

Future of Defense Task Force: Report on Implementation

March 15, 2022



Cover Photo Credit: NASA

FUTURE OF DEFENSE TASK FORCE

March 15, 2022

The Honorable Adam Smith
Chairman House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Mike Rogers
Ranking Member House Armed Services Committee
2216 Rayburn House Office Building
Washington, D.C. 20515

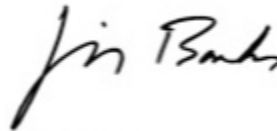
Dear Chairman Smith and Ranking Member Rogers:

Thank you for your continued support for modernizing our national security to meet a new generation of threats. I am pleased to present you with a report on the implementation of the Future of Defense Task Force.

Sincerely,



Seth Moulton
Chair
Future of Defense Task Force



Jim Banks
Chair
Future of Defense Task force

EXECUTIVE SUMMARY

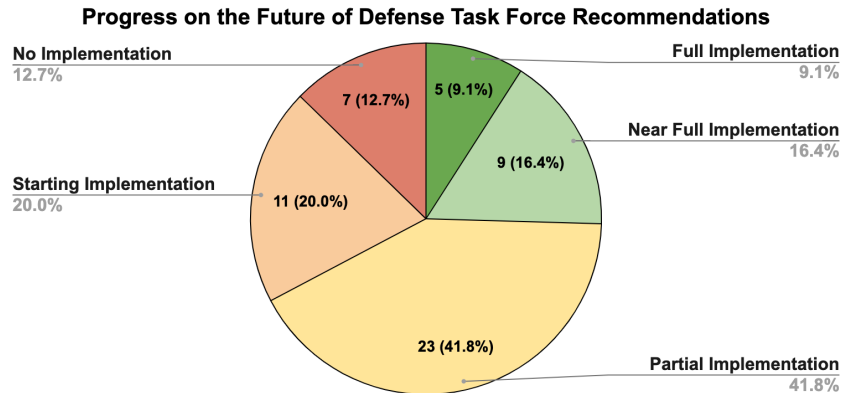
The Future Defense Task Force Report was published in September 2020 by a bipartisan group of members on the House Armed Services Committee. It provided a roadmap for the national security community for the coming decades and highlighted broad, sweeping defense modernization efforts required to address the complex challenges posed by China and Russia in a new era of great power competition.

Within the report, the Task Force made 14 recommendations with 55 unique sub-recommendations to Congress, the executive branch, industry, and academia. It called upon the Department of Defense (DoD) to refocus its efforts on these critical modernization priorities and reminded Congress, the President, and the American people of the necessary steps for ensuring America's national security in the 21st century. New administrations, shifting congressional make-up, and emerging crises can grab our attention and slow implementation, but the Task Force's recommendations remain relevant and critical to the future of our national security. This Implementation Report tracks the Task Force's recommendations in authorizing legislation, appropriations, executive orders, and other policy actions, and outlines relevant developments that have emerged in the year and a half since the Task Force published its finding

IMPLEMENTATION OF RECOMMENDATIONS

This report found that Congress, the President, and the national security community writ-large have made significant progress in the last year and a half implementing the Task Force's recommendations. Specifically, this report finds that 14 of the 55 recommendations have been fully or nearly fully

implemented, 34 of the recommendations have been partially implemented or have started to be implemented, and only 7 of the recommendations have not progressed or face significant barriers to implementation. Congress, particularly the armed services committees, have established a number of important programs, commissions, and authorities under the most recent National Defense Authorization Act (NDAA). Some notable achievements include:



Legacy Systems Report: The FY22 NDAA requires DoD to issue and brief Congress on a legacy systems report, verified by the Government Accountability Office (GAO). It will assess the capacity of currently fielded major weapons systems and capabilities to meet future operational requirements and

potential threat environments.¹ This will strengthen the DoD's request for legacy system divestment and help drive Congressional implementation of those requests.

Innovative Technologies Acceleration Pilot Program: The FY22 NDAA creates a DoD pilot program to accelerate the acquisition, development, and fielding of critical innovative technologies. This pilot will aim to shorten the time from a contract bid to using technology in the field.²

Mission Management Pilot Program: The FY22 NDAA creates a DoD mission management pilot program to test alternative procurement and acquisition methods for mission-critical operational solutions. Pilot program findings will improve new product development and acquisition procedures addressing immediate militaristic needs, essential for future combat readiness.³

Digital Talent Recruiting Officer: The FY22 NDAA requires DoD to appoint a Chief Digital Recruiting Officer to identify technological skill gaps and recruit civilians with programming, computer science, and other related backgrounds. The Chief Digital Recruiting Officer would aim to fill those gaps, thereby improving the capacity to obtain and sustain critical digital talent.⁴

National Defense Science and Technology Strategy: The FY22 NDAA codifies a National Defense Science and Technology Strategy that DoD must create and update along with the National Defense Strategy. Among other requirements, the strategy must identify and address short-term, mid-term, and long-term science and technology priorities and investment goals.⁵

National Security Commission on Emerging Biotechnology: The FY22 NDAA creates an independent National Security Commission on Emerging Biotechnology to review advances in biotechnology and associated technologies. The Commission will evaluate the current and potential impact of biotechnology on US national security and defense.⁶

Commission on Planning, Programming, Budgeting, and Execution Reform: The FY22 NDAA creates an independent Commission on Planning, Programming, Budgeting, and Execution Reform. This

¹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 146 - Review and Briefing on Fielded Major Weapon Systems* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

² Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 834 - Pilot Program to Accelerate the Procurement and Fielding of Innovative Technologies* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

³ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 871 - Mission Management Pilot Program* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁴ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 909 - Digital Talent Recruiting Officer* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁵ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 211 - Codification of National Defense Science and Technology Strategy* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁶ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1091 - National Security Commission on Emerging Biotechnology* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

Commission will advise DoD and Congress on potential improvements in defense planning, programming, budgeting, and execution that define the government's yearly defense budget.⁷

NOTEWORTHY FINDINGS

This implementation review highlights critical areas where the national security community has made exceptional progress, and areas where the national security community must take further action. It also reveals enduring challenges and considerations for the national security community going forward.

The fight to retire outdated legacy systems is just beginning. While members of the Task Force successfully commissioned a DoD report on legacy systems, going forward this report must be paired with actual divestment of outdated systems and reinvestment in new capabilities. In a constrained budget environment, it is critical to maximize the impact of every dollar spent: DoD must use its legacy systems report as leverage to push for future divestments, and Congress must support those divestment requests and pass them into law.

Budgeting & acquisition reform will make or break our future military capabilities. DoD's budgeting and acquisition processes may seem far removed from the battlefield, but they serve as the gatekeeper for new capabilities getting into the hands of the warfighter. Task Force members took critical steps to push budgeting and acquisition reform, but the processes are still painfully slow and unnecessarily convoluted. Without continued analysis and action, these processes will continue to block agility and adaptability throughout the Department.

We need next-generation international partnerships to face next-generation threats. The Task Force saw progress in building traditional international partnerships, but we must also consider new models beyond traditional military agreements and forge links across technology, finance, and more. Competition in national security extends far beyond the bounds of the military, and our adversaries increasingly operate in global, rather than purely regional, contexts. Our partnerships and treaties should reflect that reality going forward.

Talent recruitment and retention continues to be a major barrier. Congress and the Department have taken steps to improve the talent pipeline, but many of these efforts are scattershot and fail to address foundational challenges within the national security workforce. The Department needs to take a more holistic and systematic approach to identify and address its workforce challenges: without the right workforce, the Department will struggle to sustain and build on the progress it has made in other areas of the Task Force's report.

Declining national service, in and out of the military, is the next big threat to the nation. Of the 14 recommendations in this report, the national service-oriented recommendations have seen the least progress. National service is a critical mechanism for encouraging the civic engagement required to make our democracy function, and national service rates can be used as a key metric to measure the American

⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1004 - Commission on Planning, Programming, Budgeting, and Execution Reform* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

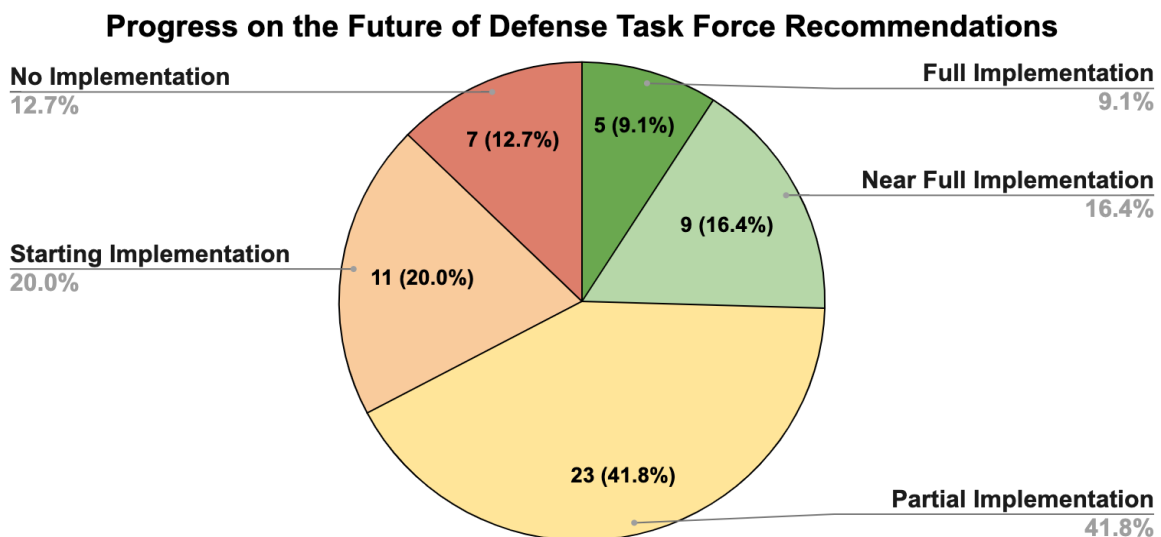
people's investment and trust in our nation's government. The ongoing decline in national service and the lack of progress implementing related Task Force recommendations suggests an impending threat to the nation.

In sum, our efforts to prepare for the long-term threats of great power competition have come a long way in the year and a half since the Future of Defense Task Force released its final report. Congress and the executive branch have taken critical steps to implement recommendations, and the implementation process itself has unveiled enduring challenges and priorities for the national security community to focus on going forward. With this in mind, Congress, the executive branch, and the national security community writ-large must use this momentum to continue the push for critical modernization, investments, and reform and strengthen US national security throughout the 21st century.

EVALUATION SUMMARY

The following color-coding system⁸ was used to evaluate the progress made on each of the Future of Defense Task Force's recommendations.

Color	Ranking	Description
	Full Implementation	Public law, executive order, or other action that fully codifies the recommendation
	Near Full Implementation	Most of the recommendation has been fully codified and the remainder is forthcoming
	Partial Implementation	Codification of parts/all of the recommendation is forthcoming or parts of the recommendation are already codified
	Starting Implementation	There is significant effort to begin codifying the recommendation
	No Implementation	No effort is being taken to codify the recommendation or there are significant barriers to codification



⁸ Inspired by evaluation system of the Cyber Solarium Commission, *2021 Annual Report on Implementation* (Aug. 2021) (online at <https://www.solarium.gov/public-communications/2021-annual-report-on-implementation>)

RECOMMENDATION IMPLEMENTATION EVALUATION

#	Description of Recommendation	Evaluation
1	Using the Manhattan Project as a model, the United States must undertake and win the artificial intelligence race by leading in the invention and deployment of AI while establishing the standards for its public and private use. Although the Department of Defense has increased investment in AI and established the Joint Artificial Intelligence Center to assist with the transition and deployment of AI capabilities, cultural resistance to its wider adoption remains. Congress and the Department of Defense must take additional action to overcome these barriers.	
1.1	Require every Major Defense Acquisition Program to evaluate at least one AI or autonomous alternative prior to funding.	
1.2	Require all new Major Defense Acquisition Programs to be AI-ready and nest with existing and planned joint all-domain command and control networks.	
1.3	Expand DoD's authorities and abilities to evaluate high technology readiness level items and technologies.	
2	Because of the United States' commitment to human rights, and to ensure those rights are enshrined in its use, the United States should lead in the formulation and ratification of a global treaty on artificial intelligence in the vein of the Geneva Conventions, the Chemical Weapons Convention, and the Nuclear Non-Proliferation Treaty to establish guardrails and protections for the civilian and military use of AI. Nations that adhere to democratic principles should lead in the creation of the global treaty, which would establish accountability, promote collaboration and transparency, ensure fairness, and limit the harmful use of AI. The treaty should further establish an international code of ethics and privacy protections that ensure personal freedoms and liberties globally. The document must be amendable to allow for advancements in technology, and the stated goal must be for all nations, especially those that are developing and employing AI, to be included as signatories.	
2.1	Create a global treaty, which would establish accountability, promote collaboration and transparency, ensure fairness, and limit the harmful use of AI.	
3	The United States must ensure supply chain resiliency within both the military and civilian sectors by establishing reliable manufacturing sources and incentivizing the return of manufacturing to the homeland through fiscal policy, tax incentives, and other financial and policy measures.	
3.1	Form a National Supply Chain Intelligence Center under the Director of National Intelligence to monitor and protect US supply chain interests.	
3.2	Identify and eliminate single points of failure within DoD supply chain.	

3.3	Bolster and expand the Information and Communications Technology Supply Chain Risk Management Task Force within the Department of Homeland Security to identify and secure the civilian supply chain equities that affect US national security interests.	
3.4	Strengthen the Committee on Foreign Investment in the United States (CFIUS) and the Foreign Investment Risk Review Modernization Act (FIRRMA) regulations to include additional industries relevant to AI, quantum computing, sensing, autonomy, space, and robotics.	
4	To compete against 21st century adversaries, Congress and the Department of Defense must identify, replace, and retire costly and ineffective legacy platforms. The Task Force recommends 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 studies should survey all services, agencies and entities within the Department of Defense to include hardware, weapons systems, basing, and force structure with an emphasis on agility, technology, and an expanded forward foot print, and the studies should make recommendations for future force structure and investment. Following completion of the studies, a panel should be convened, comprising Congress, the Department of Defense, and representatives from the industrial base to make recommendations on which platforms should be retired, replaced or recapitalized.	
4.1	Studies should survey all legacy services, agencies, and entities within DoD to include hardware, weapons systems, basing, and force structure.	
5	The US homeland remains uniquely vulnerable to adversaries who are increasing their ability to wage cyberwarfare against civilian populations through attacks on infrastructure, financial institutions, and healthcare facilities, among others. The United States should prioritize cyber-attack and gray zone defense capabilities within both the Department of Defense and the private sector.	
5.1	Examine the relationship between executive branch departments and agencies with independent regulatory agencies overseeing critical infrastructure sectors to ensure that information related to cybersecurity is shared by default, rather than by exception.	
5.2	Create parity between the defense industrial base and other critical infrastructure sectors by establishing an independent regulatory agency to define and enforce threat-informed cybersecurity standards through regular assessments.	
5.3	Bolster the partnership between US Cyber Command and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, notably the operational partnership in national defense and incident response.	

5.4	Develop tactical cyber operational forces within all military services to integrate them into conventional kinetic operations to foster interoperability between conventional operational activities and cyberspace activities.	
5.5	Ensure that DoD recruits and fosters a technologically astute workforce that can develop and procure the requisite capability to mitigate potential vulnerabilities.	
5.6	Create tax and other financial incentives for the private sector to invest in cybersecurity and prepare for gray zone attacks.	
6	Because an engaged and informed electorate is essential for a republic to endure, the United States should expand voluntary National Service programs. Promoting volunteerism and active engagement in democracy bolsters our national security through participation and shared experiences.	
6.1	Integrate military, national, and public service to create interoperability within these sectors.	
6.2	Initiate paid, year-of-service programs with civilian, military, and private-sector pathways for youth.	
6.3	Incentivize service through student loan deferment and forgiveness.	
6.4	Create mentorship and apprentice opportunities within national service programs.	
6.5	Encourage civics and personal citizenship curricula in public schools.	
7	To maintain its global preeminence in scientific and technological innovation and the associated economic and military advantage, the United States should increase its investment in foundational science and technology research by committing to spending at least one percent of the country's gross domestic product on basic government-supported research and development.	
7.1	The Pentagon should increase funding for science and technology research programs to meet the 3.4 percent of the overall defense budget recommended by the Defense Science Board.	
7.2	Expand funding for historically successful innovation efforts such as Defense Advanced Research Projects Agency, the national and defense research laboratories, and university partnerships.	
7.3	Require the military services to spend at least one percent of their overall budgets on the integration of new technologies.	
7.4	Establish target funding levels with defense allies for investment in science and technology research.	

8	To maintain its technological advantage over competitors, the Pentagon must continue to improve its ability to leverage private sector innovation at scale, including that from non-traditional companies, recognizing that the private sector, not the government, is now the leader in research and development investment.	
8.1	Increase funding for successful innovation efforts such as the Defense Innovation Unit, AFWERX, Army Futures Command, and others that successfully bridge the gap between innovative organizations and the military ten-fold, and robustly fund established drivers of innovation within DoD.	
8.2	Restore DoD Rapid Innovation Fund, which was authorized in FY11, to assess, fund, and accelerate innovative technology solutions for the warfighter.	
8.3	Create additional opportunities for collaboration and shared experience between DoD, private sector, and academia through the expansion of programs such as Hacking for Defense and partnerships with groups such as the Silicon Valley Defense Working Group.	
9	To sustain the world order that has allowed the United States to prosper and thrive for more than 70 years, the United States must foster new and creative partnerships for a changing world while strengthening existing alliances and security agreements. Such engagements will further vital US national security interests by ensuring placement, access, resiliency and redundancy while creating complex problem sets for adversaries.	
9.1	Enhance essential partnerships with North Atlantic Treaty Organization and FiveEyes intelligence partners, Canada, United Kingdom, Australia, and New Zealand— as well as with Japan and South Korea.	
9.2	Develop a modern Western Hemisphere policy that protects US Latin and Central American interests and alliances while simultaneously expanding a robust Arctic Strategy.	
9.3	Bolster ties with allies in the Middle East, notably Israel and Jordan.	
9.4	Strengthen relations with longstanding Asian security partners such as Thailand, the Philippines, Taiwan, and Singapore while growing relationships with India, Vietnam, Indonesia and Malaysia, among others.	
9.5	Cultivate economic and diplomatic cooperation with non-traditional allies, especially in Asia and Africa.	
9.6	Increase foreign military sales with security partners and bolster the International Military Education and Training program following enhanced vetting	
9.7	Extend New START and negotiate a follow-on agreement.	

10	Recognizing that human capital is our most important asset, the United States should increase its investment in science, technology, engineering, and mathematics within the Department of Defense and foster STEM talent through a whole-of-government approach to ensure the nation's scientific and technological advantage in the public and private sectors endures.	
10.1	Invest in STEM primary education.	
10.2	Attract and retain foreign STEM talent to study and work in the United States through specialized visas and scholarships.	
10.3	Improve hiring pathways and increase compensation for STEM careers at the Pentagon and in the private sector; create a military commissioning source for STEM talent.	
10.4	Streamline security clearances by beginning the vetting process in graduate school.	
10.5	Build STEM incentives into the service academies through scholarships and curricula.	
10.6	Enable and incentivize "Tour of Duty" opportunities for private sector technical talent to serve tours within DoD.	
11	To maintain the United States' military advantage against emerging threats, the Pentagon must refine its operational concepts by employing new technologies and methods to deter future conflicts and compete in the gray zone of hybrid warfare.	
11.1	The Pentagon, Congress, and the Intelligence Community should work in tandem to identify trends and threats 10 to 30 years beyond the normal budget cycle while expanding entities within their respective organizations to incorporate long-term planning.	
11.2	DoD should adhere to a whole-of-government approach and work with other departments such as State and Treasury to develop and execute a comprehensive strategy to compete in the gray zone.	
11.3	Create a task force to ensure a diverse group of stakeholders, including Congress, academia, think tanks, and the private sector are engaged in developing imaginative solutions to emerging military challenges and in assessing the Pentagon's efforts.	
11.4	Increase funding for wargaming and large-force joint exercises to assess new operational concepts; increase prototyping and testing with the emerging technologies needed to underpin these concepts.	
11.5	Prioritize the development and procurement of critical capabilities for future	

	conflict models such as resilient command and control networks, logistics capabilities and the defense of forward and expeditionary basing.	
11.6	Invest in programs of record to directly support emerging operational concepts.	
12	The United States is operating under an authorization for the use of military force that is nearly two decades old. Emerging threat streams require the United States to make strategic choices and prioritize its military actions. Congress must uphold its constitutional obligation to determine how and where the United States employs its military force by passing an updated AUMF. Revising the AUMF ensures that the United States can operate in a dynamic threat environment while signaling to both allies and adversaries that America is committed to the lawful pursuit of its military endeavors.	
12.1	Congress should reaffirm its constitutional obligation by evaluating the nation's national security objectives and military strategy by passing an updated AUMF.	
13	To incorporate the technology necessary to maintain the United States' military supremacy, the Pentagon must continue refining its acquisition process to be more agile and less risk averse so that it can fully leverage emerging technologies and capabilities at scale.	
13.1	Review defense acquisition regulations to make them less onerous, particularly for non-traditional entities seeking to partner with DoD	
13.2	Train and incentivize the acquisition workforce to utilize existing flexible authorities to quickly push innovative technology to warfighters in the field.	
13.3	Incentivize calculated risk by providing funding for emerging technologies through programs of record at scale; allow a less-than-perfect success rate.	
13.4	Significantly increase opportunities for operators in the field, the acquisition force, program managers, and industry to partner and work together to more quickly develop requirements and identify solutions.	
13.5	Structure the acquisition process, particularly for programs heavily dependent on software and technology, to be continuous and more closely aligned with the iterative process used to develop software and emerging technologies.	
13.6	Employ the Air Force "Kessel Run" model, which works directly with operational units for rapid development and field testing.	
14	To thwart emerging threats and compete with adversaries who seek to undermine the United States beyond military realms to include economic, information, and political domains, the nation should reconfigure a coordinated, whole-of-government strategy to update the national security structure, which was established in the 1940's primarily to focus on the rise of communism. This reimagination of the national security structure would partner the Department	

	of State with the Department of Defense to ensure diplomatic parity and leadership.	
14.1	The State Department should lead the nation's whole-of-government effort, and its funding and staffing should be exponentially increased to reflect its expanded role and prominence. Congress should allocate funding to hire additional foreign service officers and expand the Global Engagement Center to counter foreign propaganda and misinformation.	
14.2	Congress should commission a varied group of national security experts and practitioners to undertake a wide-ranging review of the national security structure and strategy for adapting and restructuring them to incorporate new technologies and operational concepts and thus compete in the 21st century.	

EVALUATION OF PROGRESS ON RECOMMENDATIONS

Note: This section explores various pieces of legislation that address aspects of the Task Force's recommendations. Mention of any specific bill is not an endorsement by either of the authors.

Recommendation 1

Using the Manhattan Project as a model, the United States must undertake and win the artificial intelligence race by leading in the invention and deployment of AI while establishing the standards for its public and private use. Although the Department of Defense has increased investment in AI and established the Joint Artificial Intelligence Center to assist with the transition and deployment of AI capabilities, cultural resistance to its wider adoption remains. Congress and the Department of Defense must take additional action to overcome these barriers.

1.1 - Require every Major Defense Acquisition Program to evaluate at least one AI or autonomous alternative prior to funding

Starting Implementation - Section 246⁹ of the FY22 NDAA requires a report on autonomy integration in major weapon systems. This report demonstrates a continued Congressional interest in technological weapon systems integration and encourages DoD to further integrate autonomy and AI into its systems.

1.2 - Require all new Major Defense Acquisition Programs to be AI-ready and nest with existing and planned joint all-domain command and control (JADC2) networks

No Implementation - While Congress fully expects DoD to make Major Defense Acquisition Programs compatible with AI and JADC2,¹⁰ there are no current proposals in Congress to make this a requirement.

1.3 - Expand DoD's authorities and abilities to evaluate high technology readiness level items and technologies that satisfy defense requirements to reduce risk for major acquisition programs, lower procurement costs, and accelerate the fielding of critical capabilities

Partial Implementation - Section 836¹¹ of the FY22 NDAA requires the Undersecretary of Defense for Acquisition and Sustainment to recruit software development professionals to work in acquisition and sustainment. This step would improve the Department's ability to identify, evaluate, and acquire technologies reliant on software, but the Department is still weighed down by slow and outdated

⁹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 246 - Report on Autonomy Integration in Major Weapon Systems* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹⁰ John R. Hoehn, *Joint All-Domain Command and Control (JADC2)*, Congressional Research Service (Jul. 1, 2021) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11493>)

¹¹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 836 - Cadre of Software Development and Acquisition Experts* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

acquisition processes that slow down the fielding of critical capabilities and must examine these processes further to meet the intention of this recommendation.

Recommendation 2

Because of the United States' commitment to human rights, and to ensure those rights are enshrined in its use, the United States should lead in the formulation and ratification of a global treaty on artificial intelligence in the vein of the Geneva Conventions, the Chemical Weapons Convention, and the Nuclear Non-Proliferation Treaty to establish guardrails and protections for the civilian and military use of AI. Nations that adhere to democratic principles should lead in the creation of the global treaty, which would establish accountability, promote collaboration and transparency, ensure fairness, and limit the harmful use of AI. The treaty should further establish an international code of ethics and privacy protections that ensure personal freedoms and liberties globally, the document must be amendable to allow for advancements in technology, and the stated goal must be for all nations, especially those that are developing and employing AI, to be included as signatories.

2.1 - Create a global treaty, which would establish accountability, promote collaboration and transparency, ensure fairness, and limit the harmful use of AI

Starting Implementation - In recent years, the DoD released a set of guidelines for the ethical use of AI in defense contexts¹² that has served as a reference point for multiple efforts to shape global AI principles. The EU has recently created binding regulations on the uses of AI¹³ within the EU, and there is an opportunity for the United States to build on this effort to create transatlantic norms for AI use. Additionally, the United Nations Educational, Scientific, and Cultural Organization (UNESCO) has adopted a non-binding resolution¹⁴ on the ethics of artificial intelligence signed by 193 countries that could serve as the basis for stronger action by the UN moving forward.

Recommendation 3

The United States must ensure supply chain resiliency within both the military and civilian sectors by establishing reliable manufacturing sources and incentivizing the return of manufacturing to the homeland through fiscal policy, tax incentives, and other financial and policy measures.

3.1 - Form a National Supply Chain Intelligence Center under the Director of National Intelligence to monitor and protect US supply chain interests

¹² Joint Artificial Intelligence Center, *A Closer Look: DoD AI Ethical Principles* (Feb. 24, 2020) (online at https://www.ai.mil/blog_02_24_20-dod-ai_principles.html)

¹³ European Union Publications Office, *Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts* (2021) (online at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>)

¹⁴ UN News, *193 countries adopt first-ever global agreement on the Ethics of Artificial Intelligence* (Nov. 25, 2021) (online at <https://news.un.org/en/story/2021/11/1106612>)

No Implementation - While the National Counterintelligence and Security Center (NCSC) under the Office of the Director of National Intelligence (ODNI) has labeled supply chain threats as a critical issue similar to cybersecurity threats,¹⁵ there are no efforts at the moment to establish a National Supply Chain Intelligence Center under the ODNI.

3.2 - Identify and eliminate single points of failure within DoD supply chain

Partial Implementation - Congress and the administration have identified points of failure across DoD's supply chain, but many remain unaddressed. On February 24, 2021, President Biden issued Executive Order 14017 calling for a report on supply chain issues related to semiconductors, large capacity batteries, critical minerals and materials, and active pharmaceutical ingredients, and this report was released on June 8, 2021.¹⁶ The report identified key problems across these sectors, some of which were related to defense activities. In July 2021 the Congressional Task Force on Defense Critical Supply Chains report¹⁷ highlighted additional points of concern related to DoD supply chain security. Both reports included recommendations to Congress and the administration, many of which are in the policy-formulation or implementation process. One particularly pressing need is the recapitalization of the National Defense Stockpile¹⁸ to ensure that DoD maintains access to critical resources like rare earth materials if our overseas supply chains are interrupted.

3.3 - Bolster and expand the Information and Communications Technology Supply Chain Risk Management Task Force within the Department of Homeland Security to identify and secure the civilian supply chain equities that affect US national security interests

Full Implementation - In January 2021, the Critical Infrastructure Security Agency (CISA) extended the Information and Communications Technology and Supply Chain Risk Management Task Force for six months.¹⁹ This extension allows the task force to build upon previous working groups with the Information Sharing Working Group, such as the the Small and Medium Business Working Group, the Product Use Acceleration Working Group, and the Study Group on Lessons Learned from Recent Software Supply Chain Attacks. This will also allow the task force to cement its recommendations and set up the Critical Infrastructure Security Agency (CISA) for success in supply chain management in the future.

¹⁵ Office of the Director of National Intelligence, *Supply Chain Risk Management* (online at <https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats>)

¹⁶ White House, *Fact Sheet: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities* (June 8, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/fact-sheet-biden-harris-administration-announces-supply-chain-disruptions-task-force-to-address-short-term-supply-chain-discontinuities/>)

¹⁷ Congressman Mike Gallagher, *Gallagher, Slotkin Release Final Report on Defense Critical Supply Chain* (Jul. 22, 2021) (online at <https://gallagher.house.gov/media/press-releases/gallagher-slotkin-release-final-report-defense-critical-supply-chain>)

¹⁸ G. James Herrera, *National Stockpiles: Background and Issues for Congress*, Congressional Research Service (Jun. 15, 2020) (online at <https://crsreports.congress.gov/product/pdf/IF/IF11574>)

¹⁹ Cybersecurity and Infrastructure Security Agency, *Task Force Establishes Way Forward After Charter Extension: Year 2.5* (Mar. 4, 2021) (online at <https://www.cisa.gov/blog/2021/03/04/task-force-establishes-way-forward-after-charter-extension-year-25>)

3.4 - Strengthen the Committee on Foreign Investment in the United States (CFIUS) and the Foreign Investment Risk Review Modernization Act (FIRRMA) regulations to include additional industries relevant to AI, quantum computing, sensing, autonomy, space, and robotics

Partial Implementation - Under the Export Control and Reform Act (ECRA) that was included in the FY19 NDAA,²⁰ the Department of Commerce Bureau of Industry and Security (BIS) was directed to define what “emerging and foundational technologies” would be subject to control under CFIUS and FIRRMA. In early 2020, BIS published a list²¹ of six emerging technologies including sub-orbital aircraft and additive manufacturing. Later that year, BIS published an advanced notice of proposed rules²² concerning foundational technologies that will be subject to CFIUS and FIRRMA controls, and this list of foundational technologies is expected to be announced soon. To continue progress on this recommendation, the Departments of Commerce, Defense, Homeland Security, and other relevant stakeholders must work to share information about threats and bad actors with the private sector in a timely manner.

Recommendation 4

To compete against 21st century adversaries, Congress and the Department of Defense must identify, replace, and retire costly and ineffective legacy platforms. The Task Force recommends 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 studies should survey all services, agencies and entities within the Department of Defense to include hardware, weapons systems, basing, and force structure with an emphasis on agility, technology, and an expanded forward foot print, studies should make recommendations for future force structure and investment. Following completion of the studies, a panel should be convened, comprising Congress, the Department of Defense, and representatives from the industrial base to make recommendations on which platforms should be retired, replaced or recapitalized.

4.1 - Studies should survey all legacy services, agencies and entities within DoD to include hardware, weapons systems, basing, and force structure

Near Full Implementation - Section 146²³ of the FY22 NDAA requires DoD to issue and brief Congress on a legacy systems report assessing the capacity of currently fielded major weapons and legacy systems

²⁰ Library of Congress, *John S. McCain National Defense Authorization Act for Fiscal Year 2019: Sections 1741-1768 - Export Controls Act of 2018* (Aug. 13, 2018) (online at <https://www.congress.gov/bill/115th-congress/house-bill/5515>)

²¹ Industry and Security Bureau, *Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary*, Federal Register (Oct. 5, 2020) (online at <https://www.federalregister.gov/documents/2020/10/05/2020-18334/implementation-of-certain-new-controls-on-emerging-technologies-agreed-at-wassenaar-arrangement-2019>)

²² Industry and Security Bureau, *Identification and Review of Controls for Certain Foundational Technologies*, Federal Register (Oct. 27, 2020) (online at <https://www.federalregister.gov/documents/2020/08/27/2020-18910/identification-and-review-of-controls-for-certain-foundational-technologies>)

²³ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 146 - Review and Briefing on Fielded Major Weapon Systems* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

to meet future operational requirements and potential threat environments. As Congress waits for the completion of this report, it must continue to engage with DoD to evaluate the operational capabilities of legacy systems in new threat environments. Congress must also reevaluate this issue after this report is delivered.

Recommendation 5

The US homeland remains uniquely vulnerable to adversaries who are increasing their ability to wage cyberwarfare against civilian populations through attacks on infrastructure, financial institutions, and healthcare facilities, among others. The United States should prioritize cyber-attack and gray zone defense capabilities within both the Department of Defense and the private sector.

5.1 - Examine the relationship between executive branch departments and agencies with independent regulatory agencies overseeing critical infrastructure sectors to ensure that information related to cybersecurity is shared by default, rather than by exception

Partial Implementation - In recent years, the federal government has made progress reducing barriers to information sharing and improving coordination across government and critical infrastructure sectors. Section 2 of Executive Order 14028,²⁴ Improving Our Nation's Cybersecurity, ordered CISA, the FBI, and elements of the intelligence community to remove contractual barriers to cyber threat information sharing between the public and private sectors. The Joint Cyber Defense Collaborative,²⁵ stood up by CISA in 2021, will also improve information sharing between federal government and private technology and cybersecurity companies. The newly established National Cyber Director²⁶ will coordinate cybersecurity efforts between government and critical infrastructure sectors, and Congress should continue to appropriate funding for this office to ensure continued improvement in coordinated cyber threat information sharing. Despite this success, some critical infrastructure operation firms remain wary of some forms of information sharing such as breach reporting due to fears about civil liability and loss of shareholder confidence. To counter these challenges, the Senate Permanent Select Committee on Intelligence has proposed mandatory information sharing on events like cyber breaches by companies operating critical infrastructure.²⁷ This proposal has received bipartisan support, and Congress should continue to consider other mechanisms of improving information sharing across the public and private sector.

²⁴ Executive Office of the President, *Improving the Nation's Cybersecurity*, Federal Register (May 17, 2021) (online at <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>)

²⁵ Cybersecurity and Infrastructure Security Agency, *CISA Launches New Joint Cyber Defense Collaborative* (Aug. 5, 2021) (online at <https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative>)

²⁶ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 1752 - National Cyber Director* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

²⁷ Senator Mark Warner, *Following Solar Winds & Colonial Hacks, Leading National Security Senators Introduce Bipartisan Cyber Reporting Bill* (Jul. 21, 2021) (online at <https://www.warner.senate.gov/public/index.cfm/2021/7/following-solarwinds-colonial-hacks-leading-national-security-senators-introduce-bipartisan-cyber-reporting-bill>)

5.2 - Create parity between the defense industrial base and other critical infrastructure sectors by establishing an independent regulatory agency to define and enforce threat-informed cybersecurity standards through regular assessments

Starting Implementation - Each critical infrastructure sector has an affiliated Sector Risk Management Agency (SRMA),²⁸ as defined in Section 9002 of the FY21 NDAA, that defines rules for individual sectors. While this allows regulations to be tailored to a specific industry, the lack of consistent baseline requirements across sectors makes it harder to ensure that cybersecurity standards across critical infrastructure meet a minimum requirement. While CISA and the National Cyber Director coordinate and advise across critical infrastructure sectors, there is currently no federal body that clearly provides and enforces uniform standards guidance across sectors.

5.3 - Bolster the partnership between US Cyber Command (USCYBERCOM) and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, notably the operational partnership in national defense and incident response

Full Implementation - In recent years CISA and USCYBERCOM have taken steps to improve their integration and partnership through new authorities and offices. In 2021, USCYBERCOM and CISA issued multiple²⁹ joint cybersecurity advisories³⁰ on nation state hacking activities that demonstrated ongoing dialogue and cooperation between the two organizations. The new National Cyber Director³¹ leading inter-agency cybersecurity coordination can play a key role in further integration of USCYBERCOM's national defense role and CISA's incident response role. Section 1513³² of the FY22 NDAA establishes a DoD report on their information-sharing measures with CISA regarding critical infrastructure threats, and Congress must continue to conduct oversight on both CISA and USCYBERCOM to ensure that this integration and cooperation continues. Additionally, the DoD and DHS have multiple memorandums of understanding to improve information sharing and personnel sharing, but a recent DHS Inspector General report found that the implementation of these memorandums fell short of their ideal outcomes, suggesting that there is still more progress to be made.³³

²⁸ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 9002 - Sector Risk Management Agencies* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

²⁹ Cybersecurity and Infrastructure Security Agency, *CISA, Treasury, FBI And USCYBERCOM Release Cyber Alert on Latest North Korea Bank Robbing Scheme* (Aug. 26, 2020) (online at <https://www.cisa.gov/news/2020/08/26/cisa-treasury-fbi-and-uscibercom-release-cyber-alert-latest-north-korea-bank>)

³⁰ United States Cyber Command, *US Cyber Command, DHS-CISA Release Russian Malware Samples Tied to Solar Winds Compromise* (Apr. 15, 2021) (online at <https://www.cybercom.mil/Media/News/Article/2574011/us-cyber-command-dhs-cisa-release-russian-malware-samples-tied-to-solarwinds-co/>)

³¹ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 1752 - National Cyber Director* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

³² Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1513 - Report on Potential Department of Defense Support and Assistance for Increasing the Awareness of the Cybersecurity and Infrastructure Security Agency of Cyber Threats and Vulnerabilities Affecting Critical Infrastructure* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

³³ Office of the Inspector General, *DHS Needs Additional Oversight and Documentation to Ensure Progress in Joint Cybersecurity Efforts*, Department of Homeland Security (Nov. 17, 2021) (online at <https://www.oig.dhs.gov/sites/default/files/assets/2021-11/OIG-22-06-Nov21.pdf>)

5.4 - Develop tactical cyber operational forces within all military services to integrate them into conventional kinetic operations to foster interoperability between conventional operational activities and cyberspace activities

Starting Implementation - USCYBERCOM currently conducts the majority of cyber operations for the armed services. Since authority to deploy offensive cyber capabilities still remains in the hands of the president and senior officers, integration and interoperability between cyber and conventional activities at the tactical level remains limited to activities like intelligence support. Section 1505³⁴ to the FY22 NDAA begins to address this problem by defining new roles and responsibilities for cyber operations integration in DoD and a number of combatant commands.

5.5 - Ensure that DoD recruits and fosters a technologically astute workforce that can develop and procure the requisite capability to mitigate potential vulnerabilities

Partial Implementation - The past two NDAs included provisions to ensure that DoD has an effective, technologically astute workforce in critical fields like cybersecurity. Sections 9403 and 9404³⁵ of the FY21 NDAA update Congressional guidance and requirements on the successful CyberCorps Scholarship-for-Service program designed to train and hire cybersecurity students into federal agencies, including DoD. The FY22 NDAA includes Section 1506,³⁶ which requires DoD to conduct a number of cybersecurity personnel reports, and Section 909,³⁷ which appoints a Chief Digital Recruiting Officer within DoD to oversee the recruitment of civilians with programming, computer science, and other related backgrounds. These measures build upon previous efforts to improve hiring of a technologically sophisticated workforce such as the establishment of excepted service for cyber positions in the FY16 NDAA.³⁸ While these requirements are a step in the right direction, the Department must continue to focus on recruiting technical talent with the support of Congress.

5.6 - Create tax and other financial incentives for the private sector to invest in cybersecurity and prepare for gray zone attacks

No Implementation - While there are a handful of financial incentives provided for specific sectors and locales, there are no tax or financial incentives that apply broadly across the private sector. The Federal Energy Regulatory Commission (FERC) recently issued a Notice of Proposed Rulemaking³⁹ that would establish incentives to invest in cybersecurity beyond the minimum standards required by FERC. Pursuant

³⁴ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1505 - Operational Technology and Mission-Relevant Terrain in Cyberspace* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

³⁵ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 9403 - Modifications to Federal Cyber Scholarship-for-Service Program, Section 9404 - Additional Modifications to Federal Cyber Scholarship-for-Service Program* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

³⁶ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1506 - Matters Concerning Cyber Personnel Requirements* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

³⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 909 - Digital Talent Recruiting Officer* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

³⁸ Library of Congress, *National Defense Authorization Act for Fiscal Year 2016, Section 1107 - United States Cyber Command Workforce* (Nov. 25, 2015) (online at *National Defense Authorization Act for Fiscal Year 2016*)

³⁹ Federal Energy Regulatory Commission, *Cybersecurity Incentives*, Federal Register (Feb. 5, 2021) (online at <https://www.federalregister.gov/documents/2021/02/05/2021-01986/cybersecurity-incentives>)

to Executive Order 13636⁴⁰ in 2013, the Department of the Treasury⁴¹ and the Department of Commerce⁴² decided not to explore tax incentives due to the difficulty of targeting incentives and potential effectiveness concerns. Instead, they recommended bolstering the private cyber insurance industry through the adoption of rigorous standards and frameworks to underwrite insurance policies. The Department of Treasury and Department of Commerce should reconsider these analyses as the cybersecurity threat landscape has significantly changed since 2013.

Recommendation 6

Because an engaged and informed electorate is essential for a republic to endure, the United States should expand voluntary National Service programs. Promoting volunteerism and active engagement in democracy bolsters our national security through participation and shared experiences.

6.1 - Integrate military, national, and public service to create interoperability within these sectors to promote expansion of National Service programs

No Implementation - Veterans display a preference for national service jobs and professional pipelines from AmeriCorps and the Peace Corps, creating informal links across the three sectors, but no further cross-sector integration has been formally implemented or proposed since the Future of Defense Task Force Report was released.

6.2 - Initiate paid, year-of-service programs with civilian, military, and private-sector pathways for youth to promote expansion of National Service programs

No Implementation - Paid, year-of-service programs currently exist for specific sectors like the AmeriCorps program for education, the Peace Corps program for international development, and the US Digital Service program for technology in government. However, no new programs have been proposed since the Future of Defense Task Force Report was released.

6.3 - Incentivize service through student loan deferment and forgiveness

Starting Implementation - Several national service and student loan forgiveness programs currently exist, particularly for veterans. Beyond those existing programs, there are a number of proposals to strengthen and expand these programs that need to be passed into law. The Segal AmeriCorps Education

⁴⁰ President Barack Obama, *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity*, White House (Feb 12, 2013) (online at <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>)

⁴¹ United States Treasury Department, *Summary Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636* (2013) (online at [https://www.treasury.gov/press-center/Documents/Treasury%20Report%20\(Summary\)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf](https://www.treasury.gov/press-center/Documents/Treasury%20Report%20(Summary)%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf))

⁴² United States Commerce Department, *Discussion Of Recommendations To The President On Incentives For Critical Infrastructure Owners And Operators To Join A Voluntary Cybersecurity Program* (2013), (online at https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf)

Award Tax Relief Act, S. 2075⁴³ would ensure that AmeriCorps educational rewards wouldn't count in taxable income and provide a much-needed tax break. Additionally, the National Service GI Bill Act, H.R. 5829,⁴⁴ introduced during the drafting of the Future of Defense Task Force Report, would allow AmeriCorps volunteers to pay in-state tuition in the states where they served. Finally, the GI Restoration Act, H.R. 5905⁴⁵ would provide national service benefits to the descendants of African-American veterans of WW2 who were historically denied access to these benefits. Congress must prioritize the passage of these acts to improve public service incentivization.

6.4 - Create mentorship and apprentice opportunities within national service programs

Starting Implementation - Congress has put forward a handful of proposals to create mentorship and apprenticeship opportunities within national service programs, and should continue to explore further options to expand on and add to existing proposals. One notable proposal is S. 2274,⁴⁶ the Federal Cybersecurity Workforce Expansion Act, which gives CISA the authority to establish apprenticeship programs related to cybersecurity within the agency in an effort to expand the cybersecurity workforce within the federal government. This bill is an excellent model for future efforts to create apprenticeship programs within the federal government and other national service programs.

6.5 - Encourage civics and personal citizenship curricula in public schools to promote participation in National Service programs

Starting Implementation - A recent survey by the University of Pennsylvania⁴⁷ found that only 56% of American adults could correctly name the three branches of government, highlighting the critical importance of civic education for the American people. While civics and personal citizenship education is a long-term problem that is difficult to address in the short time since the release of the Future of Defense Task Report, some proposals are up for consideration. The Teaching Engaged Citizenship Act, H.R. 5288,⁴⁸ would expand federal civic education grants, establish an Office of Civic Education within the Department of Education, and require frequent administration of the National Assessments of Education Progress for civics similar to reading and mathematics assessments. The Civics Learning Act, H.R. 400,⁴⁹ would expand the scope and size of existing Department of Education grants programs to teach civics in public schools.

Recommendation 7

⁴³ Library of Congress, Segal AmeriCorps Education Award Tax Relief Act of 2021 (Jun. 16, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/2075>)

⁴⁴ Library of Congress, The National Service GI Bill Act (Feb. 10, 2020) (online at <https://www.congress.gov/bill/116th-congress/house-bill/5829>)

⁴⁵ Library of Congress, Sgt. Isaac Woodard, Jr. and Sgt. Joseph H. Maddox GI Bill Restoration Act of 2021 (Nov. 5, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/5905>)

⁴⁶ Library of Congress, *Federal Cybersecurity Workforce Expansion Act* (Nov. 3, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/2274>)

⁴⁷ Annenberg Public Policy Center, *Annenberg Civics Knowledge Survey*, University of Pennsylvania (2021) (online at <https://www.annenbergpublicpolicycenter.org/political-communication/civics-knowledge-survey/>)

⁴⁸ Library of Congress, *Teaching Engaged Citizenship Act of 2021* (Sep. 20, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/5288>)

⁴⁹ Library of Congress, *Civics Learning Act of 2021* (Jan. 21, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/400>)

To maintain its global preeminence in scientific and technological innovation and the associated economic and military advantage, the United States should increase its investment in foundational science and technology research by committing to spending at least one percent of the country's gross domestic product on basic government-supported research and development.

7.1 - The Pentagon should increase funding for science and technology research programs to meet the 3.4 percent of the overall defense budget recommended by the Defense Science Board

Partial Implementation - The FY22 NDAA⁵⁰ increased funding for basic research, applied research, and advanced technology development across the Department to 2.23% of the total budget (\$16.56 billion). This is incrementally higher than the 2.1% (\$14.65 billion) in FY21⁵¹ and 2.07% (\$14.63 billion) in FY20,⁵² but still falls below the recommended 3.4%.

7.2 - Expand funding for historically successful innovation efforts such as Defense Advanced Research Projects Agency, the national and defense research laboratories, and university partnerships

Full Implementation - The FY22 NDAA authorized \$4.56 billion⁵³ for DARPA, an increase from the \$3.57 and \$3.50 billion authorized in the FY20 and FY21 NDAAs.⁵⁴ It also allocated \$663 million⁵⁵ for University Research Initiatives, National Defense Education Programs, and funding for defense research at HBCUs and minority-serving institutions above the \$531 million in FY21⁵⁶ and \$535 million in

⁵⁰ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁵¹ Library of Congress, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Title XLII - Research, Development, Test, and Evaluation Funding Tables (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

⁵² Library of Congress, *National Defense Authorization Act for Fiscal Year 2020: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/senate-bill/1790>)

⁵³ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁵⁴ Department of Defense, *Department of Defense Fiscal Year (FY) 2022 Budget Estimates, Defense Advanced Research Projects Agency, Defense-Wide Justification Book Volume 1 of 5, Research, Development, Test & Evaluation, Defense-Wide* (May 2021) (online at https://www.darpa.mil/attachments/DARPA_PB_2022_19MAY2021_FINAL.pdf)

The FY20 and FY21 figures were taken directly from the cited justification book. The FY22 figure was calculated using the budget lines in the cited justification book and the associated changes to those budget lines made by Congress before the passage of the National Defense Authorization Act for Fiscal Year 2022.

⁵⁵ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁵⁶ Library of Congress, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Title XLII - Research, Development, Test, and Evaluation Funding Tables (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

FY20.⁵⁷ Congress should continue to increase funding for these critical efforts to ensure US military access to cutting edge research in critical areas.

7.3 - Require the military services to spend at least one percent of their overall budgets on the integration of new technologies

Near Full Implementation - In the FY22 NDAA, the DoD requested approximately \$112 billion for Research, Development, Testing, and Evaluation (RDT&E) which was a 5% increase over the enacted FY21 level and was the largest such request for RDT&E historically.⁵⁸ Going by service, the Air Force requested \$28.8 billion for RDT&E which included significant growth for the Air Force's Advanced Battle Management System, the Air Force's main program to connect and improve information sharing between aircraft and command and control nodes.⁵⁹ The Navy requested \$22.6 billion for RDT&E, \$2.5 billion more than FY21, and included a \$1.3 billion request for conventional prompt strike hypersonics research.⁶⁰ The Space Force requested \$11.3 billion for RDT&E⁶¹ which included a threefold increase⁶² for RDT&E funding for the Space Development Agency. While the Army saw a \$4 billion decrease in RDT&E funding consistent with an overall decrease in funding, it maintained support for its signature programs such as long-range precision fires.⁶³ Overall, the DoD and the services have significantly increased funding for RDT&E which will improve the military's ability to integrate new technologies.

7.4 - Establish target funding levels with defense allies for investment in science and technology research

Partial Implementation - While there has been no discussion on establishing target funding levels for science and technology research with defense allies, there have been several recent developments and proposals to improve international technology partnerships. The AUKUS partnership⁶⁴ between the US, UK, and Australia, while mainly focused on providing conventionally-armed nuclear-powered submarines, also promotes technology cooperation by including partnership on technologies ranging from AI to quantum computing.⁶⁵ This could be used as a template for broader science and technology research cooperation initiatives with like-minded countries. Additionally, Congress has introduced the Democracy

⁵⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2020: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/senate-bill/1790>)

⁵⁸ Jackson Barnett, *DOD Asks for \$112B in R&D Funding in Budget Request*, FedScoop (May 28, 2021) (online at <https://www.fedscoop.com/dod-research-and-development-budget-request-fy-22/>)

⁵⁹ John Tirpak, *Air Force Budget Seeks Addition by Subtraction*, Air Force Magazine (Jun. 30, 2021) (online at <https://www.airforcemag.com/article/world-18/>)

⁶⁰ Christopher Cavas, *Fleet Growth Stymied by Navy Budget Request*, United States Naval Institute (May 28, 2021) (online at <https://news.usni.org/2021/05/28/fleet-growth-stymied-by-fiscal-year-2022-navy-budget-request>)

⁶¹ Stew Magnuson, *Budget 2022: Space Force Prioritizes R&D Replacing Vulnerable Systems*, National Defense Magazine (May 28, 2021) (online at <https://www.nationaldefensemagazine.org/articles/2021/5/28/space-force-prioritizes-rd-replacing-vulnerable-systems>)

⁶² John Tirpak, *Air Force Budget Seeks Addition by Subtraction*, Air Force Magazine (Jun. 30, 2021) (online at <https://www.airforcemag.com/article/world-18/>)

⁶³ US Army Public Affairs, *Army Releases Fiscal Year 2022 Budget Proposal* (May 28, 2021) (online at https://www.army.mil/article/246996/army_releases_fiscal_year_2022_budget_proposal)

⁶⁴ White House, *Joint Leaders Statement on AUKUS* (Sep. 15, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/>)

⁶⁵ Arzan Tarapore, *AUKUS is Deeper Than Just Submarines*, Stanford University - Freeman Spogli Institute of International Studies (Sep. 29, 2021) (online at <https://fsi.stanford.edu/news/aukus-deeper-just-submarines>)

Technology Partnership Act,⁶⁶ which would create an International Technology Partnership Office and an International Technology Partnership Fund within the State Department and the Treasury Department, respectively. These steps will facilitate technological defense partnerships and coordinated funding levels with our allies going forward.

Recommendation 8

To maintain its technological advantage over competitors, the Pentagon must continue to improve its ability to leverage private sector innovation at scale, including that from non-traditional companies, recognizing that the private sector, not the government, is now the leader in research and development investment.

8.1 - Increase funding for successful innovation efforts such as the Defense Innovation Unit, AFWERX, Army Futures Command, and others that successfully bridge the gap between innovative organizations and the military ten-fold, and robustly fund established drivers of innovation within DoD

Partial Implementation - DoD has increased its funding for some innovative organizations, but has decreased funding for others. The FY22 NDAA authorized \$31.8 million⁶⁷ for the Defense Innovation Unit, which is an increase over the FY21⁶⁸ and FY20⁶⁹ authorizations of \$26.1 million and \$29.3 million, respectively. On the other hand, the FY22 NDAA only authorized \$14.7 million for AFWERX, a decrease from the FY20 spending level of \$20.1 million.⁷⁰ Overall, DoD needs to invest more into these programs to fully institutionalize these capabilities.

8.2 - Restore DoD Rapid Innovation Fund, which was authorized in FY11, to assess, fund, and accelerate innovative technology solutions for the warfighter

Full Implementation - The FY22 NDAA authorizes \$75 million for the Rapid Innovation Program,⁷¹ which was inspired by the Rapid Innovation Fund. Going forward, Congress should continue to fund the

⁶⁶ Library of Congress, *Democracy Technology Partnership Act* (May 20, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/3426>)

⁶⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

⁶⁸ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

⁶⁹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2020: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/senate-bill/1790>)

⁷⁰ The AFWERX budget in FY21 was transferred to Operations & Maintenance and did not get a line number in the FY21 Justification Books. FY20 funding here: Department of Defense, *Department of Defense Fiscal Year (FY) 2022 Budget Estimates, Air Force Justification Book Volume 2 of 3 Research, Development, Test & Evaluation, Air Force* (May 2021) (online at https://www.saffm.hq.af.mil/Portals/84/documents/FY22/RDTE_FY22%20DAF%20J-Book%20-%203600%20-%200AF%20RDT%20and%20E%20Vol%20II.pdf?ver=KpJJbVq68o32dSvkjuv_Iw%3d%3d)

⁷¹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

Rapid Innovation Program and similar programs that aim to assess, fund, and accelerate innovative technology solutions for the warfighter.

8.3 - Create additional opportunities for collaboration and shared experience between DoD, private sector, and academia through the expansion of programs such as Hacking for Defense and partnerships with groups such as the Silicon Valley Defense Working Group

Partial Implementation - DoD has made some progress expanding its partnerships with the private sector, and academia. Section 219 of the FY21 NDAA⁷² established new activities within the Department to better partner with academia and private organizations like Hacking for Defense using existing authorities. Nonprofit groups like the Silicon Valley Defense Working Group (SVDG) continue to engage effectively with both DoD and Congress including, notably, a reaction and recommendations for implementation⁷³ of the Future of Defense Task Force Report. These efforts and organizations are commendable and should continue to receive the cooperation and support of DoD and Congress.

Recommendation 9

To sustain the world order that has allowed the United States to prosper and thrive for more than 70 years, the United States must foster new and creative partnerships for a changing world while strengthening existing alliances and security agreements. Such engagements will further vital US national security interests by ensuring placement, access, resiliency and redundancy while creating complex problem sets for adversaries.

9.1 - Enhance essential partnerships with North Atlantic Treaty Organization (NATO) and FiveEyes intelligence partners, Canada, United Kingdom, Australia, and New Zealand— as well as with Japan and South Korea

Near Full Implementation - As the US shifts its national security focus away from the Middle East and towards the Indo-Pacific, significant steps have been taken to improve our alliances with the Five Eyes, Japan, and South Korea. Most notably, the AUKUS⁷⁴ partnership announced in September 2021 between Australia, the UK, and the US will provide conventionally-armed, nuclear-powered submarines to Australia and enhance defense, technology, and economic cooperation. We must further strengthen America's alliances in the region by improving trilateral defense and security cooperation between the US, Japan, and South Korea. Additionally, Russia's invasion of Ukraine demonstrated the critical role of NATO in defending the security of Europe. The United States must continue to demonstrate its commitment to NATO through investments and policy going forward.

9.2 - Develop a modern Western Hemisphere policy that protects US Latin and Central American interests and alliances while simultaneously expanding a robust Arctic Strategy

⁷² Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 219 - National Security Innovation Partnerships* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

⁷³ Silicon Valley Defense Group, *SVDG Reaction: The Future of Defense Task Force Report* (2020) (online at <https://www.siliconvalleydefense.org/current-initiatives/svdg-reaction-the-future-of-defense-task-force-report>)

⁷⁴ White House, *Joint Leaders Statement on AUKUS* (Sep. 15, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/>)

Near Full Implementation - Since September 2020, there have been several Western Hemispheric policy reforms focused on Latin and Central America and the Arctic. The Biden administration targeted humanitarian aid through USAID and the USDA⁷⁵ and fostered private sector partnerships⁷⁶ in the Northern Triangle region and Central America. Since the release of DoD's Arctic strategy in June 2019,⁷⁷ the Army,⁷⁸ Navy,⁷⁹ and Air Force⁸⁰ have also outlined their specific roles and defense strategies in the region. DoD should continue to iterate on its policies related to these regions in the context of great power competition and regional security goals.

9.3 - Bolster ties with allies in the Middle East, notably Israel and Jordan

Near Full Implementation - The US has continued to improve ties with critical partners in the Middle East to counter violent extremism and establish a united front against an increasingly assertive Iran. The Abraham Accords,⁸¹ which the US helped broker and continues to support, opened the door to the normalization of relations between Israel and Morocco, Bahrain, and the United Arab Emirates. The United States should continue to build on this agreement to normalize relations between Israel and the other Gulf countries, increase regional counter-terrorism cooperation, and mitigate the actions of Iran. Congress also maintains a close security relationship with Israel, demonstrated by recent actions like the replacement of Israeli Iron Dome missile interceptors in September 2021.⁸²

9.4 - Strengthen relations with longstanding Asian security partners such as Thailand, the Philippines, Taiwan, and Singapore while growing relationships with India, Vietnam, Indonesia and Malaysia, among others

Near Full Implementation - As the United States shifts its strategic focus towards the Indo-Pacific, we have improved our relations with our regional allies and partners. In 2021, the Philippines restored our Visiting Forces Agreement⁸³ following a diplomatic visit led by Secretary Austin. Vice President Harris

⁷⁵ White House, *Fact Sheet: Urgent Relief to Central America* (Apr. 26, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/26/fact-sheet-urgent-relief-to-central-america/>)

⁷⁶ White House, *Fact Sheet: Vice President Harris Launches a Call to Action to the Private Sector to Deepen Investment in the Northern Triangle* (May 27, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/27/fact-sheet-vice-president-harris-launches-a-call-to-action-to-the-private-sector-to-deepen-investment-in-the-northern-triangle/>)

⁷⁷ Department of Defense, *Report to Congress Department of Defense Arctic Strategy* (Jun. 2019) (online at <https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF>)

⁷⁸ United States Army, *Army Announces Release of Arctic Strategy* (Mar. 16, 2021) (online at https://www.army.mil/article/244261/army_announces_release_of_arctic_strategy)

⁷⁹ United States Navy, *Department of the Navy Releases Strategic Blueprint for a Blue Arctic* (Jan. 5, 2021) (online at <https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2463000/departments-of-the-navy-rel-eases-strategic-blueprint-for-a-blue-arctic/>)

⁸⁰ United States Air Force, *Department of the Air Force Arctic Strategy* (Jul. 21, 2020) (online at <https://www.af.mil/Portals/1/documents/2020SAF/July/ArcticStrategy.pdf>)

⁸¹ State Department, *The Abraham Accords Declaration* (2020) (online at <https://www.state.gov/the-abraham-accords/>)

⁸² Tony Bertuca, *House Passes \$1B Iron Dome Supplemental in Lopsided Vote*, Inside Defense (Sep. 23, 2021) (online at <https://insidedefense.com/insider/house-passes-1b-iron-dome-supplemental-lopsided-vote>)

⁸³ Jim Garamone, *Philippine President Restores Visiting Forces Agreement with US*, Department of Defense (Jul. 30, 2021) (online at <https://www.defense.gov/News/News-Stories/Article/Article/2713638/philippine-president-restores-visiting-forces-agreement-with-us/>)

has recently visited Singapore and Vietnam⁸⁴ with a focus on improving our regional diplomatic and economic ties. Although the Taiwan Relations Act restricts the actions of the administration in mitigating increased Chinese aggression towards Taiwan, recent congressional visits⁸⁵ have served as a signal of our support of Taiwan. Additionally, recent meetings between President Biden and Prime Minister Modi of India⁸⁶ allow for future coordination between our nations, especially the mitigation of an increasingly aggressive China and violent extremism in Taliban-ruled Afghanistan. We must continue to strengthen these relationships to counteract the growing Chinese sphere of influence.

9.5 - Cultivate economic and diplomatic cooperation with non-traditional allies, especially in Asia and Africa

Partial Implementation - The US must strengthen our global diplomatic ties beyond our traditional European and East Asian allies. The recent Summit for Democracy, which drew participation from countries across Africa, Asia, Latin America, and Eastern Europe,⁸⁷ was a good first step. However, this global campaign has been hindered by delays⁸⁸ to the Senatorial confirmation of Ambassadors to many of these countries.

9.6 - Increase foreign military sales with security partners and bolster the International Military Education and Training program following enhanced vetting

Partial Implementation - The Biden administration has not released official numbers on total foreign military sales (FMS) for FY21, but it has demonstrated its willingness to approve military sales to our treaty allies through multiple transfers executed in the last year. In addition to this, the administration is in the process of changing its guidelines for FMS to incorporate concerns about human rights into approval decisions. The amount requested and appropriated for International Military Education and Training (IMET) in State Department appropriations has remained at \$112.9 million across FY20,⁸⁹ FY21,⁹⁰ and FY22.⁹¹ The administration should continue to support FMS for countries sharing US principles and values, and increase funding for IMET.

⁸⁴ White House, *Statement from Senior Advisor and Chief Spokesperson Symone Sanders on Vice President Kamala Harris's Upcoming Visit to Singapore and Vietnam* (Jul. 30, 2021) (online at <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/30/statement-from-senior-advisor-and-chief-spokesperson-symone-sanders-on-vice-president-kamala-harris-upcoming-visit-to-singapore-and-vietnam/>)

⁸⁵ Associated Press, *US Lawmakers Meet with Taiwan's President in a Surprise Visit*, National Public Radio (Nov. 26, 2021) (online at

<https://www.npr.org/2021/11/26/1059317314/us-lawmakers-meet-with-taiwan-president-in-surprise-visit>)

⁸⁶ White House, *Remarks by President Biden and Prime Minister Modi of the Republic of India Before Bilateral Meeting* (Sep. 24, 2021) (online at

<https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/09/24/remarks-by-president-biden-and-prime-minister-modi-of-the-republic-of-india-before-bilateral-meeting/>)

⁸⁷ State Department, *Summit for Democracy: Invited Participants* (2021) (online at <https://www.state.gov/participant-list-the-summit-for-democracy/>)

⁸⁸ Andrew Desiderio, *Dems Launch Talks to Break Cruz-Hawley Blockade of Biden Ambassadors*, Politico (Dec. 14, 2021) (online at <https://www.politico.com/news/2021/12/14/democrats-cruz-hawley-biden-ambassadors-524220>)

⁸⁹ Library of Congress, *Further Consolidated Appropriations Act, 2020: Division G - Title IV* (Dec. 20, 2019) (online at <https://www.congress.gov/bill/116th-congress/house-bill/1865>)

⁹⁰ Library of Congress, *Consolidated Appropriations Act, 2021: Division K - Title IV* (Dec. 27, 2020) (online at <https://www.congress.gov/bill/116th-congress/house-bill/133>)

⁹¹ Department of State, *Congressional Budget Justification Department of State, Foreign Operations, and Related Programs, Fiscal Year 2022* (2021), https://www.state.gov/wp-content/uploads/2021/05/FY-2022-State_USAID-Congressional-Budget-Justification.pdf

9.7 - Extend New START and negotiate a follow-on agreement

Partial Implementation - Shortly before its expiration, President Biden and Vladimir Putin agreed to extend New START through February 4, 2026.⁹² The US has engaged in strategic stability talks with Russia on future arms control efforts⁹³ and the US and China are starting strategic stability talks⁹⁴ with the potential to discuss arms control in future meetings. However, China's recent buildup of their nuclear forces,⁹⁵ Russia's buildup of their non-strategic nuclear weapons arsenal,⁹⁶ and the lack of a clear path towards trilateral arms control may limit future US/Russia/China arms control.

Recommendation 10

Recognizing that human capital is our most important asset, the United States should increase its investment in science, technology, engineering, and mathematics within the Department of Defense and foster STEM talent through a whole-of-government approach to ensure the nation's scientific and technological advantage in the public and private sectors endures.

10.1 - Invest in STEM primary education

Starting Implementation - While funding has increased for middle and high school STEM education, primary STEM education needs more investment. Congress increased funding from \$1.28 billion in FY20 to \$1.34 billion in FY21 for state Career and Technical education grants particularly for middle and high schools,⁹⁷ and there are proposals in Congress that may further increase funding in FY22 to \$1.4 to \$1.5 billion.⁹⁸ While this funding is important, more programs specifically targeted at STEM education in elementary schools are needed.

10.2 - Attract and retain foreign STEM talent to study and work in the United States through specialized visas and scholarships

Starting Implementation - There are still barriers to attracting and retaining foreign STEM talent, but several proposals in Congress aim to address these barriers. One notable proposal is H.R. 5924, the Keep

⁹² Kingston Reif and Shannon Bugos, *U.S., Russia Extend New START for Five Years*, Arms Control Association (Mar. 2021) (online at <https://www.armscontrol.org/act/2021-03/news/us-russia-extend-new-start-five-years>)

⁹³ Shannon Bugos, *U.S., Russia Establish Strategic Stability Groups*, Arms Control Association (Nov. 2021) (online at <https://www.armscontrol.org/act/2021-11/news/us-russia-establish-strategic-stability-groups>)

⁹⁴ David Brunnstrom, Michael Martina, and Tom Daly, *Biden and Xi Agree to Look at Possible Arms Control Talks - Biden Adviser*, Reuters (Nov. 17, 2021) (online at <https://www.reuters.com/business/media-telecom/biden-xi-agree-look-possible-arms-control-talks-biden-adviser-2021-11-16/>)

⁹⁵ Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2021) (online at <https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF>)

⁹⁶ Hans Kristensen and Matt Korda, *Nuclear Notebook: Russian Nuclear Weapons, 2021*, Bulletin of the Atomic Scientists (Mar. 18, 2021) (online at <https://doi.org/10.1080/00963402.2021.1885869>)

⁹⁷ Department of Education, *Fiscal Year 2022 Budget Summary* (2021) (online at <https://www2.ed.gov/about/overview/budget/budget22/summary/22summary.pdf>)

⁹⁸ American Institute of Physics, *FY22 Budget Outlook: STEM Education* (Dec. 9, 2021) (online at <https://www.aip.org/fyi/2021/fy22-budget-outlook-stem-education>)

STEM Talent Act of 2021,⁹⁹ which would exempt foreign nationals holding a masters or PhD degree in a STEM field from a US university from the immigrant visa numerical limitations. A similar proposal to exempt foreign nationals from this numerical limitation has been proposed by the National Security Commission on Artificial Intelligence¹⁰⁰ whose commissioners urged Congress to pass legislation on this issue. Simple, straightforward immigration reform targeted at this population would ensure that the US maintains access to the best STEM talent in the world.

10.3 - Improve hiring pathways and increase compensation for STEM careers at the Pentagon and in the private sector; create a military commissioning source for STEM talent

Partial Implementation - While the DoD clearly recognizes the need to increase its pool of STEM talent and has taken significant positive steps to solve this problem, this problem requires longer-term attention to fully address. A recent RAND study¹⁰¹ found that computer and information systems managers, software developers, and computer programmers in the federal government, who consist of a third of all STEM workers in the federal government, earn significantly less income annually than their private sector counterparts. To ensure the long-term sustainability of the federal government's STEM talent pool, the federal government, including DoD, must increase salaries to compete with the private sector. Each service can commission Direct Commission Officers (DCOs) up to the rank of Colonel, as authorized by the FY19 NDAA,¹⁰² differently based on needs and cultures and helps them to commission STEM talent. The Army¹⁰³ has an expansive program to recruit DCOs with expertise including IT and cybersecurity. The Marine Corps is also overhauling its personnel policies to recruit and retain more technical talent.¹⁰⁴ Some of the new proposals may allow Marines to get training and experience in the private sector or at a university after retirement, or even return to the Marine Corps at a higher rank to fill a specialized position. Long-term reforms are needed to ensure sustainable access to STEM talent.

10.4 - Streamline security clearances by beginning the vetting process in graduate school

No Implementation - The security clearance process is recognized as a familiar barrier to federal employment, especially for graduate STEM students, and the COVID-19 pandemic has negatively impacted the speed of the security clearance process even further. Despite the parameters set by the FY20 Intelligence Authorization Act stating that 90% of all secret clearances and top secretary clearances

⁹⁹ Library of Congress, *Keep STEM Talent Act of 2021* (Nov. 9, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/5924>)

¹⁰⁰ Eric Schmidt and Robert Work, Letter to the Leadership of the Senate Committee on the Judiciary, National Security Commission on Artificial Intelligence (Apr. 12, 2020) (online at https://federalnewsnetwork.com/wp-content/uploads/2021/04/STEM-Immigration-Letter_Senate-Judiciary_20210411-1.pdf)

¹⁰¹ Kathryn A. Edwards, Maria McColleston, Brian Phillips, Hannah Acheson-Field, Isabel Leamon, Noah Johnson, and Maria C. Lytell, *Compensation and Benefits for Science, Technology, Engineering, and Mathematics (STEM) Workers*, RAND Corporation (2021) (online at <https://doi.org/10.7249/RR4267>)

¹⁰² Library of Congress, *John S. McCain National Defense Authorization Act for Fiscal Year 2019: Section 501 - Repeal of Requirement for Ability to Complete 20 Years of Service by Age 62 as Qualification for Original Appointment as a Regular Commissioned Officer; Section 502 - Enhancement of Availability of Constructive Service Credit for Private Sector Training or Experience Upon Original Appointment as a Commissioned Officer* (Aug. 13, 2018) (online at <https://www.congress.gov/bill/115th-congress/house-bill/5515>)

¹⁰³ United States Army, *Direct Commissioning* (2022) (online at <https://talent.army.mil/direct-commissioning/>)

¹⁰⁴ United States Marine Corps, *Talent Management 2030* (Nov. 2021) (online at https://www.hqmc.marines.mil/Portals/142/Users/183/35/4535/Talent%20Management%202030_November%202021.pdf)

should be adjudicated within 30 and 90 days respectively,¹⁰⁵ processing for the fastest 90% of applicants is still 112 days for secret clearances and 181 days respectively for secret and top secret clearances as of Q4 2021, a rate that has slowed over the course of 2021.¹⁰⁶ As long as the lengthy security clearance process remains a major barrier to federal employment, graduate students, especially those in STEM fields, will further be incentivized to find employment in the private sector instead of public service.

10.5 - Build STEM incentives into the service academies through scholarships and curricula

Near Full Implementation - STEM education is a significant part of a cadet's or midshipman's experience at a US military academy and has evolved to include modern technical tracks like cybersecurity as part of the core curriculum in response to the intensification of the technological competition with our adversaries. The US Military Academy at West Point,¹⁰⁷ the US Naval Academy,¹⁰⁸ and the US Air Force Academy¹⁰⁹ all require students to take at least 25% of all coursework in mathematics, chemistry, biology, physics, engineering, and, more recently, cybersecurity. These academies also offer majors in STEM fields, comparable to what one would find at normal universities of similar size. The service academies should continue their focuses on STEM and encourage its students to pursue technical fields in their military careers.

10.6 - Enable and incentivize "Tour of Duty" opportunities for private sector technical talent to serve tours within DoD

No Implementation - There are currently proposals in Congress to establish civilian reserve programs, but they face opposition. The Civilian Cyber Security Reserve Act¹¹⁰ would establish a pilot program for private sector civilians with technical backgrounds to register to assist the government in a reserve capacity. It was proposed but not included in the final FY22 NDAA. Going forward, Congress must prioritize opportunities like these to increase integration of private sector technical talent into federal government.

Recommendation 11

To maintain the United States' military advantage against emerging threats, the Pentagon must refine its operational concepts by employing new technologies and methods to deter future conflicts and compete in the gray zone of hybrid warfare.

¹⁰⁵ Library of Congress, *Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020: Section 604 - Goals for Promptness of Determinations Regarding Security Clearances* (May 22, 2019) (online at <https://www.congress.gov/bill/116th-congress/house-bill/3494>)

¹⁰⁶ Lindy Kyzer, *How Long Does it Take to Process a Clearance? Q4 2021*, Cleared Jobs (Oct. 25, 2021) (online at <https://news.clearancejobs.com/2021/10/25/how-long-does-it-take-to-process-a-clearance-q4-2021/>)

¹⁰⁷ Carolann Koleci, Eileen Kowalski, and Kenneth McDonald, *STEM Education Within the West Point Experience*, *Journal of College Science Teaching* (Jul. 2021) (online at <https://www.nsta.org/journal-college-science-teaching/journal-college-science-teaching-julyaugust-2021/stem-education>)

¹⁰⁸ United States Naval Academy, *Course Requirements - Core* (2022) (online at <https://www.usna.edu/Academics/Majors-and-Courses/Course-Requirements-Core.php>)

¹⁰⁹ United States Air Force Academy, *Core Curriculum* (2022) (online at <https://www.usafa.edu/academics/core-curriculum/>)

¹¹⁰ Library of Congress, *Civilian Cyber Security Reserve Act* (Apr. 29, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/2894>)

11.1 - The Pentagon, Congress, and the Intelligence Community should work in tandem to identify trends and threats 10 to 30 years beyond the normal budget cycle while expanding entities within their respective organizations to incorporate long-term planning

Partial Implementation - Congress has passed strategies for the organization and long-term planning in key areas, including technology, within DoD, Congress, and the Intelligence Community, but more comprehensive reform is necessary. The FY22 NDAA includes a National Defense Science and Technology Strategy¹¹¹ that DoD must create and update alongside the National Defense Strategy. Among other requirements, the strategy must address the Department's short-term, mid-term, and long-term priorities, goals, and investments and coordinate with other government agencies, including the intelligence community. These strategies are a sign of progress, but long-term comprehensive reform is needed to ensure that Congress, DoD, and the intelligence community are coordinating their efforts and can effectively address long-term issues.

11.2 - DoD should adhere to a whole-of-government approach and work with other departments such as State and Treasury to develop and execute a comprehensive strategy to compete in the gray zone

Partial Implementation - DoD has integrated a whole-of-government approach into some of its strategy development, and must continue to drive that approach into implementation of those strategies. The National Defense Strategy (NDS) will base US strategy on integrated deterrence¹¹² or the integration of all instruments of national power to deter adversaries, including those under the State and Treasury departments. This includes traditional domains such as air, sea, and land and non-traditional domains such as cyber, space, information, and other gray zone domains below the level of armed conflict.¹¹³ The administration needs to release an updated NDS to guide the integrated deterrence framework as well as organize the administration around the operationalization of this strategy, and should ensure that the NDS drafting and implementation includes close coordination with Departments of State and Treasury.

11.3 - Create a task force to ensure a diverse group of stakeholders, including Congress, academia, think tanks, and the private sector are engaged in developing imaginative solutions to emerging military challenges and in assessing the Pentagon's efforts

Starting Implementation - DoD has identified some key barriers to innovation and progress, but has not yet stood up a task force that would look holistically at the emerging challenges facing the Department. One area where DoD and Congress have made progress is with the Commission on Planning,

¹¹¹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 211 - Codification of National Defense Science and Technology Strategy* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹¹² Jim Garamone, *Concept of Integrated Deterrence Will Be Key to National Defense Strategy*, DOD Official Says, Department of Defense (Dec. 8, 2021) (online at <https://www.defense.gov/News/News-Stories/Article/Article/2866963/concept-of-integrated-deterrence-will-be-key-to-national-defense-strategy-dod-o/>)

¹¹³ Terry Moon Cronk, *DOD Official Outlines 2022 National Defense Strategy in CNAS Forum*, Department of Defense (online at <https://www.defense.gov/News/News-Stories/Article/Article/2869837/dod-official-outlines-2022-national-defense-strategy-in-cnas-forum/>)

Programming, Budgeting, and Execution Reform that was established in the FY22 NDAA.¹¹⁴ The commission will be made up of civilians not employed by the federal government with subject matter expertise appointed by the Secretary of Defense, bipartisan congressional leadership, and bipartisan leadership of the Armed Services and Defense Appropriations committees. The Commission will write a report evaluating how DoD's planning, programming, budgeting, and execution process meets current and future defensive threat requirements. While this is encouraging progress, Congress, the administration, academia, think tanks, and the private sector must work more closely together to comprehensively review the Pentagon's efforts on emerging military challenges beyond budgeting and acquisition challenges.

11.4 - Increase funding for wargaming and large-force joint exercises to assess new operational concepts; increase prototyping and testing with the emerging technologies needed to underpin these concepts

Full Implementation - As DoD's use of emerging technologies and associated operational concepts matures, efforts and budgets to prototype, test, and wargame have increased to meet those needs. On prototyping and testing, the FY22 NDAA significantly increased funding for Advanced Component Development and Prototyping¹¹⁵ when compared to previous years. Specifically, the FY22 NDAA authorized spending of \$32.27 billion (4.36% of the total budget), in comparison to \$27.37 billion (3.93%) and \$26.72 billion (3.79%) in FY21¹¹⁶ and FY20.¹¹⁷ DoD has significantly enhanced its abilities to prototype, test, and wargame with emerging technologies and new operational concepts, and should continue to invest in those capabilities going forward.

11.5 - Prioritize the development and procurement of critical capabilities for future conflict models such as resilient command and control networks, logistics capabilities and the defense of forward and expeditionary basing

Near Full Implementation - DoD is investing heavily in and prioritizing the procurement of an array of critical capabilities that are essential for succeeding in future conflicts. For example, JADC2 focuses on the improvement of military capability networks in preparation for a future conflict and is beginning to move out of the development phase and into the implementation phase in 2022.¹¹⁸ Another example is the rocket cargo program which is an early phase research and development project to create rockets capable of transporting many tons of cargo in contested logistics environments. The FY22 NDAA authorized \$47.9 million as requested in the President's budget¹¹⁹ which is significantly higher than the FY21

¹¹⁴ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1004 - Commission on Planning, Programming, Budgeting, and Execution Reform* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹¹⁵ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹¹⁶ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

¹¹⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2020: Title XLII - Research, Development, Test, and Evaluation Funding Tables* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/senate-bill/1790>)

¹¹⁸ Andrew Eversden, *It's 'delivery time' on JADC2: 2022 Preview*, Breaking Defense (Dec. 30, 2021) (online at <https://breakingdefense.com/2021/12/its-delivery-time-on-jadc2-2022-preview/>)

¹¹⁹ Department of Defense, *Fiscal Year (FY) 2022 Budget Estimates, Air Force, Justification Book Volume 1 of 3, Research, Development, Test & Evaluation, Air Force* (May 2021) (online at https://www.saffm.hq.af.mil/Portals/84/documents/FY22/RDTE_/FY22_PB_RDTE_Vol-I.pdf)

authorization of \$9.7 million for this. Other examples of DoD programs focused on these issues include long-range precision fires,¹²⁰ which include a broad portfolio of surface-to-surface missiles including hypersonics that will be able to quickly and accurately hit a target beyond 300km. DoD says that it is on track to test and produce an initial capability by the mid-2020s.¹²¹ The Marine Corps has conducted a number of exercises in expeditionary basing¹²² and planned future exercises with allies in the Indo-Pacific¹²³ to investigate viability and improve this operational capability. These programs demonstrate a widespread commitment to and resourcing of capabilities that will set the Department up for success against future threats.

11.6 - Invest in programs of record to directly support emerging operational concepts

Partial Implementation - Congress has authorized DoD to establish new programs of record to support innovation and identify lessons for fielding rapid solutions to future critical problems. The FY22 NDAA establishes a pilot program to accelerate the procurement and fielding of emerging technologies so that, in the future, DoD can rapidly develop and deploy innovative technologies to support new operational concepts and critical defense missions.¹²⁴ The FY22 NDAA also creates a pilot program to evaluate possible improvements to DoD's rapid procurement of capabilities with cross-service operational needs.¹²⁵ It selects projects that meet these criteria and uses their development and fielding process to identify lessons to improve mission outcomes and internal processes. Congress should create other authorities and requirements for DoD similar to these and convert these pilot programs to permanent programs if they are successful, and must provide matching funds through appropriations.

Recommendation 12

The United States is operating under an authorization for the use of military force that is nearly two decades old. Emerging threat streams require the United States to make strategic choices and prioritize its military actions. Congress must uphold its constitutional obligation to determine how and where the United States employs its military force by passing an updated AUMF. Revising the AUMF ensures that the United States can operate in a dynamic threat

¹²⁰ United States Army, *Long Range Precision Fires (LRPF)* (2022) (online at <https://asc.army.mil/web/portfolio-item/long-range-precision-fires-lrpf/>)

¹²¹ David Vergun, *Official Says DOD on Track to Accelerate Delivery of Hypersonic Weapons*, *Department of Defense* (Jun. 9, 2021) (online at <https://www.defense.gov/News/News-Stories/Article/Article/2651014/official-says-dod-on-track-to-accelerate-delivery-of-hypersonic-weapons/>)

¹²² United States Indo-Pacific Command, *Expeditionary Advanced Basing Capabilities on Display during Exercise Noble Fury* (Oct. 14, 2020) (online at <https://www.pacom.mil/Media/News/News-Article-View/Article/2382277/expeditionary-advanced-basing-capabilities-on-display-during-exercise-noble-fury/>)

¹²³ Mallory Shelbourne, *Marine Corps Ready to Conduct EABO Experiments with Allies in Indo-Pacific*, *United States Naval Institute* (Apr. 20, 2021) (online at <https://news.usni.org/2021/04/20/marine-corps-ready-to-conduct-eabo-experiments-with-allies-in-indo-pacific>)

¹²⁴ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 834 - Pilot Program to Accelerate the Procurement and Fielding of Innovative Technologies* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹²⁵ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 871 - Mission Management Pilot Program* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

environment while signaling to both allies and adversaries that America is committed to the lawful pursuit of its military endeavors.

12.1 - Congress should reaffirm its constitutional obligation by evaluating the nation's national security objectives and military strategy by passing an updated AUMF

Starting Implementation - In 2021, the House passed H.R. 256¹²⁶ which would have repealed the 2002 Iraq AUMF if signed into public law. However, this bill has been stalled in the Senate. The National Security Reform and Accountability Act¹²⁷ has been introduced in the House and the National Security Powers Act¹²⁸ has been introduced in the Senate. These bills would reassert Congress's power on a number of critical national security decision-making processes including the use of force without tying the President's hands so much that it is impossible to respond to national emergencies. While it is encouraging that Congress is engaging in these debates, Congress has not passed legislation that would reaffirm its constitutional obligation or implement updated AUMFs.

Recommendation 13

To incorporate the technology necessary to maintain the United States' military supremacy, the Pentagon must continue refining its acquisition process to be more agile and less risk averse so that it can fully leverage emerging technologies and capabilities at scale.

13.1 - Review defense acquisition regulations to make them less onerous, particularly for non-traditional entities seeking to partner with DoD

Partial Implementation - Congress and DoD have taken some steps to reduce the burden of defense acquisition regulations on the private sector, but this still falls short of a more rigorous, department-wide overhaul. The FY21 NDAA requires the Secretary of Defense to overhaul its guidance and support for small businesses in the national technology and industrial base so that these companies can more easily cover gaps in DoD's acquisition needs.¹²⁹ However, companies continue to face daunting bureaucratic requirements and unnecessary red tape that disincentivizes non-traditional companies from partnering with the Department. The Commission on Planning, Programming, Budgeting, and Execution Reform that was established in the FY22 NDAA¹³⁰ will serve as an important mechanism for the Department to better understand and improve its acquisition regulations.

¹²⁶ Library of Congress, *To Repeal the Authorization for Use of Military Force Against Iraq Resolution of 2002* (Mar. 25, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/256>)

¹²⁷ Library of Congress, *National Security Reforms and Accountability Act* (Sep. 29, 2021) (online at <https://www.congress.gov/bill/117th-congress/house-bill/5410>)

¹²⁸ Library of Congress, *National Security Powers Act of 2021* (Jul. 20, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/2391>)

¹²⁹ Library of Congress, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021: Section 861 - Initiatives to Support Small Businesses in the National Technology and Industrial Base* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/house-bill/6395>)

¹³⁰ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1004 - Commission on Planning, Programming, Budgeting, and Execution Reform* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

13.2 - Train and incentivize the acquisition workforce to utilize existing flexible authorities to quickly push innovative technology to warfighters in the field

Partial Implementation - The FY22 National Defense Authorization Act requires DoD to establish a cadre of software development and acquisition experts by 2023 to support the Department's efforts in procuring innovative software products.¹³¹ While this mandate will likely improve DoD's software acquisition capabilities, the Department must also improve its acquisition mechanisms and processes to enable its acquisition workforce to be more efficient and effective.

13.3 - Incentivize calculated risk by providing funding for emerging technologies through programs of record at scale; allow a less-than-perfect success rate

Partial Implementation - Congress has created a number of pilot programs within DoD to improve the acquisition of emerging technologies on an accelerated timeline. The FY22 NDAA creates a pilot program for emerging technologies acquisition for "high priority defense modernization activities" that require DoD to use "significantly novel" acquisition practices.¹³² The goal of this program is to improve DoD's emerging technologies acquisition practices through internal mechanism reforms and to make updated acquisition authority recommendations to Congress. The FY22 NDAA also creates a pilot program to accelerate the procurement of emerging technologies with the goal of improving the Department's capability to develop and field innovative technologies.¹³³ Congress and DoD must continue to build on those pilots using the lessons-learned from failures rather than ending programs that do not immediately reap the desired outcome.

13.4 - Significantly increase opportunities for operators in the field, the acquisition force, program managers, and industry to partner and work together to more quickly develop requirements and identify solutions

Partial Implementation - Congress and DoD should work to increase opportunities for partnerships and collaboration between the Department and industry. One notable program that regularly creates partnerships with governmental and industrial organizations is DefenseWerx¹³⁴ and its associated groups like SOFWERX,¹³⁵ which focuses on partnerships between industry and the special operations community. Additionally, AFWERX¹³⁶ and DIU provide strong models for how a government organization can work to create opportunities for these partnerships. Within the Combatant Commands, there is further evidence of partnership and integration between industry and operators. NAVCENT recently stood up Task Force 59, which aims to rapidly integrate unmanned systems and artificial

¹³¹ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 836 - Cadre of Software Development and Acquisition Experts* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹³² Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 833 - Pilot Program on Acquisition Practices for Emerging Technologies* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹³³ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 834 - Pilot Program to Accelerate the Procurement and Fielding of Innovative Technologies* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

¹³⁴ DefenseWerx, *About Us* (2022) (online at <https://defensewerx.org/about/>)

¹³⁵ Michael Bottoms, *SOFWERX: A Smart Factory of Innovation Helping the Warfighter*, United States Special Operations Command (Feb. 2, 2018) (online at <https://www.socom.mil/pages/SOFWERX--A-smart-factory-of-innovation-helping-the-warfighter.aspx>)

¹³⁶ AFWerx, *About Us* (2022) (online at <https://afwerx.com/about-us/>)

intelligence with maritime operations in the 5th Fleet area of operations by partnering closely with industry.¹³⁷ Efforts like these should be models for broader integration of operators, the acquisition force, program managers, and industry throughout the defense enterprise.

13.5 - Structure the acquisition process, particularly for programs heavily dependent on software and technology, to be continuous and more closely aligned with the iterative process used to develop software and emerging technologies

Partial Implementation - The FY20 NDAA gives DoD some authority to initiate the restructuring of software-dependent acquisition programs so that they are similar to common software engineering and development practices.¹³⁸ These rapid and continuous development-centered contracts will allow for upgrades to deployed software products, and this new authority is similar to the iterative development process commonly used in software engineering. DoD must continue to expand these authorities to make them more widely accessible to the Services and ensure that all software-centric programs are able to use a more iterative approach to acquisition and sustainment.

13.6 - Employ the Air Force “Kessel Run” model, which works directly with operational units for rapid development and field testing

Partial Implementation - The Air Force has expanded its Kessel Run program to integrate the development and testing framework with the rest of the service. Kessel Run recently signed an agreement with Air Combat Command to rapidly modernize the command using modern software development techniques.¹³⁹ Kessel Run signed another agreement with the Air Force’s other major innovation group, Platform One, to further coordinate efforts across the service.¹⁴⁰ Other military services must follow the Air Force’s lead and adopt a similar model.

Recommendation 14

To thwart emerging threats and compete with adversaries who seek to undermine the United States beyond military realms to include economic, information, and political domains, the nation should reconfigure a coordinated, whole-of-government strategy to update the national security structure, which was established in the 1940’s primarily to focus on the rise of communism. This reimagination of the national security structure would partner the Department of State with the Department of Defense to ensure diplomatic parity and leadership.

¹³⁷ Roland Franklin, *U.S. 5th Fleet Launches New Task Force to Integrate Unmanned Systems*, US Naval Forces Central Command (Sep. 9, 2021) (online at <https://www.cusnc.navy.mil/Media/News/Display/Article/2768468/us-5th-fleet-launches-new-task-force-to-integrate-unmanned-systems/>)

¹³⁸ Library of Congress, *National Defense Authorization Act for Fiscal Year 2020: Section 800 - Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems* (Jan. 1, 2021) (online at <https://www.congress.gov/bill/116th-congress/senate-bill/1790>)

¹³⁹ Greg Hadley, *Kessel Run Signs ‘Historic’ Agreement With ACC. Here’s What It Means*, Air Force Magazine (Oct. 22, 2021) (online at <https://www.airforcemag.com/kessel-run-acc-historic-agreement/>)

¹⁴⁰ Jackson Barnett, *Air Force’s Kessel Run and Platform One Ink Collaboration Agreement*, Fedcoop (Nov. 16, 2021) (online at <https://www.fedscoop.com/kessel-run-and-platform-one-sign-collaboration-agreement/>)

14.1 - The State Department should lead the nation's whole-of-government effort, and its funding and staffing should be exponentially increased to reflect its expanded role and prominence. Congress should allocate funding to hire additional foreign service officers and expand the Global Engagement Center to counter foreign propaganda and misinformation

Partial Implementation - The President's FY22 Budget requested \$58.5 billion for the State Department,¹⁴¹ which is an increase over the \$41 billion requested in FY21¹⁴² and the \$40 billion requested in FY20.¹⁴³ The budget request increase reflects the State Department's leading role in US foreign policy under the Biden administration compared to its more muted role in US foreign policy under the previous administration. This funding will reinvigorate a US State Department plagued by resignations of senior and mid-level officials, allow for the hiring of more foreign service officers, and revitalize US foreign aid programs. The budget request for the Global Engagement Center in FY22 was \$53 million¹⁴⁴ lower than both the \$138 million¹⁴⁵ requested in FY21 and the \$60 million¹⁴⁶ requested and appropriated in FY20. The State Department should continue to expand this program and take a leading role in shaping a whole-of-government security strategy going forward.

14.2 - Congress should commission a varied group of national security experts and practitioners to undertake a wide-ranging review of the national security structure and strategy for adapting and restructuring them to incorporate new technologies and operational concepts and thus compete in the 21st Century

Near Full Implementation - Congress has begun a wide-ranging review of the US national security structure and strategy that addresses new technologies and operational concepts. The FY22 National Defense Authorization Act includes the National Defense Science and Technology Strategy¹⁴⁷ that DoD must release alongside the National Defense Strategy. It will address science and technology priorities, goals, and investments the Department is making to address short-term, mid-term, and long-term threats

¹⁴¹ Department of State, *Congressional Budget Justification Department of State, Foreign Operations, and Related Programs, Fiscal Year 2022* (2021) (online at https://www.state.gov/wp-content/uploads/2021/05/FY-2022-State_USAID-Congressional-Budget-Justification.pdf)

¹⁴² Department of State, *Congressional Budget Justification Department of State, Foreign Operations, and Related Programs, Fiscal Year 2021* (2020) (online at <https://www.state.gov/wp-content/uploads/2020/02/FY-2021-CBJ-Final-508compliant.pdf>)

¹⁴³ Department of State, *Congressional Budget Justification Department of State, Foreign Operations, and Related Programs, Fiscal Year 2020* (2019) (online at <https://www.state.gov/wp-content/uploads/2019/05/FY-2020-CBJ-FINAL.pdf>)

¹⁴⁴ Department of State, *Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement, Fiscal Year 2022* (2021) (online at <https://www.state.gov/wp-content/uploads/2021/07/FY-22-CBJ-A1-Full-Book-Final-as-of-07092021.pdf>)

¹⁴⁵ Department of State, *Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement, Fiscal Year 2021* (2020) (online at <https://www.state.gov/wp-content/uploads/2020/03/FY21-CBJ-Appendix-1-FINAL-for-GPA-Mar-26-2020.pdf>)

¹⁴⁶ House Committee on Appropriations: State, Foreign Operations, and Related Programs, *FY2020 Joint Explanatory Statement* (2019) (online at <https://appropriations.house.gov/sites/democrats.appropriations.house.gov/files/HR%201865%20-%20Division%20G%20-%20SFOPs%20SOM%20FY20.pdf>)

¹⁴⁷ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 211 - Codification of National Defense Science and Technology Strategy* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)

and challenges. The FY22 NDAA also creates a Commission on the National Defense Strategy.¹⁴⁸ While it is not technology-focused, the commission will undertake a broad, wide-ranging review of the entire national security structure and the National Defense Strategy which guides it. While these measures fall short of a wide-ranging, independent review focused on emerging technologies and operational concepts, they provide a solid foundation for analysis of emerging threats.

¹⁴⁸ Library of Congress, *National Defense Authorization Act for Fiscal Year 2022: Section 1095 - Commission on the National Defense Strategy* (Dec. 27, 2021) (online at <https://www.congress.gov/bill/117th-congress/senate-bill/1605>)