Authorization Act (NDAA) for Fiscal Year 2022, establish a Steering Committee on Emerging Technology and National Security Threats and designate that it be tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence.**¹⁸⁴

¹⁸¹ This action is described in greater detail in the Chapter 2 Blueprint for Action, which designates a member of the Steering Committee on Emerging Technology the Executive Agent responsible for developing the Technology Annex and outlines the recommended contents and use for the Annex.

¹⁸² Notably, section 236 of the FY 2021 NDAA designates the Director of the Joint Artificial Intelligence Center as a direct report to the Deputy Secretary of Defense. See Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

¹⁸³ This echoes an action in the Chapter 2 Blueprint for Action, which emphasizes that to reduce redundancies, increase interoperability, and drive a system-of-systems approach to requirements development and management, USD(R&E) must have a stronger role in the Joint Requirements Oversight Council.

¹⁸⁴ As indicated above, DoD and ODNI have the authority to establish such a forum without legislative action. However, codifying it into law will ensure that it is sustained through leadership transitions. The defense committees could consider using the FY 2022 NDAA to amend section 236 of the FY 2021 NDAA. As written, section 236 only “permits” the establishment of such a committee; additionally, the provision does not clearly denote chairs of the committee and does not include any Intelligence Community representation. This recommendation is also discussed in Chapter 5 of this report. Additionally, Chapters 2 and 5 of this report recommend establishing funds to mature, operationally prototype, and transition exceptionally promising AI-enabled technologies. For DoD, USD(R&E) would control those funds and, for the IC, the ODNI CTO would control those funds. Those investments should be informed by the Steering Committee on Emerging Technology.

Recommendation: Develop Innovative Warfighting Concepts.

Battlefield advantage will shift to those who harness superior data, connectivity, compute power, algorithms, and overall system security to new warfighting concepts. Developing new operational concepts requires Services to incentivize experimentation, and foster a culture of “thinking Red”—in other words, considering the strategies of potential adversaries when developing operational concepts.

Actions for the Department of Defense:

- **Develop innovative operational concepts that integrate new warfighting capabilities with emerging technologies:**
 - The Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs should issue a memorandum directing Components and Services to develop a complete deterrence concept for systems warfare that leverages human-machine teaming, AI, and associated technology to prevail against intelligent adversary systems of systems.
 - Under the guidance from the tri-chair Steering Committee on Emerging Technology, USD R&E should receive \$5 million for a team (approximately 20 people) in FY 2022 funding to research and develop new AI-enabled capabilities for development and testing of advanced operational concepts. This project must be done in conjunction with DARPA and other capability offices to share the costs of filling technological gaps discovered during the analytic process.
 - These operational concepts should be institutionalized in classified DoD documents that drive comprehensive force development and investment prioritization. Confidential demonstrations should be executed to realize the deterrence concept.
- **Integrate AI-enabled applications into all major Joint and Service exercises and, as appropriate, into other existing exercises, wargames, and table-top exercises.**
 - The Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs should issue a memorandum calling for inclusion of AI and other emerging technologies into existing exercises, wargames, and table-top exercises. This includes large-scale exercises and smaller, more frequent events at all echelons.
 - The purpose of this would be to realize connectivity between systems and sensors, rapid data analysis, faster and more informed decision making, and more distributed operations.
 - Concept writers should participate in all major technology demonstrations.
 - Develop performance objectives and associated metrics to assess integration of AI-enabled applications into exercises, wargames, experiments, and TTXs.
- **Incentivize experimentation with AI-enabled applications through the Warfighting Lab Incentive Fund (WLIF).**

DRAFT NSCAI DOCUMENT

- DoD should incentivize experimentation with AI applications across the Department at every level possible by establishing either a special category or prioritized evaluation criteria within the WLIF for proposals that incorporate AI applications.
 - Experimentation with AI-enabled applications are particularly well-suited for the space, cyber, and information domains because of the high volumes of 24/7 data generated in these domains.
- The Steering Committee on Emerging Technology should provide annual guidance for selection of WLIF proposals for funding based on priorities developed in the Technology Annex to the NDS.
- DoD should increase WLIF funding by \$10 million annually specifically for AI-enabled applications.¹⁸⁵
- **Encourage a culture of “thinking Red.”**
 - DoD working closely with the Intelligence Community should develop a granular understanding of our main competitors’ approach to systems confrontation. This will help the Department to better understand our competitors’ operational concepts and to eventually avoid battlefield surprise.
 - Joint Warfare Analysis Center (JWAC) should be the lead to develop competitors’ operational concepts. Estimate \$2.5M allocation for a 10-week, 10 game series devoted to mastering red thinking.
 - Red-thinking games must 1) integrate deterrence-credibility stretch problems from key classified DoD documents; 2) clear denial concepts for our most stressing scenarios; 3) conducted with realistic basing and naval posture; 4) the highest standards of incorporating the best available intelligence; 5) the highest standards of AI-enabled modeling and simulation that ingest and mimic red operations; 6) rigorous two-player adjudication with physics level detail on red capabilities; and 7) rapid turnaround on force development considerations for the Secretary of Defense.
 - The Office of the Secretary of Defense and the Joint Staff should issue a memorandum directing all military educational institutions to foster in their curriculum the culture of “thinking Red.”

Actions for Congress:

- **Congress should appropriate an additional \$17.5 million to DoD’s budget to support innovative concept development.**

¹⁸⁵ FY 2021 O&M funding was \$42.4M. J7 received 110 proposals for FY 2021 WLIF funding and selected 20 experimentation efforts. NSCAI staff discussions with JS/J7.

Recommendation: Establish AI and digital readiness performance goals.

To drive outcomes and accountability and provide a means for oversight of Department efforts regulated to AI, DoD should establish key performance objectives and accompanying metrics for AI and digital readiness.¹⁸⁶

Actions for the Department of Defense:

- **By the end of 2021, establish AI and digital readiness performance goals.** To achieve more substantial integration of AI across DoD, the Deputy Secretary of Defense should:
 - Direct DoD components to assess military AI and digital readiness through existing readiness management forums and processes. The Steering Committee on Emerging Technology should work closely with the Under Secretary of Defense for Personnel and Readiness,¹⁸⁷ the Joint Staff, and the JAIC to ensure the identified AI and digital readiness performance objectives are incorporated into the military services' readiness reporting recovery frameworks, and resourcing strategies.
 - Direct the military services to accelerate review of specific skill gaps in AI, to inform recruitment and talent management strategies and **provide a report within 12 months.**
 - Assess the number of civilian personnel needed in software developer, software engineer, knowledge management, data scientist, and AI career fields for both management and specialist tracks.
 - Assess the number of military personnel needed in software development, data science, and AI career fields, in both management and specialist tracks, and for commissioned and enlisted personnel.
 - Assess the specialties and personnel required for a DoD and military service digital corps.
 - Establish annual retraining and recruiting goals to create and maintain the personnel described above.
 - **Direct the military services, in coordination with the Undersecretary of Defense (Acquisition and Sustainment), the Joint Staff, and the Defense Logistics Agency, and enabled by enterprise services and expertise at the JAIC, to prioritize integration of AI into logistics and sustainment systems wherever possible.**

¹⁸⁶ General Charles Q. Brown, Jr. & General David H. Berger, *To Compete with China and Russia, the U.S. Military Must Redefine 'Readiness'*, Washington Post (Feb. 1, 2021), <https://www.washingtonpost.com/opinions/2021/02/01/brown-berger-military-readiness/>.

¹⁸⁷ "P&R must enable, guide, and assess a strategically ready Department of Defense for employment by the Joint warfighter when and where it is needed, adaptive to the strategic geopolitical and threat environments, and evolving military-technological advances." *Preserving Our Competitive Advantage, Personnel And Readiness Strategy For 2030*, U.S. Department of Defense at 13 (Oct. 2020), https://prhome.defense.gov/Portals/52/Documents/Strategy/PR_Strategy_FINAL_.pdf?ver=KY6Vacn3kT1Gd9fNxnR34w%3D%3D.

- The Deputy Secretary of Defense should issue a memorandum directing the military services to accelerate use of AI and apply commercial best practices in predictive analytics for maintenance and supply chain to optimize all classes of supply, equipment and parts.¹⁸⁸ The Deputy Secretary of Defense should establish a \$100 million fund, administered by the Undersecretary of Defense (Acquisition and Sustainment) to provide matching contributions to service and agency efforts based on estimated financial or operational return on investment.
- By the end of 2021, the Undersecretary of Defense (Acquisition and Sustainment) supported by Senior Acquisition Executives and in coordination with the DoD CDO and the JAIC will establish performance objectives and identify best approaches to achieve data-ready systems in logistics and sustainment systems to support application of AI. Disparate conditions of data-readiness in existing and future systems will require differential approaches to achieve AI-readiness. Broadly, these categories of data-readiness are:
 - Systems with proprietary vendor data (ex. F-35 Joint Strike Fighter, M1 Abrams Tank).
 - Systems with government-owned data (ex. Maintenance and Availability Data Warehouse).
 - Systems that are data-ready (government-owned data that has been documented/tagged for storage/discovery and has published schema for data access (ex. Next Generation Air Dominance, T-7 Redtail, Ground Based Strategic Deterrent).

Actions for Congress:

- **Require the Secretary of Defense to establish performance objectives and accompanying metrics for AI and digital readiness and provide an update to Congress no later than 120 days after approving these goals.**

Recommendation: Develop and Fund Advanced Technologies and R&D.

Development and fielding of advanced AI-enabled technologies will remain a critical component of DoD's ability to achieve decision advantage on the battlefield.

Actions for the Department of Defense:

- **Define a joint warfighting network architecture by the end of 2021.** OSD CIO and the Joint Staff in coordination with the services should issue a memorandum directing the architecture for a secure, warfighting command and control network. A Service-agnostic warfighting network will enable better integration of AI-enabled technologies with

¹⁸⁸ In the FY 2021 NDAA, Title II, section 234, Congress directed “the Secretary of Defense to identify a set of no fewer than five use cases of the application of existing artificial intelligence enabled systems to support improved management of enterprise acquisition, personnel, audit, or financial management functions, or other appropriate management functions, that are consistent with reform efforts that support the National Defense Strategy.” Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

current and future weapon systems. The OSD CIO should provide \$5M to the right entity to accomplish this design.

- **Invest in priority AI R&D with the support areas that could support future military capabilities.** To accelerate adoption of AI in warfighting missions, the Undersecretary of Defense (R&E) should increase investments¹⁸⁹ in the following priority R&D areas to support future AI-enabled warfighting capability. If advanced, this could build near- and long-term AI-driven capabilities for competitive advantage in a future method of conflict defined by AI. These should be viewed as investments in deterrence in the interim—pursuing critical incremental advancements—and in the long term—building new capabilities yet to be determined that will sustain overmatch. Investments should include:
 - USD R&E with the support from DARPA should prioritize AI R&D for the following topics:
 - The future of teaming—to advance human-AI and AI-AI teaming.
 - Advanced scene understanding.
 - Intelligent edge devices, computing, and networking.
 - Robust and resilient AI.
 - Testing and Evaluation, Verification and Validation (TEVV).
 - Integrated AI, modeling, and simulation for decision support.
 - Autonomous AI systems.
 - Toward more general artificial intelligence.

Recommendation: Promote AI interoperability and the adoption of critical emerging technologies among allies and partners.

America’s enduring relationships with allies and partners represent asymmetric advantages over competitors and adversaries. Differential adoption of AI across military alliances and intelligence partnerships creates interoperability risk that threatens allies’ political and military cohesion, the resiliency of alliance structures, and the efficacy of coalition operations. The recommendations that follow reflect a holistic approach to furthering cooperation around AI and emerging technologies in the context of defense, intelligence, and security arrangements. They focus on interoperability and improving capacity and capability development to foster competitive military and intelligence advantages.

Component 1: Enhance Five Eyes efforts to achieve interoperable AI systems.

Actions for the Department of Defense and the Office of the Director of National Intelligence:

- **Coordinate with Five Eyes officials to conduct assessments of the comparative strengths and gaps in AI-related technologies and applications among the Five Eyes allies.**

¹⁸⁹ With additional funding for DoD investments in AI R&D recommended in the Chapter 2 Blueprint for Action.

DRAFT NSCAI DOCUMENT

- Assessments would evaluate Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) across the alliance for adopting AI, and future plans for AI-enabled warfighting architectures.
- **Coordinate with Five Eyes officials to develop a five-year plan for improving AI interoperability across the Five Eyes alliance.**
 - Proposed plans should include, among other things, combined research priorities, development objectives, experimentation, methods to facilitate data sharing, use cases, and common standards for TEVV of AI-enabled systems and interoperability standards. It should also include stress tests for supply chains in critical industries and corresponding risk-mitigation measures.
 - In developing plans, Five Eyes leaders should enhance ongoing efforts of the Technical Cooperation Program,¹⁹⁰ through the AI Strategic Challenge (AISC), to further align interoperable AI systems.
 - Five Eyes leaders should continue to advance the joint development of intelligence products by expanding efforts to “increase collection access and reliability, improve the quality and quantity of partner data and analysis, align strategic capabilities and emerging technologies, and promote compatibility across digital architectures and analytic tradecraft.”¹⁹¹

Actions for the Department of Defense:

- **Direct a series of AI demonstration pilot projects and host an AI wargame and experimentation series.**
 - Based on the recommended assessments and planning above, the Secretary of Defense should (a) direct a series of AI demonstration pilot projects in areas such as predictive maintenance, autonomous logistics, and sensor fusion with Five Eyes partners across the Future Years Defense Program; and (b) host an AI wargame and experimentation series, beginning with Five Eyes allies.

Component 2: Accelerate NATO AI adoption.

NATO and its member states recognize that AI-related technology has transformative potential for collective security. Coordinated, accelerated, responsible adoption of AI must be an urgent priority across the Alliance in order to address the challenge presented by algorithmic warfare.¹⁹² NATO allies need to dedicate personnel and resources to support the development and

¹⁹⁰ DoD Instruction 3100.08: *The Technical Cooperation Program (TTCP)*, U.S. Department of Defense (Oct. 15, 2018), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/310008p.pdf?ver=2017-11-30-114948-343>.

¹⁹¹ *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*, Office of the Director of National Intelligence at 10 (Jan. 16, 2019), <https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf>.

¹⁹² Memorandum from Robert O. Work, Deputy Secretary of Defense, *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*, U.S. Department of Defense (Apr. 26, 2017), https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf.

operational applications of AI-related, and other Emerging and Disruptive Technologies (EDTs).

Actions for the Departments of Defense and State:

- **Provide clear policy guidance, technical expertise, and resource support to assist and accelerate NATO’s AI-related initiatives to:**
 - Ensure AI technologies are incorporated into the *NATO Defense Planning Process*, *NATO Warfighting Capstone Concept*, and plans for *Deterrence and Defense of the Euro-Atlantic Area*;
 - Evaluate DOTMLPF-P for AI adoption and future plans for AI-enabled warfighting architecture and interoperability in allied or coalition environments;
 - Support and coordinate development and adoption of foundational definitions, operational and data-sharing practices, technical standards and architectures focused on interoperability, privacy, and responsible, legal deployment of AI;
 - Ensure the *NATO Science and Technology Strategy* anticipates technological developments to guide NATO and national research and development priorities;
 - Develop NATO international staff and allied nation technical expertise;
 - Conduct simulations, wargaming, experimentation, and pilot projects with use cases for data fusion, data exploitation, and interoperability; and
 - Assist in the collaboration with partners beyond the NATO Alliance, including industry and academia.
- **Develop, with NATO allies, a proposal for an Alliance-wide AI Implementation Strategy deliverable for NATO Heads of State.**
 - The proposal should build upon key recommendations of the NATO Reflection Group report submitted to the Secretary General,¹⁹³ and should provide guidance on the areas identified above.¹⁹⁴

Component 3: Foster the JAIC AI Partnership for Defense (AI PfD) as a critical vehicle to further AI defense and security cooperation.

Launched in 2020, the AI PfD is a DoD-led effort to convene partner nations to “provide values-based global leadership” on adoption of AI in the defense and security context.¹⁹⁵ Current members include Australia, Canada, Denmark, Estonia, Finland, France, Israel, Japan, Norway, South Korea, Sweden, and the United Kingdom.

¹⁹³ *NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General*, NATO at 29-31 (Nov. 25, 2020), https://www.nato.int/cps/en/natohq/news_179730.htm.

¹⁹⁴ For further detail, see *Interim Report and Third Quarter Recommendations*, NSCAI at 187-195 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

¹⁹⁵ The AI PfD seeks to align “like-minded nations to promote the responsible use of AI, advance shared interests and best practices on AI ethics implementation, establish frameworks to facilitate cooperation, and coordinate strategic messaging on AI policy.” *Joint Statement*, AI Partnership for Defense (Sept. 15-16, 2020), https://www.ai.mil/docs/AI_PfD_Joint_Statement_09_16_20.pdf. The AI PfD held its second formal dialogue in January 2021. *DoD Joint AI Center Facilitates Second International AI Dialogue for Defense*, JAIC (Jan. 27, 2021), https://www.ai.mil/news_01_27_21-dod_joint_ai_center_facilitates_second_international_ai_dialogue_for_defense.html.

Action for the Department of Defense:

- **Prioritize and foster the AI PfD as a critical space for democratic allies and partners to work through defense issues on AI.**
 - The AI PfD can enhance U.S. efforts to accelerate AI adoption across NATO by supporting key foundational efforts related to data governance and management, infrastructure and technical, legal and ethics expertise. DoD and Congress should provide continued support to enable the AI PfD to further AI cooperation on defense and security with key allies and partners.

Component 4: Incorporate AI into Indo-Pacific defense cooperation efforts.

Increased opportunities exist for collaboration with Quadrilateral Security Dialogue (Quad) partners India, Japan, and Australia, and other nations committed to advancing a free and open Indo-Pacific region.

Actions for the Departments of Defense and State:

- **Build on the Quad framework and negotiate formal AI-related defense and intelligence cooperation agreements in the Indo-Pacific region with Australia, India, and Japan, as well as with New Zealand, South Korea, and Vietnam.**
 - This could be done in connection with broader conventional defense and intelligence relationships, and existing security cooperation agreements, or in a standalone manner, bilaterally or multilaterally. The U.S. government should also prioritize AI interoperability at ministerial and working level meetings.

Component 5: Create an Atlantic-Pacific Security Technology Partnership to improve defense and intelligence interoperability across Europe and the Indo-Pacific.

An Atlantic-Pacific technology partnership would seek to improve capability and interoperability by bringing together technology innovation with allied and partner militaries and intelligence communities, whether in a NATO, coalition, or other multinational context.

Action for the Departments of Defense and State:

- **Advance a deliberate NATO partnership with Indo-Pacific allies and partners for AI-enabled defense cooperation.**
 - A NATO-Indo-Pacific partnership focused on AI is needed to facilitate early collaboration and lay the groundwork for interoperability among different allied and partner warfighting architectures.
 - Plans for such a partnership should include guidance from the tri-chair Steering

DRAFT NSCAI DOCUMENT

Committee on Emerging Technology for data sharing, common standards, wargame and experimentation, and improving interoperability of AI systems and warfighting architectures.

Component 6: Modify authorities and processes in order to improve DoD's ability to conduct international capability development.

DoD requires more flexibility in its ability to develop, test, and field AI-enabled systems with existing and new foreign partners, both public and private.

Action for Congress:

- **Expand the flexibility and the agility of the Secretary of Defense's authority to engage in cooperative R&D agreements.**
 - Legislation should permit DoD to pursue cooperative projects with private companies, academic research centers, and defense- and non-defense governmental entities within NATO, major non-NATO allies, and friendly foreign countries, without a direct showing to the improvement of conventional defense capabilities.
 - Legislation should also account for partners' non-monetary contributions, including the value of R&D capabilities and the strategic partnerships, when assessing potential projects.

Actions for the Department of Defense:

- **Review and revise policies related to International Armaments Cooperation to provide flexibility for AI and software driven partnerships.**
 - The review should include policies related to technology transfer, national disclosure, information and equipment use, equitability requirements, funding requirements, and contracting.
 - DoD should update policies to provide greater delegation of authorities to Military Departments and Defense Agencies to conclude international agreements.
- **Revise DoD Instruction (DoDI) 5530.03, "International Agreements,"¹⁹⁶ to provide appropriate guidance on AI and software-driven partnerships.**
 - DoDI 5530.03 should be revised to (a) enable continuous collaboration on evolutionary hardware and software products that need continuous update across research, development, testing, evaluation, and operational deployment with international partners; (b) provide sufficiently flexible entry and exit criteria for

¹⁹⁶ DoD Instruction 5530.03: *International Agreements*, U.S. Department of Defense (Dec. 4, 2019), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/553003p.PDF>.

all types of international partners (governmental, industry, and academic) to facilitate capabilities, products, knowledge, and services at the point of need; and (c) provide guidance for acceptable thresholds and limits to balance the protection and promotion aspects of AI-related capability development with international partners.¹⁹⁷

DRAFT

¹⁹⁷ This includes policies related to tech transfer, national disclosure and information/equipment use, equitability and funding requirements, and contracting.

[BLANK PAGE]

DRAFT

Chapter 5: AI and the Future of National Intelligence Blueprint for Action

Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission. However, critical barriers keep the Intelligence Community (IC) from turning this potential into real capabilities that are scaled across agencies.

An Ambitious Agenda: AI-Ready by 2025. To build on the progress that individual agencies have made, the IC should set the ambitious goal of adopting and integrating AI-enabled capabilities across every possible aspect of the intelligence enterprise as part of a larger vision for the future of intelligence.

Recommendation: Empower the IC's science and technology leadership.

Actions for Office of the Director of National Intelligence (ODNI):

- **The DNI should designate the Director of Science and Technology (S&T) as the IC Chief Technology Officer (CTO)¹⁹⁸ and direct the IC CTO to:**
 - Develop and monitor IC-wide metrics for AI investments, AI implementation, AI outcomes, and AI readiness.
 - Ensure maximum sharing and reuse of AI models, code, and tools across the IC to prevent unnecessary duplication where possible.
 - Establish policies on, and supervise, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.
 - After congressional approval and appropriation, manage a fund that would allow the ODNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.
- **The IC CTO, in coordination with the IC Chief Information Officer (CIO), Chief Data Officer (CDO), and Chief Information Security Officer, should oversee the establishment of common technical standards and policies for the IC. These standards and policies should be coordinated with the DoD to promote maximum interoperability, reciprocity, and data-sharing¹⁹⁹ in the following areas:**

¹⁹⁸ We envision the IC CTO as having roles, responsibilities, and authorities similar to the Under Secretary of Defense for Research and Engineering (USD(R&E)) within the DoD and to help the IC implement guidance and priorities established by the Steering Committee on Emerging Technology and the Technology Competitiveness Council.

¹⁹⁹ In Chapter 3 of this report, the Commission recommends the creation of a Steering Committee on Emerging Technology that is tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director for National Intelligence. This Committee should act as a forum through which to drive coordination between the IC and DoD, including the Chief Technology Officers.

DRAFT NSCAI DOCUMENT

- An Application Programming Interface (API) driven open architecture and associated policies that support the infrastructure to enable AI.²⁰⁰
 - Multi-level security standards for technical solutions allowing the movement of data across security clearance levels and the policies to enable it.
 - Data tagging and labeling.
 - Data sharing and access, including incentives for data stewards that reward their ability to share their data; shift the culture such that data stewards make it a default practice of externalizing their data via APIs, with appropriate levels of access restriction and control.
 - Common standards for machine readable processing, exploitation, and dissemination (PED) products.
 - Automated and reciprocal Authority to Operate (ATO) processes that include rapid code certification and accreditation processes.
 - Documentation strategies for data, models, and systems, and of the AI lifecycle, infrastructure to support traceability, training and testing procedures, and human-AI design guidelines.²⁰¹
 - Technical standards for algorithms in support of interpretability and explanation, and policies to strengthen accountability.
 - Technologies and operational policies that align with privacy preservation, fairness, inclusion, human rights, and documentation of value considerations and trade-offs.²⁰²
 - Alternative hiring authorities for term-limited appointments appropriate for technical positions, such as special Government employees (SGE), highly qualified experts (HQE), and Intergovernmental Personnel Act (IPA) detailees.
 - Expanding the use of prize challenges as alternatives to traditional procurement.
 - Program and contracting guidance for well documented and hardened APIs, data access and sharing across the IC, and provisions for the sharing and reuse of software products across the IC.
- **The IC CTO, in coordination with DoD, should develop a technology annex to the National Intelligence Strategy (NIS).**²⁰³
 - The annex should establish technology roadmaps to adopt AI-enabled applications to solve operational intelligence requirements. The annex should address current issues within the IC, to include:

²⁰⁰ Consistent with the DoD digital ecosystem described in the Chapter 2 Blueprint for Action, the API driven open architecture should: 1) define a common set of well-documented common interfaces for the ecosystem's key components and building blocks; 2) support and integrate the work of existing pathfinders up and down the ecosystem technology stack; and 3) incorporate the process elements for data authorizations and continuous software ATO reciprocity.

²⁰¹ Chapter 7 of this report provides more details on improving documentation practices for achieving baseline robust and reliable AI.

²⁰² Chapter 8 of this report provides details on developing and testing systems per goals of privacy preservation and fairness.

²⁰³ A technology annex to the NIS should complement the technology annex to the National Defense Strategy (NDS) recommended in Chapter 2 of this report. The recommended Executive Agent for the technology annex to the NDS (see the Chapter 2 Blueprint for Action), the Undersecretary of Defense for Research and Engineering (USD(R&E)) should act as the primary interlocutor with the IC CTO for the creation of an technology annex to the NIS.

DRAFT NSCAI DOCUMENT

- Aligning technical standards and policies with DoD to ensure seamless interoperability as well as make the Executive Branch a better customer and more attractive market for industry.
- Identify and promote acquisition reforms and methods that ensure the IC can rapidly procure and field systems to its intelligence professionals.
- The technology annex to the NIS should, at a minimum, include:
 - Intelligence support requirements, including how the IC analyzes the global environment and monitors technological advancements, adversarial capability development, scientific and technical cooperation among U.S. competitors, and emerging threats.
 - Functional requirements and technical capabilities necessary to enable concepts that address each challenge.
 - A prioritized, time-phased plan for developing or acquiring such technical capabilities, that takes into account research and development timelines, a strategy for public private partnerships, and a strategy for connecting researchers to end users for early prototyping, experimentation, and iteration.
 - Additional or revised acquisition policies and workforce training requirements to enable IC personnel to identify, procure, integrate, and operate the technologies necessary to address the intelligence requirements.
 - Infrastructure requirements for developing and deploying technical capabilities, including data, compute, storage, and network needs; a resourced and prioritized plan for establishing such infrastructure; and an analysis of the testing, evaluation, verification, and validation (TEVV) requirements to support prototyping and experimentation and a resourced plan to implement them, including standards, testbeds, and red-teams for testing AI systems against digital “denial & deception” attacks.
 - Consideration of human factor elements associated with priority technical capabilities, including innovative human-centric approaches to user interface, human-machine teaming, and workflow integration.
 - Consideration of interoperability with allies and partners, including areas for sharing of data, tools, and intelligence products.
 - Flexibility to adapt and iterate annex implementation at the speed of technological advancement.
- **ODNI should advance and continue to build out a purpose-built IC Information Technology Environment (ITE) that can fuse intelligence from different domains and sources.**
 - The IC ITE should be built in concert with the DoD digital ecosystem outlined in Chapter 2 of this report; they should focus on a federated system that is interoperable, integrated, and designed with building block services using the same interfaces as the DoD ecosystem.

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

- The IC should accelerate ad hoc work and continuous experimentation to learn better how to integrate their systems.
 - Intelligence fusion promised by AI can only occur when all relevant data is made available across all systems. Building on the promise of IC ITE, the IC CIO and CTO should work with their counterparts across the IC and mission partners to ensure that IC integration and interoperability are given priority when evaluating technology investments.
 - The IC CTO should establish a multi-agency accredited learning environment and test bed where ad-hoc work and continuous experimentation can occur using all relevant intelligence data.

Actions for Congress:

- **Designate the Director of S&T within ODNI as the IC CTO and grant that position additional authorities for establishing policies on, and supervising, IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.**
- **Establish a fund that would allow the DNI to identify and invest in AI applications with outsized potential that may not have an identified source of agency or program funding as they near the end of their S&T life cycle.**
- **Grant the Director of National Intelligence sufficient budgetary authorities to enforce technical standards across the IC, including the ability to fence or otherwise withhold funding for programs that are not compliant with established common standards and policies.**
- **Establish a 10-year, \$1 billion, Program of Record to provide long-term, predictable funding for technologies identified in the technology annex to the National Intelligence Strategy.**
 - This funding should target programs or departments with a proven track record of transitioning new or critical technologies to meet mission needs.

Recommendation: Change risk management practices to accelerate new technology adoption.

Actions for ODNI:

- **Establish an IT Modernization Senior Risk Management Council (IT SRMC).**
 - The IT SRMC should be tri-chaired by the IC CTO, CIO, and CDO to promote the effective governance of significant risk across the IC.
 - The IT SRMC should report to the Principal Deputy Director of National Security (PDDNI).

DRAFT NSCAI DOCUMENT

- The IT SRMC should become a regular briefing entity in the Deputies Executive Committee (DEXCOM).
- The IT SRMC should include a senior member from the following IC entities:
 - ODNI Office of General Counsel;
 - ODNI Office of Civil Liberties, Privacy, and Transparency;
 - ODNI Mission Integration Directorate; and
 - Each intelligence agency and service branch.
- The IT SRMC responsibilities should include:
 - Reviewing existing policies or creating new policies to ensure the IC uses informed risk acceptance and management practices when considering the adoption and use of AI technologies.
 - Advising the DNI on enterprise risk associated with not adopting AI technologies.
- **Address shortcomings in the current implementation of the National Institute of Standards & Technology (NIST) Federal Information Security Modernization Act (FISMA) Risk Management Framework (RMF).**²⁰⁴
 - Recommendations from the IT SMRC should inform the operational risk of *not* adopting a new technology as a balance to the technical risks considered in the RMF, allowing agencies to make better informed decisions on what systems it chooses to bring on line or delay.
 - The IC should automate the implementation and simultaneous assessment of RMF considerations to the greatest extent possible.
 - Agencies within the IC often implement the RMF with different, but associated policies that can prevent reciprocal accreditation and make it difficult to share tools among agencies.
 - The IC should make accreditation reciprocity within the RMF the standard and apply a high level of scrutiny to any agency that seeks to not recognize the accreditation of others.

Actions for Congress:

- **Assess the IC's approach to risk and work with the IC to ensure the proper balance between risk acceptance, risk management, and risk avoidance.**

²⁰⁴ For more information, see *FISMA Implementation Project*, NIST (Dec. 3, 2020), <https://csrc.nist.gov/projects/risk-management/rmf-overview>.

Recommendation: Improve coordination between the IC and DoD.

Actions for ODNI:

- **In coordination with the Secretary of Defense, the DNI should immediately issue a directive designating the PDDNI as a standing member and/or co-chair to the tri-chair Steering Committee on Emerging Technology.**²⁰⁵
 - Absent of Congressional action, the Director of National Intelligence should work with the Secretary of Defense and members of the Steering Committee on Emerging Technology, including the Deputy Secretary of Defense and Under Secretary of Defense for Intelligence and Security, to identify the method and means to drive sustained coordination on emerging technology intelligence, policy, and resourcing.
- **Assist DoD, as requested, in developing the technology annex to the National Defense Strategy.**²⁰⁶
- **Work with DoD to establish an AI integration team focused on maximizing knowledge, data, and model sharing across and between the IC and DoD.**

Actions for Congress:

- **Revise the National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA) provision authorizing a Steering Committee on Emerging Technology by designating it to be tri-chaired by the Deputy Secretary of Defense, the Vice Chairman of the Joint Chiefs of Staff, and the Principal Deputy Director of National Intelligence.**²⁰⁷

Recommendation: Capitalize on AI-enabled analysis of open source and publicly available information.

²⁰⁵ The Chapter 3 Blueprint for Action calls for the Secretary of Defense, with support from the Director of National Intelligence, to issue a directive immediately establishing a tri-chair Steering Committee on Emerging Technology to oversee development of concepts and capabilities that include emerging and disruptive technologies to meet the current and future operational challenges facing the nation.

²⁰⁶ For a full discussion of the Technology Annex to the National Defense Strategy, see Chapter 2 of this report.

²⁰⁷ This action mirrors the Chapter 3 Blueprint for Action. While DoD and ODNI have the authority to establish such a forum without legislative action, codifying it into law will ensure that it is sustained through leadership transitions. If, at the drafting of the FY 2022 NDAA, the DoD and ODNI have established the tri-chaired Steering Committee recommended herein, Congress should use the FY 2022 NDAA to codify the body into law. If DoD and ODNI have not established the Committee as described in this report, Congress should include in the FY 2022 NDAA a provision revising the FY 2021 NDAA, section 236, which permits the creation of a Steering Committee on Emerging Technology, but is not structured effectively to improve coordination between the DoD and the IC. For a full discussion of section 236, see the Chapter 3 Blueprint for Action. The Commission also recommends that the legislative language be sufficiently broad so as to enable flexibility in the Steering Committee's roles and responsibilities should they need to adapt as emerging technologies and Department efforts evolve. See the Draft Legislative Language Appendix to this report.

Actions for ODNI:

- **Develop a coordinated and federated approach to integrate open source intelligence into all current intelligence processes and products. ODNI should promote coordination by taking the following actions:**
 - Develop common standards and policies that enable the individual agencies to be more effective, such as contracting publicly available data sources for common use across the IC and clarifying or updating policy guidance on the appropriate use of publicly available and open source information, including with respect to privacy and civil liberties for U.S. persons or entities.
 - Support the IC by identifying reliable industry partners across the spectrum of information sources and creating contract vehicles to rapidly integrate them into intelligence work across the IC. This should include establishing a pilot project to test “data-for-tools” exchanges in public-private partnerships.
 - Aid the IC in communicating emerging risks and threats to industry and academia by coordinating the right expertise from across the IC—for example, by connecting non-government entities to the Federal Bureau of Investigation for counter-intelligence guidance, or to the U.S. Cyber Command/National Security Agency for cybersecurity.
 - Develop a robust capability for bringing in individuals without security clearances or awaiting security clearance adjudication and allowing them to work on unclassified projects that directly support the IC.
- **Each individual agency should develop open source capabilities focused on the specialized applications of open source and publicly available information within their unique intelligence domains.**

Recommendation: Aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC.

Actions for ODNI:

- **Develop an implementation plan for security clearance reform for clearances at the Top Secret and above level including detailed timelines and metrics. The implementation plan should include:**
 - A collaborative effort with the private sector and academia to develop data-informed behavioral approaches to understanding risk factors and security clearance adjudication.²⁰⁸

²⁰⁸ For more information on the need for an academic and scientific review of behavioral approaches to security clearance adjudication, see David Luckey, et al., *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?*, RAND Corporation at 28-34 (2019), https://www.rand.org/pubs/research_reports/RR2684.html.

DRAFT NSCAI DOCUMENT

- Reforming identity management to ensure there is seamless security clearance reciprocity across the IC.
- A mechanism to enforce security clearance reciprocity among members of the IC and DoD.

Actions for Congress:

- **Congress should require the DNI to develop an implementation plan for security clearance reform for clearances at the Top Secret and above level including detailed timelines and metrics.**
- **Where necessary, Congress should reinforce the DNI's authority as head of the IC to enforce uniform security clearance policies and practices across the IC.**
- **Congress should require the DNI and the directors of the major intelligence services to regularly report on progress to the oversight committees.**

[BLANK PAGE]

DRAFT

Chapter 6: Technical Talent in Government Blueprint for Action

The United States government needs digital experts now or it will remain unprepared to buy, build, and use AI and its associated technologies. Expanding digital expertise is the most important step the government can take to modernize. While this challenge is recognized, few parts of government have adequately invested in building their digital workforce.

To expand its digital and AI digital workforce, the government needs to

- **Organize** technologists within government through a talent management system designed to house highly skilled specialists;
- **Recruit** people that already have the skills the government needs, such as industry experts, academics, and recent college graduates;
- **Build** its own workforce by training and educating current government employees; and
- **Employ** its digital workforce more effectively to ensure digital talent can perform meaningful work once they are in government.

Organize

Recommendation: Create Digital Corps for Cabinet-Level Departments and Select Agencies to Organize the Government’s Technical Workforce

How a digital workforce is organized is as important as the workforce’s level of expertise. We propose creating Digital Corps for Cabinet-level departments and select agencies that would recruit, train, and educate personnel; place personnel in and remove personnel from digital workforce billets; manage digital careers; and set standards for digital workforce qualifications. Agencies would create billets for members of the Digital Corps, and provide guidance to members of the Digital Corps about the work they perform.

Existing Models: The Army’s Medical Corps—Full scaling of specialized talent will only happen if hired personnel have freedom to solve technical challenges. Many existing strategies for personnel management are inadequate due to a shortage of people in government agencies who can properly manage such specialized talent. A notable counterexample to this, which serves as an inspiration to our Digital Corps model, is the U.S. Army’s Medical Corps. The Medical Corps organizes experts with specialized healthcare skills that do not fit into the Army’s traditional talent management framework.²⁰⁹ Nurses and doctors receive education and training as civilians, but their skill sets are crucial to the Army’s healthcare system. So, the Medical Corps talent management framework was created to house these medical professionals in a way that maximizes their ability to practice medicine within the Army. Like the Medical Corps, the Digital Corps should have specialized personnel policies, guidelines for promotion, training resources, and certifications for personnel to demonstrate proficiency in new digital areas.

²⁰⁹ Jim Perkins, et al., *Don’t Just Copy and Paste: A Better Model for Managing Military Technologists*, War on the Rocks (Aug. 24, 2020), <https://warontherocks.com/2020/08/dont-just-copy-and-paste-a-better-model-for-managing-military-technologists/>.

Notably, a Digital Corps would not be comparable to either the Marine Corps or a Space Service, as it would not have a service secretary or a distinct theater or domain, and its members would work for existing services or agencies.

Roles Within the Digital Corps—Career fields are distinct from core competencies—skills that every Digital Corps member should possess prior to hiring—such as modern stack software development, deployment, and data-informed decision-making. Training resources for each career field should be made available to Digital Corps members across every agency. Departments and agencies must also be cognizant that digital talent is rarely interchangeable across different skill sets—for example, database architecture, machine learning, and user experience design all fall into different career fields with near-zero overlap. Digital Corps members should be allowed to focus on any one of the following additional career fields:

- Software Development
- Data Science
- Artificial Intelligence
- DevOps and site reliability engineering
- Human-centered product design
- Product Management
- Security
- Data governance and use
- Emerging technologies²¹⁰

Digital Corps technologists should be able to continue to promote without leaving their focus area and move upward into management. Many private tech companies distinguish between their engineering and engineering management tracks, so that skilled engineers are not incentivized to become managers solely for the sake of career advancement. The Army’s Medical Corps follows a similar model. Once promoted, officers highly competent in their medical specialty can either continue as clinicians or become administrators and managers within the Medical Service Corps.

Staffing and Digital Corps Billets—Cabinet-level departments and select agencies should develop their own Digital Corps rather than relying on a single, government-wide Digital Corps. For Corps members, this approach creates well-defined tracks for career progression and stronger incentives to stay. This approach also makes it easier for departments and agencies to identify and invest in in-house talent for future technology projects.

Each Cabinet-level department and select agency should create designated billets to be filled by qualified members of its Digital Corps based on skills and experience. In addition, each should maintain a central talent repository with Corps members’ portfolios of prior digital projects completed with the agency. Departments and agencies can then search this repository to find the most suitable Corps member to fill each billet. Taking inspiration from software development

²¹⁰ These fields were selected from a combination of NSCAI’s Third Quarter recommendations and Partnership for Public Service’s *Tech Talent for 21st Century Government*. See *Interim Report and Third Quarter Recommendations*, NSCAI (Oct. 2020), <https://www.nscai.gov/previous-reports/>; *Tech Talent for 21st Century Government*, Partnership for Public Service: Tech Talent Project (Apr. 2020), <https://ourpublicservice.org/wp-content/uploads/2020/04/Tech-Talent-for-21st-Century-Government.pdf>.

companies, one method of reliably measuring skill proficiency is to conduct digital interviews consisting of case questions and whiteboarding exercises. We recommend that billets be filled based on candidates' performance in these interviews, chosen career field, and prior project experience (possibly while filling other billets within the same agency at an earlier date).

Actions for Departments and Select Agencies:

- Allocate resources towards the creation of Digital Corps modeled after the Army's Medical Corps.
- Develop Digital Corps training resources in the forms of licensed instructional videos, tutorials, and coursework for each of the 9 career fields listed.
- Create agency-specific talent repositories where Corps members can list project portfolios, source code (where permitted), and career field training badges.
- Create billets and fill them through interviews, evaluation of Corps members' career field training, and other relevant experiences.
- Develop parallel management-oriented and technical-oriented tracks for each Corps member's career progression, with set standards for promotion per agency.

Recruit

The government needs to improve its ability to attract scarce AI talent from the private sector, academia, and recent college graduates. Doing so requires making paths to service as easy as possible for as many technologists as possible.

Many AI and other digital practitioners are interested in working with the government and can and would do so as either full-time employees or part-time employees. Of those desiring full-time employment, some seek an entire career as a government civilian or in the military. Others, while willing to work with the U.S. Government full-time, are less willing to make long-term commitments or to dedicate as much of their time, and instead desire to become short-term employees, fellows, talent exchange participants, or military reservists. A third group is willing to work with or for the government part-time, but are unwilling to become full-time civilian employees and have no desire to serve as part of the military. To improve recruiting, the government needs to improve the hiring process and build mechanisms for part-time civilian service.

Recommendation: Create a National Reserve Digital Corps

The government would benefit from access to a larger portion of the country's total digital workforce. Many government digital projects suffer from lack of access to digital expertise. The U.S. Government should establish a civilian National Reserve Digital Corps (NRDC) modeled after the military reserves' service commitments and incentive structure. Members of the NRDC would become civilian special government employees (SGEs),²¹¹ and work at least 38 days each

²¹¹ A special government employee is "an officer or employee of the executive or legislative branch of the United States Government . . . who is retained, designated, appointed, or employed to perform, with or without compensation, for not to exceed one hundred and thirty days during any period of three hundred and sixty-five consecutive days." 18 U.S.C. § 202.

year as short-term advisors, instructors, or developers across the government.²¹² Longer-term positions would be established on an individual basis. While short-term volunteers are not a substitute for full-time employees, they can help improve AI education for both technologists and non-technical leaders, perform data triage and acquisition, help guide projects and frame technical solutions, build bridges between the public and private sector, and other important tasks.²¹³ Several AI practitioners within the United States Government have said during interviews with the NSCAI that their projects would benefit from the kind of reserve corps we propose here.

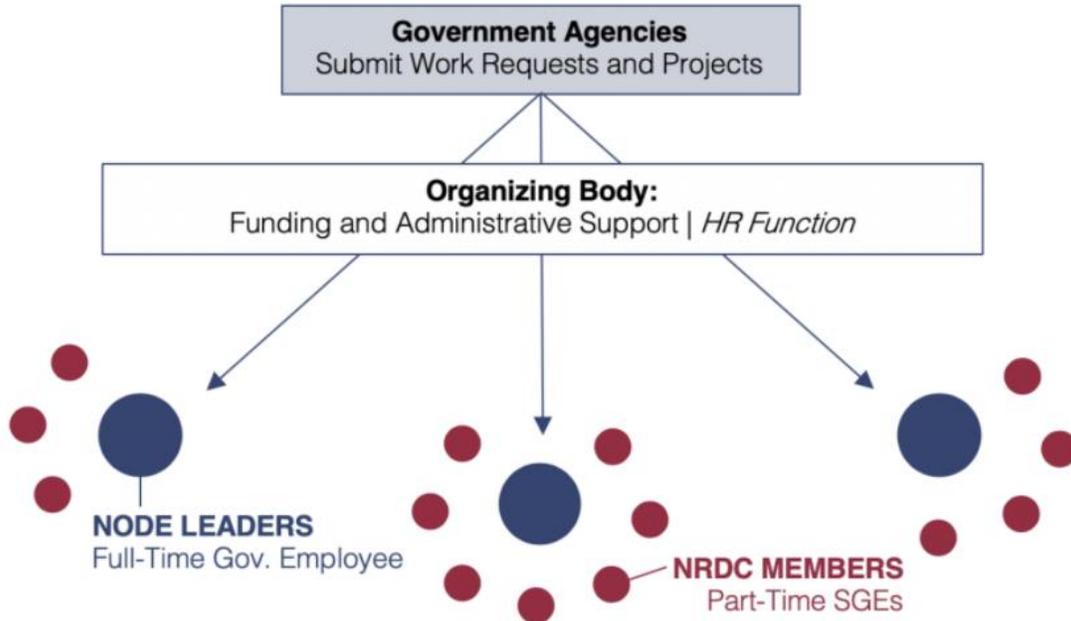


Figure 1: Illustrating the NRDC

General Structure.—We recommend establishing and managing the NRDC as a set of nodes that fall under the supervision of the Office of Management and Budget (OMB). Each node would be aligned with a full-time government employee leader selected by OMB rather than geography, digital applications, or government agency. In effect, OMB would select node leaders, who would then be responsible for recruiting and organizing their team. In addition to selecting node leaders, OMB would establish standards, ensure nodes meet government client requirements, provide funding and administrative support, maintain security clearances, establish access to an agile development environment and tools, and facilitate technical exchange meetings, when appropriate, to ensure stovepipes are not created.

²¹² Members of the military reserves typically serve two to three days a month, and one 14-day obligation a year, averaging around 38 days a year.

²¹³ Organizations that employ full-time technical experts in temporary positions, such as the United States Digital Service or Defense Digital Service, already exist, and have proven successful. The NRDC is an alternative for experts that cannot or do not want to pursue a full-time route.

Recruitment.—Each node would be responsible for recruiting and screening its digital experts. Notably, OMB would not be responsible for establishing qualification standards for members of the NRDC. While volunteers would need to be able to pass a background check and would not be employees of a foreign government (though they might be foreign nationals), node leaders would be empowered to screen and select volunteers, and to recruit experts from within NRDC for specific tasks. OMB would provide administrative support, much like a human resources team in a private sector company.²¹⁴

Project Selection.—Projects would be selected in three ways:

- Selection by a node after contact with a government client,
- OMB would direct a node to take on a project, and
- Node leadership would approve individual projects driven by a perceived need that is not tied to a request from a government client.

Government clients would directly contact node leaders or OMB. Nodes would be responsible for establishing relationships with government agencies and selecting projects, but OMB would be responsible for ensuring that agencies' requests are received and that nodes contribute to NRDC's mission and vision. Individual projects that are not driven by a government client's request would be pursued at the node leadership's discretion.

Relationship with Government Agencies.—Members of the NRDC would work with agencies on a project-to-project basis— such as consulting for a specific project or teaching a specific course. They would not have a commitment to work with the same agency consistently. Government agencies would be responsible for paying for their projects, including the cost for reservist time.

Relationship with Civilian Employers.—Members of the NRDC and their civilian employers would be bound by the same rules as the military reserve under the Uniformed Services Employment and Reemployment Rights Act (USERRA).²¹⁵ Members would be responsible for identifying conflicts of interest and removing themselves as appropriate. Employers would not be able to discriminate against members of NRDC, fire them, or delay promotions as a consequence of spending time serving in NRDC.²¹⁶ Implementation could take the form of a legislative recommendation to modify USERRA or a proposal modeled after USERRA.

Incentivizing Reservist Participation.—Civilian reservists in this program would benefit in several ways. They would gain an opportunity to contribute to their country, do exciting, meaningful work, and attain awareness of work and advances in a community that differs from their own. They may also benefit from the following incentives:

²¹⁴ Some administrative functions, such as background checks, security clearance processing, processing tax paperwork, and others, would place an unnecessary burden on local nodes and should be addressed by a central body such as OMB.

²¹⁵ *Uniformed Services Employment and Reemployment Rights Act of 1994*, U.S. Department of Justice (Aug. 6, 2015), <https://www.justice.gov/crt-military/userra-statute>.

²¹⁶ Frank Whitney, *Employment Rights of the National Guard & Reserve*, U.S. Department of Justice (last accessed Jan. 1, 2021), <https://www.justice.gov/sites/default/files/usao-ednc/legacy/2011/04/29/EmploymentRights.pdf>.

- The government should create an NRDC scholarship program modeled after the Reserve Officer Training Corps. Universities would select students through a competitive process to receive full tuition and study specific disciplines related to digital technology. In return for accepting the scholarship, graduates would spend part of their summers during school in government internships. Between their freshman and sophomore years, students would spend six weeks becoming familiar with a range of U.S. Government departments and agencies. Between their sophomore and junior years, students would spend six weeks as an intern at a specific government agency or office. Between their junior and senior years, students would spend another six weeks interning at a specific agency or office. Upon graduation, scholarship recipients would spend five years serving in the NRDC, beginning as a GS-7 and advancing to a GS-11 over the course of five years. Students would also begin the security clearance process at least two years before graduating.²¹⁷
- The NRDC should include a training and continuing education fund for all members. The NRDC would pay up to \$50,000 to each reservist to attend training and educational opportunities related to AI or to pay for student loans. Educational opportunities would include conferences, seminars, degree and certificate granting programs, and other opportunities. An incentive explicitly tied to continuing education would increase the perceived and actual competency of AI reservists. It would also attract those with an active interest in continuing education, especially new practitioners seeking to establish themselves.

How NRDC Would Work: An Example.—The following is a hypothetical example of how the NRDC would function. In this example, OMB would begin creating a node by selecting a leader that would be trusted to establish and manage a team of reservists. OMB selects “Jennifer,” a full-time government employee working within the NRDC division of OMB, to lead a new NRDC node. Jennifer decides to organize her node functionally rather than regionally. Using existing government tools and her professional contacts, she recruits people from across the country, most of whom have backgrounds in healthcare data management or recent graduates with degrees related to the field. She also recruits from within the NRDC by posting open positions on online job boards. During the recruitment process, OMB provides financial support for recruitment efforts, travel money, and processes new reservist administrative paperwork, including security clearance applications.

After the node is established and the team is in place, a government agency—in this example, the Centers for Disease Control and Prevention (CDC)—realizes it has two digital needs it cannot meet internally: improving a database and training their workforce in new data management practices at the National Center for Chronic Disease Prevention and Health Promotion. After reaching out to OMB, they determine that Jennifer’s node is the best fit, and request assistance. After examining the request and her team’s workload, Jennifer determines that she would support the CDC’s database improvement request with a four-person team and support workforce training with a two-person team. The four-person team spends 14 days examining the

²¹⁷ All reservists would apply for security clearances, but this should not imply that reservists would work primarily on classified materials. A large part of the work needed to modernize the government is unclassified.

existing database and making updates to the database. The two-person team spends ten days on site at the National Center for Chronic Disease Prevention and Health Promotion speaking with leaders and employees about their data management needs and the current state of the workforce's skill level, developing curriculum, and teaching data management best practices.

The teams Jennifer selects to support the CDC include Michael. Michael received a four-year scholarship from NRDC to study computer science as an undergraduate. After graduating three years ago, he began working full-time as a data analyst at a healthcare company and working part-time on NRDC projects he coordinates with his node leader. He also used his education stipend to pay for an online course from MIT last year. This hypothetical shows that an NRDC can effectively increase the U.S. digital talent, connect private-sector workers with a government agency, and create a pathway for that connection to solve an actual problem.

Actions for Congress:

- **Pass legislation establishing the NRDC within OMB**
 - Grant OMB direct-hire authorities to hire node leaders and reservists.
 - The NRDC should offer full tuition scholarships to students studying specific disciplines related to national security digital technology for up to four years in exchange for five years of service as a member of the NRDC. This could be done by including service in the NRDC as an option for people with degrees in digital fields to pay off service obligations incurred as a result of education received in the Defense Civilian Training Corps.²¹⁸
 - Legislation should authorize up to \$50,000 in educational benefits for courses, seminars, conferences, and other educational opportunities that are approved by OMB. It should also ensure that members of the NRDC receive the same employment protections as military reservists under USERRA. This can be done by amending USERRA to cover “service in the uniformed services or the National Reserve Digital Corps.”
 - Congress should make a two-year appropriation of \$16 million to pay for initial administrative, scholarship, and education benefits.
- **Evaluate NRDC Success**
 - Use three metrics to evaluate NRDC's success: 1) the number of technologists who participate annually; 2) evaluations of results from government clients; and 3) evaluations of results from reservists. OMB should establish the central, organizing function for the NRDC within six months of the passage of legislation, and establish five nodes and a mechanism for distributing educational benefits within nine months of the passage of legislation.

Actions for OMB:

²¹⁸ The Defense Civil Training Corps was created by the National Defense Authorization Act for Fiscal Year 2020. See Pub. Law 116-92, sec. 860, National Defense Authorization Act for Fiscal Year 2020, 116th Cong. (2019).

- **Immediately upon receiving authority from Congress, establish a National Reserve Digital Corps with systems and processes designed to:**
 - Select and hire node leaders;
 - Encourage potential government clients to contact NRDC nodes, or OMB, with potential problems to resolve;
 - Ensure government client needs are met by NRDC nodes;
 - Provide funding for education supplements and scholarship programs;
 - Provide administrative support (including for security clearances);
 - Establish node access to development environments and tools;
 - Facilitate technical exchange meetings; and
 - Match recipients of NRDC scholarships with node leaders.

- **At the outset, establish five NRDC nodes. Each node leader should be responsible for:**
 - Recruiting and hiring reservists,
 - Ensuring the quality of their work, and
 - For partnering with government agencies.

Recommendation: Create Digital Talent Recruiting Offices Aligned with Digital Corps

Executive Branch agencies should create agency level digital talent offices of up to 20 personnel responsible for recruiting both early career and experienced professionals. Recruiting offices would monitor their agencies' need for specific types of digital talent. The offices would be empowered to recruit technologists virtually, by attending conferences, career fairs, recruiting on college campuses, and offering scholarships, recruiting bonuses, referral bonuses, non-traditional recruiting techniques such as prize competitions, and other recruiting mechanisms. A recruiting office would assume responsibility for their agency's digital talent recruitment efforts, e.g. Science, Mathematics and Research for Transformation (SMART) Scholarship-for-Service, and partner with agency human resources offices to use direct-hire authorities and the Intergovernmental Personnel Act (IPA) to accelerate hiring. This would help scale digital talent recruitment by creating a central, empowered organization that focuses on a specific mission; concentrates expertise and funds; would help experts move in and out of government positions throughout their career; and can develop relationships with universities and private-sector companies.

Actions for Congress:

- **Amend section 230 of the FY2020 NDAA. (Armed Services Committees)**
 - The DoD should be required to appoint a civilian official responsible for digital engineering talent recruitment policies and their implementation.

DRAFT NSCAI DOCUMENT

- The civilian official should be supported by a digital talent recruiting office with the Office of the Undersecretary for Personnel and Readiness, as described above.
- **Require the Office of the Director of National Intelligence (ODNI) to create a digital talent recruiting office. (Intelligence Committees)**
 - The office should work with the IC to identify their agencies' needs for specific types of digital talent;
 - Recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses;
 - Integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and
 - Partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.
- **Require the Department of Homeland Security (DHS) to create a digital talent recruiting office (Senate Homeland Security and Governmental Affairs Committee and the House Committee on Homeland Security)**
 - The office should work with DHS to identify their agencies' needs for specific types of digital talent;
 - Recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses;
 - Integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and
 - Partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.
- **Require the Department of Energy (DoE) to create a digital talent recruiting office (Senate Committee on Energy and Natural Resources and the House Committee on Energy and Commerce)**
 - The office should work with DoE to identify their agencies' needs for specific types of digital talent;
 - Recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses;
 - Integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and
 - Partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

Actions for DoD, including U.S. military services, DOE, DHS, and the ODNI:

- **Create digital talent recruiting offices.**

DRAFT NSCAI DOCUMENT

- Offices should work with their agencies to identify their need for specific types of digital talent;
- Recruit technologists by attending conferences, career fairs, and actively recruiting on college campuses;
- Integrate federal scholarship for service programs into agency recruiting; offer recruitment and referral bonuses; and
- Partner with their agencies' human resource teams to use direct-hire authorities to accelerate hiring.

Recommendation: Grant exemption from OPM General Schedule Qualification Policies for Specific Billets and Position Descriptions

AI practitioners applying for positions within the federal government and their hiring agencies are constrained by OPM minimum qualification standards. While these standards are important, and have increased fairness in hiring, they also prevent expert technologists that do not have master's degrees, and in some cases bachelor's degrees or comparable work experience, from joining the government at a reasonable level of compensation. For example, a 19 year-old software developer or AI practitioner might have a proven track record on cybersecurity or in AI competitions, but can only enter the government as a GS-7. To reduce this hiring challenge, the government should allow agencies to exempt certain billets from OPM general schedule qualification policies, and instead allow local hiring managers to make an independent decision about both hiring and pay grade based on evaluations, prior work, alternative certification programs, or practical experience.

Actions for Congress:

- **Direct the Office of Personnel Management to amend 5 CFR § 338.301, on service appointments.**
 - Allow service secretaries and cabinet officials to create exceptions from the Qualification Standards for General Schedule Positions by individual billet or position description.

Actions for OPM and Military Services:

- OPM should create and execute a process by which federal departments and agencies can apply for billets or position descriptions to be exempt from general schedule qualification policies.
- Two-star and above commands and their civilian equivalents should declare individual billets and position descriptions exempt from OPM qualification standards without approval from OPM or any more senior authority.

Recommendation: Expand the CyberCorps: Scholarship for Service

The CyberCorps: Scholarship for Service (SFS) is a recruiting program designed to attract students studying IT, cybersecurity, and related fields into the USG. Expanding it could bring in more people with AI-related skills. It is managed by the National Science Foundation in partnership with the Office of Personnel Management and the Department of Homeland Security. Students enrolled in the program receive a scholarship in exchange for an obligation to work in an approved government agency for a period of time equal to the time covered by the scholarship. Seventy undergraduate and graduate institutions participate in SFS by selecting students for the program, and since 2001, 3,600 students have received scholarships, 94 percent of whom went on to serve in government.²¹⁹ Hiring typically takes place during annual online and in-person career fairs.²²⁰

It should be noted that cyber and AI are different fields. Expanding CyberCorps: SFS to CyberCorps and AI: SFS would avoid increasing administrative burdens. This should not be taken as an indication that AI and cyber are synonymous, as the education and skills for each field differ.

Actions for Congress:

- **Amend the CyberCorps: SFS, as defined by section 230 of the National Defense Authorization Act for Fiscal Year 2020.**
 - Include digital engineers,
 - Pay for up to four years of scholarships, and
 - Include the opportunity to begin the security clearance process.
- **Amend 15 U.S.C. § 7442 subsection (a).**
 - “...recruit and train the next generation of information technology professionals, digital engineers, artificial intelligence practitioners, data engineers, data analysts, data scientists, industrial control system security professionals, security managers, and cybersecurity course instructors to meet the needs of the cybersecurity mission for Federal, State, local, tribal, and territorial governments.”
- **Amend 15 U.S.C. § 7442 subsection (b).**
 - Provide an opportunity for scholarship recipients to initiate their security clearance process at least one year before their planned graduation date.

²¹⁹ Engagement with government officials on August 22, 2019, February 7, 2020, and March 9, 2020.

²²⁰ *CyberCorps: Scholarship for Service*, U.S. Office of Personnel Management (last accessed Jan. 1, 2021), <https://www.sfs.opm.gov/>.

- **Amend 15 U.S.C. § 7442 subsection (c).**
 - Allow the scholarship to last for 4 years.

Actions for the National Science Foundation and Office of Personnel Management:

- **Broaden the CyberCorps: SFS.**
 - Pay for up to four years,
 - Include fields falling under digital engineering, as those fields are defined by the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92, section 230): “the discipline and set of skills involved in the creation, processing, transmission, integration, and storage of digital data, including data science, machine learning, software engineering, software product management, and artificial intelligence product management.”

Recommendation: Establish a STEM Corps

A bipartisan group of members of the House Armed Services Committee have proposed H.R. 6526, STEM Corps Act of 2020. The proposal would authorize the appropriation of \$5 million per fiscal year, with \$500,000 for administrative costs and an advisory board. The program provides a maximum scholarship of \$40,000 per student per year. Scholarship recipients would serve in different capacities within the DoD for a minimum of three years, with an option to either remain in the DoD or transfer to a private-sector company that has contributed to STEM Corps funding. The proposal requires participants to be paid at a rate not less than GS-6 for the first three years of their obligation and at not less than as a GS-10 during their fourth year. This proposal has the potential to significantly increase the number of personnel with STEM backgrounds in the DoD civilian workforce for a relatively low cost if a sufficient number of private-sector companies contribute. The potential for recipients to transfer to the private sector after three years of government service may create retention issues, but it may also serve as a mechanism to create bridges between the DoD and private sector companies.

Actions for Congress:

- **Establish a STEM Corps in the FY 2022 NDAA.**
- **Set aside \$5 million for a STEM Corps for FY2022 and each fiscal year thereafter.**

Actions for the DoD:

- **With congressional authorization and appropriation, establish an office to manage and establish a STEM Corps as described above,**
- **Include a scholarship program, advisory board, private-sector partnership program, and STEM Corps member management program.**

Build

The government will not be able to come out of its workforce deficit through recruiting alone. AI and digital talent is simply too scarce in the United States. In 2020, there were more than 430,000 open computer science jobs in the United States, while only 71,000 new computer scientists graduate from American universities each year.²²¹ To overcome the challenges presented by AI and digital talent scarcity, the government should deliberately focus on building its AI and digital workforce.

Recommendation: Create a United States Digital Service Academy

The United States needs a new academy to train future public servants in digital skills. Civil servants play a critical and often underappreciated role in government. They hold much of the government's niche, long-term expertise. This is especially true for the digital expertise that is badly needed for the government to modernize. Methods like the competitive service and scholarship for service programs have helped recruit talent, but as the government's needs changed, those approaches will no longer address the full scope of the government's needs. Bolder measures are necessary to produce the broad, diverse, and technically educated workforce the government needs.

Our proposed United States Digital Service Academy (USDSA) would be an accredited, degree-granting university that receives government funding,²²² be an independent entity within the Federal government, and have the mission to help meet the government's needs for digital expertise. It would be advised by an interagency board that would be assisted by a federal advisory committee composed of commercial and academic leaders in emerging technology.

Existing Models: The Military Service Academies. The USDSA should be modeled off of the five U.S. military service academies but should produce trained government civilians not only to the military departments, but also to civilian departments and agencies beyond DoD.²²³

The five military service academies each produce commissioned officers for the armed forces.²²⁴ The academies select cadets and midshipmen through a congressional and presidential nomination process, followed by a competitive admissions process. The cadets and midshipmen, who are government employees, exchange a commitment to serve after graduation for a tuition-free education. Many choose this path for the opportunity to serve; the free tuition and education often are considered a bonus. Those who depart prior to meeting the minimum requirements for

²²¹ Code.org (last accessed Jan. 11, 2021), <https://code.org/promote>. See also Oren Etzioni, *What Trump's Executive Order on AI Is Missing: America Needs a Special Visa Program Aimed at Attracting More AI Experts and Specialists*, Wired (Feb. 13, 2019), <https://www.wired.com/story/what-trumps-executive-order-on-ai-is-missing/>.

²²² The USDSA should also have the authority to accept gifts, particularly to help fund its establishment.

²²³ The Council on Foreign Relations report, *Innovation and National Security: Keeping Our Edge*, recommends creating a digital military service academy. James Manyika & William McRaven, *Innovation and National Security: Keeping Our Edge*, Council on Foreign Relations (Sept. 2019), <https://www.cfr.org/report/keeping-our-edge/>. Our recommendation is for a civilian digital service academy that would not produce any uniformed military personnel.

²²⁴ The five academies include the United States Military Academy, the United States Naval Academy, the United States Coast Guard Academy, the United States Merchant Marine Academy, and the United States Air Force Academy.

graduation still incur either a service commitment or financial requirement to pay back education received upon their departure from the schools.

The academies contribute between 15 and 20 percent of the new junior officers to their respective services each year—the largest single commissioning source. Academy graduates also play an outsized role in the military services’ senior leadership.²²⁵ As a result, the academies help shape the identity and culture of their services, including their standards and ethical norms. USDSA would be comparable to the other service academies in many ways. It would be a degree granting institution focused on producing leaders for the United States Government. USDSA students, like military service academy students, would not pay for tuition, or room and board, and would have a post-graduation service obligation. Americans should expect USDSA graduates to seek to serve, to lead the nation’s digital workforce, and to ensure the United States sets an example of intelligent, responsible, and ethical high-tech leadership.

Key Differences Between USDSA and the Military Service Academies. The USDSA would differ in significant ways. First and foremost, USDSA students would enter the institution to become civil servants. They would know that their education would be repaid in the form of a five-year obligation to serve in government, which would begin upon graduation when they become a civil servant at a GS-7 level. Exclusively producing civil servants would eliminate the need for students to complete commissioning requirements, simplifying the school’s curriculum and administrative burdens, and reduce the need for expansive campus real estate for training and parade grounds. It would also make USDSA less redundant, as the military service academies already produce hundreds of computer scientists, electrical engineers, and mathematicians every year.

USDSA students would also have a more STEM-focused education. While the core curriculum would ensure broad exposure to different fields, students would have a highly technical education. A wide variety of technical majors could include AI, software engineering, electrical science and engineering, computer science, molecular biology, computational biology, biological engineering, cybersecurity, data science, mathematics, physics, human-computer interaction, robotics, and design. Students could also blend those majors with humanities and social science disciplines such as political science, economics, ethics and philosophy, or history.

A third difference would be that USDSA graduates would serve across the Federal government. To avoid both perceived and real parochial bias from the organizations that administer service academies, USDSA would be administered as an independent Federal entity. The minimum and maximum number of graduates who would serve in each department or agency would be determined annually by an interagency board.²²⁶

²²⁵ Joseph Moreno & Robert Scales, *The Military Academies Strike Back*, *The Chronicle of Higher Education* (Nov. 12, 2012), <https://www.chronicle.com/article/the-military-academies-strike-back/>. As an example, 5 Secretaries of the Navy, 29 Chiefs of Naval Operations, and nine Commandants of the Marine Corps graduated from the United States Naval Academy.

²²⁶ Each military service academy has a maximum and minimum number of positions available for every available career field, causing some graduates to receive career fields other than their first choice. Similarly, USDSA graduating classes would have a minimum and maximum number of civilian graduates that join each military department or government agency.

Mission Statement of the USDSA. We propose the following: “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.”

The Student Experience. During their first year, students would begin the Academy’s core curriculum, explore some electives to help determine their major, and take a summer internship or fellowship. The core curriculum is envisioned to include, among other things, American history, government, and law, as well as composition, mathematics, computer science, and the physical and biological sciences. Once summer arrives, students would participate in summer internships with private sector companies.

Students would select their major early in their second year, begin concentrating on their technical field, and continue their core curriculum. They would also initiate their security clearance application process. The goal would be for all students to graduate with at least a secret clearance. After completing the classroom portion of their second year, students would complete internships in two government agencies, which would help them focus their goals for government service.

During their third year, USDSA students would increase the focus on their major, complete the majority of their core curriculum, and begin committing to a government agency. Similar to the military service academies, attendance of the first day of class at the start of their third year serves as a commitment to five years of government service upon graduation. After completing the classroom portion of the third year, students would participate in another private sector internship.

Students would commit to a particular government agency and career field during the first weeks of their fourth year and begin the job placement process. To select a department and career field, students would create a rank ordered list of career fields within departments, agencies, and services. The USDSA would then match student preferences to the government’s needs as identified by an annual interagency process. After successfully completing all academic requirements, students would graduate as GS-7s, with the potential to progress rapidly to GS-11. After completing their service obligation, USDSA graduates would have the opportunity to transition to the NRDC.

Accreditation. In order to receive federal funding, the USDSA would take the required steps to complete the accreditation process through a regional accreditation organization. The accreditation organization would be determined based on the physical location of the institution and recognized by the Department of Education and Council for Higher Education Accreditation.²²⁷ Membership in such an organization ensures academic quality throughout the institution’s lifespan, as accreditation requires ongoing assessment for improvement. Future employers are able to affirm the credentials of USDSA graduates, the academy is able to accept

²²⁷ The military service academies are accredited by different regional accreditation organizations recognized by the U.S. Secretary of Education and Council for Higher Education. Their engineering programs are generally accredited by the Accreditation Board for Engineering and Technology, Inc.

DRAFT NSCAI DOCUMENT

charitable donations, and post-graduate programs recognize the validity of undergraduate degrees through accreditation. Based on the location of USDSA, the institution would also work with the hosting state to determine compliance with all core standards and processes.²²⁸

Proposed Implementation Plan for the USDSA:

Phase One (Years 1-2)

- Identify and secure an appropriate site for initial USDSA build-out with room for future expansion.
- Identify gaps in the government's current and envisioned digital workforce by an interagency task force under Office of Personnel Management leadership.
- Establish the USDSA administration as a new Executive Branch agency with an individual appropriation that will be responsible for the phased implementation plan and the management of the institution.
- Recruit tenure-track faculty.
- Recruit adjunct faculty, primarily from private-sector technology companies.²²⁹
- Grant the USDSA the authority to accept outside funds and gifts from individuals and corporations for startup, maintenance, and infrastructure costs.
- Appropriate \$40 million to pay for administrative costs.
- Satisfy the necessary requirements set by the Department of Education as well as the state USDSA is in for degree-granting approval.
- Apply for degree program specific accreditation through Computing Accreditation Commission on Colleges of Accreditation Board for Engineering and Technology.²³⁰
- Apply for accreditation with a Regional Accrediting Organization approved by the Department of Education and Council for Higher Education Accreditation in order to be granted "Candidate" status.
- Construct initial physical infrastructure.
- Appropriate additional costs for the selection and purchase of the physical location and construction of infrastructure.

Phase Two (Years 3-5)

- Begin classes with an initial class of 500 students at the beginning of year three.²³¹
- Demonstrate compliance with all requirements and standards of the regional accrediting organization in order to be granted Membership status.

Phase Three (Years 6-7)

²²⁸ State approval and accreditation are not the same, but both are required.

²²⁹ Recruitment will rely on private-sector champions to recruit high-profile adjunct faculty that can serve as beacons that will attract additional faculty and high-quality students.

²³⁰ The Computing Accreditation Commission on Colleges of Accreditation Board for Engineering and Technology is a nonprofit, ISO 9001 certified organization that accredits college and university programs in applied and natural science, computing, engineering and engineering technology.

²³¹ For comparison, since 2001, C:SFS has had 3,600 graduates, or about 189 graduates per year according to program officials NSCAI spoke with on March 9, 2020.

DRAFT NSCAI DOCUMENT

- Graduate the first class.
- Ongoing improvement through accreditation assessments.
- Assess, and as appropriate, expand class sizes.

Actions for Congress:

- **Authorize the establishment of the USDSA.**
 - An independent entity with a mandate to establish the institution described above.
 - Appropriate \$40 million dollars over two years to pay for the USDSA's initial administrative costs.

Actions for the Office of Personnel Management:

- **Begin an interagency process to identify skill and personnel gaps in the federal government's digital workforce.**

Employ

Digitally talented people should be able to reasonably expect to spend a career performing meaningful work focused on their field of expertise in government. Without such an expectation, they are unlikely to join the government workforce, and without their experience matching expectations, they are unlikely to stay for long.

Recommendation: Establish Career Fields for Government Civilians in Software Development, Software Engineering, Data Science, Knowledge Management, and Artificial Intelligence

Government civilians play a critical role in the national security enterprise. A significant portion of the government's AI talent is likely to exist in the civilian workforce. Government civilians currently do not have career paths outside of research and development that allow them to focus on software development, data science, or AI for the majority of their career. This results in a highly limited ability to recruit talent from outside of government, an inability for an individual to focus on a skill set for an extended time, a lack of continuing education opportunities for these government civilians, and retention issues. It also causes the government to struggle to identify and manage the software development, data science, and AI talent within its workforce.²³² Digitally focused occupational series will better allow the government to track and manage its digital workforce, to attract new talent that wants to focus on a technical skill set, and to create new positions.

The government should create software development, software engineering, data science, knowledge management, and AI occupational series. This combination of occupational series

²³² This analysis is based on the NSCAI staff conducting more than 100 interviews with government officials between May 2019 and May 2020. This feedback has emerged as a common theme in nearly all of NSCAI's workforce discussions. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

would significantly improve the government's ability to recruit and manage experts that will supervise the collection and curation of data, build human-machine interfaces, and help end users generate and act on data-informed insights. Many successful private-sector organizations use a version of this combination of skills.²³³ The government should follow their example.

Actions for Congress:

- **Require OPM to draft software development, software engineering, data science, knowledge management, and artificial intelligence occupational series classification policies no later than 270 days after the passage of the legislation.**

Actions for OPM:

- **Create software development, software engineering, data science, knowledge management, and artificial intelligence occupational series.**
- **Accelerate the creation of new digital occupational series.**
 - Rather than waiting for agencies to provide a formal request for a new occupational series, ask agencies to provide supporting documents and subject matter experts to study and draft a classification policy for each occupational series.

Recommendation: Establish Digital Career Fields for Military Personnel

Digital subject matter experts' inability to spend a career working on digital topics while serving in the military is arguably the single most important issue impeding military modernization.²³⁴ Much like their civilian counterparts, U.S. military personnel do not have career paths that allow them to focus on software development, data science, or AI for the majority of their career.²³⁵ The military has established career fields for doctors and lawyers that allow them to focus on a technical field, develop their skill over time, and advance within their service. The military is choosing not to do the same for many types of digital talent. While some of the services train some operational research and systems analysis (ORSA) personnel to perform machine learning and AI tasks, these personnel may be shifted to work on other ORSA tasks rather than AI. Phrased differently, AI practitioners have some background in ORSA, but not all ORSA personnel are trained to work in machine learning or AI.²³⁶

This results in a reduced ability to recruit talent outside of the Government, an inability to focus on a skill set for an extended time, a lack of continuing education opportunities, and retention

²³³ NSCAI staff interview with a private-sector company (Sept. 9, 2019); NSCAI staff interview with a private-sector company (Sept. 19, 2019); NSCAI staff interview with a private-sector company (Apr. 24, 2020).

²³⁴ NSCAI staff interviews with government and private-sector senior leaders (May 6, 2020).

²³⁵ *Workforce Now: Responding to the Digital Readiness Crisis in Today's Military*, Defense Innovation Board at 1-7 (2019), https://media.defense.gov/2019/Oct/31/2002204196/-1/-1/0/WORKFORCE_NOW.PDF.

²³⁶ NSCAI staff has interviewed several ORSA personnel performing AI related tasks. All agreed when asked that a separate career field for artificial intelligence or data science is needed. Existing initiatives make some progress, but do not adequately address the lack of career fields for digital talent.

issues. It also causes the government to struggle to identify and manage the software development, data science, and AI talent within its workforce.²³⁷ These problems are particularly acute for military personnel, who are required to regularly change positions and move into manager roles or face eventual discharge from the military. The lack of digital career fields also causes the military services to struggle to identify and manage the software development, data science, and AI talent within their workforces.²³⁸ As long as this state continues, the military should not expect to achieve better results for its digital modernization than its legal and medical fields would have without career fields for lawyers and doctors.

The military services should have primary career fields that allow military personnel to focus on software development, data science, or artificial intelligence for their entire career, either as managers or technical specialists.

Actions for Congress:

- **Require the military service chiefs to create career fields focused on software development, data science, and artificial intelligence.**
 - Congress should amend section 230 of the FY 2020 NDAA to require the military service chiefs to create career fields focused on software development, career fields focused on data science, and career fields focused on artificial intelligence for both commissioned officers and enlisted personnel, and, as appropriate, warrant officers.
 - Military personnel should be able to join these career fields either upon entry into the military, or by transferring into the field after serving a period in another career field. These career fields should have options that allow personnel to either follow a path to senior leadership positions, or specialize and focus on technical skill sets. Those that specialize and focus on technical skill sets should not have to leave their focus area and move into management positions to continue to promote. Legislation should not restrict the military services to only two career fields, but rather require each service to create at least two career fields, and more at their discretion. The military services should be required to create the career fields within one year of passage of legislation.

²³⁷ The NSCAI staff has conducted more than 100 interviews with government officials between May 2019 and May 2020. This feedback has emerged as a common theme in nearly all of NSCAI's workforce discussions. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

²³⁸ NSCAI's *First Quarter Recommendations* included an addition to the Armed Services Vocational Aptitude Battery to test for computational thinking that would help identify aptitude and a test for coding language proficiency that would help identify skill. *First Quarter Recommendations*, NSCAI at 33-35 (Mar. 2020), <https://www.nscai.gov/previous-reports/>. Both tests will be helpful, but will not meet their full utility without digital career fields. In conversations with NSCAI, numerous government officials continuously identified a lack of digital career fields as a key impediment to talent management. See e.g., NSCAI interviews with government officials (June 7, 2019); NSCAI interviews with government officials (May 17, 2019).

Actions for the Military Services:

- **Create career fields that allow military personnel to focus on software development, career fields that allow military personnel to focus on data science, and career fields that allow military personnel to focus on artificial intelligence.**
 - While remaining consistent with service personnel policies and procedures, these career fields should be open to both enlisted personnel and commissioned officers, and, as appropriate, warrant officers.
 - Military personnel should be able to join these career fields either upon entry into the military, or by transferring into the field after serving a period in another career field.
 - These career fields should have options that allow personnel to either follow a path to senior leadership positions, or specialize and focus on technical skill sets. Those that specialize and focus on technical skill sets should not have to leave their focus area and move into management positions to continue to promote.

Recommendation: Provide Government Technologists with World-Class Tools, Data Sets, and Infrastructure.

Highly skilled technologists working in government are regularly denied access to software engineering tools. They have to jump bureaucratic hurdles to accomplish basic job functions such as sharing source code or downloading data sets, leading to frustration and periods of idling. 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. Capabilities include software engineering tools, access to software libraries, open-source support, and infrastructure for large-scale collaboration. Employees within the AI career field in particular will need access to further specialized resources such as curated data sets and compute power.

In order to be effective, developers need to be able to find and view source code written by other developers before them. Being unaware of existing code repositories often leads to writing redundant software that meets a different set of quality standards and robustness than existing software. To prevent this, each member of the AI career field needs access to a shared, enterprise-level repository of AI software and tools, similar to that recommended in Chapter 2 of this report for the Department of Defense. This repository should house source code available to all AI developers within a government agency.

Each government agency should create enterprise-scale solutions for source code management across multiple software projects. This does not mean that every developer in an agency will be able to modify every single project in a repository—with protocols for delegated access, a system administrator can set project-specific read and write permissions for each AI developer. New software projects should be set up to allow ubiquitous unit testing as code is written, and automatic integration into a code review process to ensure robust and bug-free output. Following these guidelines will promote a culture of software engineering excellence, emphasizing to

technologists that it is possible to work in government while remaining at the forefront of a digital field.

For new developers who join an agency, onboarding procedures must include separate instructions for pushing their new code to this repository as well as instructions on how to navigate the software catalog and search for existing source code.

All career fields also need unobstructed access to the latest open-source libraries and tools. Over time, technologists develop individual preferences for their software development environment, opting for custom software development kits (SDKs), debugging tools, cloud tools, version control software, and data visualization platforms on local machines. To ensure productivity and developer satisfaction, agencies must give each developer the authority to install vetted, authorized tools on their local machines.

AI developers use open-source software libraries for training machine learning models and making them production-ready for real-world use. To harness the full power of these essential libraries, AI developers should have access to vetted libraries, but also to compute power while training their machine learning models. Models train very slowly on a local machine because of the complexity of underlying mathematical calculations in the training process. As a result, AI developers prefer to train them rapidly through automatic deployment pipelines on commercially available platforms, or another external service. Smoothing the transition from local software development to cloud services is critical for any organization using AI and ML.²³⁹

Actions for Departments and Agencies (including but not limited to the Department of Energy, Department of Homeland Security, Department of State, Department of Commerce, and Department of Justice):²⁴⁰

- **Ensure software developers and engineers, data scientists, and AI practitioners:**
 - Have access to systems with capabilities comparable to Repo One and Platform One;
 - Are authorized to install custom software licenses, debugging tools, cloud deployment tools, version control software, and data visualization platforms on their computers;
 - Have agency-specific resources for cloud-based compute power that AI developers can harness to train machine learning models with greater speed.

²³⁹ 2020 Interim Report and Third Quarter Recommendations, NSCAI at 37-38 (Oct. 2020), <https://www.nscai.gov/previous-reports/>.

²⁴⁰ See Chapter 2 of this report for a detailed description of how DoD would implement this plan.

[BLANK PAGE]

DRAFT

Chapter 7: Establishing Justified Confidence in AI Systems Blueprint for Action

A Holistic Framework for Ensuring Justified Confidence in AI Systems

The U.S. Government should align on a common understanding of critical steps needed to ensure justified confidence in AI systems, including confidence in their responsible development and use. The Commission has outlined such a strategy in the *Key Considerations*. The *Key Considerations* document provide a framework for the responsible development and fielding of AI that should be adopted by all agencies critical to national security. The framework includes near-term recommendations and topics that agencies should give priority consideration, practices that should be implemented immediately, and policies that should be defined or updated to reflect new AI considerations.

Based on robust feedback from departments and agencies including Department of Defense (DoD), Intelligence Community (IC), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Department of Energy (DoE), Department of State (DoS), and Department of Health and Human Services (HHS), as well as the GSA AI Community of Practice, the *Key Considerations* also outlines areas needing future work and targeted investment to overcome current challenges. Agencies that have already adopted AI principles noted broad alignment between the *Key Considerations* framework and their AI principles. For instance, the framework's recommended practices help operationalize the AI Principles of the DoD and IC²⁴¹ and the Principles for Use of AI in Government.²⁴²

The implementation of the *Key Considerations*' recommendations for future action will be important not only for agencies, but also for cooperation across the world on the responsible development and fielding of AI.²⁴³ Further, while the Commission's mandate led to a focus on recommendations specific to national security entities in our report, many recommendations we elevate in the *Key Considerations* are relevant to the whole country, including other sectors and industry.

Heads of departments and agencies critical to national security should implement the *Key Considerations* as a framework for the responsible development and fielding of AI systems. Agencies, at a minimum, include the DoD, IC, FBI, DHS, DoE, DoS, and HHS. Implementing the *Key Considerations* includes developing policies and processes to adopt the framework's recommended practices, monitoring their implementation, and continually refining them as best practices evolve. While this framework covers dozens of practices that contribute toward an ideal state of responsible development and fielding, some practices will be more critical than others

²⁴¹ See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence Supporting Visuals*, NSCAI (July 2020), <https://www.nscai.gov/wp-content/uploads/2021/01/Key-Considerations-Supporting-Visuals.pdf>.

²⁴² See Donald J. Trump, *Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, The White House (Dec. 3, 2020), <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/>. The Principles for Use of AI in Government do not apply to national security agencies; however, they do apply to agencies the Commission considers critical for national security (e.g., Department of State and Department of Health and Human Services).

²⁴³ *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 29-30 (July 2020), <https://www.nscai.gov/previous-reports/>.

depending on the stakes and context, and complying with them will require different costs and resources. This Blueprint for Action provides details on the key actions from this framework that all departments and agencies critical to national security can and should take now as a priority, and investments and resources that the government should make available to further responsible AI across all agencies. **These span recommendations for Leadership; Robust and Reliable AI; Human-AI Interaction and Teaming; Testing and Evaluation, Verification and Validation; and Accountability and Governance.**

Recommendations for Leadership

Actions for DoD, IC, FBI, DHS, DoE, DoS, and HHS:

- **Every department and agency critical to national security and each branch of the armed services, at a minimum, should have a dedicated, full-time Responsible AI Lead who is part of the senior leadership team. Responsible AI Leads must have dedicated staff, resources and authority to succeed in their roles. Every lead should have at least two full-time staff to effectively fulfill the following:**
 - The Responsible AI Lead in each department should oversee the implementation of the *Key Considerations* recommended practices alongside the department/agency's respective AI principles.²⁴⁴ This includes driving policy development and training programs for the department and internally coordinating Responsible AI leads in the department's supporting branches or agencies (as applicable) to ensure synergistic implementation of such policies and programs. The department lead should determine the Responsible AI governance structure to ensure centralized and consistent policies²⁴⁵ are applied across the department.
 - The department Responsible AI Lead and those supporting Responsible AI leads should collectively:
 - provide Responsible AI training to relevant personnel;
 - serve as subject matter experts regarding existing and proposed Responsible AI policy and best practices;
 - shape procurement policy and guidance for product managers to ensure alignment with recommended practices and adopted AI principles;
 - build a central repository of Responsible AI work going on in the department, and lessons learned from practical implementation across the department, to help streamline department efforts;
 - ensure interagency knowledge sharing for responsible AI, including iterative sharing of best practices, resources and tools, evolving risks and vulnerabilities, and other lessons learned from practical implementation;
 - annually produce a report for Congress on department resources received, any additional resources needed, and an update on required policy work and implementation of recommended practices.

²⁴⁴ For each of the metrics and technical measures mentioned in the *Key Considerations*, it will be important to have measurable outcomes against which success can be determined. See *Making Responsible AI the Norm Rather than the Exception*, Montreal AI Ethics Institute at 9 (Jan. 13, 2021), <https://arxiv.org/pdf/2101.11832.pdf> [hereinafter MAIEI Report].

²⁴⁵ This includes, for example, "Accountability and Governance" policy work identified below in this Blueprint for Action.

DRAFT NSCAI DOCUMENT

- Where possible, centralized assessments and shared learnings should be communicated across a department's elements or branches, to avoid units spending unnecessary and duplicative resources and to accelerate practices that reduce friction in workflows. Responsible AI Leads in each department should consider the Learning, Knowledge, and Information Exchange (LKIE) framework as a way to accelerate organizational knowledge within their department given the need to leverage collective insights that are gleaned from on-the-ground experience where the *Key Considerations* will be put into practice rather than letting the insights sit in silos.²⁴⁶ Furthermore, having Responsible AI "champions"²⁴⁷ who "socialize" this knowledge can help to transfer the knowledge within and across different U.S. Government agencies and components.²⁴⁸
- Borrowing from the world of cybersecurity, the Lead also should consider coordinating the adoption of an empirically-driven prioritization matrix for risk management.²⁴⁹

Action for the National AI Initiative Office:

- **In addition to the National AI Initiative responsibilities defined in the National Defense Authorization Act for Fiscal Year 2021 (FY 2021 NDAA),²⁵⁰ the Office should create a standing body of multi-disciplinary experts who can be voluntarily called upon by agencies as a resource to provide advice on Responsible AI issues.** The group should include people with expertise at the intersection of AI and other fields such as ethics, law, policy, economics, cognitive science, and technology including adversarial AI techniques. As the government upskills and diversifies its workforce with AI expertise, this standing body of experts should help fill gaps in multi-disciplinary expertise that can be called upon by agencies as needed for processes including multi-disciplinary risk assessment, human-AI teaming assessments, and red-teaming.
- Leveraging this in-house expertise, and serving as the central resource for best practice sharing across agencies, it should also:
 - Maintain a Learning, Knowledge, and Information Exchange repository to benefit all agencies;
 - A repository compiling insights across agencies (e.g., per the LKIE framework mentioned above) would accelerate organizational knowledge and support interagency sharing of insights gleaned from on-the-ground

²⁴⁶ MAIEI Report at 11-16.

²⁴⁷ "AI champions" are a cross-functional group of ambassadors, who can, for example, consider ways to operationalize AI ethical principles and serve as internal advocates and evangelists for responsible AI. See *Department of Defense Joint Artificial Intelligence Center Responsible AI Champions Pilot*, DoD (last accessed Feb. 3, 2021), https://www.ai.mil/docs/08_21_20_responsible_ai_champions_pilot.pdf; Tim O'Brien, et al., *How Global Tech Companies can Champion Ethical AI*, World Economic Forum (Jan. 14, 2020), <https://www.weforum.org/agenda/2020/01/tech-companies-ethics-responsible-ai-microsoft/>.

²⁴⁸ MAIEI Report at 12.

²⁴⁹ MAIEI Report at 20-23.

²⁵⁰ Pub. L. 116-283, Div. E., Title LI, sec. 5102, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

practice—rather than letting such insights sit in silos.²⁵¹ These collective insights would be generalized from bright spots of successful AI adoption and from lessons learned from AI adoptions that faced problems in development or use.²⁵² Centralized insights will also provide a resource to help agencies address critical questions that will arise as AI capabilities evolve. Examples of potential critical questions include how to support redress with updated policies and procedures; how to efficiently monitor behavior in operation; and how to effectively measure and address changes introduced by technical refresh. With technical refresh, it is necessary to analyze results carefully. Even if overall performance may be steady or improve after a refresh, the aggregate performance can mask certain parts of the performance envelope where results are significantly skewed and problematic.

- Maintain a qualified products list supported by third-party testing to facilitate agile and trusted procurement.²⁵³

Action for Congress:

- **To enable departments and agencies critical to national security to execute Responsible AI work department-wide, and to encourage necessary appointments of Responsible AI personnel, Congress should appropriate an estimated \$21.5 million each fiscal year to fund billets.**
 - Organizations that have high mission complexity and diverse components may need more support staff and/or Responsible AI Leads to be allocated across the organization. The Commission recommends that at a minimum the following is needed:
 - For the DoD, a department-wide Responsible AI (RAI) Lead and supporting RAI Leads for each branch of the armed services, with each lead supported by two staff members;
 - For the Intelligence Community, an ODNI RAI Lead and supporting RAI Leads for each IC agency, with each lead supported by two staff members;
 - For the DOE, a RAI Lead and a supporting RAI Lead for the National Laboratories, with each lead supported by two staff members; and

²⁵¹ MAIEI Report at 11-16.

²⁵² For instance, this could include communication of failure modes, (e.g., when a system produces a formally correct, but unsafe outcome), and instances to establish a shared understanding of how and where the systems go wrong. Leveraging this, agencies should tap into USG network-wide expertise to address those failures. See Ram Shankar Siva Kumar, et al., *Failure Modes in Machine Learning*, Microsoft (Nov. 11, 2019), <https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning>; MAIEI Report at 7.

²⁵³ A qualified product list could, for example, enable agencies to have a shared awareness of vendors whose systems have undergone independent, third-party testing as described in Chapter 8 (See ‘Establish third-party testing center(s) to allow independent, third-party testing of national security-related AI systems that could impact US persons’) as well as reinforce commercial product attention to these concerns. Approved third party test organizations often act as gatekeepers for approved or qualified product lists. Examples include NIST NVLAP approved third party testing organizations and FIPS third-party accredited testing labs. See Bradley Moore, et al., *NIST Handbook 150-17: NVLAP Cryptographic and Security Testing*, National Institute of Standards and Technology (Apr. 2020), <https://doi.org/10.6028/NIST.HB.150-17-2020>; *Approved Products List*, GSA ID Management (Feb. 1, 2021), <https://www.idmanagement.gov/approved-products-list/>.

- For the FBI, DHS, and HHS, a RAI Lead in each respective organization who is supported by two staff members.²⁵⁴

Recommendations for Robust and Reliable AI

Action for the Office of Science and Technology Policy (National AI Initiative Office):

- **Focus federal research and development (R&D) investments on advancing AI security and robustness, to help agencies better identify and mitigate evolving AI system vulnerabilities.** Confidence in the robustness and reliability of AI systems requires insight into the development process and the operational performance of the system. Insight into the development process is supported by capturing decisions and development artifacts for review; insight into operational performance is supported by runtime instrumentation and monitoring to capture details of execution. In both development and operation, there is a need to invest in R&D for better tools to facilitate the capture of needed processes and data. R&D should also advance interpretability capabilities to better understand if AI systems are operating as intended. And R&D should support better characterization of performance envelopes to enable the gradual rollout and adoption of AI systems. ‘Robust AI’ is included among the priority research areas found in Chapter 11 of this report.

Action for all Departments and Agencies

Create a National AI Assurance Framework. All government agencies will need to develop and apply an adversarial machine learning threat framework to address how key AI systems could be attacked and should be defended. An analytical framework can help to categorize threats to government AI systems, and assist analysts with detecting, responding to, and remediating threats and vulnerabilities.²⁵⁵ This framework must address supply chain threats to data and models as well as adversarial AI attacks.²⁵⁶ The framework will support assurance of data authenticity and data and model integrity. “Create a National AI Assurance framework” is included among recommendations found in Chapter 1 of this report.

Action for DoD and the Office of the Director of National Intelligence (ODNI):

- **Create dedicated red teams for adversarial testing.** Such red teams should assume an offensive posture, dedicated to trying to break systems and make them violate rules for

²⁵⁴ Collectively, considering both Responsible AI leads and supporting staff, this recommendation proposes 21 full-time employees (FTEs) for the DoD; 54 for the IC; 3 for the FBI; 3 for DHS; 6 for DoE; 3 for HHS; and 3 for DoS.

²⁵⁵ There are various public and private efforts on going. See for instance the MITRE-Microsoft adversarial ML framework, Ram Shankar Siva Kumar & Ann Johnson, *Cyberattacks Against Machine Learning Systems Are More Common than You Think*, Microsoft Security (Oct. 22, 2020), <https://www.microsoft.com/security/blog/2020/10/22/cyberattacks-against-machine-learning-systems-are-more-common-than-you-think/>; *Adversarial AI Threat Matrix: Case Studies*, MITRE (last accessed Jan. 10, 2021), <https://github.com/mitre/advmlthreatmatrix/blob/master/pages/case-studies-page.md>.

²⁵⁶ *NISTIR 8269 (Draft): A Taxonomy and Terminology of Adversarial Machine Learning*, National Institute of Standards of Technology (Oct. 2019), <https://csrc.nist.gov/publications/detail/nistir/8269/draft>.

appropriate behavior.²⁵⁷ Because of the scarcity of required expertise and experience for AI red teams, the DoD and ODNI should consider establishing enterprise-wide communities of AI red teaming and vulnerability testing capabilities that could be applied to multiple AI developments. The Commission supports the aligned recommendation by WestExec Advisors that the DoD and ODNI should consider “standing up a national AI and ML red team as a central hub to test against adversarial attacks, pulling together DoD operators and analysts, AI researchers, T&E, CIA, DIA, NSA, and other IC components, as appropriate. This would be an independent red-teaming organization that would have both the technical and intelligence expertise to mimic realistic adversary attacks in a simulated operational environment.”²⁵⁸

Actions for Agencies Critical to National Security:²⁵⁹

To Meet Baseline Criteria for Robust and Reliable AI –

- **Upgrade development, procurement, and acquisition strategies to ensure that those accountable for the development, procurement, or acquisition of an AI system (e.g., program managers) adopt the following practices:**
 - **Consult an interdisciplinary group of experts to conduct hazard analysis and risk assessments.** These should cover, as relevant to the context: potential disparate impact related to unwanted bias; privacy and civil liberties; international humanitarian law; human rights;²⁶⁰ system security against targeted attacks;²⁶¹ risks of technology being leaked, stolen, or weaponized by adversaries against the U.S.;²⁶² and steps taken to mitigate identified risks. Agencies should specify in their respective strategies who will consult such a group and who will ultimately make final decisions based on the group’s advice.
 - **Improve documentation practices.** Produce documentation describing the data used for training and testing; model(s); other relevant systems (including connections and dependencies within systems); required maintenance (for datasets

²⁵⁷ See *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 21-22 (July 2020), <https://www.nscai.gov/wp-content/uploads/2021/01/Key-Considerations-for-Responsible-Development-Fielding-of-AI.pdf>.

²⁵⁸ See Michele Flournoy, et al., *Building Trust Through Testing* (Oct. 2020), <https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf>.

²⁵⁹ As noted above, the Commission considers these, at a minimum, to include the DoD, IC, DHS, FBI, DoE, Department of State, and HHS.

²⁶⁰ For more on the importance of human rights impact assessments of AI systems, see *Report of the Special Rapporteur to the General Assembly on AI and its impact on freedom of opinion and expression*, UN Human Rights Office of the High Commissioner (2018), <https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ReportGA73.aspx>. For an example of a human rights risk assessment for AI in categories such as nondiscrimination and equality, political participation, privacy, and freedom of expression, see Mark Latonero, *Governing Artificial Intelligence: Upholding Human Rights & Dignity*, Data Society (Oct. 2018), https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf.

²⁶¹ These can include reidentification attacks. Departments and agencies should use privacy protections such as robust anonymization that can withstand sophisticated reidentification attacks, and when possible, privacy-preserving technology such as differential privacy, federated learning, and ML with encryption of data and models.

²⁶² For exemplary risk assessment questions that IARPA has used, see Richard Danzig, *Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority*, Center for a New American Security at 22 (June 28, 2018), <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-Technology-Roulette-DoSproof2v2.pdf?mtime=20180628072101>.

and models) and technical refresh when the system is used in a different operational environment. For data, documentation should include how data were sampled and their provenance. For synthetic data, documentation should also include details on how the data were generated.²⁶³

- **Build overall system architectures to limit the consequences of system failure.** Agencies should build an overall system architecture that monitors component performance and handles errors when anomalies are detected; build AI components to be self-protecting (validating input data) and self-checking (validating data passed to the rest of the system); and include aggressive stress testing. As with all high consequence software systems, where technically feasible it is important that high consequence AI systems have overall system architectures that support robust recovery and repair or fail-fast and fail-over to a reliable degraded mode safe system. There should be clear mechanisms for disengaging and deactivating the system when things go wrong.²⁶⁴

Recommendations for Human-AI Interaction and Teaming

Action for Department of Defense:

- **Invest in a sustained, multi-disciplinary initiative to enhance human-AI teaming through the Service Laboratories and DARPA.**
 - This initiative should focus on maximizing the benefits of human-AI interaction; better measuring human performance and capabilities when working with AI systems; and helping AI systems better understand contextual nuances of a situation. Advances in human-machine teaming will enable human interactions with AI-enabled systems to move from the current model of interaction where the human is the “operator” of the machine, to a future in which humans are able to have a “teammate” relationship with machines. Specific funding should be dedicated to research on how to improve human-machine teaming and interaction when it involves human life-safety or lethal deployment of a system. Additional research is urgently needed which should address the following issues, among others: delegation of authority, observability, predictability, directability, communication, and trust.
 - R&D investment should also focus on the following:
 - Developing improved human performance assessment, an essential element for AI to understand when and how an appropriate AI intervention should be made.
 - Developing new approaches to humans and AI establishing and maintaining common ground in support of collaboration, particularly cognitive collaboration. This encompasses how a newly established human-AI team scaffolds its mutual understanding and then how it extends it to creatively and collaboratively tackle new challenges.

²⁶³ Such documentation should support assurances of the authenticity, integrity and provenance of data.

²⁶⁴ MAIEI Report at 9 (This includes “building fail safes and backup modes that don’t have to rely on continuous access to the ‘intelligent’ elements and have graceful failures that minimize harm.”).

- Developing new approaches to trust calibration in human-AI teams. This includes helping people understand when AI is approaching or outside the bounds of its competency envelope, and likewise helping machines understand when people are approaching their limits. The two together will help the human-AI team calibrate trust appropriately and shape their interaction for improved team performance.²⁶⁵ “Enhanced human-AI interaction and teaming” is included among the priority research areas found in Chapter 11 of this report. This recommendation also maps to the overall DoD R&D funding recommendation in Chapter 3 of this report.

Actions for Agencies Critical to National Security:

Meet Baseline Criteria for Effective Human-AI Interaction and Teaming –

- **National security departments and agencies should clarify policies on human roles and functions, develop designs that optimize human-machine interaction, and provide ongoing and organization-wide AI training.**
 - **Develop design methodologies that improve our understanding of human-AI interaction and provide specific guidance and requirements that can be assessed.**²⁶⁶ These methodologies should clearly delineate requirements of potential human-AI teaming alternatives and identify whether a proposed solution is likely to meet those requirements or not.
 - Designs should mitigate automation bias (that places unjustified confidence in the results of computation) and unjustified reliance on humans as a failsafe mechanism. They should provide accurate cues to the human operator about the level of confidence the system has in its results/behaviors.
 - **Ensure policies provide ethical bounds regarding when and where AI is appropriate within a human-AI team in a given context.**
 - Policies should identify what functions humans should perform across the AI lifecycle; bound assignments and functions, including autonomous functionality; define when tasks should be handed off between a human and machine based on bounds; and require feedback loops to inform oversight and ensure systems operate as expected.
 - **Provide ongoing training to help the workforce better interact, collaborate with, and be supported by AI systems—including understanding AI tools.**²⁶⁷ As relevant, employees across departments and agencies, and the DoD in particular, should, at a minimum:

²⁶⁵ See Brian Wilder, et al., *Learning to Complement Humans*, Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (2020), <https://www.ijcai.org/Proceedings/2020/0212.pdf>.

²⁶⁶ For an example of applicable guidelines, see Saleema Amershi, et al., *Guidelines for Human-AI Interaction*, CHI '19: Proceedings of the CHI Conference on Human Factors in Computing Systems (May 2019), <https://dl.acm.org/doi/10.1145/3290605.3300233>.

²⁶⁷ For more on training, see *Key Considerations for Responsible Development & Fielding of Artificial Intelligence*, NSCAI at 34 (July 2020).

- gain familiarity with AI tools (e.g., through everyday interaction), including use of AI systems in realistic situations and provide continual feedback to integrate improvements;²⁶⁸
- receive education that includes fundamentals of AI and data science, including coverage of key descriptors of performance and probabilities;²⁶⁹
- receive training on interpreting performance standards and metrics correctly and making informed decisions based on them;²⁷⁰
- gain an understanding of both the fundamental concepts and the high-level concepts in terms how the system components interact with each other;²⁷¹
- have training to recognize human cognitive biases so that human operators interacting with machines can recognize where they might be succumbing to such bias;²⁷²
- receive ongoing refresher trainings suited to system operators. Refresher trainings are appropriate when systems are deployed in new settings and unfamiliar scenarios, and when predictive models are revised with additional training data as system performance may shift, introducing behaviors that are unfamiliar to operators.²⁷³

Recommendations for Testing and Evaluation, Verification and Validation

Action for the Department of Defense:

- **DoD should tailor and develop TEVV policies and capabilities to meet the changes needed for AI as AI-enabled systems grow in number, scope, and complexity in the Department.**²⁷⁴

This should address the following elements:

- **Establish a testing and evaluation, verification and validation (TEVV) framework and culture** that integrates testing as a continuous part of requirements specification, development, deployment, training, and maintenance and includes run-time monitoring of operational behavior.²⁷⁵ An AI testing framework should:
 - Establish a process for writing testable and verifiable AI requirement specifications that characterize realistic operational performance.²⁷⁶

²⁶⁸ Such everyday interaction and continual feedback loops will further enhance TEVV.

²⁶⁹ See *Key Considerations* (Training); MAIEI Report at 7.

²⁷⁰ MAIEI Report at 7.

²⁷¹ MAIEI Report at 7.

²⁷² MAIEI Report at 7.

²⁷³ See *Key Considerations* (Periodic Certification and Refresh).

²⁷⁴ To the greatest extent possible, DoD should develop TEVV policies and capabilities in coordination with the Office of the Director of National Security.

²⁷⁵ To achieve this, heavy investment is needed that supports requirements generation/traceability, the integration of heterogeneous test data at all stages of testing, and the use of extensive M&S, test automation, and data analytics wherever feasible.

²⁷⁶ This should be framed broadly, providing left/right limits that provide guidance but do not limit innovation.

- Provide testing methodologies and metrics that enable evaluation of these requirements—including principles of ethical and responsible AI, trustworthiness, robustness, and adversarial resilience.²⁷⁷
- Define requirements for performance reevaluation related to new usage scenarios and environments, and distribution over time.
- Encourage incorporation of operational usage workflow and requirements from the defined use case into the testing.
- Issue data quality standards to appropriately select the composition of training and testing sets.
- Support the use of common modular cognitive architectures within suitable application domains that expose standard interface points for test harnessing—supporting scalability through increased automation along with federated development and testing.
- Support a cyclical DevSecOps-based approach, starting on the inside and working outward, with AI components, system integration, human-machine interfaces, and operations (including human-AI and multi-AI interactions).
- Remain flexible enough to support diverse missions with changing requirements over time.
- **Extend existing and develop new TEVV methods and tools for dealing with complex, stochastic, and non-stationary systems, including the design of experiments, real-time monitoring of states and behaviors, and the analysis of results.** These methods/tools need to account for human-system interactions (HSI) and their impact on system behavior, system-system interactions and their effect on emergent behavior across a group of systems, and adversarial attacks, via both conventional cyberattacks, and nascent perceptual adversarial AI attacks. Risk assurance concepts should be extended beyond simple “stop-light” charts of consequence and likelihood for a risk being realized and leverage tools that support developing assurance cases that present verifiable claims about system behavior and provide reviewable arguments and evidence to support the claims.²⁷⁸
- **Make TEVV tools and capabilities readily available across the DoD,** including downloadable and configurable AI TEVV software stacks.²⁷⁹ In addition, the DoD should ensure tools that support TEVV and reliability and robustness goals are available department-wide including tools for bias detection, explainability, and documentation across the product lifecycle (e.g., of data inputs and system outputs).
- **Update existing and create new live, virtual, and constructive test ranges for AI-enabled systems (blending modeling and simulation, augmented reality, and cyber physical system environments).** Upgraded test ranges should include live-virtual-constructive environments, the ability to capture data from testing, and the ability to evaluate data from operations. They should support: 1) the full exploration of potential system states and behaviors over a range of run-times and fidelity levels;

²⁷⁷ These testing methodologies and metrics should support robust red teaming, meeting the DoD’s particular needs for solutions hardened to adversarial actions.

²⁷⁸ Miles Brundage, et al., *Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*, arXiv (Apr. 20, 2020), <https://arxiv.org/abs/2004.07213>.

²⁷⁹ TEVV tools and software stacks should be shared across the Department using the AI Digital Ecosystem described in Chapter 2 of this report.

- 2) the co-development of AI-system functionality and concepts of operations (CONOPS) associated with human-system and system-system teaming; and 3) a fuller understanding of the impact of adversarial activities undertaken to counter these systems. Build these capabilities upon extensive modeling and simulation (M&S) facilities, human and constructive adversarial “red teams”, virtual and augmented reality enablers, full instrumentation, and post-run big data analytics capability.
- **Support the T&E community by restructuring the processes that underlie requirements specification, system design, T&E itself, and CONOPS development.** This includes continuing DoD investments and policies supporting architecting software-intensive systems using common frameworks and composable subsystems,²⁸⁰ the inclusion of runtime instrumentation (adding the capture of internal states of the system, analogous to a flight data recorder on aircraft) in system design and monitoring during operation,²⁸¹ the proper curation and protection of data used in training these systems, and a heavy investment in successively sophisticated M&S, starting at the requirements stage and proceeding through development, TEVV, and operator training.

Action for the National Institutes of Standards and Technology (NIST):

- **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.**²⁸²

Over time, as the science of how to test systems across responsible AI attributes evolves, NIST should provide guidance on:

- Metrics to assess system performance per responsible AI attributes (e.g., fairness, interpretability, reliability, robustness) and according to application/context profiles. This should include:
 - Definitions, taxonomy, and metrics needed to enable agencies to better assess AI performance and vulnerabilities.
 - Metrics and benchmarks to assess reliability of model explanations.²⁸³
- For each of the metrics and technical measures created, NIST should also provide measurable outcomes against which success can be determined.²⁸⁴

In the near-term, NIST should also provide guidance on:

²⁸⁰ Such frameworks for composing testable AI systems should be established and accessed through the AI Digital Ecosystem described in Chapter 2 of this report.

²⁸¹ See e.g., Software Acquisition Pathway Interim Policy and Procedures, Memorandum from the Undersecretary of Defense, to Joint Chiefs of Staff and Department of Defense Staff (Jan. 3, 2020), [https://www.acq.osd.mil/ae/assets/docs/USA002825-19%20Signed%20Memo%20\(Software\).pdf](https://www.acq.osd.mil/ae/assets/docs/USA002825-19%20Signed%20Memo%20(Software).pdf) (stating that program managers are required to “achieve ... continuous runtime monitoring of operational software”).

²⁸² This recommendation is in line with Congress’ expansion of NIST’s mission regarding AI standards in the FY 2021 NDAA, section 5301 to include: “advance collaborative frameworks, standards, guidelines” for AI, “support the development of a risk-mitigation framework” for AI systems, and “support the development of technical standards and guidelines” to promote trustworthy AI systems.” Pub. L. 116-283, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

²⁸³ “Documentation of the assumptions and limitations of the benchmarks so created will also be essential in helping those utilizing them to make sure they will get the intended intelligence from it rather than becoming falsely confident about the system.” MAIEI Report at 9.

²⁸⁴ MAIEI Report at 9.

DRAFT NSCAI DOCUMENT

- Standards for testing intentional and unintentional failure modes.
- Exemplar datasets for benchmarking and evaluation, including robustness testing and red teaming.
- Defining characteristics of AI data quality and training environment fidelity (to support adequate performance and governance).

In conducting the above, NIST should publish quarterly updates to inform departments and agencies about the trustworthy frameworks, standards, and metrics work it is planning.²⁸⁵

Action for the Office of Science and Technology Policy - National AI Initiative Office:

- **The federal government should increase R&D investment to improve our understanding of how to conduct TEVV.** This is needed to better understand how to efficiently and effectively test AI systems to provide objective assurance to support a justified level of confidence, build checks and balances in systems, and how to monitor and mitigate unexpected behavior in a composed system-of-systems or when systems interact. Such R&D should advance our understanding of how to test system performance across responsible AI attributes (e.g., fairness, interpretability, reliability, and robustness). This recommendation is echoed by the priority research areas found in Chapter 11 of this report, including “TEVV of AI Systems” and “standard methods and metrics for evaluating degrees of auditability, traceability, interpretability, explainability, and reliability.” For more information, see also Chapter 3 of this report.

Actions for Agencies Critical to National Security:

- **To ensure optimal performance of AI systems, national security departments and agencies should:**
 - Plan for and execute aggressive stress testing of AI components to evaluate error handling and robustness against unintentional and intentional threats under conditions of intended use.
 - Include testing for blind spots and fairness throughout development and deployment. Testing and validation should be done iteratively at strategic intervention points, especially for new deployments.
 - Clearly document system performance requirements (including identified system hazards), metrics used for TEVV, deliberations on the appropriate fairness metrics to use, and the representativeness of the test data for the anticipated operational environment.
 - Conduct red teaming to rigorously challenge AI systems, exploring their risks, limitations, and vulnerabilities including intentional and unintentional failure modes.

Recommendations for Accountability and Governance

²⁸⁵ Doing so will enable departments and agencies to plan and prioritize any internal standards work accordingly (e.g. avoiding redundant or obsolete efforts).

Actions for Agencies Critical to National Security:

- **Adapt and extend existing policies to ensure accountability is established and documented across the AI lifecycle for any given AI system and its components.**²⁸⁶
- **Establish clear requirements about information that should be captured about the development process**²⁸⁷ (via traceability) **and about system performance and behavior in operation (via run-time monitoring)** to support reliability and robustness as well as auditing for oversight. Instrumentation to support monitoring can contribute to insights about system performance, but must be provided thoughtfully to prevent new openings for external espionage or tampering with AI systems.²⁸⁸
 - Guidance should include technical audit trail requirements per mission needs for high-stakes systems.
- **Institute comprehensive oversight and enforcement practices.**
 - Agencies should identify or establish new policies, due to the novelty and advancement of AI technologies, that:
 - allow individuals to raise concerns about irresponsible AI development (e.g., through an ombudsman); and
 - provide layers of human oversight or redundancy so that high-stakes decisions do not rely entirely on determinations made by the AI system.²⁸⁹
 - Adapt and extend oversight practices to include reporting requirements²⁹⁰ for AI systems; a mechanism to allow for thorough review of the most sensitive and high-risk AI systems (to ensure auditability and compliance with deployment requirements); an appealable process for those found at fault of developing or using AI irresponsibly; and grievance processes for those affected by the actions of AI systems.²⁹¹

²⁸⁶ As noted in the *Key Considerations* (Accountability and Governance), agencies should determine and document who is accountable for a specific AI system or any given part of an AI system and the processes involved with it. This should identify who is responsible for the development or procurement; operation (including the system's inferences, recommendations, and actions during usage) and maintenance of an AI system; as well as the authorization of a system and enforcement of policies for use. See *Key Considerations* at 37.

²⁸⁷ For a list of recommended information that documentation should note about system development, see the *Key Considerations* Appendix to this report.

²⁸⁸ For example, "APIs are 'doors' to access digital infrastructures thus, the security and resilience of digital environments will also depend on the robustness of the API infrastructure." V. Lorenzino, et al., *Application Programming Interfaces in Governments: Why, What and How*, European Union Joint Research Centre (2020), <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/application-programming-interfaces-governments-why-what-and-how>.

²⁸⁹ See Frances Duffy, *Ethical Considerations for Use of Commercial AI*, John Hopkins Applied Physics Laboratory at 31 (Dec. 2020). For example, DoD Directive 3000.09 requires human oversight in the targeting and execution process for lethal autonomous weapons. See *DoD Directive 3000.09: Autonomy in Weapons Systems*, U.S. Department of Defense (May 8, 2017), <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>.

²⁹⁰ For example, reporting risk and impact assessment, steps taken to mitigate such risks, and system performance during testing and fielding.

²⁹¹ As with all consequential software systems, developers and adopters of consequential AI systems must adapt and extend existing support for oversight, audit, reporting, and appealable accountability for developing or using systems irresponsibly, and a redress process where appropriate for those affected by system actions. Existing frameworks must be tailored to reflect issues of concern with AI-based systems (particularly based on machine learning). These issues of concern are discussed in more detail in the *Key Considerations* Appendix.

DRAFT NSCAI DOCUMENT

- Establish selection criteria that indicate if and when specific recommended practices (as found in the *Key Considerations*) need to be used according to system and mission risks.
- Define triggers that would require escalated review of an AI system.

DRAFT

[BLANK PAGE]

DRAFT

Chapter 8: Upholding Democratic Values: Privacy, Civil Liberties, and Civil Rights in Uses of AI for National Security Blueprint for Action

The U.S. needs an approach for adopting AI domestically for national security that upholds and bolsters respect for democratic values, including privacy, civil liberties and civil rights. Such an approach must strengthen, provide, and show leadership with regard to (1) transparency, (2) approaches for AI system development and testing, (3) the ability to contest AI decisions, (4) oversight over AI development and use, and (5) legislative and regulatory controls on how AI is used. Our recommendations include immediate actions that the President, the Congress, and agencies should take; a comprehensive assessment by a Task Force that leads to reforms for AI governance and oversight; and areas for continued work. The recommendations are aimed at assuring that AI systems used by national security agencies uphold democratic values. Secondly, the adoption of these recommendations can earn and inspire public confidence, both domestically and abroad, in uses of AI by national security agencies.

Recommendation Set 1: Increase Public Transparency about AI Use through Improved Reporting

Actions for Congress:

- **For AI systems that involve U.S. persons, require AI Risk Assessment Reports and AI Impact Assessments to assess the privacy, civil liberties and civil rights implications for each new qualifying AI system or significant system refresh.**
 - The Commission proposes Congress require elements of the Intelligence Community (coordinated by the Office of the Director of National Intelligence (ODNI)) as well as, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI), to prepare and publish AI Risk Assessment Reports and AI Impact Assessment to assess the privacy, civil liberties, and civil rights implications of each new qualifying AI system or significant system refresh. The Commission recognizes the current requirements for privacy impact assessments and civil liberties impact assessments done at agencies as required by current statute. AI-related technologies may be reviewed by these, but are not fully/adequately captured by the current assessments. The Commission’s recommendation intends to augment these requirements.
 - The AI Risk Assessment Report and AI Impact Assessments would be required for “new qualifying AI systems” and for “significant system refreshes.” The Commission proposes that the Task Force described [later] in this blueprint be charged with determining the decision procedures for identifying which AI systems and significant system refreshes would require an AI Risk Assessment Reports and AI Impact Assessments.

DRAFT NSCAI DOCUMENT

- The intent of the AI Risk Assessment Report and AI Impact Assessment is to ensure potential impacts are considered *and* mitigated while avoiding an unnecessary increase in compliance burdens.
 - Legislated frameworks for ensuring effective and pragmatic risk mitigation (with the ability to categorize systems per risk and determine the appropriate mitigations if any) exist in other models that can be used as a template (e.g. FISMA).
- The **AI Risk Assessment Report** should include a detailed analysis of system implications for, and **steps to mitigate and track risks (e.g., through metrics) to:**
 - Freedom of expression (e.g., is the AI-enabled surveillance targeting people because of their First Amendment protected activity or is the AI-enabled government surveillance causing or may potentially cause a chilling effect?);
 - Equal protection (e.g., is the AI-enabled surveillance biased towards a protected class? What are the likely effects the new technology or program will have on key demographics such as race, gender, or disability?);
 - Privacy (e.g., is a warrant required for the government action? Are minimization and query processes sufficient/satisfactory?); and
 - Redress and due process (e.g., what mechanisms exist, or limitations have been accepted, for providing redress for adverse government actions taken based on information generated by the AI system?).
 - The assessment should account for the environment in which the AI system will be deployed, including its interactions with other AI tools and programs that collect personally identifiable information (PII).
- **AI Impact Assessment** should be made available periodically, but no less than annually, to the agency's PCL Office to determine the degree to which a qualifying AI system remains compliant with the constraints and metrics established in the Risk Assessment . AI Impact Assessments should be based on outcomes, impacts, and metrics collected during system use, and determine if the existing validation processes should be improved.
- **Resources and staffing.** PCL Offices should assess the resources, including staff, needed to adequately complete the above. Agency heads should support additional resourcing for PCL Offices as part of the annual budget process.
- **Disclosure notices.** Congress should require ODNI, DHS and the FBI to review non-public and/or classified AI programs once the program is shut down for declassification and/or disclosure.

Action for the President:

DRAFT NSCAI DOCUMENT

DRAFT NSCAI DOCUMENT

- **Should Congress not require new privacy, civil liberties, and civil rights reporting (as identified above), the President through an Executive Order should require that agencies conduct AI Risk Assessment Reporting and AI Impact Assessments as described above.**

Actions for DHS and the FBI:

- **DHS and the FBI should impose new obligations for System of Record Notices (SORNs) and Privacy Impact Assessments (PIAs) specific to AI systems to ensure that they provide richer information.**
 - SORNs and PIAs should provide a holistic picture about the collection, use, and storage of personal information by any AI system, including its connections to existing systems and accounting for the layering of different surveillance technologies where applicable. Agency practices do not sufficiently support the production of SORNs and PIAs that adequately depict how AI systems collect, use, and store personal information.²⁹²
 - DHS and the FBI should require that all PIAs include description of the algorithm(s) used and purpose of the algorithm(s); the potential for inferring additional information about individuals from the aggregation of multiple data sources; and importantly, the measures that will be used to address these risks.
 - DHS and the FBI should require that SORNs provide more specificity in describing types of data collected, data sources and the connections between data sources, and who will use such data and why.
- **DHS and the FBI should take steps to increase public transparency about the AI systems they employ.**
 - DHS has recently started an effort to improve transparency and those efforts should be prioritized and assessed as they are implemented.²⁹³
 - The FBI should implement similar reforms to improve transparency.
- **DHS and the FBI should make their websites easier for the public to navigate and ensure the websites are regularly updated.** Privacy, Civil Liberties, and Civil

²⁹² For instance, a recent DHS IG report criticizes DHS Privacy Office for not establishing controls to ensure that privacy compliance documentation is complete and submitted as required, and specifically noted DHS had not performed required periodic reviews for new and evolving privacy risks. DHS IG, DHS Privacy Office Needs to Improve Oversight of Department-wide Activities, Programs, and Initiatives, OIG-21-06, (Nov. 4, 2020). Civil society members have noted that PIAs and SORNs are often too opaque to be helpful, and that agencies sometimes try to shoehorn new data collections under older SORNs and PIAs. See *Comments of the Electronic Frontier Foundation Regarding System of Records Notices 09-90-2001,09-90-2002*, Electronic Frontier Foundation (Aug. 17, 2020), https://www.eff.org/files/2020/08/17/2020-08-17_-_eff_comments_re_hhs_regs_re_covid_data.pdf (criticizing two SORNs issued by the Department of Health and Human Services during the pandemic, as “overly vague in describing the categories of data collected, the data sources, and the proposed routine uses of the data”).

²⁹³ The Commission acknowledges DHS’s steps to improve public records as noted in the DHS AI Strategy: “Future AI systems implemented by DHS will require a public release of system information with appropriate exceptions for certain sensitive military and intelligence systems, and some exceptions for law enforcement activities. DHS will produce a framework for releasing AI system information and a process for public comment.” See *U.S. Department of Homeland Security Artificial Intelligence Strategy*, U.S. Department of Homeland Security at 14 (Dec. 3, 2020), <https://www.dhs.gov/publication/us-department-homeland-security-artificial-intelligence-strategy>.

Rights Risk and Impact Assessment Reports, related semi-annual reports, PIAs, and SORNs should be located in a central place; have clearly marked dates next to the title, and chronologically ordered, and published in a timely manner. DHS and the FBI should seek public comments annually about the navigability of their websites and potential improvements.

Recommendation Set 2: Develop & Test Systems per Goals of Privacy Preservation and Fairness

Actions for the President:

- **Through Executive Order, the President should require the Director of National Intelligence, the Secretary of Homeland Security, and the Director of the FBI to take the following actions:**
- **Implement steps to mitigate privacy, civil liberties, and civil rights risks associated with any AI system on an iterative basis and require documentation of all accepted risks.**
 - In implementing steps to achieve this objective, the Commission recommends that ODNI, DHS and the FBI adopt practices from the Key Considerations. In particular:
 - Use privacy protections such as robust anonymization that can withstand sophisticated reidentification attacks, and when possible, privacy-preserving technology such as differential privacy, federated learning, and machine learning (ML) with encryption of data and models.²⁹⁴
 - Mitigate bias in development and testing. For development, conduct stakeholder engagement to establish consensus on the definition of fairness metrics to be used for the specific development and identify necessary constraints on system behavior to protect civil rights and avoid inequitable outcomes.²⁹⁵ In testing, confirm that identified constraints are enforced.²⁹⁶ Testing to expose unintended bias should include testing for and documentation of different types of error rates (e.g., differences in false positive or false negative rates) or disparate outcomes across demographics.²⁹⁷

²⁹⁴ To support agencies in this goal, federal R&D investment should continue to advance the state of the art for preserving personal privacy. For information regarding the critical AI research areas the Commission recommends OSTP prioritize, see the Chapter 9 Blueprint for Action. Agencies should also assign responsibility for assessing the state of the practice and encouraging federated learning and anonymization pilots for government databases used in machine learning developments (e.g., to Chief Data Officers at each agency).

²⁹⁵ Development practices should also include documenting trade-offs made, including optimizations that cause a tradeoff in performance across fairness metrics.

²⁹⁶ For instance, constraints about proxies for national origin or protected classes used for rules based system predictions.

²⁹⁷ For an extensive list of practices see the Key Considerations Appendix. These include: (1) Documenting operating thresholds including those that yield different true positive and false positive rates or different precision and recall across demographics; (2) Assessing the representativeness of data and model for the specific context at hand; (3) Using tools to probe for unwanted bias in data, inferences, and recommendations; (4) Testing for fairness and articulating the approach, performance, and metrics used.

DRAFT NSCAI DOCUMENT

- Use AI-tools to support assessing fairness (e.g. industry tools cited in the Key Considerations)²⁹⁸
- Ensure the ML-ops toolchains include routine calibration of agreed upon fairness metrics throughout continuous development and integration.²⁹⁹
- Assess model performance and system impact during fielding on an ongoing basis, including emergent behavior, to ensure compliance with privacy, civil rights, and civil liberties objectives.³⁰⁰
- **Designate an office, committee, or team in each agency to conduct a pre-deployment review of AI technologies that will impact privacy, civil liberties, and civil rights, including relevant documentation.**
 - This should include review in advance of their deployment and for compliance over the lifespan of the system.³⁰¹ An office in each Intelligence Community agency, DHS, and the FBI should be equipped to assess data, model and system documentation, and testing results of technologies per their intended use.
 - In undertaking this review, the Commission recommends the designated office use the *Key Considerations*.

Actions for Congress:

- **Establish third-party testing center(s) to allow independent, third-party testing of national security-related AI systems that could impact US persons.**
 - Congress should authorize NIST to sponsor a University Affiliated Research Center (UARC), Federally Funded Research & Development Center (FFRDC) and/or lab to provide independent, third-party testing. To enable this process, Congress should fund NIST to create a Third-Party AI Testing Lab program under the NIST National Voluntary Laboratory Accreditation Program.³⁰²
 - The third-party test mechanism's mandate should be to:
 - Tailor metric assessment per agency mission and authorities;

²⁹⁸ Examples of tools available to assist in assessing and mitigating bias in systems relying on machine learning include Aequitas by the University of Chicago, Fairlearn by Microsoft, AI Fairness 360 by IBM, and PAIR and ML-fairness-gym by Google. Microsoft's AI Fairness checklist provides an example of an industry tool to support fairness assessments. See Michael A. Madaio et al., *Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI*, CHI 2020 (Apr. 25-30, 2020), <http://www.jennwv.com/papers/checklists.pdf>.

²⁹⁹ A widely used Industry example of a fairness metric is Equality of Opportunity (EEO), defined in *Machine Learning Glossary: Fairness*, Google Developers (Feb. 11, 2020), <https://developers.google.com/machine-learning/glossary/fairness>. Note that EEO is suited for some contexts and a poor fit for others—this is why careful deliberation of the operational metrics for fairness must be established early in the development process.

³⁰⁰ For an extensive list of practices see the Key Considerations Appendix. Select practices include: (1) Assessing statistical results for performance over time to detect emergent bias; (2) Recurrent testing and validation at strategic milestones, especially for new deployments and classes of tasks; (3) Continuously monitoring AI system performance, including the use of high-fidelity traces to determine if a system is going outside of acceptable parameters (e.g., for fairness and privacy leakage) pre-deployment and in operation.

³⁰¹ ML systems in particular require ongoing assessments of privacy and fairness assurances, including the specific definition of fairness being assumed.

³⁰² This requires the creation of an AI TEVV handbook, a culmination of applied research, to create the testing protocols that should be carried out by third-party testing lab(s) and the accreditation procedures by which labs can become certified.

- Develop an approach for testing both software products that can be installed in a test facility and cloud-based services;
 - Establish binding data dissemination agreements with stakeholders of the system to be tested (e.g., the agency requesting testing and relevant vendors and data owners);
 - Collaborate with the agency seeking testing to reach consensus on how to handle the test data provided and the test results and analyses.³⁰³
- Third-party test center(s) should allow government vendors to share proprietary data without fear of it being exposed to competitors; and offer the benefits of an aggregated view of performance across a sector or collection of corporations and aggregated best practices.
 - Third-party test center(s) should be used by agencies prior to procuring or fielding high-consequence systems that impact U.S. persons, and use should be considered to overcome in-house testing limitations.
- **Require the Department of Justice (DOJ), in consultation with the Privacy and Civil Liberties Oversight Board (PCLOB), to develop binding guidance for the use of third-party testing (e.g., thresholds for high-consequence systems or unprecedented factors) of AI systems.**³⁰⁴
 - This should include criteria for when an AI system may pose high enough risk for privacy, civil liberties and civil rights that it would trigger a testing requirement by a third-party. In forming such guidance, PCLOB and the DOJ should consult with PCL Officers in federal agencies.

Acknowledgment of continued work for the technical community and legal experts

There are significant unresolved tensions between various technical approaches to preserving civil rights and civil liberties and current and anticipated legal frameworks. For example, scholars have expressed concern “that technical and legal approaches to mitigating bias will diverge so much that laws prohibiting algorithmic bias will fail in practice to weed out biased algorithms and technical methods designed to address algorithmic bias will be deemed illegally discriminatory.”³⁰⁵ Continued work in the technical, legal, and policy domains is required to find a consensus balance that addresses technical approaches to preserving privacy, civil liberties, and civil rights and evolving policy.

³⁰³ In some cases, exposure of test results could reveal weaknesses in a national security system that could be exploited by an adversary.

³⁰⁴ As noted in Ethical Considerations for Commercial Use of AI, “rigorous testing is particularly important for high-risk applications, and standards should be established to determine the nature of those applications.”

³⁰⁵ Alice Xiang, *Reconciling Legal and Technical Approaches to Algorithmic Bias*, Tennessee Law Review at 7 (July 13, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3650635. See also Zachary Lipton, et al., *Does Mitigating ML's Impact Disparity Require Treatment Disparity?*, arXiv (Jan. 11, 2019), <https://arxiv.org/abs/1711.07076> (Some approaches to mitigate disparate outcomes explicitly make use of membership in protected classes such as race or gender, and are demonstrably more equitable than comparable algorithms that are “blind” to protected classes.).

Recommendation Set 3: Strengthen the ability of those aggrieved by AI to seek redress and have due process.

Actions for FBI and DHS:

- **The FBI and DHS should each conduct a review of its respective policies and practices related to AI technology to ensure that parties aggrieved by government action involving the use of AI, including through system actions or misuse, can seek redress and clearly know how to do so. At least annually, the FBI and DHS shall assess if updates or changes are required based on their respective reviews.**
 - This review should determine whether notice of AI use in decision making is adequately provided to aggrieved parties to enable redress, as well as the degree of auditability and interpretability needed to contest.
 - The FBI and/or DHS review team—which must include the Offices of Privacy and Civil Liberties—should submit recommendations to their respective agency heads for any regulatory and/or policy changes necessary to amend existing redress mechanisms to reflect issues raised by the use of an AI-enabled system.
 - The Attorney General, working with the Director of the FBI, and the Secretary of Homeland Security, respectively, should direct appropriate actions to ensure that each agency
 - provides adequate redress, based on the recommendations of the review, and
 - provides the public with clear, updated guidance on how to seek redress in situations covered by the review, including by posting relevant information on their websites.

Actions for the Attorney General:

- **Issue federal guidance on AI and due process. This guidance should describe how relevant agencies should safeguard the due process rights of U.S. persons when AI use may lead to a deprivation of life or liberty.** This should include what obligations agencies have to disclose on its use of AI³⁰⁶ to a criminal defendant in a timely manner prior to trial or hearing (i.e., notice obligations), including the role that AI played leading to an arrest, charge, or criminal prosecution. Such guidance should be incorporated into agency operational guidelines.

Acknowledgment of continued work by the judicial and/or legislative branches:

³⁰⁶ Disclosure requirements should be specific to each application of AI. See Frances Duffy, *Ethical Considerations for Use of Commercial AI*, Johns Hopkins Applied Physics Laboratory at 31 (Dec. 2020) (“Appropriate disclosure requirements should be created for the purposes of traceability in a court case or for the government’s own internal use.”).

The above actions should ensure that agencies receive clear guidance on AI-related redress and due process³⁰⁷ in the interim as Congress and/or the courts weigh in on federal requirements. Continued work will be needed to provide baseline guidance with the evolution of AI capabilities and their application,³⁰⁸ and to address open questions on the federal rules of evidence and criminal procedure as they relate to AI.³⁰⁹

Recommendation Set 4: Strengthen Oversight and Governance Mechanisms to Address Current and Evolving Concerns

Actions for Congress:

- **Strengthen the Privacy and Civil Liberties Oversight Board’s (PCLOB) ability to provide meaningful oversight and advice to the federal government’s use of AI-enabled technologies for counterterrorism purposes.** To achieve this, Congress should provide for a targeted expansion of PCLOB’s authorities and appropriations as follows.
 - *Awareness of AI programs.* As part of PCLOB’s authority to access all relevant material from agencies, agencies should be required to provide PCLOB notice *prior* to the fielding or repurposing of an AI system, as well as any associated privacy, civil liberties, and civil rights impact assessments.
 - *Visibility into technology.* Agencies should be required to provide to PCLOB, upon PCLOB’s request, specific information about technology used in any AI system, including: the data used for AI systems (e.g. documentation regarding the data collection processes for AI-enabled tools and programs, including disclosure and consent processes); models used (and supporting model documentation regarding training and testing); and model repurposing (beyond that context for which it was trained/approved).
 - *Resources and other organizational requirements.* PCLOB requires an increase to its resources, both in terms of talent and funding, to achieve its mission and manage its portfolio as AI adoption increases. PCLOB should provide Congress with a self-assessment of its resources and organizational structure given the expected increase of AI-related programs that fall under its current mandate and responsibilities.

- **Empower DHS Offices of Privacy and Civil Rights and Civil Liberties.**

³⁰⁷ As noted in the *Key Considerations*, existing policies for contestability should be assessed and updated as needed to ensure accountability and to mitigate errors through feedback loops.

³⁰⁸ Due process rights require that individuals have the ability to meaningfully challenge a decision made against them. In federal criminal trials, this includes having the government’s explanation of how an unfavorable decision was reached, so it can be contested. In cases where AI-assisted or AI-enabled decisions are made, certain AI techniques will be less conducive to due process. See Danielle Keats Citron, *Technological Due Process*, Washington University Law Review (2008), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview; see also Ryan Calo & Danielle Keats Citron, *The Automated Administrative State: A Crisis of Legitimacy*, Emory Law Journal (Apr. 3, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3553590.

³⁰⁹ For instance, evidentiary standards for admitting AI evidence in court have yet to be developed and are not encompassed in current *Daubert* standards guidance.

DRAFT NSCAI DOCUMENT

Congress should bolster the roles of DHS' Office of Privacy and Office of Civil Rights and Civil Liberties by requiring the Chief Civil Rights and Civil Liberties Officer, in coordination with the Privacy Officer, to play an integral role in the legal and approval processes for the procurement and use of AI-enabled systems, including associated data of machine learning systems in DHS. As part of this legislation, the Privacy and Civil Rights and Civil Liberties offices should report back to Congress concerning additional staffing or funding resources that are required to satisfy this mandate.

Action for the Secretary of Homeland Security:

- **Ensure the Privacy Officer and the CRCL Officer receive permanent seats in the new DHS enterprise-wide AI Coordination and Advisory Council.** Such appointments are needed in order to meaningfully satisfy the DHS AI Strategy objective entitled "Formalize AI Governance Processes at DHS."³¹⁰

Actions for the President:

- **Through Executive Order, require stronger coordination and alignment among oversight and audit organizations through creation of an interagency working group focused on oversight and audit.** Voluntary compliance by agencies with AI documentation and testing requirements should be supported by rigorous, technically informed oversight. To achieve this and overcome current auditing impediments, a standing body (e.g., an interagency working group) should align and coordinate to enhance AI oversight and audit with respect to privacy, civil liberties and civil rights. This includes system auditability such that the government can monitor and trace the steps that produced a system's output,³¹¹ and auditing to ensure systems are not being misused.
 - *Composition:* Organizations should include the Department of Justice Intelligence Oversight Section; Office of the Inspector General of the Intelligence Community; the Government Accountability Office; the Privacy & Civil Liberties Oversight Board; Civil Liberties and Privacy Offices of national security agencies; the National Security Council, and the Office of Science & Technology Policy.
 - *Function:* The interagency working group should provide a forum for members to substantively and regularly address and share information. The working group should:

³¹⁰ DHS's Artificial Intelligence Strategy, dated December 2020, includes the establishment of a DHS enterprise-wide AI Coordination and Advisory Council composed of internal subject matter experts to monitor and support the adoption of AI technology by DHS Components. See *U.S. Department of Homeland Security Artificial Intelligence Strategy*, U.S. Department of Homeland Security at 10 (Dec. 3, 2020), <https://www.dhs.gov/publication/us-department-homeland-security-artificial-intelligence-strategy>.

³¹¹ For issues relevant to AI system audits, see *Global Perspectives and Insights: The IIA's Artificial Intelligence Auditing Framework Part*, Institute of Internal Auditors (2018), <https://na.theiia.org/periodicals/Public%20Documents/GPI-Artificial-Intelligence-Part-II.pdf>.

DRAFT NSCAI DOCUMENT

- Develop an inventory of the types of AI-relevant oversight and audit currently performed by and anticipated by the participant organizations;
- Develop an inventory of specific capabilities developed in each organization to address AI oversight and audit;
- Assess available AI-enabled tools that can be adapted to support more effective and efficient oversight and audit;
 - Tools that support financial audit³¹² and model risk management³¹³ are examples of advances in applying AI to improve the efficiency and scalability of audits that should be reviewed for adoption.
- Identify priority investment requirements for each organization to address current needs;
- Identify priority research topics for open S&T gaps in supporting AI oversight and audit, including research gaps in applications of AI in support of privacy and civil liberties (e.g., ML techniques for classification, recommendation, anomaly detection and other applications)³¹⁴ and extending tools such as those that support financial audits and model risk management;
- Recommend policy or legislative changes for specific authorities granted to the individual organizations;
- Address mission and focus overlap among representative organizations; and
- Issue reports, at a minimum annually, on key oversight and audit activities as well as S&T gaps.

Action for the President or Congress:

- **Establish a task force to assess the privacy and civil rights and civil liberties implications of AI and emerging technologies.**

The goal of the task force would be to identify gaps and make recommendations to ensure that uses of AI and associated data in U.S. government operations comport with U.S. law and values, and to study organizational reforms that would support this goal. Specifically, it should assess existing policy and legal gaps for current AI applications and emerging technologies, and make recommendations for:

- legislative and regulatory reforms on the development and fielding of AI and emerging technologies;³¹⁵ and
- institutional changes to ensure sustained assessment and recurring guidance on privacy and civil liberties implications of AI applications and emerging technologies.

³¹² See e.g., Audit Map (last accessed Jan. 3, 2021), <https://auditmap.ai/>; *The Next Generation of Internal Auditing— Are You Ready?*, Protiviti (2018), https://www.protiviti.com/sites/default/files/united_states/insights/next-generation-internal-audit.pdf.

³¹³ See e.g., Bernhard Babel, et al., *Derisking Machine Learning and Artificial Intelligence*, McKinsey & Company (Feb. 19, 2019), <https://www.mckinsey.com/business-functions/risk/our-insights/derisking-machine-learning-and-artificial-intelligence>; Saqib Aziz & Michael Dowling, *Machine Learning and AI for Risk Management*, *Disrupting Finance* at 33-50 (Dec. 7, 2018), https://link.springer.com/chapter/10.1007/978-3-030-02330-0_3.

³¹⁴ Xuning (Mike) Tang & Yihua Astle, *The Impact of Deep Learning on Anomaly Detection*, *Law.com* (Aug. 10, 2020), <https://www.law.com/legaltechnews/2020/08/10/the-impact-of-deep-learning-on-anomaly-detection/>.

³¹⁵ Examples include baseline AI standards and policy guidance for biometric identification technologies; for government procurement of commercial AI products; and for federal data privacy standards.

As mentioned in Chapter 8 of this report, the advancement of AI requires a forward-looking approach to oversight that anticipates the continued evolution and adoption of new technologies, and better positions the government to manage their employment responsibly well into the future. The Commission assesses that to achieve this goal, a new task force is needed.

The Commission recommends that the President or Congress create a task force with the proposed membership, structure, function, and priorities identified below.

For expediency, the President should:

- **Issue an Executive Order that creates a task force charged with recommending reforms for AI governance and oversight.**
 - **Membership and structure.** The President should create a task force in the Executive Office of the President to develop recommendations on ensuring adequate AI governance and oversight. The President should designate a senior official to lead the task force. Members should include the heads of OMB, NIST, PCLOB, GAO, and the DOJ Civil Rights Office; and Chief Civil Liberties and Privacy Officers and Inspectors General of all national security agencies. In addition, the task force should include representatives from civil society (including organizational leaders with expertise in privacy, civil liberties and civil rights), industry, and academia. The National AI Advisory Committee Subcommittee on AI and Law Enforcement should also be represented.³¹⁶
 - **Function.** The task force should be charged with the following responsibilities:
 - Conducting a macro assessment of the privacy and civil rights and civil liberties implications of the capabilities of AI and emerging technologies
 - Making recommendations for legislative and regulatory reforms on the development and fielding of AI and emerging technologies, including associated data, in the following key areas:
 - *Privacy, Civil Liberties, and Civil Rights (P/CLCR) reporting.* Binding guidance on when the IC, DHS, and FBI should prepare and publish an AI Risk Assessment Report and AI Impact Assessments - specifically what constitutes a qualifying AI system or significant system refresh (as discussed in the first recommendation of Chapter 8 of this report)
 - *Biometric technologies.* This should include baseline standards for federal government use of biometric identification technologies, including but not limited to facial recognition.

³¹⁶ In the FY 2021 NDAA, Congress directed the Secretary of Commerce, in consultation with other senior Executive Branch officials, to establish the National AI Advisory Committee, including a Subcommittee on AI and Law Enforcement. The Subcommittee is tasked to “provide advice to the President on matters relating to the development of artificial intelligence relating to law enforcement.” Pub. L. 116-283, sec. 5104 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 134 Stat. 3388 (2021).

- To address the urgent need for baseline standards and safeguards regarding facial recognition, this should include assessing gaps in federal legislation, gathering input from agency stakeholders (and their legal counsel) currently using facial recognition for national security missions; privacy, civil liberties, and civil rights experts inside and outside of government, including PCLOB; and from the public at large in order to make facial recognition legislation recommendations.
- Beyond facial recognition, guidance will be needed regarding other biometric identification tools including voiceprints.
- *Government procurement of commercial AI products.* This should include contractual best practices for ensuring industry AI products (including associated data) procured by the government uphold privacy, civil liberties, and civil rights expectations (including privacy, information security, fairness/non-discrimination, auditability, and accountability). This should include third-party requirements that should be incorporated into procurement terms that speak to responsible AI objectives, including for testing validation.³¹⁷ Consideration should be given to both government-off-the-shelf and commercial-off-the-shelf (COTS) procurement.³¹⁸
- *Data privacy and retention.* Updates to and reforms of government data privacy and retention requirements to address AI implications.
- Making recommendations for institutional changes to ensure sustained assessment and recurring guidance on privacy and civil liberties implications of AI applications and emerging technologies.
 - Evolving AI capabilities are poised to challenge existing expectations for privacy, civil liberties, and civil rights, and civil liberties.³¹⁹ In light of this, the task force should assess the utility of a new entity within the federal government to regulate and

³¹⁷ These should seek to encourage contracts with companies that have transparent policies and practices in support of traceability and auditability and those that share information about how their technology works and how it performs in independent testing.

³¹⁸ “Federal government acquisition regulations require that agencies procure software commercially off-the-shelf whenever possible, due to their cost effectiveness. Only when no comparable systems exist are agencies permitted to develop government off-the-shelf solutions.” See Frances Duffy, *Ethical Considerations for Use of Commercial AI*, Johns Hopkins Applied Physics Laboratory at S-1 (Dec. 2020). As standards and requirements for system development and testing evolve, it may be helpful for the government to “establish and maintain a list of COTS AI technologies that have been vetted and approved for micro-purchasing, based on their consistency with government security and testing standards, as well as their transparency.” This could facilitate both rapid procurement and proper assessment of a vendor’s consistency with Responsible AI practices. See Frances Duffy, *Supplement to Ethical Considerations for Commercial Use of AI: Implications of Acquisition Scale*, Johns Hopkins Applied Physics Laboratory (forthcoming).

³¹⁹ For example, policymakers and legislators will need to direct future attention to policies to preserve PCL as technological capabilities for ubiquitous sensing grow, e.g., in smart cities. In the future, ubiquitous sensing may make it impossible to distinguish U.S. persons’ data versus non-US persons’ data for AI analytics. Another example for continued consideration includes the role of AI in filtering to remove U.S. persons’ information from bulk data and conversely using AI to reveal such information, as minimization and de-minimization guidance may evolve based on AI efficacy relative to the status quo.

DRAFT NSCAI DOCUMENT

provide government-wide oversight of AI use by the federal government.

- In evaluating options for a new entity, the task force should consider the following:
 - Authorities and resources necessary for the new entity to provide ongoing guidance and baseline standards for:
 - The Federal Government’s development, acquisition, and fielding of AI technologies to ensure they comport with privacy, civil liberties, and civil rights and civil liberties law and values, and to include guardrails for their use and disallowed outcomes³²⁰ to be incorporated in policy and embedded in system development;
 - Transparency to oversight entities and the public regarding the Federal Government’s use of AI systems and the performance of those systems;
 - Existing interagency and intra-agency efforts to address AI oversight; and
 - The unique needs of national security, law enforcement, and other government missions with respect to AI systems and potential implications for privacy, civil liberties, and civil rights, and civil liberties.
- After considering the potential utility of a new organization, make recommendations on organizational placement and structure, composition, authorities, and resources needed.
 - Assessing ongoing efforts to adapt regulation of the private sector’s AI adoption,³²¹ and as appropriate, consider and recommend institutional or organizational changes to facilitate adequate regulation of commercial development and fielding of AI and associated data.
 - **Reporting.** The task force should issue a report to the President with its legislative and regulatory recommendations on a rolling basis, but no later than within 180 days of its creation. It should issue a report to the President with its recommendations for organizational changes within 1 year of its creation. The Commission recommends that the report be provided to Congress to ensure transparency and assist Congress in examining these critical issues.
- **In the alternative, Congress should mandate the existence of this task force as outlined above.**

³²⁰ Disallowed outcomes and guidance will need to be updated over time as community norms and technical capabilities change.

³²¹ See, for example, *Remarks of Commissioner Rebecca Kelly Slaughter: Algorithms and Economic Justice*, FTC (Jan. 24, 2020) https://www.ftc.gov/system/files/documents/public_statements/1564883/remarks_of_commissioner_rebecca_kelly_slaughter_on_algorithmic_and_economic_justice_01-24-2020.pdf; *Artificial Intelligence and Machine Learning in Software as a Medical Device*, U.S. Food and Drug Administration (Jan. 2021), <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device>.

Acknowledgment of continued work to update and clarify legal frameworks on key issues in data protection and data privacy:

A comprehensive approach to upholding privacy and civil liberties in the AI era requires tackling several large, unresolved policy and legal questions regarding data protection and data privacy. Detailed recommendations on these issues would extend beyond the scope of this Commission’s mandate, but we identify them here in order to urge further study and congressional action.

- *Legal concerns over federal use of third-party data.* Congress and/or the Judiciary should assess the adequacy of current legal constraints over the federal government’s obtainment and use of third-party data, including data acquired from data brokers. Either through evolving case law or legislation, agencies would benefit from clarity surrounding the Fourth Amendment’s application on third party data.³²² In the meantime, agencies should provide transparency on their respective policies and legal basis for accessing and using commercial data.³²³
- *National data protection standards.* Data privacy policies and standards that apply to government agencies alone will be inadequate, and in some cases may harm national security interests.³²⁴ This is particularly important considering how adversaries (both state and nonstate actors) can access and use data collected about U.S. persons. As Congress considers proposals for national data security and privacy protection, it should ensure any future legislation addresses the issue of microtargeting. As noted in Chapter 1 of this report, AI systems will create new capabilities for state actors to target individuals with precision as well as numerous aspects of our society like cities, supply chains, universities, corporations, infrastructure, and financial transactions. Strong data privacy protections will be necessary for a multitude of reasons, including to shield the United States from this new phenomenon.
- *National framework for use of biometric technologies.* In the absence of federal legislation regulating the use of facial recognition, the existing patchwork of state and

³²² See Byron Tau, *Homeland Security Watchdog to Probe Department’s Use of Phone Location Data*, Wall Street Journal (Dec. 2, 2020), <https://www.wsj.com/articles/homeland-security-watchdog-to-probe-departments-use-of-phone-location-data-11606910402> (reporting that “DHS’s general counsel began examining [the agency’s use of location tracking data] after concerns were raised by several offices within the department that use of the technology wasn’t compatible with [Carpenter],” and that the DHS IG planned to investigate the matter).

³²³ In ODNI Director Avril D. Haines’ confirmation hearing, she was asked about the IC’s use of commercially available location data. She testified that she would “try to publicize, essentially, a framework that helps people understand the circumstances under which we do that and the legal basis that we do that under. . . I think that’s part of what’s critical to promoting transparency generally so that people have an understanding of the guidelines under which the intelligence community operates.” Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, New York Times (Jan. 22, 2021), <https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html>.

³²⁴ Investigative reporting and opinion pieces have underscored the national security threats involved with smartphone location data. Charlie Warzel & Stuart A. Thompson, *They Stormed the Capitol. Their Apps Tracked Them*, New York Times (Feb. 5, 2021), <https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html?referringSource=articleShare>; Stuart A. Thompson & Charlie Warzel, *How to Track President Trump*, (Dec. 20, 2019), <https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html>; Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, New York Times (Dec. 19, 2019), <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.

local laws and regulations creates a number of difficulties for government officials, industry, and the public. This has led to actions including: companies prohibiting the sale of facial recognition to law enforcement,³²⁵ and local government bans on the use of facial recognition have emerged from coast to coast.³²⁶ The lack of a consistent federal approach is also a liability for national security agencies when best practices are not used locally.³²⁷ In developing regulation, it will be critical that policy and legislation account not only for facial recognition, but other types of biometric identification that, when combined with other AI technology, can introduce additional concerns.³²⁸

³²⁵ See Larry Magid, *IBM, Microsoft And Amazon Not Letting Police Use Their Facial Recognition Technology* (June 12, 2020), <https://www.forbes.com/sites/larrymagid/2020/06/12/ibm-microsoft-and-amazon-not-letting-police-use-their-facial-recognition-technology/?sh=34b473dc1887>; Asa Fitch, *Microsoft Pledges Not to Sell Facial-Recognition Tools to Police Absent National Rules*, Wall Street Journal (June 11, 2020),

<https://www.wsj.com/articles/microsoft-pledges-not-to-sell-facial-recognition-technology-to-police-absent-national-rules-11591895282>.

³²⁶ See *Ban Facial Recognition*, Fight for the Future (last accessed Feb. 4, 2021), <https://www.banfacialrecognition.com/map/>.

³²⁷ The Department of Defense, the Drug Enforcement Administration, Immigrations and Customs Enforcement, the Internal Revenue Service, the Social Security Administration, the U.S. Air Force Office of Special Investigations, and the U.S. Marshals Service have all had access to one or more state or local face recognition systems. See Clare Garvie, et al., *The Perpetual Lineup: Unregulated Police Face Recognition in America*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016), <https://www.perpetuallineup.org/>.

³²⁸ Such types of identification aided by AI include voice recognition and gait detection. An example of additional risks includes when biometric identification is coupled with other advancing capabilities—for instance for identity recognition or for emotion recognition. See *Emotional Entanglement: China's Emotion Recognition Market and its Implications for Human Rights*, Article 19 (Jan. 2021), <https://www.article19.org/wp-content/uploads/2021/01/ER-Tech-China-Report.pdf>. See also Drew Harwell & Eva Dou, *Huawei Tested AI Software that Could Recognize Uighur Minorities and Alert Police, Report Says*, Washington Post (Dec. 8, 2020), <https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/>; Parmy Olson, *The Quiet Growth of Race Detection Software Sparks Concerns Over Bias*, Wall Street Journal (Aug. 14, 2020), <https://www.wsj.com/articles/the-quiet-growth-of-race-detection-software-sparks-concerns-over-bias-11597378154>.

END OF PART I

DRAFT