National Security Commission Artificial Intelligence Act of 2018 (HR 5356 / S 2806, 115th Congress)

Proposes the establishment of a temporary National Security Commission on Artificial Intelligence to assess and recommend the development of artificial intelligence to support the US's national security interests and advantage.

Updated last June 5, 2018 for the 03/20/2018 version of HR 5356 and the 05/09/2018 version of S 2806.

WHAT IT DOES

HR 5356 / S 2806 proposes the establishment of a temporary National Security Commission on Artificial Intelligence that would be independent from the Federal Government and terminate no later than October 2020. The purpose and responsibilities of the Commission would be to review the current state of artificial intelligence (AI) and associated technologies to better equip the nation with the means of addressing its national security needs including economic risks, needs of the Department of Defense (DOD), and other security risks as defined by the Commission.

Artificial Intelligence Defined – For the purposes of this bill, Artificial intelligence and related technologies are defined as the following:

- Artificial systems capable of performing tasks in dynamic circumstances with minimal human oversight and/or are capable of iteratively learn and improve given new data;
- Computer software or hardware systems capable of human-like perception, cognition, planning, learning, communication, and/or physical action to perform tasks;
- Artificial systems that can mirror the mental and physical capabilities of a human using technologies and techniques such as machine learning, neural networks, and cognitive architectures; and
- Artificial systems designed to act rationally to accomplish tasks as a physical robot or virtual decision agent by means of perception, planning, reasoning, learning, communication and decision making, and acting.

Scope of the Commission’s Review – While the Commission may broaden the scope of its review, the bill prioritizes the Commission's review of the following considerations:

- Competitive AI Advantage – maintaining national strategic advantages through the development of AI research and technological capabilities, such as quantum and high-performance computing, related to national security, public-private partnerships, and investments;
- Global AI Trends and Developments – the assessment of international cooperation and competitiveness in AI investment, use, and development;
- AI Research and Investment – increasing effective investment in basic and advanced AI research and technologies in private, public, academic, and combined initiatives;
- AI Workforce Training and Education – establishing effective and incentivizing education programs in science, technology, engineering, and math to ensure a competitive AI workforce;
- AI Legal and Ethical Risks – consideration for future legal and ethical risks associated with the use and development of AI in dynamic international conflict and humanitarian settings;
- Data Standardization, Securitization, and Privatization – establishment of best practices to ensure that data use related to AI research and development is standardized, made open-source when possible, made secure from breach or corruption, and
upholds the privacy of any persons involved.

Commission Reports – Within 180 days of the Commission’s commencement, a report of the Commission’s initial findings, recommendations, and progress must be submitted to the President and Congress. Within a year of the Commission’s commencement, a comprehensive report detailing the findings and recommendations from entire scope of the Commission’s review must be submitted to the President and Congress.

Commission Membership and Funding – the proposed Commission would consist of 11 members appointed for the life of the Commission within 90 days of the bill’s enactment by the Secretary of Defense (3 total) and the Chairpersons and ranking minority members of the Committees on Armed Services of the Senate and House of Representatives (2 each). Appointed members would be considered Federal Employees (as per 5 U.S.C 2105) and would select the Commission’s Chair and Vice Chair members. Funding for the Commission’s duties would be appropriated from the DOD and are capped at $10,000,000.

RELEVANT SCIENCE

While the Act provides its own definitions, there is currently no universally agreed-upon definition of artificial intelligence. The term "intelligence" is understood as a measure of a machine’s ability to successfully achieve an intended goal. Like humans, machines exhibit varying levels of intelligence subject to the machine’s design and training. However, there are different perspectives on how to define and categorize AI.

In 2009, a foundational textbook classified AI into four categories:

- Ones that think like humans;
- Ones that think rationally;
- Ones that act like humans; and
- Ones that act rationally.

Most of the progress seen in AI has been considered “narrow,” having addressed specific problem domains like playing games, driving cars, or recognizing faces in images. In recent years, AI applications have surpassed human abilities in some narrow tasks, and rapid progress is expected to continue, opening new opportunities in critical areas such as health, education, energy, and the environment. This contrasts with “general” AI, which would replicate intelligent behavior equal to or surpassing human abilities across the full range of cognitive tasks. Experts involved with the National Science and Technology Council (NSTC) Committee on Technology believe that it will take decades before society advances to artificial "general" intelligence.

According to Stanford University’s 100-year study of AI, by 2010, advances in three key areas of technology intersected to increase the promise of AI in the US economy:

- **Big data**: Large quantities of structured and unstructured data amassed daily from e-commerce, business, science, government, and social media. As datasets increase in size and quantity, so too do concerns of data standardization, securitization, and privatization.
- **Standardization**: data provided by multiple parties from multiple sources need to be converted to a common format to allow for consistent collaboration and application by researchers and programs.
- **Securitization**: sensitive data must be protected from unauthorized access, manipulation, and application of data throughout the computing system where data is used and stored. A common form of ensuring data security is called “Authentication” where authorized users must verify their identity through multiple methods such as providing a password and a generated passcode sent to the user’s phone.
- **Privatization**: while a subset of data securitization, data privatization relates to efforts to prevent the disclosure of sensitive information contained in the data such as health, financial, and criminal records. Privatization efforts include anonymizing data as well as providing users transparent indication of who will have access to their data for what purposes.
- **Quantum and high-performance computing**: Greater storage and parallel processing of big data made possible by emerging...
computing methods.

- **Quantum computing**: whereas traditional computers rely on storing and reading information in binary bits, quantum computers make use of new understandings of quantum mechanics that allow information to be read and stored exponentially faster and simultaneously on non-binary quantum bits or “qubits”.

- **High-performance computing**: while quantum computing can exponentially increase the abilities of single computers, advancement in high-performance computing enables the simultaneous application of multiple sets of computers, called “clusters”, to solve problems. Both quantum and high-performance computing allow for faster and more efficient problem solving, however these new capabilities could also be applied to nefarious uses that will have to be guarded against.

- **Machine learning**: the basis for many of the recent advances in AI. Machine learning is a method of data analysis that attempts to find structure (or a pattern) within a data set without human intervention. Machine learning systems search through data to look for patterns and adjust program actions accordingly, a process defined as training the system. To perform this process, an algorithm (called a model) is given a training set (or teaching set) of data, which it uses to answer a question. For example, for a driverless car, a programmer could provide a teaching set of images tagged either “pedestrian” or “not pedestrian.” The programmer could then show the computer a series of new photos, which it could then categorize as pedestrians or non-pedestrians. Machine learning would then continue to independently add to the teaching set. Every identified image, right or wrong, expands the teaching set, and the program effectively gets “smarter” and better at completing its task over time.

- **Machine learning algorithms are often categorized as supervised or unsupervised. In supervised learning, the system is presented with example inputs along with desired outputs, and the system tries to derive a general rule that maps input to outputs. In unsupervised learning, no desired outputs are given, and the system is left to find patterns independently.**

- **Deep learning is a subfield in machine learning. Unlike traditional machine learning algorithms that are linear, deep learning utilizes multiple units (or neurons) stacked in a hierarchy of increasing complexity and abstraction inspired by structure of human brain. Deep learning systems consist of multiple layers and each layer consists of multiple units. Each unit combines a set of input values to produce an output value, which in turn is passed to the other unit downstream. Deep learning enables the recognition of extremely complex, precise patterns in data.**

Experimental research in artificial intelligence includes several key areas that mimic human behaviors, including reasoning, knowledge representation, planning, natural language processing, perception, and generalized intelligence:

- **Reasoning includes performing sophisticated mental tasks that people can do (e.g., play chess, solve math problems).**
- **Knowledge representation is information about real-world objects the AI can use to solve various problems. Knowledge in this context is usable information about a domain, and the representation is the form of the knowledge used by the AI.**
- **Planning and navigation includes processes related to how a robot moves from one place to another. This includes identifying safe and efficient paths, dealing with relevant objects (e.g., doors), and manipulating physical objects.**
- **Natural language processing includes interpreting and delivering audible speech to and from users.**
- **Perception research includes improving the capability of computer systems to use sensors to detect and perceive data in a manner that replicates humans’ use of senses to acquire and synthesize information from the world around them.**

Ultimately, success in the discrete AI research domains could be combined to achieve generalized intelligence, or a fully autonomous “thinking” robot with advanced abilities such as emotional intelligence, creativity, intuition, and morality. Such autonomous agents could open new ethical and legal complications that will need to be adequately assessed and planned for. For instance, autonomous agents or programs may, as a product of their autonomy, operate outside the expectations of their creators. In the event that the agent or program’s creators have not implemented comprehensive stop gaps, the agent or program may inadvertently cause unintended harm to allies or adversaries. Whether the creators of the agents or programs are liable for any harms, and whether the harms should be given the same status of acts of war, is yet to be determined.

**RELEVANT EXPERTS**

Vincent Conitzer, Ph.D. is Kimberly J. Jenkins University Professor of New Technologies, Professor of Computer Science, Professor of Economics, and Professor of Philosophy at Duke University.
As AI technologies grow more capable, there is increasing concern about their potential impact, across a variety of domains (economic, military, social, scientific) and timescales. We can already see many high-impact developments on the horizon, and on top of that the potential for surprise is very high. Becoming and remaining well informed is essential for decision makers.

Relevant Publications:


BACKGROUND

The National Security Commission Artificial Intelligence Act of 2018 follows a series of reports issued by the NSTC [Committee on Technology](https://www.whitehouse.gov/nsti) in 2016. The first was [Preparing for the Future of Artificial Intelligence](https://www.whitehouse.gov/ostp/preparing-for-the-future-of-artificial-intelligence) (SciPol brief available), which surveyed the current state of AI, its existing and potential applications, and the questions that progress in AI raises for society and public policy. The second, [National Artificial Intelligence Research and Development Strategic Plan](https://www.whitehouse.gov/ostp/national-artificial-intelligence-research-and-development-strategic-plan) (SciPol brief available), prioritized key federal research and development investments to maximize the benefits of AI technology. The third and final report, [Artificial Intelligence, Automation, and the Economy](https://www.whitehouse.gov/ostp/artificial-intelligence-automation-and-the-economy) (SciPol brief available) provides a review of the positive and negative effects of AI-driven automation on the US economy and describes three broad strategies designed to augment the benefits and reduce the costs.

These three reports were produced following the White House's June 22, 2016, [Public Request for Information (RFI)](https://www.whitehouse.gov/ostp/public-requests-for-information) regarding AI as well as a series of workshops addressing the applications of AI. The workshops included:

- **AI: Law, and Policy** (May 24, 2016);
- **AI for Social Good** (June 7, 2016);
- **Future of AI: Emerging Topics and Societal Benefit at the Global Entrepreneurship Summit** (June 23, 2016);
- **Safety and Control for AI** (June 28, 2016); and
- **Social and Economic Impacts of AI** (July 7, 2016).

The National Security Commission Artificial Intelligence Act of 2018 also follows the introduction of similar bills proposed described below under “Related Policies” that further support the provision of Federal insights to AI applications beyond national security interests.

ENDORSEMENTS & OPPOSITION

At present, there has not been any publicly reported endorsement of or opposition to this bill.

However, on February 21, 2018, the Bulletin of the Atomic Scientists, which manages the international Doomsday Clock, have recognized in a [study](https://thebulletin.org/2018/02/ai-and-national-security/) on Artificial Intelligence and National Security that, "advances in AI will affect national security by driving change in three areas: military superiority, information superiority, and economic superiority." The Bulletin of the Atomic Scientists study also recommends that the US invest in continued research and assessment of AI to ensure national security interests.

STATUS

HR 5356 was [introduced](https://www.congress.gov/bill/115th-congress/house-bill/5356) in the House of Representatives on March 20, 2018, when it was referred to the [Committee on Armed Forces](https://www.govinfo.gov/content/package?pubNumber=h120-125)
Services, and in addition to the Committees on Education and the Workforce, Foreign Affairs, Science, Space, and Technology, and Energy and Commerce. On March 21, 2018, the bill was later referred to the sub-committee Emerging Threats and Capabilities by the Committee on Armed Services. On May 22, 2018 the bill was referred to the House Subcommittee on Research and Technology.

S 2806 was introduced on the Senate on May 9, 2018, when it was referred to the Committee on Commerce, Science, and Transportation.

RELATED POLICIES

HR 4625 and S 2217, the FUTURE of Artificial Intelligence Act of 2017 – Introduced by Representative Maria Cantwell (D-WA-1), Representative Todd Young (R-IN-9), and Senator Ed Markey (D-MA) are bills currently under review in both chambers of Congress to require the Department of Commerce to establish the Federal Advisory Committee on the Development and Implementation of Artificial Intelligence (SciPol Brief Available).

HR 1576, the Innovation Corps Act of 2017 – introduced on March 16, 2017 in the House of Representatives by Representative Doris Matsui (D-CA-6) to require the Department of Commerce to establish a competitive program (the Innovation Corps) to fund the establishment or support of education programs that retrain workers displaced from their jobs by automation to provide such workers with skills needed for jobs in science, technology, engineering, or mathematics (STEM) fields (SciPol brief available).

POLICY HISTORY

While other bills related to AI and national security have been considered by Congress, HR 5365 / S 2806 is the first of its kind with respect to establishing a temporary commission to assess AI's role and future for the United States' national security.

SPONSORS

HR 5365
Sponsor: Representative Elise M. Stefanik (R-NY-21)

Cosponsors:
- Representative James R. Langevin (D-RI-2)
- Representative Austin Scott (R-GA-8)
- Representative Jody B. Hice (R-GA-10)
- Representative Seth Moulton (D-MA-6)
- Representative Bradley Byrne (R-AL-1)

S 2806
Sponsor: Senator Joni Ernst (R-IA)

Cosponsor: Senator Catherine Cortez-Masto (D-NV)

PRIMARY AUTHOR

Scott "Esko" Brummel, MA Bioethics and Science Policy