

# EMERGING SCIENCE AND TECHNOLOGY TRENDS

A Report of the IDA Science  
and Technology Policy Institute

JUNE 2019

**IDA**

SCIENCE AND  
TECHNOLOGY  
POLICY INSTITUTE



The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

### **About This Publication**

This work was conducted by the IDA Science and Technology Policy Institute under IDA's Central Research Program, Project AE-20-S281, "Science & Technology Futures Working Group."

### **For More Information**

Jason A. Gallo, Project Leader  
jgallo@ida.org, 202-419-3729

Mark S. Taylor, Acting Director, Science and Technology Policy Institute  
mtaylor@ida.org, 202-419-5491

### **Copyright Notice**

© 2019 Institute for Defense Analyses  
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at FAR 52.227-14 [Dec 2017].



Jason Gallo  
Emily Sylak-Glassman  
Susannah Howieson  
Mark Taylor  
William Doane  
Ian Simon  
Christopher Clavin  
Becaja Caldwell  
Katherine Kowal  
Cara Cavanaugh  
Abhiram Sanka



## Executive Summary

---

As scientific research and technology development evolve, it is crucial to U.S. economic vitality and national security that the executive branch of the Federal Government anticipates and responds to emerging science and technology (S&T) trends. These trends will affect the missions of multiple Federal departments, agencies, offices, and programs, and will require coordinated attention to be addressed effectively. To identify emerging S&T trends that will require coordinated interagency attention in the near term, the IDA Science and Technology Policy Institute (STPI) held two workshops with subject matter experts in the fall of 2018. Invited participants represented diverse disciplines and areas of expertise, including participants from the private sector, academia, Federal agencies, and former Office of Science and Technology Policy (OSTP) leaders from Republican and Democratic administrations.

Prior to each workshop, STPI researchers and workshop participants identified a large set of initial S&T trends for consideration. Through guided discussion and a voting exercise in each session, participants pinpointed 3–5 specific topics, based on their expertise, as the most critical for the executive branch to address through coordinated, interagency action in the near term. The following topics were recognized across both sessions as the most critical to address in the near-term.

### **Strengthening the Nation’s Resilience to Natural Hazards Given a Changing Climate**

Changes in precipitation patterns and temperature means and extremes, as well as a rising sea level, are already impacting ecosystems, communities, the built environment, economic sectors, military installations, and critical and civil infrastructure across the United States. Given the scientific consensus on the fact that the climate is changing,<sup>1</sup> the question that the country now faces is what to do about it. There is no single agency in charge of researching, funding, and implementing adaptation measures; rather, there is a patchwork of efforts that spans nearly every Federal agency. It is therefore important to enhance coordination among agencies and leverage expertise from each to enhance resiliency as well as strengthen interaction with State, local, and Tribal government partners and private sector actors to best prepare for and adapt to natural hazards given a changing climate.

---

<sup>1</sup> U.S. Global Change Research Program (USGCRP). 2018. *Impacts, Risk, and Adaptation in the United States: Fourth National Climate Assessment, Volume II* [Reidmiller, D. R., C.W. Avery, D.R. Easterling, K.E. Kunkel, K.L.M. Lewis, T.K. Maycock, and B.C. Stewart (eds.)]. U.S. Global Change Research Program, Washington, DC, USA, 1515 pp. doi: 10.7930/NCA4.2018

### **Harnessing Advances in the Life Sciences**

Advances in biotechnology, molecular biology, and health information technology are driving innovation in the agriculture, behavioral science, biomedical science, energy, and healthcare sectors. Over 20 separate Federal agencies have directly supported research or contributed to interagency activities related to the emergence of biotechnology as a major driver of the U.S. economy. Additionally, there is a large and diverse set of stakeholders across these sectors with varying interests, equities, and vulnerabilities that must be considered. It is important that the Executive Office of the President (EOP) and Federal agencies work collaboratively to establish a policy framework that promotes responsible research and development (R&D) across the life sciences, adequately anticipates risk, and protects stakeholders from adverse actions and outcomes.

### **Maintaining and Improving Science Infrastructure**

The U.S. R&D enterprise requires a skilled and empowered S&T workforce, state of the art facilities and equipment, and a flexible policy and regulatory environment. A few key areas that need immediate attention are: investments in large R&D facilities, such as trusted foundries and wind tunnels; the competitiveness of the U.S. manufacturing base; training, hiring, and flow of government scientists and engineers; and rules and requirements surrounding technology transfer and commercialization of federally funded R&D. This area would benefit from interagency coordination to develop an overarching strategy for maintaining and improving U.S. science infrastructure, with a focus on the key areas identified above.

### **Strengthening the Built Environment**

The built environment, comprised of the Nation's critical infrastructure and buildings, is a set of dynamic technological systems that are continually in use and in need of maintenance and upgrade. Critical infrastructure systems, such as electric power grids, communications, and transportation, provide the United States with a number of vital services that support the Nation's economy, security, and health.<sup>2</sup> Maintenance of the built environment is an inherently collaborative effort between the public and private sector. Given there is no single agency accountable for all of these responsibilities, and many new technologies are emerging that could substantially improve how the built environment is planned, maintained, and developed (e.g. autonomous vehicles, advanced materials for construction), it is important that the executive branch establish a unified vision for the next generation of the built environment and develop interagency policies to ensure its necessary maintenance and improvement.

---

<sup>2</sup> National Research Council. 2009. *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives: Report of a Workshop*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/12638>.

### **Improving Cybersecurity Research and Implementation**

Our society and infrastructure depend on computing technologies to provide convenience, ensure security, and protect human life, and it is therefore vital that cybersecurity be a primary concern for all stakeholders. Public policy needs to articulate clearly the societal benefits and concerns that technology should address, rather than dictating the specific features of the technology. This creates a space within which innovators can experiment and understand their role in developing and ensuring the safety of new technologies. New models are needed to characterize the security of systems, to quantify the degree of security, to qualify the conditions under which security is maintained, and to be able to document and share information concerning security best practices, methods, and incidents. The Federal Government should increase coordination of interagency cybersecurity R&D efforts and ensure increased implementation of security measures and reporting standards across agencies, the public and private sectors, and within the general public.

### **Protecting the Science Communication Environment**

The science communication environment “is the interaction of processes and cues that citizens, organizations, governments, and a host of other stakeholders use to identify valid science and align it with their value systems, understanding of the world, and ultimately decisions.”<sup>3</sup> Effective science communication plays a critical role in the transmission of relevant information to stakeholders. Research from the field of “the science of science communication” plays an important part in understanding and improving the processes for communicating scientific knowledge, how that knowledge is received and used by decision-makers, and how different and multiple forms of mediation and framing of scientific knowledge affect its dissemination, diffusion, and uptake. For the United States to maximize returns on its substantial investments in scientific research and technology development while adequately addressing risk and ethical considerations, workshop participants stressed the importance of protecting the science communication environment to ensure the timely availability of accurate data and information to improve public and private sector decisions. Proactive interagency coordination is necessary to improve the understanding of the science communication environment and protect it from threats such as misinformation. Federal agencies should act as trusted intermediaries for the scientific community, public and private sector decision-makers, and citizens.

---

<sup>3</sup> Jamieson, Kathleen Hall, Dan Kahan, and Dietram A. Scheufele. 2017. "Introduction: Why Science Communication?" *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017. <https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.1>

## Engaging in Artificial Intelligence and Autonomy Research and Development

Artificial intelligence (AI) and autonomy, coupled with robotics and advances in data mining and high-performance computing, are transforming the application of computing to complex problem solving with large potential social, political, economic, and security ramifications. AI and autonomous systems could potentially increase productivity, improve decision-making, and provide insights into complex problems.<sup>4</sup> AI algorithms, and the data sets used to train AI and autonomous systems, reflect structural issues within society and organizations and reinforce existing patterns that disadvantage some groups and individuals.<sup>5</sup> As AI and machine learning techniques become ubiquitous, the biases encoded in algorithms or structural inequalities reflected within data sets have the potential for negative unintended consequences. Responsible EOP offices and Federal agencies should coordinate to create a regulatory environment that promotes responsible AI and autonomy R&D that is broadly beneficial to society and the economy.

The recommended actions that the executive branch can undertake to address these emerging S&T topics are included in Table 1.

---

<sup>4</sup> United States Congress. House Subcommittees on Research and Technology and Energy, Committee on Science, Space, and Technology. 2018. *Artificial Intelligence Emerging Opportunities, Challenges, and Implications for Policy and Research*. 26 June 2018. (Statement of Timothy M. Persons, United States Government Accountability Office).

<sup>5</sup> Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, 2018.

**Table 1. Recommended executive branch actions to address emerging S&T topics identified by workshop participants.**

Topic	Recommendation
Strengthening the Nation's Resilience to Natural Hazards Given a Changing Climate	<ul style="list-style-type: none"> <li>• Develop a comprehensive, interagency strategy to help the Federal Government, State, local, and Tribal governments, economic sectors, businesses, and individuals prepare for the effects of a changing climate.</li> <li>• Ensure that products and services aimed at increasing resilience to natural hazards are developed and disseminated in ways that make the information discoverable, accessible, and usable.</li> <li>• Develop a plan for addressing gaps in the collection of Earth observations.</li> <li>• Convene an interagency task force co-chaired by the Department of Defense (DOD), Department of Homeland Security (DHS), and the U.S. Global Change Research Program to develop an action plan to address the threats that the changing climate poses to critical and civil infrastructure, the built environment, military installations, and the ability of the emergency response system to adequately protect lives and property.</li> </ul>
Harnessing Advances in the Life Sciences	<ul style="list-style-type: none"> <li>• Convene stakeholders and subject matter experts to fully understand the extent, components, and value of the bioeconomy.</li> </ul>
Maintaining and Improving Science Infrastructure	<ul style="list-style-type: none"> <li>• Develop an overarching strategy for maintaining and improving U.S. science infrastructure.</li> <li>• Identify a set of critical Federal laboratory facilities and infrastructure and large scale research infrastructure that need focused attention and investment.</li> <li>• Identify potential workforce pipeline issues (including retention) and ways in which to train and inspire scientists.</li> <li>• Strategically focus training in areas that lack people, including in emerging areas of R&amp;D.</li> <li>• Increase the speed and efficiency of the clearance granting process and expand the ability for agencies to grant clearances to technical experts from industry and academia to assume temporary duties in government during a crisis.</li> <li>• Enable Federal, industry, and academic staff to trade places through rotations.</li> <li>• Increase the speed and efficiency of Federal agency hiring to enable agencies to hire qualified individuals within 60 to 90 days of submitting an application.</li> <li>• Develop a policy framework that increases the ability of universities to transfer technologies and techniques developed with Federal funds to the marketplace and increases coordination between universities, venture capital groups, and national laboratories.</li> </ul>

EMERGING SCIENCE AND TECHNOLOGY TRENDS

Topic	Recommendation
Strengthening the Built Environment	<ul style="list-style-type: none"> <li>• Identify opportunities for the executive branch to aid the development and deployment of advanced technologies that improve cities and urban living.</li> <li>• Set joint priorities for establishing infrastructure performance design requirements that ensure future Federal investments into existing or new infrastructure are designed to be resilient to future hazards.</li> <li>• Identify how the public and private sectors can set joint priorities and work together to advance electricity distribution system performance as new technologies increase demands on existing distribution system infrastructure.</li> </ul>
Improving Cybersecurity Research and Implementation	<ul style="list-style-type: none"> <li>• Develop policies that articulate clearly the societal benefits and concerns that technology should address, rather than dictating the specific features of the technology.</li> <li>• Create a policy framework where liability for action or inaction can be reasoned about and quantified, providing insurers and businesses with a reasonable basis for engaging in and managing the risks of new technology.</li> <li>• Adopt a targeted investment strategy through purchasing, cost sharing, prizes, and awards to further encourage businesses to address public cybersecurity needs where there exists a failure of the market to do so.</li> <li>• Incentivize the development of new models to characterize the security of systems, to quantify the degree of security, to qualify the conditions under which security is maintained, and to be able to document and share information concerning security best practices, methods, and incidents.</li> <li>• Explore including cybersecurity as a component of continuity of operations</li> </ul>
Protecting the Science Communication Environment	<ul style="list-style-type: none"> <li>• Conduct a comprehensive assessment of the current U.S. science communication environment.</li> <li>• Develop a Federal action plan to protect and improve the science communication environment based on the results of the comprehensive assessment.</li> <li>• Develop and disseminate fact sheets, case studies, or issue-briefs on emerging S&amp;T issues that clearly address what the executive branch projects potential benefits might be, what it understands about potential risks, and where there may be differential outcomes for stakeholder groups.</li> <li>• Develop and disseminate fact sheets, case studies, or issue-briefs that document the contribution of scientific and technical information to decisions that impact public and private sector activity.</li> </ul>

EMERGING SCIENCE AND TECHNOLOGY TRENDS

Topic	Recommendation
Engaging in Artificial Intelligence and Autonomy Research and Development	<ul style="list-style-type: none"> <li>• Engage in technology assessments for new and emerging applications of AI and autonomous systems.</li> <li>• Develop a mechanism to solicit public feedback on how potential regulations or policy changes could impact U.S. competitiveness.</li> <li>• Establish a Federal Advisory Committee to bring together industry and academic representatives to produce a report to provide guidance to Federal agencies.</li> <li>• Convene a permanent, interagency body with the goal of promoting the protection of participants in federally supported research with particular attention to the consideration of emerging ethical issues, including new developments in medicine, science, and technology.</li> </ul>

R&D that supports the national and homeland security of the United States plays an integral role in maintaining strategic security and foreign policy advantages and contributes to the economic competitiveness of key domestic sectors such as biotechnology, manufacturing, and information and communication technology and services. Workshop participants identified several national and homeland security issues that cut across agency missions, including the development of a high-skilled workforce, identification of foreign scientific and technical advances that pose security risks to the U.S., protection of intellectual property, and understanding the security implications of foreign investment in the U.S.

The recommended actions that the executive branch can undertake to address these emerging national and homeland security S&T topics are included in Table 2.

**Table 2. Recommended executive branch actions to address emerging national and homeland security S&T topics identified by workshop participants.**

National and Homeland Security Consideration	Recommendation
Ceding Competitive Advantage to Adversaries in Biotechnology	<ul style="list-style-type: none"> <li>• Establish an interagency group to identify and track international biotechnology developments, identify threats to both public health and U.S. competitiveness, and issue guidance to U.S. researchers on developing these technologies.</li> </ul>

EMERGING SCIENCE AND TECHNOLOGY TRENDS

National and Homeland Security Consideration	Recommendation
Balancing National Security and Commercial Activity	<ul style="list-style-type: none"><li data-bbox="597 296 1414 417">• Establish an interagency group to address challenges to civil, defense, and intelligence agency space missions from commercial developments, while ensuring the global competitiveness of the U.S. space industry.</li><li data-bbox="597 428 1414 550">• Improve access to trusted domestic microelectronic foundries for both national security and civil commercial sector use by working with the National Institute of Standards and Technology and DHS to establish a civil trusted foundries initiative to partner with the DOD.</li><li data-bbox="597 560 1414 682">• Establish a Federal Advisory Committee that draws on private sector and academic expertise in the semiconductor and microelectronics fabrication to advise the executive branch on securing advanced technology development.</li><li data-bbox="597 693 1414 779">• Establish a task force to address civil and critical infrastructure vulnerabilities due to commercial information and communication technologies.</li></ul>

## Contents

---

1.	Introduction .....	1
A.	Background .....	1
B.	Methods .....	1
1.	Forum Planning.....	1
2.	Background Information Given to Participants .....	2
3.	Process to Identify 3–5 Emerging S&T Topics .....	2
4.	Discussion of Emerging S&T Topics.....	3
5.	Post-Forum Analysis.....	3
2.	Highlighted Topics for Executive Branch Action.....	5
A.	Strengthening the Nation’s Resilience to Natural Hazards Given a Changing Climate .....	5
1.	Why should the executive branch address this topic? .....	7
2.	How should the executive branch address this topic? .....	8
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	9
B.	Harnessing Advances in the Life Sciences .....	9
1.	Why should the Federal Government address this topic?.....	10
2.	How should the executive branch address this topic? .....	11
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	11
C.	Maintaining and Improving Science Infrastructure.....	12
1.	Why should the executive branch address this topic? .....	12
2.	How should the executive branch address this topic? .....	15
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	16
D.	Strengthening the Built Environment.....	16
1.	Why should the executive branch address this topic? .....	18
2.	How should the executive branch address this topic? .....	19
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	20
E.	Improving Cybersecurity Research and Implementation .....	20
1.	Why should the executive branch address this topic? .....	21
2.	How should the executive branch address this topic? .....	22
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	23
F.	Protecting the Science Communication Environment.....	23
1.	Why should the executive branch address this topic? .....	25

EMERGING SCIENCE AND TECHNOLOGY TRENDS

2.	How should the executive branch address this topic? .....	26
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	28
G.	Engaging in Artificial Intelligence (AI) and Autonomy Research and Development .....	28
1.	Why should the executive branch address this topic? .....	29
2.	How should the executive branch address this topic? .....	31
3.	What issues or potential consequences should the executive branch consider if this topic is or is not addressed? .....	31
3.	Cross-Cutting National and Homeland Security S&T Considerations .....	33
1.	Ceding Competitive Advantage to Adversaries in Biotechnology .....	33
2.	Balancing National Security and Commercial Activity .....	34
4.	Conclusion .....	39
	Appendix A. List of Emerging S&T Trends .....	A-1
	Appendix B. List of Participants .....	B-1
	Abbreviations .....	C-1
	References.....	D-1

# 1. Introduction

---

## A. Background

In order to identify and advise the executive branch of the Federal Government on emerging science and technology (S&T) issues, the IDA Science and Technology Policy Institute (STPI) held two workshops with subject matter experts (SMEs) in the fall of 2018, along with STPI and IDA Systems and Analyses Center (SAC) researchers and management, to help identify emerging S&T trends that will require interagency attention and that the executive branch should be prepared to address in the near term.

This chapter details the methods used to develop the list of emerging S&T trends considered and discussed by workshop participants and the process used to identify the topics that are the most critical for the executive branch to address through coordinated, interagency action. The topics, along with information about why and how the executive branch should address them and potential considerations if they are not addressed, are discussed in Chapter 2. Chapter 3 details the cross-cutting national security considerations, and Chapter 4 summarizes the recommendations for executive branch action.

## B. Methods

### 1. Forum Planning

STPI developed a list of potential SMEs with a diverse set of perspectives, including experience in the Federal Government, State Government, the private sector, and academia. This list of invitees included former Office of Science and Technology Policy (OSTP) staff from Republican and Democratic administrations, current and former leaders of Federal agencies, multiple members of the IDA Board of Trustees, as well as alumni of the Defense Science Studies Group (DSSG), a program directed by IDA and sponsored by the Defense Advanced Research Projects Agency (DARPA) that introduces science and engineering professors to the United States' security challenges. The expertise of the invitees included biology, chemistry, communication, computer science, Earth science, economics, engineering, law, medicine, and physics, and participants at all career stages were invited. Due to overwhelming interest in attending, STPI decided to hold two workshops. The first workshop was held on October 30, 2018 with 10 SMEs, and the second was held on November 15, 2018 with 11 SMEs. A list of participants is included in Appendix A.

To maximize the productivity of the workshop, STPI had participants identify a broad list of emerging S&T trends ahead of time, which the group reviewed prior to attending. In

advance of each workshop, STPI researchers sent an email to all participants asking (1) What are emerging S&T trends of national interest or concern that require interagency attention that the executive branch should address in the near-term?, and (2) What are the implications of the executive branch not addressing these trends? The purpose of each workshop was to discuss the collection of identified trends and then, through guided discussion and a voting exercise, identify 3–5 specific topics as the most critical for the executive branch to address through coordinated, interagency action within the next two years.

STPI researchers included all relevant participant-submitted S&T trends. For each trend, STPI edited the submissions for consistency and conducted additional research when needed. Based on the responses, STPI developed a list of 20 trends for the October 30 workshop. Following the October 30 workshop, STPI received five additional trends from the November 15 workshop participants. These trends were added to the original 20 trends and circulated those to participants. The complete list of trends shared with participants prior to the November 15 workshop is included in Appendix B.

## **2. Background Information Given to Participants**

Prior to discussing S&T trends, participants were given background information about the workshop’s aims. Participants were briefed by IDA and STPI management to provide context to each workshop’s goal of identifying 3–5 emerging S&T topics that require interagency attention. For each of these topics, participants were asked to discuss why the topic is relevant, specific actions that the executive branch can initiate in the near term to address the topic, anticipated outcomes of these actions, potential consequences of inaction, and any other factors that the executive branch should consider. Participants were also provided a list of potential interagency “policy tools” that the executive branch has at its disposal, such as convening and supporting interagency initiatives among the Executive Office of the President (EOP) and Federal agencies, providing input to the S&T budget-making process, and communicating S&T priorities to the private sector, academia, and the general public. These were provided to help ensure that participants consider whether topics are well-suited to coordinated executive branch action.

## **3. Process to Identify 3–5 Emerging S&T Topics**

The general process to select 3–5 emerging S&T topics was: (1) guided group discussion of topics, (2) individual voting, and (3) guided group discussion of voting results. During the guided group discussion of topics, participants were asked whether any topics should be added or subtracted from the list, and whether any topics should be reframed or merged. Following the discussion, the participants were given a list of the remaining topics, reflecting any changes the group had suggested, and were asked to vote for the 50% of topics that they thought were most important for the executive branch to address. Participants were asked

to specifically consider which topics are well-suited for coordinated executive branch action given the policy tools that it has at its disposal, and on which topics it could take near-term action. Once participants submitted their votes, STPI researchers summed up the votes and displayed the results. The group was then asked to use the results to determine which 3–5 topics are the most critical for the executive branch to address. STPI researchers permitted the groups to choose more than five topics if the group thought it was necessary.

#### **4. Discussion of Emerging S&T Topics**

For each of the topics selected, the participants were asked to discuss the following questions:

- Why is this topic relevant to the executive branch?
- What actions can the executive branch take to address the topic in the near term?
- What are the anticipated outcomes of executive branch action and how will those actions change the trajectory of this field or issue?
- What are the possible outcomes of inaction?
- What are the alternative viewpoints, potential unintended consequences, or potential negative outcomes that should be considered?

#### **5. Post-Forum Analysis**

Based on the total input from both sessions, STPI researchers developed a list of topics highlighted by workshop participants, developed summaries of each topic, and identified priority areas addressed by both groups and areas strongly identified in either session. To develop this report, notes from both sessions were supplemented with additional research and relevant literature. For each topic, STPI developed a description, and summarized responses to the following questions

- Why should the executive branch address this topic?
- How should the executive branch address this topic?
- What issues or potential consequences should the executive branch consider if the topic is or is not addressed?

A draft document was circulated to all participants for feedback before finalization.



## 2. Highlighted Topics for Executive Branch Action

---

### A. Strengthening the Nation's Resilience to Natural Hazards Given a Changing Climate

Helping Americans prepare for natural hazards and risks intensified by a changing climate was identified as a key issue for the executive branch by both sets of workshop participants. Changes in precipitation patterns and temperature means and extremes, as well as a rising sea level, are already impacting communities, economic sectors, and ecosystems across the United States. Given the scientific consensus on the fact that the climate is changing,<sup>6</sup> the question that the country now faces is what to do about it.

The changing climate is affecting Earth system processes in various ways, many of which are interconnected and highly impactful to economic, national, and homeland security in the U.S. The agriculture sector, which yields roughly \$300 billion dollars a year in commodities, will exacerbate stresses on agricultural plants and animals, potentially threatening our food security.<sup>7</sup> The 2019 *National Intelligence Strategy* notes that areas threatened by a changing climate are causing growing influxes of migrants, refugees, and internally displaced persons.<sup>8</sup> In January 2019, in response to Section 355 of the National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91), the Department of Defense (DOD) Office of the Under Secretary of Defense for Acquisition and Sustainment issued a *Report on Effects of a Changing Climate to the Department of Defense*, stating that “effects of a changing climate are a national security issue” with the potential to affect “missions, operational plans, and installations.”<sup>9</sup> The United States faces a number of

---

<sup>6</sup> USGCRP. 2018. *Impacts, Risk, and Adaptation in the United States: Fourth National Climate Assessment, Volume II*. [Reidmiller, D. R., C.W. Avery, D.R. Easterling, K.E. Kunkel, K.L.M. Lewis, T.K. Maycock, and B.C. Stewart (eds.)]. U.S. Global Change Research Program, Washington, DC, USA, 1515 pp. doi: 10.7930/NCA4.2018

<sup>7</sup> USDA. 2013. *Climate Change and Agriculture in the United States: Effects and Adaptation*. USDA Technical Bulletin 1935. [https://www.usda.gov/oce/climate\\_change/effects\\_2012/CC%20and%20Agriculture%20Report%20\(02-04-2013\)b.pdf](https://www.usda.gov/oce/climate_change/effects_2012/CC%20and%20Agriculture%20Report%20(02-04-2013)b.pdf)

<sup>8</sup> Office of the Director of National Intelligence. 2019. *National Intelligence Strategy of the United States of America*. [https://www.dni.gov/files/ODNI/documents/National\\_Intelligence\\_Strategy\\_2019.pdf](https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf)

<sup>9</sup> Department of Defense. Office of the Under Secretary of Defense for Acquisition and Sustainment. 2019. *Report on Effects of a Changing Climate to the Department of Defense*. Page 2.

challenges associated with a warming atmosphere and ocean, diminishing amounts of snow and ice, and a rising sea level, for which it needs to prepare.<sup>10</sup>

Workshop participants noted that the changing climate necessarily had profound national and homeland security implications. In his statement for the record to the Senate Select Committee on Intelligence, the Director of National Intelligence, Daniel Coats, reflecting the collective insights of the U.S. Intelligence Community noted that “Global environmental and ecological degradation, as well as a changing climate, are likely to fuel competition for resources, economic distress, and social discontent through 2019 and beyond.<sup>11</sup> The statement highlights the threats that irreversible damage to ecosystems; extreme weather events; changes in heat wave, drought, and flooding frequency and intensity; and diminishing sea ice in the Arctic pose to national, homeland, and economic security. It also addresses the potential for global instability due to human health effects and displacement attributable to changing climatic conditions and environmental degradation. The *Fourth National Climate Assessment*, released in 2018, asserts that “Climate change creates new risks and exacerbates existing vulnerabilities in communities across the United States, presenting growing challenges to human health and safety, quality of life, and the rate of economic growth,” all of which have homeland security implications.<sup>12</sup>

While the hazards posed by a changing climate seem daunting, adaptation actions can help build resilience and mitigate the associated costs.<sup>13</sup> Measures that individuals can take include elevating the furnace in a home susceptible to flooding, installing hurricane wind-resistant roofs, and planting drought-resistant seeds. Communities can decide to prevent development within a floodplain, build seawalls and other protective infrastructure, enact stricter building codes, and use design standards that take into account projected hazards rather than historical hazards. Promoting actions that individuals, communities, businesses, and economic sectors can undertake to mitigate risks from natural hazards will help improve resilience on a national level.

---

<sup>10</sup> Intergovernmental Panel on Climate Change. 2013. *Climate Change 2013: The Physical Science Basis*. [Stocker, T.F., D. Qin, G.-K. Plattner, M. Tignor, S.K. Allen, J. Boschung, A. Nauels, Y. Xia, V. Bex and P.M. Midgley (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA.

<sup>11</sup> Coats, Daniel. “Worldwide Threat Assessment of the U.S. Intelligence Community.” Statement for the Record. Senate Select Committee on Intelligence. Washington, DC. January 29, 2019. Page 23.

<sup>12</sup> USGCRP. 2018. *Impacts, Risk, and Adaptation in the United States: Fourth National Climate Assessment, Volume II*. [Reidmiller, D. R., C.W. Avery, D.R. Easterling, K.E. Kunkel, K.L.M. Lewis, T.K. Maycock, and B.C. Stewart (eds.)]. U.S. Global Change Research Program, Washington, DC, USA, 1515 pp. doi: 10.7930/NCA4.2018

<sup>13</sup> Ibid.

## 1. Why should the executive branch address this topic?

The topic of climate change has been increasingly politicized in the national discourse, with climate science either promoted or dismissed by those that either favor or disagree with regulatory policies that are influenced by that science.<sup>14</sup> This politicization is preventing individuals, communities, and businesses from taking actions that would enhance their resilience.

There is a need for the coordinated collection of continuous, high-quality, calibrated observations of the atmosphere, cryosphere, hydrosphere, and biosphere. These observations are necessary both to understand the current status of the Earth's climate system and also to improve the models that project the future state of the climate. While reducing the uncertainty in future projections can help improve the information accessible to decision-makers, focusing on what is unknown rather than what is known has continued to seed doubt on climate science and bolster arguments that action can wait until the science is settled. The continuing need for observations and modeling efforts to reduce levels of uncertainty does not eliminate the need to take action given the information on which the scientific community has already reached consensus. Refocusing the national discussion away from the causes of climate change to what to do given that the climate is changing will promote communities, businesses, and individuals to undertake activities that reduce their vulnerabilities and increase their adaptive capacity, ultimately saving lives and property.

There is no single agency in charge of researching, funding, and implementing climate adaptation measures; rather, there is a patchwork of efforts that spans nearly every Federal agency. The Federal Emergency Management Agency offers funding for pre-disaster mitigation actions. The U.S. Department of Housing and Urban Development gives disaster recovery funding that can be used to help communities prepare for subsequent disasters. The U.S. Department of Agriculture (USDA), the National Oceanic and Atmospheric Administration, and multiple departments within the Department of the Interior operate regional centers that give climate and hazard information to different target users. The topic of climate adaptation and natural hazard resilience is partially covered by two interagency subcommittees but is the focus of neither. The executive branch should bring together expertise from across the agencies to discuss how the United States can and should ready the Federal Government; State, local, and Tribal governments; individuals, businesses, and economic sectors to prepare for and adapt to natural hazards.

---

<sup>14</sup> McCright, Aaron M., and Riley E. Dunlap. 2011. "The Politicization of Climate Change and Polarization in the American Public's Views of Global Warming, 2001–2010." *The Sociological Quarterly*, 52:2, 155-194, DOI: 10.1111/j.1533-8525.2011.01198.x

## 2. How should the executive branch address this topic?

In order to improve the Nation's resilience to natural hazards, the executive branch could:

- Develop a comprehensive, interagency strategy to help the Federal Government, State, local, and Tribal governments, economic sectors, businesses, and individuals prepare for the effects of a changing climate.
- Ensure that products and services aimed at increasing resilience to natural hazards are developed and disseminated in ways that make the information discoverable, accessible, and usable.
- Develop a plan for addressing gaps in the collection of Earth observations. Continuous, high-quality, calibrated, observations of the atmosphere, cryosphere, hydrosphere, and biosphere are all necessary to improve the models used to project the future state of the climate.
- Convene an interagency task force co-chaired by the DOD, Department of Homeland Security (DHS), and the U.S. Global Change Research Program to develop an action plan to address the threats that the changing climate poses to critical and civil infrastructure, the built environment, military installations, and the ability of the emergency response system to adequately protect lives and property.

This strategy could be developed either by a new interagency group focused on resilience and adaptation, or by existing interagency groups. The DOD views activities to mitigate the risks of a changing climate as being a component of broader risk management frameworks.<sup>15</sup> The interagency strategy proposed above could provide guidance for addressing natural hazards as part of a broader plan for risk management.

A strategy on natural hazard resilience can help de-politicize the use of climate information by focusing on the actions needed to become more resilient to the effects of extreme weather events. Certain types of events, such as temperature and precipitation extremes, have changed in frequency, intensity, and duration as the climate system has

---

<sup>15</sup> Naval Facilities Engineering Command. 2017. *Climate Change Installation Adaptation and Resilience*. January 2017.  
[https://www.fedcenter.gov/\\_kd/Items/actions.cfm?action=Show&item\\_id=31041&destination=ShowItem](https://www.fedcenter.gov/_kd/Items/actions.cfm?action=Show&item_id=31041&destination=ShowItem)

warmed.<sup>16,17</sup> By focusing on adaptation, the executive branch can ensure that the United States is capitalizing on new opportunities to manage risks wisely, maintain international competitiveness, and enhance resilience.

### **3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

Proactively addressing adaptation will be more cost-effective than a reactive approach. A recent report by the U.S. Environmental Protection Agency states that “proactive adaptation measures implemented in anticipation of future climate change risks are generally more cost-effective in reducing damages than reactive adaptation responses implemented after impacts have already occurred.”<sup>18</sup> In addition to the direct economic costs of waiting until hazards have already occurred, there is the potential for the U.S. to lose a competitive advantage internationally. Given that other nations are addressing the impacts of a changing climate, loss of U.S. participation means that other countries may shape a global approach without consideration for U.S. interests.

In developing an adaptation strategy the executive branch should, at the interagency level, consider whether to include climate intervention research. The National Academy of Sciences has issued reports examining carbon dioxide removal and albedo modification as potential strategies to counter the impacts of a changing climate and recommended a deliberative process to examine the types of governance that would be needed for this type of research.<sup>19</sup> Given that these interventions have potentially large scale impacts, it is incumbent on the executive branch to find a coordinated way to determine whether this research should be included as part of a comprehensive strategy.

## **B. Harnessing Advances in the Life Sciences**

Research and development (R&D) in rapidly emerging fields such as molecular biology, biotechnology, and health information technology are driving advances in the agriculture, behavioral science, biomedical science, energy, and healthcare sectors. These advances cross traditional government agency jurisdictions, industry sectors, and academic disciplines and

---

<sup>16</sup> National Academies of Sciences, Engineering, and Medicine. 2016. *Attribution of Extreme Weather Events in the Context of Climate Change*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/21852>.

<sup>17</sup> Climate Science Special Report. “Highlights of the Findings of the U.S. Global Change Research Program Climate Science Special Report.” Accessed 8 January 2019. <https://science2017.globalchange.gov/chapter/executive-summary/>

<sup>18</sup> Martinich, Jeremy and Allison Crimmins. 2017. *Multi-Model Framework for Quantitative Sectoral Impacts Analysis: A Technical Report for the Fourth National Climate Assessment*. 10.13140/RG.2.2.14466.79045.

<sup>19</sup> National Academies of Sciences, Engineering, and Medicine. 2015. *Report in Brief: Climate Intervention*. <http://dels.nas.edu/resources/static-assets/materials-based-on-reports/reports-in-brief/climate-intervention-brief-final.pdf>

have the potential to provide enormous benefits but also to increase health and security risks. As this occurs, and other countries expand their investments in these fields, it is incumbent on the U.S. to develop a policy framework that promotes responsible R&D across the life sciences, adequately anticipates risk, and protects stakeholders from adverse actions and outcomes. The scientific and security communities should continue collaboration to develop measures to detect and manage misuse of advances in the life sciences, while allowing responsible R&D to flourish.

### 1. Why should the Federal Government address this topic?

Over 20 separate Federal agencies have directly supported research or contributed to interagency activities related to the biotechnology sector and its implications for the U.S. economy. Additionally, there is a large and diverse set of stakeholders across these sectors with varying interests, equities, and vulnerabilities that must be considered. In 2012, as an initial step toward developing a policy framework to promote responsible R&D in the life sciences, the Federal Government began to identify emerging bio-based R&D and their contributions to the country with the *National Bioeconomy Blueprint*.<sup>20</sup> According to the *Blueprint*, “A bioeconomy is based on the use of research and development in the biological sciences to create economic activity and public benefit. The U.S. bioeconomy is all around us: new drugs and diagnostics for improved human health, higher-yielding food crops, emerging biofuels to reduce dependency on oil, and bio-based chemical intermediates, to name just a few.” The document describes aspects of the bioeconomy related to health, energy, agriculture, and the environment, and discusses ongoing research initiatives, technology transfer activities, workforce development strategies, regulatory reinvention approaches, and public-private partnerships intended to ensure U.S. leadership in these areas. It does not, however, describe new initiatives to be undertaken, nor does it discuss potential economic and security risks.

Outside of the U.S., the European Commission, Finland, France, Germany, South Africa, and the United Kingdom have published overarching bioeconomy strategies. Several other countries have published national guidance documents on bioeconomy issues without using the term. Six countries of interest had no published bioeconomy strategy, but did have a national-level biotechnology or biotechnology-aligned strategy: Argentina, China, India, Japan, Singapore, and South Korea. For example, *The 13th Five-Year Plan for Economic and Social Development of the People’s Republic of China (2016-2020)* was published in 2016 by the Central Committee of the Communist Party of China. This plan is a general overview

---

<sup>20</sup> The White House. 2012. *National Bioeconomy Blueprint*.  
[https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national\\_bioeconomy\\_blueprint\\_april\\_2012.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf)

of proposed development areas, including agricultural modernization, optimized modern industrial systems, the cyber economy, and innovation-driven development.

There have been two publicized examples of attempted bioeconomic espionage by Chinese nationals in which attempts were made to steal proprietary material for the purpose of developing better agricultural products in China. With rapid advances in life sciences R&D and the growth of a U.S. bioeconomy come increasing security risks and threats to physical proprietary materials and bioinformatics.

## **2. How should the executive branch address this topic?**

In order to maintain responsible R&D in the life sciences and generate value through the bioeconomy, the executive branch could:

- Convene stakeholders and subject matter experts to fully understand the extent, components, and value of the bioeconomy. This group should include academic researchers, private sector technologists, bioethicists, healthcare and health data analysts, behavioral and cognitive scientists, and national security and intelligence community representatives, among others.

The objective of convening these stakeholders and understanding their interests and perspectives is to craft a policy and regulatory environment that: (1) allows universities to translate basic research and ideas to the marketplace in an easier and efficient manner; (2) enables the adoption of advances in the life sciences to more rapidly decrease medical treatment costs; (3) provides guidance to address unintended consequences, such as ethical implications and risks to individual privacy and liberty; and (4) promotes the integration of the life sciences with other disciplines to increase awareness of emerging biotech R&D among stakeholders.

## **3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

Public and private sector investment in life sciences R&D has enabled recent generations to live longer, but failure to responsibly address the opportunities and risks associated with advances in the life sciences may mean that citizens are unable to further benefit from novel biotechnology breakthroughs. Of particular concern is the potential offshoring of life sciences R&D and biotechnology industries, possibly to countries with looser regulatory regimes. This both raises the risk that certain strains of R&D move completely out of the U.S. and that irresponsible R&D increases the risk posed to human and environmental health from biohazards. For instance, a loss of domestic drug development and production capacity could diminish access to world class drugs and medicines for U.S. healthcare consumers.

In addition to the many national strategies and policy documents that are guiding other nations' investments in the bioeconomy, the U.S. National Academy of Sciences has convened a series of workshops entitled, "Safeguarding the Bioeconomy" to explore the opportunities and risks associated with advances in the life sciences. As one of the few major economies without a policy guidance document on the bioeconomy, the U.S. could easily see China becoming the primary driver in the bioeconomy sector, allowing its life sciences R&D centers and biotechnology industries to achieve a competitive advantage over U.S. counterparts and set global standards that may run counter to U.S. interests.

### **C. Maintaining and Improving Science Infrastructure**

One of the cross-cutting themes to emerge from the S&T Future Workshops was the critical importance of maintaining and advancing the infrastructure that underpins all scientific progress in the U.S. The U.S. R&D enterprise requires a skilled and empowered S&T workforce, state of the art facilities and equipment, and a flexible policy and regulatory environment. Participants discussed how other nations are investing substantially in their infrastructure to become leaders in certain S&T areas, which may have implications for continued U.S. leadership and relevancy on topics. The experts highlighted a few key areas that needed immediate focus to ensure a robust science infrastructure: investments in large research facilities; competitiveness of the U.S. manufacturing base; training, hiring, and flow of government scientists and engineers; and rules and requirements surrounding technology transfer and commercialization of federally funded R&D.

#### **1. Why should the executive branch address this topic?**

Participants used a broad definition of what could be covered under science infrastructure to include improving existing research facilities, inspiring the workforce, and adopting regulations that facilitate further development of federally funded technologies. The particular areas of focus that participants discussed fell into three categories: (1) government science, technology, engineering, and mathematics (STEM) workforce, (2) Federal laboratory infrastructure and large scale research facilities, and (3) rules and requirements for technology transfer and commercialization. Each of these topics is discussed in more detail below.

The rallying cry around the shortage of STEM workers<sup>21</sup> has proven to be an oversimplification of a more complex situation—academia is generally oversupplied, but the

---

<sup>21</sup> President's Council of Advisors on Science and Technology. 2012. *Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Mathematics*. [https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-engage-to-excel-final\\_2-25-12.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-engage-to-excel-final_2-25-12.pdf)

government and industry have shortfalls in specific areas.<sup>22</sup> In addition, while the STEM workforce is growing, the lack of diversity in the STEM workforce, particularly the underrepresentation of African Americans and Latinos, remains a persistent issue.<sup>23</sup> The participants argued that without civil service reform, we will lose S&T capabilities that we need. The experts agree—for example, the Partnership for Public Service and the Volcker Alliance have developed a plan to renew the civil service by improving how the government recruits, develops, and manages its workforce.<sup>24</sup> Training and retraining is a key component to a healthy STEM workforce as S&T fields change over time. The Federal cybersecurity workforce is especially hampered by the lack of a talent pipeline, fragmented governance and uncoordinated leadership, and complicated hiring processes and rules,<sup>25</sup> and the number of cybersecurity jobs outpaces the number of people qualified to fill them in the country as a whole.<sup>26</sup> In addition, organizations are handicapped by the clearance process; the backlog has grown to more than 700,000 people and in January 2018 the Government Accountability Office (GAO) added it to its High Risk List of Federal areas in need of either broad-based transformation or specific reforms.<sup>27</sup> Enabling flow between industry, government, and academia allows a refresh of ideas and improves the quality of candidates the government can attract. While mechanisms exist for personnel exchanges, significant challenges remain and many are underutilized.<sup>28</sup> Coordination across executive branch S&T agencies is needed to collectively improve workforce practices and enhance the S&T posture of the United States.

In addition to having a strong workforce, continued technological progress is dependent on adequate R&D infrastructure. Aging and deteriorating facilities and infrastructure of Federal laboratories threaten the ability to successfully complete missions. Facilities' spending often takes a back seat to R&D, leading to ever-increasing deferred

---

<sup>22</sup> Xue, Yi, and Richard Larson. 2015. "STEM Crisis or STEM Surplus? Yes and Yes." *Monthly Labor Review*, U.S. Bureau of Labor Statistics, May 2015, <https://doi.org/10.21916/mlr.2015.14>.

<sup>23</sup> Funk, Cary, and Kim Parker. 2018. *Women and Men in STEM Often at Odds Over Workplace Equity*. Pew Research Center. Jan. 9, 2018.

<sup>24</sup> Partnership for Public Service and the Volcker Alliance. 2018. *Renewing America's Civil Service*. September 2018.

<sup>25</sup> Partnership for Public Service and Booz Allen Hamilton. 2009. *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce*. July 2009.

<sup>26</sup> Department of Homeland Security. 2018. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. September 2018.

<sup>27</sup> GAO. 2018. "GAO Adds Government-wide Personnel Security Clearance Process to 'High Risk List.'"

<sup>28</sup> Howieson, Susannah V., Elmer Yglesias, Samuel L. Blazek, and Daniel E. Basco. 2013. *Federal Personnel Exchange Mechanisms*. IDA Document D-4906, November 2013.

maintenance.<sup>29</sup> At the National Nuclear Security Administration (NNSA), for example, funding levels have consistently fallen below facility and infrastructure needs to combat maintenance deferrals and complete large scale research facilities.<sup>30</sup> In addition, defense laboratories have a difficult time competing for funding with other military infrastructure requirements.<sup>31</sup> When looking at large scale research facilities in the aerospace and aeronautics sector there are also critical gaps—stably funded wind tunnels are needed for testing, with specialized facilities needed for hypersonic vehicle testing, as the United States currently does not have the wind-tunnel capacity needed to accommodate the growing number of hypersonics programs.<sup>32,33</sup>

The knowledge and products that result from federally funded R&D, both from Federal laboratories and from other government institutions, universities, and corporations, have the potential to strengthen the economy and deliver benefits to society. The participants argued that deregulation of technology transfer is critical to our S&T future and the Nation is not adequately leveraging the investment byproducts of Federal R&D. The ownership and transfer of federally funded S&T is governed by a series of laws and associated regulations and policy that originally date back to the 1980s. As such, these laws and regulations need updates and clarification to facilitate further development of federally funded R&D to the maximum extent possible. For example, computer software and other digital products are frequently protected via copyright outside of the Federal Government. However, works created by government employees are not eligible for copyright protection.<sup>34</sup> Government researchers have reported that the prohibition on copyrighting government digital products has led to lost revenue because software is freely disseminated; there is a lack of control over potentially sensitive code; the commercial potential for partners seeking to further develop

---

<sup>29</sup> Commission to Review the Effectiveness of the National Energy Laboratories. 2015. *Securing America's Future: Realizing the Potential of the Department of Energy's National Laboratories, Volume 2*. Washington, DC: U.S. Department of Energy.

<sup>30</sup> GAO. National Nuclear Security Administration. 2017. *Action Needed to Address Affordability of Nuclear Modernization Programs*. GAO-17-341. April 2017.

<sup>31</sup> Howieson, Susannah V., Vanessa I. Peña, Stephanie S. Shipp, Kristen A. Koopman, Justin A. Scott, and Christopher T. Clavin 2013. *A Study of Facilities and Infrastructure Planning, Prioritization, and Assessment at Federal Security Laboratories (Revised)*. IDA Paper P-4916, Revised, February 2013

<sup>32</sup> American Institute of Aeronautics and Astronautics. 2008. *Infrastructure Recommendations for Implementation of Executive Order 13419—National Aeronautics Research and Development*. 11 January 2008.  
[https://www.aiaa.org/uploadedFiles/Issues\\_and\\_Advocacy/Aeronautics/windtunnelinfrastructurepaperbodaapproved011108.pdf](https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/Aeronautics/windtunnelinfrastructurepaperbodaapproved011108.pdf)

<sup>33</sup> Piscopo, Paul, Richard Hallion, Terrence Trepal, and Mark Lewis. 2014. *Study on the Ability of the U.S. Test and Evaluation Infrastructure to Effectively and Efficiently Mature Hypersonic Technologies for Defense Systems Development: Summary Analysis and Assessment*. IDA Report GR-74. Washington, DC: IDA Science and Technology Policy Institute.

<sup>34</sup> 17 U.S.C. § 105 – Subject matter of copyright: United States Government works

government work is diminished due to its lack of exclusivity; and in some cases, third parties subsequently assert copyright, and as a result, the government must pay to use its own inventions.<sup>35</sup> Another issue involves the variations across agency technology transfer policies and practice because of different interpretations of guiding legislation. There are also public misperceptions or misunderstandings of policies due to confusing or vague statutory language. The executive branch can play an important role in harmonizing guidance and regulation to provide clarity and consistency.

## 2. How should the executive branch address this topic?

Specific actions that the executive branch could take include:

- Develop an overarching strategy for maintaining and improving U.S. science infrastructure.
- Identify critical Federal laboratory facilities and infrastructure and large scale research infrastructure that need focused attention and investment. Members of the group highlighted a few areas they felt were particularly under-resourced, namely wind tunnels and flight test ranges for testing new advances in aerospace and trusted foundries for developing microelectronic technologies for both civil and national security applications.
- Identify potential workforce pipeline issues (including retention) and ways in which to train and inspire scientists.
- Strategically focus training in areas that lack people, including in emerging areas of R&D. These could include training opportunities for undergraduate and graduate students. For example, for the Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative, there is a need for engineering and life sciences cross-training into health, as well as researchers that have translational skills.
- Increase the speed and efficiency of the clearance granting process and expand the ability for agencies to grant clearances to technical experts from industry and academia to assume temporary duties in government during a crisis.
- Enable Federal, industry, and academic staff to trade places through rotations. One potential area of focus is to encourage agencies to replicate the rotator model at the National Science Foundation, DARPA, and the Advanced Research Projects

---

<sup>35</sup> Hughes, Mary E., Susannah V. Howieson, Gina K. Walejko, Nayanee Gupta, Seth Jonas et al. 2011. *Technology Transfer and Commercialization Landscape of Federal Laboratories*, Washington, DC: IDA Science and Technology Policy Institute; Howieson, Susannah V., Stephanie S. Shipp, Gina K. Walejko, Pamela B. Rambow, Vanessa Peña, et al. 2013. *Exemplar Practices for Department of Defense Technology Transfer*. Washington, DC: Science and Technology Policy Institute.

Agency-Energy, as well as expand personnel exchanges to include private sector employees. Participants asserted that energy researchers in particular should spend time in the private sector.

- Increase the speed and efficiency of Federal agency hiring to enable agencies to hire qualified individuals within 60 to 90 days of submitting an application.
- Help craft an environment that is easier for universities to translate ideas to the marketplace, as well as promote greater coordination between universities, venture capital groups, and national laboratories. Participants pointed out that entrepreneur in residence programs are successful but not widespread across government.

To help inform these efforts, the participants suggested establishing and maintaining communication channels between the EOP, Federal S&T agencies, and the scientific community.

### **3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

The group focused largely on the consequences of inaction if the United States does not address this topic. These consequences include the United States losing its economic advantage, freedom to act, and becoming increasingly dependent on other countries for critical technologies. Additionally, there could be a deterioration in the standard of the workforce capable of building and leveraging new S&T advances. As a comparison, China has taken significant strides in science and engineering (S&E) education and is now the world's number one producer of undergraduates and PhDs with S&E degrees.<sup>36</sup> Without high quality laboratory facilities and infrastructure and cutting edge large scale research infrastructure, the U.S. risks losing its S&T leadership position. This could also lead to the departure of quality S&Es, if they are drawn to superior facilities abroad. If the U.S. does work to enhance its government STEM workforce, reskilling and upskilling employees can lead to job creation. Alternatively, if training does not occur in the critical emerging areas, the S&T pipeline into government could falter, particularly if there is a single point of failure. Without updates to the technology transfer regime, the country risks technological breakthroughs languishing in university and government laboratories.

## **D. Strengthening the Built Environment**

The built environment, comprised of the critical infrastructure and buildings that together represent the Nation's cities and rural communities, is a set of dynamic

---

<sup>36</sup> Veugelers, Reinhilde. 2017. "China is the World's New Science and Technology Powerhouse." BRINK Asia. August 30, 2017.

technological systems that are continually in use and in need of maintenance and upgrade. Critical infrastructure systems, such as electric power grids, communications, and transportation, provide the United States with a number of vital services that support the Nation's economy, security, and health.<sup>37</sup> Many components of this infrastructure have degraded due to lack of investment. The American Society of Civil Engineers gave American infrastructure a D+ in their 2017 Infrastructure Report Card (representing poor to fair condition and mostly below standard), and estimated \$2.0 trillion in funding needed to raise the grade of infrastructure to a B (which would represent good to excellent condition).<sup>38</sup> The report cites a \$90 billion rehabilitation backlog for American transit systems, \$123 billion needed to address the rehabilitation backlog for American bridges, and 15,498 dams with high-hazard potential, among other needs.<sup>39</sup> The White House has a stated commitment to ensuring the Nation's infrastructure systems are maintained, upgraded, and new technologies are integrated to meet the needs of future generations.<sup>40</sup>

Ensuring the continued maintenance and operations of these systems and their operations is essential for the Nation to thrive economically. Looking into the future, the interconnected nature of these systems is likely to increase—presenting unknown challenges—and new technologies will require upgrades or altogether new infrastructure systems that will integrate with existing systems. Further, as the disasters of 2017 and 2018 have demonstrated, the current built environment remains vulnerable to increasing frequency and intensity of natural hazards, presenting a challenge of hardening these systems while rebuilding them in a manner that increases their resilience to future stronger and more frequent hazard events.<sup>41</sup> Collectively, these challenges of maintaining the existing quality built environment and its infrastructure, while providing an environment for new technologies to enhance the performance and resilience of the built environment are important S&T opportunities for the Nation.<sup>42</sup>

---

<sup>37</sup> National Research Council. 2009. *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives: Report of a Workshop*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/12638>.

<sup>38</sup> American Society of Civil Engineers. "2017 Infrastructure Report Card." Accessed 28 March 2019. <https://www.infrastructurereportcard.org/americas-grades/>

<sup>39</sup> Ibid.

<sup>40</sup> Recent examples include supporting S.3021 America's Water Infrastructure Act of 2018 (Oct 2018), proclaiming Critical Infrastructure Security and Resilience month (Oct 2018), convening a summit on AI for American Industry (May 2018).

<sup>41</sup> National Research Council. 2012. *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/13457>.

<sup>42</sup> Woetzel et al. 2018. *Smart Cities: Digital Solutions for a More Livable Future*. McKinsey Global Institute. <https://www.mckinsey.com/~media/McKinsey/Industries/Capital%20Projects%20and%20Infrastructure/Our%20Insights/Smart%20cities%20Digital%20solutions%20for%20a%20more%20livable%20future/MGI-Smart-Cities-Full-Report.ashx>

## 1. Why should the executive branch address this topic?

Maintenance of the built environment is an inherently collaborative effort between the public and private sector. The built environment's critical infrastructure is a series of highly technical systems that require the executive branch's leadership to establish priorities for new technology development and deployment, to set common standards, establish minimum safety performance and quality standards, and underwrite investments in large infrastructure projects.<sup>43</sup> To achieve a built environment that is secure and resilient, coordinated executive branch attention is needed since there is no single agency accountable for these responsibilities, and the concurrent emergence of multiple technologies (e.g. autonomous vehicles, advanced materials for construction, telecommunications infrastructure) could lead to an evolution in the processes through which the built environment is planned, maintained, and developed.

One area of focus could be building and rebuilding better cities. Cities are the economic engines of our Nation. The buildings, infrastructure systems, and the individuals that rely upon the built environment of the Nation's cities require efficient operations that respond to changing daily demands, while being flexible to meet currently unknown future demands.<sup>44</sup> There is a Federal role in ensuring organized and safe deployment of new infrastructure system technologies, which may come from advances in material science developing infrastructure with novel properties, new technologies enhancing the ability of infrastructure operators to understand the performance of their systems, or new services becoming available to consumers. There is also a Federal role to help resolve potential conflicts between interdependent infrastructure systems. Further, there are opportunities for the executive branch to support the deployment of new smart infrastructure technologies that enable increased efficiencies and high capacity of existing infrastructure systems (e.g. smart transportation systems).

Another potential area of focus that would affect many communities across the United States is increasing the resilience of critical infrastructure systems. Critical infrastructure systems, such as electric power grids, communications, and transportation, provide the Nation with a number of vital services that are essential to economic activity, security, and health.<sup>45</sup> These systems must be responsive to changes in demands from individuals, major institutions, and operators. Resilient infrastructure systems must be able to perform their intended functions during and after natural hazard events, or degrade in a predictable manner such that they can quickly be repaired and restored. Ensuring that minimum

---

<sup>43</sup> Department of Homeland Security. "Sector-Specific Agencies." Accessed February 1, 2019. <https://www.dhs.gov/sector-specific-agencies>.

<sup>44</sup> National Association of City Transportation Officials. 2018. "Blueprint for Autonomous Urbanism." Accessed February 1, 2019. <https://nacto.org/publication/bau/>

<sup>45</sup> National League of Cities. 2018. "Autonomous Vehicles: Future Scenarios." Accessed January 28, 2019. <http://avfutures.nlc.org/>

operating standards are developed and coordinated across infrastructure sectors and Federal agencies is a key activity that the executive branch could undertake.

Of the critical infrastructure systems that the executive branch may want to focus on, the generation and distribution of electricity offer opportunities to leverage the existing built environment to enhance the Nation's renewable electricity generation potential. In some locations, the development and deployment of energy storage technologies combined with microgrid technology has been attempted to achieve environmental and grid reliability objectives. Technology deployment achievements such as these represent the interface of a significant technology and built environment advance, and also foreshadow challenges to ensure future distributed energy technology deployment is achieved in such a manner that these integrated systems operate seamlessly with other elements of the built environment.<sup>46</sup>

## 2. How should the executive branch address this topic?

Federal agencies have their own respective authorities and responsibilities for establishing and enforcing standards for infrastructure systems and funding the public systems that affect the urban built environment (e.g. public transit, interstate maintenance funding, and water quality regulations).<sup>47</sup> To strengthen the built environment, the executive branch could coordinate to:

- Identify opportunities for the executive branch to aid the development and deployment of advanced technologies that improve cities and urban living. This could include efforts to pilot the deployment of new technologies, streamline permitting requirements for small-scale demonstration projects, or address challenges in reducing regulatory barriers between various infrastructure systems that have Federal oversight.
- Set joint priorities for establishing infrastructure performance design requirements that ensure future Federal investments into existing or new infrastructure are designed to be resilient to future hazards. It could also entail working with military bases or State and local governments that have been leaders in ensuring their infrastructure upgrades are designed appropriately for the next century and set examples for the Nation.

---

<sup>46</sup> National Academies of Sciences, Engineering, and Medicine. 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/24836>.

<sup>47</sup> Department of Homeland Security. 2018. "Infrastructure Systems Recovery Support Function" as part of the National Disaster Recovery Framework. [https://www.fema.gov/media-library-data/1466718036457-e2026c3a5907bf0cb86e75b3a3c51757/RSF\\_Infrastructure\\_Systems\\_0623\\_508.pdf](https://www.fema.gov/media-library-data/1466718036457-e2026c3a5907bf0cb86e75b3a3c51757/RSF_Infrastructure_Systems_0623_508.pdf)

- Identify how the public and private sectors can set joint priorities and work together to advance electricity distribution system performance as new technologies increase demands on existing distribution system infrastructure.

In order to strengthen the built environment, it will be crucial to coordinate not only with all of the Federal agencies involved, but also the State, local and Tribal governments, and the private sector.

### **3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

State and local governments are already taking steps to demonstrate the potential that advanced technologies could play in progressing elements of the built environment.<sup>48</sup> For example, communities in the Southwest are a technology demonstration ground for autonomous vehicles. As private sector companies aim to deploy advanced technology into public use, State and local governments continue to take leadership roles in facilitating their deployment. Without Federal S&T leadership, these technology advances may occur in an ad hoc manner and without minimum standards that ensure public safety or could cause setbacks in technology deployment pathways. The executive branch has an opportunity to leverage a broad set of stakeholders that have an interest in building, renovating, and designing the next generation of the Nation’s built environment to meet increasing needs, meet future demands, and ensure its resilience to the next century’s natural hazards.

## **E. Improving Cybersecurity Research and Implementation**

Security and ease of use often stand in opposition to one another. A system that is fully secure does not allow itself to interact with the outside world, while a system that is easy to use is, by definition, easy to compromise. Finding the balance between secure systems and ease of use requires incorporating security as an early—if not primary—design consideration.<sup>49</sup> Too often, technology is developed and only later security is grafted on: pacemakers and insulin pumps, self-driving vehicles, and unmanned aerial vehicles certified for public use, configurable via wireless technologies, but with no security built in or security features turned off by default. This security-eventually mindset affords malicious actors ample opportunity to exploit design features and end user configuration errors—in ways not conceived of by the inventors of technologies—which cannot be retroactively addressed.

The need for security permeates modern society from individual identity verification of humans to the complex interconnection of computational systems. Old models of security through obscurity have long been insufficient to ensure authentication of users and systems,

---

<sup>48</sup> AECOM. 2019. “The Future of Infrastructure: Voice of the People.” <https://infrastructure.aecom.com/>

<sup>49</sup> For more information, see “Cyber Assured Systems Engineering,” available at <https://www.darpa.mil/program/cyber-assured-systems-engineering>

authorization of actions, or auditing of behaviors, but remain all too common. Manufacturers regularly release products to market that have no default security or default security that is constant across a product line, making administrative usernames and passwords easy to know and easy to discover both by legitimate end users and, unfortunately, malicious actors. Social Security and bank account numbers, long considered reasonable forms of identification, now are readily available for sale on the web.

Similarly, old models that relied on ensuring a secure perimeter—firewalls, password protected portals, etc.—are manifestly inadequate in the mobile, bring-your-own-device, ad hoc computing environments extant globally today. The need for security is consistent: a consumer wishes to add a voice-activated digital assistant to their home or a military unit needs to deploy a swarm of reconnaissance drones, the need to add new devices to infrastructure quickly and securely while preventing others from adding malicious devices to your infrastructure and preventing devices from being used in unintended ways is shared.

### **1. Why should the executive branch address this topic?**

As our society and infrastructure continue to depend on computing technologies to provide convenience, ensure security, and protect human life, it is vital that cybersecurity be a primary concern for all stakeholders. The costs—financial, social, and personal—are too great for security to be an afterthought. Yet, public policy is often outpaced by technological advances. Guidance, regulations, and laws too often rely on dated definitions and assumptions about the nature and capabilities of technology. This often puts innovators at odds with existing legal frameworks and creates uncertainty about what is permissible or even desirable.

Policy makers have given much attention to cybersecurity research, development, implementation, and commercialization in recent years. The principles laid out in the 2018 *National Cyber Strategy*<sup>50</sup> and the research focuses offered in the 2016 *Federal Cybersecurity Research and Development Strategic Plan*<sup>51</sup> provide a policy model to evaluate and implement research programs and best practices suggested by academia, industry, and expert panels, such as the considerable body of work laid out by the National Academies of Sciences, Engineering, and Medicine.<sup>52</sup> This work details challenges and new directions in cybersecurity research, encryption, cyber resilience, cyber workforce

---

<sup>50</sup> The White House. 2018. *National Cyber Strategy of the United States of America*. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>

<sup>51</sup> National Science and Technology Council. 2016. *Federal Cybersecurity Research and Development Strategic Plan*. <https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf>

<sup>52</sup> For more information, see the Cybersecurity Collection: <https://www.nap.edu/collection/31/cybersecurity>

development and retention, and securing public voting systems. Basic research being undertaken by organizations such as DARPA to develop secure computing infrastructure suggests a path forward for secure-by-design computing systems.<sup>53</sup>

Some progress has been made over the past decade as the government and businesses have become more aware of the risks and costs associated with neglecting security concerns and have begun to adopt reporting standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.<sup>54</sup> Even with these efforts, there is still a need to support the implementation of cybersecurity activities, both within Federal agencies and the public and private sectors, as well as within the general public. Interagency coordination of cybersecurity R&D efforts through the Networking and Information Technology Research and Development (NITRD) Program Office should continue, and it can play an expanded role in publicly advocating for increased implementation of security measures and reporting standards across agencies, the public and private sectors, and within the general public.

## 2. How should the executive branch address this topic?

Specific actions the executive branch could take include:

- Develop policies that articulate clearly the societal benefits and concerns that technology should address, rather than dictating the specific features of the technology.
- Create a policy framework where liability for action or inaction can be reasoned about and quantified, providing insurers and businesses with a reasonable basis for engaging in and managing the risks of new technology. By increasing the liability to businesses for failing to adequately address the security goals laid out by public policy, companies can be incentivized to embed cybersecurity as an early design principle.
- Adopt a targeted investment strategy through purchasing, cost sharing, prizes, and awards to further encourage businesses to address public cybersecurity needs where there exists a failure of the market to do so.
- Incentivize the development of new models to characterize the security of systems, quantify the degree of security, qualify the conditions under which security is maintained, and be able to document and share information concerning security best practices, methods, and incidents.
- Explore including cybersecurity as a component of continuity of operations.

---

<sup>53</sup> DARPA. "Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)." Accessed March 1, 2019. <https://www.darpa.mil/program/clean-slate-design-of-resilient-adaptive-secure-hosts>

<sup>54</sup> NIST. 2018. "NIST Cybersecurity Framework." <https://www.nist.gov/cyberframework>

### 3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?

The benefits of high-quality, trustworthy, and easy to use cybersecurity include increased productivity; decreased government, business, and individual costs; increased privacy; increased public trust in systems, businesses, and government; and decreased crime.

Failure to incorporate cybersecurity concerns in the early design stage poses risks to privacy, health, wealth, property, security, and life. Compromised user accounts on a social media site by a communications provider or by an employment website risk disclosure and exploitation of information gained about citizens, which could damage reputation, employability, electability, or reveal criminal behavior. Compromised corporate systems risk disclosure of trade and design secrets, undermine consumer confidence in businesses, and can erode the value of markets. Compromised industrial systems risk damage to infrastructure, productivity, and human life. Compromised government and military systems risk damage to human life and national and global security.

## F. Protecting the Science Communication Environment

Scientific knowledge that is accurate, timely, and available to citizens as well as public and private sector institutions contributes to individual and collective well-being by providing critical information that has the potential to improve decisions and their outcomes.<sup>55, 56</sup> Since there is more scientific knowledge available to decision-makers and the general public than any individual can reasonably understand, experts and institutions play important roles as intermediaries in interpreting scientific evidence.<sup>57, 58, 59, 60</sup> Their analysis, views, positions, and opinions about scientific topics and evidence often reach relevant

---

<sup>55</sup> National Research Council. 2012. *Using Science as Evidence in Public Policy*. National Academies Press, 2012.

<sup>56</sup> Fischhoff, Baruch and Dietram A. Scheufele. 2013. "The Science of Science Communication." *PNAS* 110 (Supplement 3): 14031-14032. doi:10.1073/pnas.1312080110.

<sup>57</sup> Jamieson, Kathleen Hall, Dan Kahan, and Dietram A. Scheufele. 2017. "Introduction: Why Science Communication?" *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017. <https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.1>

<sup>58</sup> Kahan, Dan M. 2017. "On the Sources of Ordinary Science Knowledge and Extraordinary Science Ignorance." *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017. <https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.4>

<sup>59</sup> Berube, David M. 2018. "How Social Science Should Complement Scientific Discovery: Lessons from Nanoscience." *Journal of Nanoparticle Research* 20, no. 5 (2018): 120.

<sup>60</sup> Gallo, Jason. 2017. "Translating Science into Policy and Legislation: Evidence-Informed Policymaking." *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017. <https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.27>

stakeholders through mediated processes<sup>61</sup> within an increasingly complex media landscape with multiple channels for the transmission of scientific information and its interpretation.<sup>62</sup>

Stakeholders use scientific data, information, knowledge, and evidence to reach decisions within a framework that also considers individual and social values, representing a set of beliefs about a hierarchy of desired outcomes or end states that transcend specific situational concerns.<sup>63</sup> In other words, decisions are based on both evidence and values, which include a stakeholder's estimates of risk and reward. Taken together, the science communication environment "is the interaction of processes and cues that citizens, organizations, governments, and a host of other stakeholders use to identify valid science and align it with their value systems, understanding of the world, and ultimately decisions."<sup>64</sup>

Because S&T permeate so many aspects of individual, social, and political life, stakeholders must constantly make a range of decisions that incorporate scientific and technical knowledge with values in both formal and informal circumstances with a spectrum of potential consequences. Therefore, different scientific information is relevant to different decisions at different times, and some complex decisions require knowledge and information from multiple disciplines to reach an informed choice.<sup>65</sup> Effective science communication plays a critical role in the transmission of relevant information to stakeholders. Research from the field of "the science of science communication" can play an important role in understanding and improving the processes for communicating scientific knowledge, how that knowledge is received and used by decision-makers, and how different and multiple forms of mediation and framing of scientific knowledge affect its dissemination, diffusion, and uptake. To address these issues, the National Academy of Sciences hosted three Arthur M. Sackler Colloquia on the Science of Science Communication (2012, 2013, and 2017) to understand the state of empirical social science research in science communication, the dynamic communications processes surrounding scientific and technical topics, and the media landscape that shapes how scientific and technical knowledge is used in decision-making.

---

<sup>61</sup> Nisbet, Matthew C., and Dietram A. Scheufele. 2009. "What's Next for Science Communication? Promising Directions and Lingering Distractions." *American journal of botany* 96, no. 10 (2009): 1767-1778.

<sup>62</sup> National Academies of Sciences, Engineering, and Medicine. 2017. *Communicating Science Effectively: A Research Agenda*. Washington, DC: The National Academies Press. Page 7. <https://doi.org/10.17226/23674>.

<sup>63</sup> Dietz, Thomas. 2013. "Bringing Values and Deliberation to Science Communication." *Proceedings of the National Academy of Sciences* 110, no. Supplement 3 (2013): 14081-14087.

<sup>64</sup> Jamieson, Kathleen Hall, Dan Kahan, and Dietram A. Scheufele. 2017. "Introduction: Why Science Communication?" *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017. <https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.1>

<sup>65</sup> Fischhoff, Baruch. 2013. "The Sciences of Science Communication." *Proceedings of the National Academy of Sciences* 110, no. Supplement 3 (2013): 14033-14039.

## 1. Why should the executive branch address this topic?

For the United States to protect public health and safety and realize returns on its substantial investments in R&D while adequately addressing risk and ethical considerations, workshop participants stressed the importance of protecting the science communication environment to ensure the timely availability of accurate data and information to improve public and private sector decisions. Workshop participants identified the lack of a Federal entity charged with systematically addressing issues related to science communication or ensuring the integrity of the science communication environment as a concern. They also noted that while many Federal agencies engage in science communication activity, from ensuring the public availability of scientific and technical data to funding research into informal science education, these activities are not well coordinated across the executive branch.

This is, however, not a new issue. In 1963, the President's Science Advisory Committee (PSAC) issued a report entitled *Science, Government, and Information* that identified the critical role that the Federal Government should play to ensure the adequacy of science communication to ensure the vitality of the Nation's S&T enterprise. PSAC eloquently established the case for Federal involvement in science communication writing, "Since strong science and technology is a national necessity, and adequate communication is a prerequisite for strong science and technology, the health of the technical communication system must be a concern of Government."<sup>66</sup>

In addition to ensuring the vitality of the S&T enterprise, addressing the potential negative outcomes that stem from misinformation, disinformation, and poor understanding of scientific and technical information warrants attention from the executive branch. For example, measles, which the Centers for Disease Control and Prevention (CDC) declared "eliminated" due to vaccination and control measures, has reemerged in the United States over the last decade, with the CDC reporting 465 cases through April 4, 2019, the second greatest number of cases since 2000 in only a little over a quarter of the year.<sup>67</sup> The CDC reports that while the measles vaccination is extremely effective, major measles outbreaks often occur in "U.S. communities with pockets of unvaccinated people."<sup>68</sup> Many recent outbreaks of measles in the U.S. have occurred in geographic clusters,<sup>69</sup> and several recent

---

<sup>66</sup> Weinberg, Alvin V. et al. 1963. *Science, Government, and Information: The Responsibilities of the Technical Community and the Government in the Transfer of Information*. The White House, Washington, DC. January 10, 1963, Page 1.

<sup>67</sup> Centers for Disease Control and Prevention. *Measles (Rubeola)*. Last updated April 15, 2019. <https://www.cdc.gov/measles/index.html>

<sup>68</sup> Centers for Disease Control and Prevention. *Measles Cases and Outbreaks*. Last updated April 15, 2019. <https://www.cdc.gov/measles/cases-outbreaks.html>

<sup>69</sup> Omer, Saad B., Kyle S. Enger, Lawrence H. Moulton, Neal A. Halsey, Shannon Stokley, and Daniel A. Salmon. 2008. "Geographic Clustering of Nonmedical Exemptions to School Immunization Requirements and

outbreaks in the U.S. have occurred in relatively homogeneous communities with poor vaccination coverage,<sup>70, 71</sup> and in some instances misinformation or lack of accurate risk information may play a role in vaccination coverage.<sup>72, 73, 74</sup> One recent study noted active misinformation activities by troll accounts associated with the Russian Internet Research Agency between 2014 and 2017 to disseminate anti-vaccine messages to U.S. Twitter users and promote discord.<sup>75</sup> However, it is important to understand the multiple philosophical, cultural, and religious reasons that individuals and communities may have for eschewing or delaying vaccination or having low confidence in a specific vaccination, and not simply attributing low uptake solely to misinformation. Workshop participants advocated that the executive branch should play a leadership role to ensure accurate and understandable scientific information is readily available to the public to inform decisions.

The group noted that scientific discovery and technological development often outpaces the ability of Federal policies, programs, activities, and regulatory frameworks to adapt and address emerging trends as well as public perceptions about the risks and benefits of these developments. One participant used the human papilloma virus vaccine as an example to illustrate this point, highlighting how the policy debate and subsequent regulation of the vaccine was heavily shaped by public perception of the risks and benefits of the vaccine in addition to the available scientific evidence.

## 2. How should the executive branch address this topic?

Workshop participants recommended that the executive branch play a proactive role in understanding and protecting the science communication environment and act as a trusted intermediary for both the scientific community and public and private sector decision-

---

Associations with Geographic Clustering of Pertussis." *American Journal of Epidemiology*, Volume 168, Issue 12, 15 December 2008, Pages 1389–1396, <https://doi.org/10.1093/aje/kwn263>

<sup>70</sup> Gastañaduy, Paul A., Jeremy Budd, Nicholas Fisher, Susan B. Redd, Jackie Fletcher, Julie Miller, Dwight J. McFadden III et al. 2016. "A Measles Outbreak in an Underimmunized Amish Community in Ohio." *New England Journal of Medicine* 375, no. 14 (2016): 1343-1354.

<sup>71</sup> Hall, Victoria et al. 2017. "Measles Outbreak - Minnesota April-May 2017." *Morbidity and Mortality Weekly Report* vol. 66, 27 713-717. 14 Jul. 2017, doi:10.15585/mmwr.mm6627a1

<sup>72</sup> Parker, Laura. 2015. "The Anti-vaccine Generation: How Movement against Shots Got Its Start." *National Geographic* 6 (2015).

<sup>73</sup> McNeil Jr., Donald. 2019. "Scientists thought they had measles cornered. They were wrong." *New York Times*. April 3, 2019. <https://www.nytimes.com/2019/04/03/health/measles-outbreaks-ukraine-israel.html>

<sup>74</sup> Pager, Tyler. 2019. "'Monkey, rat and pig DNA': How Misinformation is Driving the Measles Outbreak Among Ultra-Orthodox Jews." April 9, 2019. <https://www.nytimes.com/2019/04/09/nyregion/jews-measles-vaccination.html>

<sup>75</sup> Broniatowski, David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. 2018. "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate." *American journal of public health* 108, no. 10: 1378-1384.

makers and citizens. This would include ensuring the availability of rigorous evidence and scientific knowledge to inform decisions; effectively communicating scientific and technical knowledge; understanding and communicating the economic, social, and environmental impacts of scientific and technical advances; and anticipating and understanding public perceptions of advances in scientific research and emerging technologies. Participants were careful to emphasize that any recommended activities that the executive branch could undertake to protect the science communication environment should be non-partisan and oriented toward improving the dissemination of factual information and context, not about managing or manipulating perceptions about certain scientific advances or technical developments.

The executive branch could establish a coordinated set of activities addressing the facets of the science communication environment listed above. This could include the establishment of an interagency group dedicated to addressing the science communication environment. The efforts of an interagency group could be supplemented by the establishment of a Federal Advisory Committee comprised of non-Federal experts to address similar issues.

An interagency group, with potential input from a dedicated FAC, could do the following:

- Conduct a comprehensive assessment of the current U.S. science communication environment. This would include evaluating its processes, the role that Federal bodies currently play, the role of non-Federal intermediaries, how Federal decisions about S&T are made, how scientific and technical evidence is developed and used in Federal decision-making, how public perceptions are shaped by scientific and technical information, and how public perceptions about the risks and benefits of scientific and technical developments are shaped.
- Develop a Federal action plan to protect and improve the science communication environment based on the results of the comprehensive assessment. The goal is to improve the responsiveness of the executive branch to emerging scientific and technical information, strengthen science communication practices across the Federal Government, develop formal ties with non-Federal science communication experts to inform Federal practices, and establish methods and metrics for understanding the impacts of Federal science communication programs.
- Develop and disseminate fact sheets, case studies, or issue-briefs on emerging S&T issues that clearly address what the executive branch projects potential benefits might be, what it understands about potential risks, and where there may be differential outcomes for stakeholder groups. These documents should highlight how these issues may affect public and private sector decision-makers and citizens.

- Develop and disseminate fact sheets, case studies, or issue-briefs that document the contribution of scientific and technical information to decisions that affect public and private sector activity.

**3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

The failure of the executive branch to address the science communication environment could inhibit effective decision-making in the public and private sectors and by citizens, potentially leading to misperceptions of benefits and risks, failure to properly protect public health, economic inefficiencies, and the unnecessary politicization of some S&T topics. This could impact the trajectories of some scientific research and technology development and limit U.S. ability realize public and environmental health gains, economic productivity and competitive advantage, and national security. Failure to anticipate and address the perceptions and legitimate concerns of the public about scientific and technical advances can lead to promising R&D stalling or being abandoned as funding and regulatory programs deal retroactively with problems that should have been foreseen.

A strong Federal program could bolster trust in scientific and technical information, improve the integrity of the scientific enterprise, and carefully address risks and unequitable societal outcomes of scientific and technical advances. It could also contribute (through both attention and funding) to increasing science communication research and awareness of relevant advances in the field at other non-Federal institutions, such as universities and foundations, which would in turn contribute to strengthening the science communication environment.

**G. Engaging in Artificial Intelligence (AI) and Autonomy Research and Development**

There is both much public excitement and concern about the development of AI and autonomous systems. AI and autonomy, coupled with robotics and advances in data mining and high-performance computing, are transforming the application of computing to complex problem solving with large potential social, political, economic, and security ramifications. Workshop participants discussed issues of privacy, transparency, fairness, and accountability and raised a number of questions including: Who is accountable for harmful results from the application of AI? What are the benefits and risks of having or not having a regulatory framework? What is the appropriate role of the executive branch with respect to AI? How should the executive branch address potential risks without stifling R&D?

## 1. Why should the executive branch address this topic?

AI and autonomous systems present opportunities for increased productivity, improved decision-making, and insights into complex problems, among others.<sup>76</sup> Already, AI is being used in a number of sectors, including the automotive, customer service, and business analytics sectors, among others. An emerging area for AI is healthcare. Recent applications include the use of AI for image analysis in radiology, pathology, and dermatology,<sup>77</sup> and the development of Watson Oncology, a partnership between IBM Watson and Memorial Sloan Kettering to identify cancer treatment options based on patients' clinical information.<sup>78</sup> One potential future application is the use of AI to diagnose mental illnesses. Some initial research has shown that some patients prefer to disclose information to intelligent systems rather than medical staff,<sup>79</sup> which may increase the likelihood of self-reporting of symptoms. AI could potentially reduce some healthcare costs, and provide a wider range of patients access to medical advice.<sup>80</sup> Biometric data gathered from wearable devices can also be used along with behavioral data to help identify individuals whose behavioral patterns may make them a risk to themselves or others. However, the myriad ethical and privacy concerns associated with this potential practice must be better understood before any adoption as part of routine medical practice.

There are a number of concerns associated with the broad adoption of AI that should be addressed. The algorithms employed in AI and machine learning, and the data sets used to train AI and autonomous systems, reflect structural inequities within society or an organization and serve to reinforce existing patterns of power that disadvantage some groups and individuals.<sup>81</sup> As AI and machine learning techniques become ubiquitous, the biases encoded in algorithms or structural inequities reflected within data sets have the potential for harmful unintended consequences. Decisions within a number of sectors such as education, housing, healthcare, finance, and banking that affect daily life increasingly rely

---

<sup>76</sup> United States Congress. House Subcommittees on Research and Technology and Energy, Committee on Science, Space, and Technology. 2018. *Artificial Intelligence Emerging Opportunities, Challenges, and Implications for Policy and Research*. 26 June 2018. (Statement of Timothy M. Persons, United States Government Accountability Office).

<sup>77</sup> Miller, D. D., & Brown, E. W. 2018. "Artificial Intelligence in Medical Practice: the Question to the Answer?" *The American journal of medicine*, 131(2), 129-133.

<sup>78</sup> Memorial Sloan Kettering Cancer Center. "Watson Oncology." Accessed 28 January 2018. <https://www.mskcc.org/about/innovative-collaborations/watson-oncology>

<sup>79</sup> Luxton, D. D. 2016. "An Introduction to Artificial Intelligence in Behavioral and Mental Health Care." *Artificial intelligence in behavioral and mental health care*, pp. 1-26.

<sup>80</sup> Garg, Parie and Sam Glick. 2018. "AI's Potential to Diagnose and Treat Mental Illness." October 22, 2018. <https://hbr.org/2018/10/ais-potential-to-diagnose-and-treat-mental-illness>

<sup>81</sup> Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, 2018.

on algorithms and AI. It is imperative to understand if and how their development and use can be responsible, ethical, and beneficial to all citizens.

Additionally, there is the possibility for training data to be infiltrated by adversaries. A research program by the Intelligence Advanced Research Activity (IARPA) called Trojans in Artificial Intelligence is targeted at combatting “Trojan attacks” on AI, such as an AI system learning to distinguish traffic signs being given example images of stop signs with a yellow square labeled “speed limit sign.” If this AI system was used on a self-driving car, there is the potential that deploying post-it notes on stop signs could cause the car to misread the stop sign as a speed limit, potentially leading to fatalities.<sup>82</sup>

The pairing of AI systems with personal information collection has significant implications for individual privacy. The collection of biometric information is getting cheaper and more common, with companies including Google and Apple using patient data to train healthcare algorithms.<sup>83</sup> Smart cities, which are being touted as safer, more efficient, and sustainable urban systems, rely on the ability to collect and analyze large amounts of data. Internet of Things (IoT) devices are capturing data about their users and providing it to the companies that produce them, as well as others that may purchase the data. The information collected from any of these methods may be combined with other collected data to give much richer information about an individual than what would be possible with a single data source.<sup>84</sup> The fact that individuals may not be aware of what data they are contributing, with whom the data will be shared, or how their information may be used in the future poses interesting questions for human subject research. How can individuals consent in any meaningful way, given such uncertainty? How can ethical researchers protect research subjects from unreasonable risk of harm? How can disciplines protect themselves from unethical researchers?

Currently, there is no national regulatory framework for AI or the collection and use of data underlying work in machine learning. For some applications that rely on AI, such as self-driving cars, there is a patchwork of State-level regulations.<sup>85</sup> Given that the advances in AI,

---

<sup>82</sup> Intelligence Advanced Research Projects Activity. “Trojans in Artificial Intelligence.” Accessed 10 January 2018. [https://www.iarpa.gov/index.php?option=com\\_content&view=article&id=1142&Itemid=443](https://www.iarpa.gov/index.php?option=com_content&view=article&id=1142&Itemid=443)

<sup>83</sup> Denton, Sarah W. and Eleonore Pauwels. 2018. *There’s Nowhere to Hide: Artificial Intelligence and Privacy in the Fourth Industrial Revolution*. The Wilson Center. Washington, DC. March 2018. <https://www.wilsoncenter.org/article/nowhere-to-hide-artificial-intelligence-and-privacy-the-fourth-industrial-revolution>

<sup>84</sup> World Economic Forum. 2017. *Shaping the Future Implications of Digital Media for Society: Valuing Personal Data and Rebuilding Trust*. January 2017. [http://www3.weforum.org/docs/WEF\\_End\\_User\\_Perspective\\_on\\_Digital\\_Media\\_Survey\\_Summary\\_2017.pdf](http://www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf)

<sup>85</sup> National Conference of State Legislatures. 2018. “Autonomous Vehicles.” November 7, 2018. <http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>

autonomy, and robotics will have wide reaching societal and ethical implications, the United States should proactively and publicly address them through improved legislative and regulatory frameworks. There is a need for coordination across the agencies of the executive branch to determine how to create a regulatory environment that protects the potential benefits of advances in AI and autonomy while ensuring its responsible development and application.

## **2. How should the executive branch address this topic?**

Given that AI and autonomous systems are rapidly developing technology areas, the principal recommendation for Federal activity is to ensure that the executive branch maintains awareness of new opportunities and areas of concern as they emerge. Specific recommended actions include:

- Engage in technology assessments for new and emerging applications of AI and autonomous systems.
- Develop a mechanism to solicit public feedback on how potential regulations or policy changes could impact U.S. competitiveness.
- Establish a Federal Advisory Committee to bring together industry and academic representatives to produce a report to provide guidance to Federal agencies. Because remaining competitive in these topics will require an interdisciplinary approach, the committee should involve experts from a range of disciplines that includes biology, communications, computer science, psychology, and social science.
- Convene a permanent, interagency body with the goal of promoting the protection of participants in federally supported research with particular attention to the consideration of emerging ethical issues, including new developments in medicine, science, and technology.

From these engagements, the executive branch can work to develop or refine policy frameworks to shape expectations and perceptions that take into account the risks with respect to Engaging with AI and autonomous systems and conducting R&D on these topics.

## **3. What issues or potential consequences should the executive branch consider if this topic is or is not addressed?**

A thoughtful policy and legal framework can help protect the further development of AI and autonomous systems. In the absence of government regulation, companies will set the standards for acceptable practices. The benefit of this approach is that it avoids the potential of over-regulation. One downside of this approach is that the interest of the companies may not be aligned with citizens and consumers. The absence of a proactive regulatory framework also means that an accident or other negative event arising from the use of AI or

autonomous systems has the potential for public backlash and the development of an ill-formed, reactive regulatory framework.

The development of this framework should be undertaken with appropriate stakeholders (including technology providers and users) to mitigate the risk of overregulation and the development of misguided regulations that stifle the industry.

If this topic is not addressed domestically, there is the potential that other countries will take a leadership role in a way that adversely affects U.S. companies and consumers. Other countries may have different perceptions with respect to privacy and risks, and by establishing clear regulatory frameworks, it may influence how companies shape their business models and how users shape expectation.

### 3. Cross-Cutting National and Homeland Security S&T Considerations

---

R&D that supports the national and homeland security of the United States plays an integral role in maintaining strategic military advantages and foreign policy leadership, while also contributing to the economic competitiveness of key domestic sectors such as biotechnology, manufacturing, and information and communication technology and services. Economic competitiveness, in turn, plays an integral role in U.S. foreign and national security policy, as the Administration’s 2017 National Security Strategy (NSS) explicitly highlights.<sup>86</sup> The Federal Government has maintained robust support for national security R&D, with the DOD accounting for 39.3% of all Federal R&D funding in FY 2017 and 48.4% in President Trump’s FY 2019 budget request.<sup>87</sup> Other Federal activities and programs that support national and homeland security as well as foster economic competitiveness are broadly distributed across civil, defense, and intelligence agencies. There is a need to coordinate activities that cut across agencies, including developing a high-skilled workforce, identifying foreign scientific and technical advances that pose a risk to the U.S., protecting intellectual property, and understanding the security implications of foreign investment in the U.S. Given the potential national and homeland security implications associated with each emerging S&T area, the executive branch will need to engage in interagency coordination and external interaction with relevant stakeholders.

#### 1. Ceding Competitive Advantage to Adversaries in Biotechnology

When asked about potential implications of executive branch inaction on many of the topics addressed in the sections above, workshop participants repeatedly highlighted the potential threat to U.S. military technological superiority and economic competitiveness posed by ceding S&T leadership to international competitors, especially China. This concern is reflected in the NSS, which directs Federal agencies to “improve their understanding of worldwide S&T trends and how they are likely to influence—or undermine—American

---

<sup>86</sup> Executive Office of the President. 2017. *National Security Strategy of the United States of America*. Washington, DC. United States, 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

<sup>87</sup> Congressional Research Service. 2018. *Federal Research and Development (R&D) Funding: FY2019*. R45150. 2018.

strategies and programs,” and also specifically identifies China as a challenger.<sup>88</sup> Understanding the implications and full range of potential applications of new technologies and scientific research is critical for maintaining national and homeland security. In April 2018, the Congressional Research Service underscored the need to anticipate potential and dual-use technologies or research applications in order to maintain technological superiority for both the United States as well as its NATO partners, particularly in light of competition from China and Russia.<sup>89</sup>

Workshop participants noted that in the life sciences, for example, advances such as gene editing and programming can both improve health outcomes and pose biohazard and biodefense risks, a point also highlighted in the 2018 *National Biodefense Strategy*.<sup>90</sup> Participants identified the use of AI in the life sciences and the use of remote sensing for public health applications as areas where peer nations, especially China, currently lead, and that U.S. failure to responsibly pursue these technologies may leave the Nation vulnerable to public health crises and biohazards. Additionally, inaction on this topic could mean that China becomes a primary driver in biomedical science, which could include setting international standards and priorities.<sup>91</sup> Ceding leadership in biotechnology through inaction could have direct impacts to U.S. national and homeland security and limit the Nation’s ability to combat threats such as bioterrorism. Recommended actions for the executive branch include:

- Establish an interagency group to identify and track international biotechnology developments, identify threats to both public health and U.S. competitiveness, and issue guidance to U.S. researchers on developing these technologies.

## 2. Balancing National Security and Commercial Activity

### Commercial Space Sector

On March 23, 2018, the White House released a *National Space Strategy Fact Sheet* that “emphasizes dynamic and cooperative interplay between the national security, commercial, and civil space sectors” and states that “securing the scientific, commercial, and national

---

<sup>88</sup> Executive Office of the President. *National Security Strategy of the United States of America*. Washington, DC, 2017. p. 20. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

<sup>89</sup> Congressional Research Service. 2018. *Transatlantic Perspectives on Defense Innovation: Issues for Congress*. R45177. 2018. Page 6.

<sup>90</sup> Executive Office of the President. 2018. *National Biodefense Strategy*. Washington, DC, 2018. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf>

<sup>91</sup> Gebelhoff, Robert. 2017. “China’s on Track to Surpass Our Investment in Science.” *Washington Post*, Jun. 20, 2017. [https://www.washingtonpost.com/news/in-theory/wp/2017/06/20/chinas-on-track-to-surpass-our-investment-in-science/?utm\\_term=.458a6ff9d350](https://www.washingtonpost.com/news/in-theory/wp/2017/06/20/chinas-on-track-to-surpass-our-investment-in-science/?utm_term=.458a6ff9d350)

security benefits of space is a top priority.”<sup>92</sup> Workshop attendees noted that to do so will require being able to balance security concerns with policies that promote responsible growth in the commercial and scientific space sectors. The growth in the number of governmental, commercial, and research satellite launches globally, especially of small satellites, may create space situational awareness and space traffic management challenges that pose unique national security challenges.<sup>93</sup> There is an explicit national security need for the DOD to maintain and enhance its role in providing space situational awareness and an increasing need for greater interagency coordination to balance the equities of the defense, intelligence, civil government, and commercial sectors in space. The U.S. can maintain global leadership in this area by fostering the development of international launch, space operations, and debris removal standards and procedures. Additionally, the Congressional Research Service has identified three broad policy issues associated with the growing commercial space industry requiring Federal attention: the multi-agency nature of current commercial space regulation, the effect of export control on U.S. space firms, and the potential for signal interference due to spectrum sharing for 5G technologies.<sup>94</sup>

These issues pose both national security and international competitiveness challenges that require interagency coordination. Recommended actions for the executive branch include:

- Establish an interagency group to address challenges to civil, defense, and intelligence agency space missions from commercial developments, while ensuring the global competitiveness of the U.S. space industry.

### Information and Communication Technology Sector

Workshop attendees also highlighted the dynamic tension between promoting growth in the commercial information and communication technology sector and national security. Concerns focused on cybersecurity, ceding competitive advantage in AI to adversaries, and the implications of the globalization of the microelectronics industry. The first two topics have been addressed in previous sections. Microelectronics are fundamental to most modern military weapons, communications, and position, navigation, and timing systems, but also represent a point of vulnerability in these systems that can either be hacked or developed to provide potential adversaries information from these systems or control over them. The DOD uses the Defense Microelectronics Activity’s Trusted Foundry Program to ensure the

---

<sup>92</sup> Executive Office of the President. 2018. *National Space Strategy Fact Sheet*. Washington, DC. <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/>

<sup>93</sup> Lal, Bhavya, Asha Balakrishnan, Becaja M. Caldwell, Reina S. Buenconsejo, and Sara A. Carioscia. 2018. *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)*. IDA Science and Technology Policy Institute. Washington, DC.

<sup>94</sup> Congressional Research Service. 2016. *Commercial Space Industry Launches a New Phase*. R44708.

integrity design and manufacturing of the microelectronics that the U.S. military relies on by certifying domestic “trusted sources” to provide a chain of custody for integrated circuits, ensure continuity of supply, and prevent adversaries from reverse engineering or understanding potential vulnerabilities.<sup>95</sup> There is a need, however, to ensure the domestic supply of advanced semiconductor technologies beyond 14nm, an area in which there are currently no trusted domestic foundries.<sup>96</sup> This could lead to the military working with foundries outside the program in order to access the most advanced microelectronics while developing new systems.

Workshop attendees highlighted the potential threat that compromised microelectronics could play in the control systems for domestic critical infrastructure such as power grids, gas and oil pipelines, water supply, and telecommunications systems. They also highlighted the increasing personal and household use of internet controlled devices with embedded microelectronics, such as programmable thermostats, home security systems, and virtual assistants. These present a number of vulnerabilities due to their connection to potentially unsecured networks as well as their use of foreign or untrusted microelectronics. Recommended actions for the executive branch include:

- Improve access to trusted domestic microelectronic foundries for both national security and civil commercial sector use by working with NIST and DHS to establish a civil trusted foundries initiative to partner with the DOD.
- Establish a Federal Advisory Committee that draws on private sector and academic expertise in the semiconductor and microelectronics fabrication to advise the executive branch on securing advanced technology development.
- Establish a task force to address civil and critical infrastructure vulnerabilities due to commercial information and communication technologies.

**a. Consequences of Action or Inaction Will Impact National and Homeland Security**

The executive branch has a number of tools at its disposal to address threats to its technological superiority and global economic competitiveness specifically focused on critical technologies, including export controls and other security programs.<sup>97</sup> In 2007, the U.S. Government Accountability Office determined that many of these programs were inadequate to “address the evolving challenges of balancing national security concerns and

---

<sup>95</sup> Defense Microelectronics Activity. “Trusted Accreditation.” Last accessed January 17, 2019. <https://www.dmea.osd.mil/trustedic.html>

<sup>96</sup> Lapedus, Mark. 2018. “A Crisis in DoD’s Trusted Foundry Program?” *Semiconductor Engineering*. October 22, 2018. <https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program/>

<sup>97</sup> GAO. 2017. *HIGH-RISK SERIES: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*. (GAO-17-317). Washington, DC. 2017. <https://www.gao.gov/assets/690/682765.pdf>

economic interests” and found in 2017 that, while some progress had been made, “additional leadership and coordination of programs and activities in the non-export control programs, among other things, is needed to identify strategic reforms that will help to advance U.S. interests.”<sup>98</sup>

The national and homeland security considerations and implications of action or inaction for each emerging S&T area was a prevalent theme throughout both forums. Consequences of action in each area are the United States gaining a competitive advantage, maintaining its position as a global leader, and improving its national and homeland security posture. Conversely, consequences of inaction for not addressing an identified area were often linked to an adverse impact to national or homeland security and the United States losing its competitive advantage in an area. Several additional areas were identified as contributing to maintaining and enhancing national and homeland security. These included improving cybersecurity measures for U.S. military and homeland security systems; understanding the vulnerability of U.S. military systems to electromagnetic disturbances, both natural and man-made; addressing new developments in wireless communications; and building coastal and extreme weather resilience.

---

<sup>98</sup> Ibid. Page 376.



## 4. Conclusion

---

Participants from each forum emphasized the need for the executive branch to ensure that the United States remains an international leader on S&T issues. Part of this leadership role includes communicating the value of rigorous and objective S&T to the public. In addition to engaging the public, participants encouraged the executive branch to leverage the expertise that exists within itself, industry, and academia to ensure that the Federal Government has access to diverse and rigorous information to inform decisions. Table 3 summarizes the recommended actions for each of the topics highlighted by workshop participants.

**Table 3. Recommended executive branch actions to address topics highlighted by workshop participants.**

Topic	Recommendation
Strengthening the Nation's Resilience to Natural Hazards Given a Changing Climate	<ul style="list-style-type: none"> <li>• Develop a comprehensive, interagency strategy to help the Federal Government, State, local, and Tribal governments, economic sectors, businesses, and individuals prepare for the effects of a changing climate.</li> <li>• Ensure that products and services aimed at increasing resilience to natural hazards are developed and disseminated in ways that make the information discoverable, accessible, and usable.</li> <li>• Develop a plan for addressing gaps in the collection of Earth observations.</li> <li>• Convene an interagency task force co-chaired by the DOD, DHS, and the U.S. Global Change Research Program to develop an action plan to address the threats that the changing climate poses to critical and civil infrastructure, the built environment, military installations, and the ability of the emergency response system to adequately protect lives and property.</li> </ul>
Harnessing Advances in the Life Sciences	<ul style="list-style-type: none"> <li>• Convene stakeholders and subject matter experts to fully understand the extent, components, and value of the bioeconomy.</li> </ul>

EMERGING SCIENCE AND TECHNOLOGY TRENDS

Topic	Recommendation
Maintaining and Improving Science Infrastructure	<ul style="list-style-type: none"> <li>• Develop an overarching strategy for maintaining and improving U.S. science infrastructure.</li> <li>• Identify a set of critical Federal laboratory facilities and infrastructure and large scale research infrastructure that need focused attention and investment.</li> <li>• Identify potential workforce pipeline issues (including retention) and ways in which to train and inspire scientists.</li> <li>• Strategically focus training in areas that lack people, including in emerging areas of R&amp;D.</li> <li>• Increase the speed and efficiency of the clearance granting process and expand the ability for agencies to grant clearances to technical experts from industry and academia to assume temporary duties in government during a crisis.</li> <li>• Enable Federal, industry, and academic staff to trade places through rotations.</li> <li>• Increase the speed and efficiency of Federal agency hiring to enable agencies to hire qualified individuals within 60 to 90 days of submitting an application.</li> <li>• Develop a policy framework that increases the ability of universities to transfer technologies and techniques developed with Federal funds to the marketplace and increases coordination between universities, venture capital groups, and national laboratories.</li> </ul>
Strengthening the Built Environment	<ul style="list-style-type: none"> <li>• Identify opportunities for the executive branch to aid the development and deployment of advanced technologies that improve cities and urban living.</li> <li>• Set joint priorities for establishing infrastructure performance design requirements that ensure future Federal investments into existing or new infrastructure are designed to be resilient to future hazards.</li> <li>• Identify how the public and private sectors can set joint priorities and work together to advance electricity distribution system performance as new technologies increase demands on existing distribution system infrastructure.</li> </ul>

EMERGING SCIENCE AND TECHNOLOGY TRENDS

Topic	Recommendation
Improving Cybersecurity Research and Implementation	<ul style="list-style-type: none"> <li>• Develop policies that articulate clearly the societal benefits and concerns that technology should address, rather than dictating the specific features of the technology.</li> <li>• Create a policy framework where liability for action or inaction can be reasoned about and quantified, providing insurers and businesses with a reasonable basis for engaging in and managing the risks of new technology.</li> <li>• Adopt a targeted investment strategy through purchasing, cost sharing, prizes, and awards to further encourage businesses to address public cybersecurity needs where there exists a failure of the market to do so.</li> <li>• Incentivize the development of new models to characterize the security of systems, to quantify the degree of security, to qualify the conditions under which security is maintained, and to be able to document and share information concerning security best practices, methods, and incidents.</li> <li>• Explore including cybersecurity as a component of continuity of operations</li> </ul>
Protecting the Science Communication Environment	<ul style="list-style-type: none"> <li>• Conduct a comprehensive assessment of the current U.S. science communication environment.</li> <li>• Develop a Federal action plan to protect and improve the science communication environment based on the results of the comprehensive assessment.</li> <li>• Develop and disseminate fact sheets, case studies, or issue-briefs on emerging S&amp;T issues that clearly address what the executive branch projects potential benefits might be, what it understands about potential risks, and where there may be differential outcomes for stakeholder groups.</li> <li>• Develop and disseminate fact sheets, case studies, or issue-briefs that document the contribution of scientific and technical information to decisions that impact public and private sector activity.</li> </ul>
Engaging in Artificial Intelligence and Autonomy Research and Development	<ul style="list-style-type: none"> <li>• Engage in technology assessments for new and emerging applications of AI and autonomous systems.</li> <li>• Develop a mechanism to solicit public feedback on how potential regulations or policy changes could impact U.S. competitiveness.</li> <li>• Establish a Federal Advisory Committee to bring together industry and academic representatives to produce a report to provide guidance to Federal agencies.</li> <li>• Convene a permanent, interagency body with the goal of promoting the protection of participants in federally supported research with particular attention to the consideration of emerging ethical issues, including new developments in medicine, science, and technology.</li> </ul>

In addition to the recommended actions above, there are a number of actions that the executive branch could undertake to address national and homeland security S&T considerations. These are included in Table 4.

**Table 4. Recommended executive branch actions to address national and homeland security S&T considerations.**

National and Homeland Security Consideration	Recommendation
Ceding Competitive Advantage to Adversaries in Biotechnology	<ul style="list-style-type: none"> <li>• Establish an interagency group to identify and track international biotechnology developments, identify threats to both public health and U.S. competitiveness, and issue guidance to U.S. researchers on developing these technologies.</li> </ul>
Balancing National Security and Commercial Activity	<ul style="list-style-type: none"> <li>• Establish an interagency group to address challenges to civil, defense, and intelligence agency space missions from commercial developments, while ensuring the global competitiveness of the U.S. space industry.</li> <li>• Improve access to trusted domestic microelectronic foundries for both national security and civil commercial sector use by working with NIST and DHS to establish a civil trusted foundries initiative to partner with the DOD.</li> <li>• Establish a Federal Advisory Committee that draws on private sector and academic expertise in the semiconductor and microelectronics fabrication to advise the executive branch on securing advanced technology development.</li> <li>• Establish a task force to address civil and critical infrastructure vulnerabilities due to commercial information and communication technologies.</li> </ul>

## **Appendix A. List of Emerging S&T Trends**

---

To maximize the productivity of the workshop, STPI had participants propose topics ahead of time, which the group reviewed prior to attending. STPI sent an email to all participants asking 1) What are emerging S&T areas of national interest or concern that the executive branch should address in the near-term?, and 2) What are the implications of the executive branch not addressing these areas? The summary of all 25 topics provided to participants for the November 15 workshop is shown below. The four topics that were discussed only during the November 15 workshop are indicated with an asterisk.

### **Biology, Health, and Medicine**

#### **Implications of Neuroscience Research and Biotechnology Development**

Advances in emerging research areas of neuroscience and biotechnology, such as in gene editing, gene drives, optogenetics, and synthetic biology have the potential to rapidly improve the landscape of human, agricultural, and environmental health. These advances are accompanied by concerns about the potential misuse of these tools for malicious purposes. The scientific and security communities should continue to engage to develop measures to detect and manage misuse, while allowing legitimate research and innovation to thrive and keep U.S. researchers on the cutting edge. It is increasingly important to assess the security implications of these capabilities and develop strategies to balance those concerns with support for peaceful advancement of U.S. research and innovation.

#### **Digital Behavioral Health\***

Behaviors are implicated in the leading drivers of disease, economic burden, and risk to national security. Data gathered with remote sensor technology from wearable devices, computer vision, social media tracking, natural language processing, and other sources could be mined using AI and predictive machine learning to enhance precision medicine and identify individuals whose behavioral patterns may make them a risk to themselves or others. Behavioral quantification can accelerate the development of safe and effective treatments, preventions, and mitigation strategies, by making subjective states (such as violent or suicidal intent) measurable objectively.

### **Digitally Enhanced Medicine\***

Enhancing the health of our Nation supports the productivity of the workforce, reduces medical costs, and supports national security through service member health and effectiveness. Advances in remote sensing technology of health status, computer vision, and AI based on big data from medical databases are poised to transform health care. Digital Medicine can drastically extend the reach and capacity of physicians and nurses, mitigating the physician and nursing shortage and addressing the health needs of underserved areas and the uninsured.

## **Information and Communications Technology**

### **New Developments in Wireless Communications**

New technological advances in wireless communications, such as 5G, and its data applications are rapidly reshaping the economy and national security. Networks will have greater capacity and less latency, enabling other technologies such as self-driving cars and enhanced virtual reality. Other issues include how much spectrum to make available for fixed and mobile terrestrial operations and whether any should be reserved for satellite use only. In addition, depending on the speed with which new developments in wireless communications are adopted, new vulnerabilities may emerge for these systems in civil and military applications. For example, the concentration and proliferation of 5G “small cells” in metropolitan areas, and the tendency for communications to rely on these systems could result in disproportionately large vulnerability in relatively concentrated areas.

### **Potential Benefits and Consequences of Harvesting and Shielding Electromagnetic Signals**

Existing electromagnetic transmissions such as Wi-Fi, TV, radio, and mobile phone signals present a wide range of potentially beneficial and strategic applications, including communications, navigation, and logistics. Technologies that can harvest the signals generated by adversaries may present national security advantages. At the same time, shielding domestic transmission signals to prevent adversaries and hackers from harvesting or disrupting them through spoofing or jamming presents a significant challenge. Protecting citizens’ privacy by safeguarding personally identifiable information, commercial proprietary data, and sensitive security signals, without restricting transmission flow, volume, and speed, is critical.

## **Advances in Computer Science**

### **Computational Social Science**

Technological advances in computer science have substantially shifted the ability to collect, analyze, and understand human behavior. Computational tools, such as data

visualization and text analytics, can inform decision-making to address traditional social science topics such as security, economic growth, and inequality.

### **Cybersecurity**

Foreign adversaries can exploit sensitive information and computer systems to destabilize financial institutions, damage infrastructure, steal private information, and undermine confidence in government institutions. The rising number of reports of successful hacking efforts and worms and malware demonstrate that new strategies are needed to improve U.S. cybersecurity. New techniques for encryption; trusted computing; and hardware, firmware, and software verification can help improve the robustness of U.S. cybersecurity systems.

### **Quantum Information Science and Enabling Technologies for Complex, Computational Problem-Solving**

Quantum information science (QIS) can improve research across a wide range of disciplines and will be foundational to advancing next generation technologies, information processing, and computing. QIS can inform the development of enabling technologies such as high-performance computing, which can be used in a variety of applications including in the medical, national security, and cybersecurity fields. Near-term expected results of QIS include next-generation time and frequency standards with unprecedented precision. In the long-term, quantum systems and computers may be able to solve complex problems, such as predicting the behavior of advanced materials, faster than classical supercomputers.

### **Earth System Science and Technology**

#### **Arctic Research**

Rapid environmental changes within the Arctic are impacting local and global weather, natural resource availability, and human health and security. Understanding the physical and ecological responses to these changes can inform efforts to manage and mitigate their direct and indirect effects.

#### **Carbon Management**

Climate change can adversely impact national security, the economy, and society. New approaches and emerging technologies to sequester carbon from the atmosphere (e.g. artificial photosynthesis) offer opportunities for the Nation to manage carbon and the potential negative effects of climate change. Additionally, novel, sustainable energy sources and renewable energy technologies offer the potential to reduce the amount of carbon released into the atmosphere while also reducing our dependence on foreign nations to meet U.S. energy needs.

### **Novel Remote Sensing Technologies**

New technologies offer the potential to collect information with greater precision, geographic coverage, and density, to enhance knowledge of the natural world and improve national security. Autonomous sampling capabilities offer the ability to improve data collection in hard-to-reach areas such as the oceans, which are a critical component of our economy and national security. Coupling remote and in situ sensing also offers the potential to increase the precision for agricultural management and decision-making.

### **Observational Systems as a National Asset**

Data from observational systems serve as the basis for informing policymaking and decision-making in many areas such as weather forecasting, hazard warning, and planting crops. Examples of these systems include satellite systems, ground-based sensing networks, and ocean observation systems. These should be designed to enable both science and applications. As policy needs grow, our underlying observations must become more comprehensive and higher quality. New methods for cost-effective observations should be developed, including systems-of-systems, community-based ad hoc observations (as from mobile phones), and more.

### **Resilience**

#### **Building and Rebuilding Better Cities\***

Cities are the economic engines of our Nation. Through public and private collaborations, they build and maintain systems and networks that provide education, healthcare, transportation, energy, water, housing, sport and much more. Building and maintaining cities requires balancing geotechnical constraints and socioeconomic needs and aspirations. Coastal cities, especially, need new tools to respond to expected aging and natural disasters. Engaging the range of relevant Federal agencies and private efforts on improving cities could be used to improve their social and economic strength and resilience.

#### **Integrated Technology Development for Electricity Production, End Use, and Supply\***

Separate program and budget structures exist for different solar technologies, building efficiency, transportation technologies, fossil energy electricity production, and electricity supply technologies involving storage, transmission, and distribution. However, there have been major technology, market, and regulatory innovations in the electric utility industry that argue for joint development. Managing the distribution grid for the purpose of optimizing renewable energy conversion and developing advanced efficiency and storage technologies offers new opportunities for experimentation and advancement of integrated energy supply and end use technologies, including consideration of electric vehicles as an energy load and storage source.

### **Mitigating the Effects of Climate Change**

Understanding and addressing the implications of climate change and undertaking actions to adapt to the changing climate is important to protect our national assets. These include understanding and managing the effects of sea level rise on coastal communities and military infrastructure, changing precipitation conditions (primarily drought) impact on farmers, the consequences of shrinking Arctic sea ice cover, and the implications of climate and weather stressors on foreign nations and our foreign interests. By understanding these changes, their implications, and how to deal with them, we best position our Nation for success. Moreover, not figuring out how to deal with these changes could put us at a significant strategic disadvantage to nations that do decipher how to manage and adapt to change.

### **Resilient Infrastructure**

Critical infrastructure systems, such as electric power grids, communications, and transportation, provide the United States with a number of vital services that support the Nation's economy, security, and health. Enhancing resilience of U.S. physical and cyber infrastructure requires a national coordinated effort and partnerships across multiple Federal and non-Federal stakeholder groups.

### **Societal Implications of Technology**

#### **Individual Social Media Use as a Vector for Civil Life and National Security**

The use of social media has allowed individuals to filter and propagate news in novel ways and is altering established patterns of social, political, and economic behavior. Anticipating the potential methods and consequences of social media exploitation raises societal and national security issues.

#### **Social Implications of Artificial Intelligence**

AI and machine learning, coupled with advances in data mining and high-performance computing, are transforming the application of computing to complex problem solving with large potential social, political, economic, and security ramifications. The algorithms employed in AI and machine learning, and the data sets used to train AI, can reflect structural issues within society or an organization and serve to reinforce existing patterns that disadvantage some groups and individuals. As AI and machine learning techniques become ubiquitous, the biases encoded in algorithms or structural inequalities reflected within data sets have the potential for negative unintended consequences. Additionally, the pairing of these computational methods with multi-domain sensing and persistent information collection has significant implications for individual privacy.

### **Wearable and Virtual Reality Technologies**

The use of wearable and virtual reality technologies has increased significantly, as they are employed in a variety of applications in health, entertainment, and fashion. Growing concerns over the amount and type of data that these technologies can collect highlights the need to develop strategies to address potential security and privacy issues associated with these devices.

### **Protecting the Science Communication Environment**

The “science communication environment” (SCE) comprises the sum total of institutions, processes, and norms that connect public decision-making with the best available scientific evidence. Conditions that disrupt these influences can be viewed as forms of SCE pollution. One particularly toxic form of such pollution consists of social meanings that fuse positions on science-informed issues with citizens’ cultural identities. This dynamic is at the root of polarization over climate change, nuclear power, and other issues. The science of science communication supplies methods for predicting which new forms of decision-relevant science are vulnerable to this pathology. Genome editing, geoengineering, and AI all merit investigation because of their affinity with existing technologies that generate polarization.

The U.S. does not currently have an agency or interagency group charged with protecting the SCE. The resulting void leaves the fate of new forms of decision-relevant science vulnerable to chance and strategic behavior. The consequences of such absence are illustrated by recent outbreaks of diseases easily prevented by vaccines where misinformation has played a role. Just as OMB now screens all administrative actions for costs and benefits, an agency or interagency body could provide verified scientific and technical information on topics of national importance.

### **Defense, Space, and Aerospace**

#### **Commercial Use of Space**

The development of new space technologies, particularly in the commercial sector, can enable dynamic non-traditional missions (e.g. asteroid mining, space travel, on-orbit servicing), many of which have major civil, defense, and societal implications. The number of companies pursuing small satellites, in particular, has grown due to reduced launch costs and advances in technology. However, the limited resources of small companies can lead to their small satellites having limited cybersecurity measures, making them vulnerable to attack.

### **New Developments in High Speed Flight**

Supersonic flight offers the potential for high-speed transportation on Earth. Supersonic civilian transport was pursued in the United States in the 1960s and realized with the Anglo-French Concorde in the 1970s. Since the demise of the Concorde, there have been no civilian supersonic transports. Recent efforts in industry and government to develop quiet supersonic aircraft hold the promise for a new era in high-speed civilian aviation. Additionally, the development of hypersonic weapons for national defense has become an area of emphasis for the DOD. While the discussion around the development of hypersonics has traditionally been focused on the defense sector, civil agencies also have the potential to make significant contributions in terms of advances in research that will enable technology development.

### **Nuclear Weapons and Missile Defense**

The Federal Government is proposing to embark on a nuclear weapons modernization program that is estimated to cost \$1.7 trillion dollars over the next 30 years. This is a complex area where decisions and choices on the offense side of the equation are connected to the defense side. Our ballistic missile defense (BMD) systems are also due for an upgrade. American intercontinental ballistic missile defenses in Alaska and California are designed against ballistic missiles, and do not work against cruise missiles, against hypersonic maneuvering missiles, or against undersea drones carrying nuclear weapons. U.S. BMD systems also do not work against raids of many attacking missiles at once or Multiple Independently-targetable Reentry Vehicle (MIRVed) systems that deliver many missiles at once.

### **Advanced Manufacturing and Robotics**

#### **Advanced Materials and Manufacturing**

Improved manufacturing processes to produce innovative materials are critical to the development of new and emerging technologies. Additive manufacturing can reduce costs to create different materials that can be used for a variety of applications and missions, from food items and 3D printed organs to advanced metal alloys. Improving computational and data tools to research, deploy, and validate new materials to meet operational needs can support U.S. efforts to address economic, national security, and environmental challenges.

#### **Innovation in Robotics, Autonomous Systems, and Automation**

Robotics, automation, and autonomous systems are increasingly changing society. From robotics in surgery to self-driving cars, these technologies and systems are enabling and enhancing functionality in a variety of sectors, including commercial space and health. In addition to promoting the advancement of these capabilities, the Nation's increasing

reliance on these technologies and their societal and security implications should be considered.

## Appendix B. List of Participants

	Name	Most Recent Affiliation
October 30	Dr. Waleed Abdalati	University of Colorado – Boulder
	Dr. Seth Cohen	University of California – San Diego
	Mr. Philip Coyle III	Center for Arms Control and Non-Proliferation
	Dr. William Gail	Global Weather Corporation
	Dr. Steven Koonin	Center for Urban Science and Progress – New York University
	Dr. Martha Krebs*	University of California - Davis
	Dr. Sarah “Holly” Lisanby	National Institutes of Health
	Dr. Jason Matheny	Center for Technology and Security – Georgetown University
	Dr. Kathie Olsen	University of Notre Dame – Washington Office
	Dr. Tara O’Toole	In-Q-Tel
November 15	Dr. Arun Seraphin	U.S. Senate Committee on Armed Services
	Dr. Iain Boyd	University of Michigan
	Dr. Brian DeMarco	University of Illinois
	Dr. Patricia Falcone	Lawrence Livermore National Laboratory
	Prof. Dan Kahan	Yale Law School
	Dr. Galen McKinley	Columbia University
	Dr. Paul Nielsen	Software Engineering Institute (SEI) at Carnegie Mellon University
	Prof. Ruth Okediji	Harvard Law School
	Dr. Philip Rubin	Haskin Laboratories and Yale University
	Dr. Alex Snoeren	University of California – San Diego
Dr. Anthony “Tony” Tether	Defense Advanced Research Projects Agency (DARPA)	
Dr. Krystyn Van Vliet	Massachusetts Institute of Technology (MIT)	

\* Dr. Martha Krebs submitted topics for the October 30 workshop but was unable to participate.

## Abbreviations

---

AI	Artificial Intelligence
BMD	Ballistic Missile Defense
CDC	Centers for Disease Control and Prevention
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DSSG	Defense Science Studies Group
EOP	Executive Office of the President
GAO	Government Accountability Office
IARPA	Intelligence Advanced Research Activity
IDA	Institute for Defense Analyses
IoT	Internet of Things
MIRVed	Multiple Independently-targetable Reentry Vehicle
NNSA	National Nuclear Security Administration
NSS	National Security Strategy
OSTP	Office of Science and Technology Policy
PSAC	President's Science Advisory Committee
QIS	Quantum Information Science
R&D	Research and Development
S&E	Science and Engineering
S&T	Science and Technology
SAC	Systems and Analyses Center
SCE	Science Communication Environment
SME	Subject Matter Expert
STEM	Science, Technology, Engineering and Mathematics
STPI	Science and Technology Policy Institute
USDA	United States Department of Agriculture

## References

---

- AECOM. 2019. "The Future of Infrastructure: Voice of the People."  
<https://infrastructure.aecom.com/>
- American Institute of Aeronautics and Astronautics. 2008. *Infrastructure Recommendations for Implementation of Executive Order 13419—National Aeronautics Research and Development*. 11 January 2008.  
[https://www.aiaa.org/uploadedFiles/Issues\\_and\\_Advocacy/Aeronautics/wind\\_tunnelinfrastructurepaperapproved011108.pdf](https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/Aeronautics/wind_tunnelinfrastructurepaperapproved011108.pdf)
- American Society of Civil Engineers. "2017 Infrastructure Report Card." Accessed 28 March 2019. <https://www.infrastructurereportcard.org/americas-grades/>
- Berube, David M. 2018. "How Social Science Should Complement Scientific Discovery: Lessons from Nanoscience." *Journal of Nanoparticle Research* 20, no. 5 (2018): 120.
- Broniatowski, David A., Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn, and Mark Dredze. 2018. "Weaponized health communication: Twitter bots and Russian trolls amplify the vaccine debate." *American journal of public health* 108, no. 10 (2018): 1378-1384.
- Centers for Disease Control and Prevention. *Measles (Rubeola)*. Last updated April 15, 2019. <https://www.cdc.gov/measles/index.html>
- . *Measles Cases and Outbreaks*. Last updated April 15, 2019.  
<https://www.cdc.gov/measles/cases-outbreaks.html>
- Climate Science Special Report. "Highlights of the Findings of the U.S. Global Change Research Program Climate Science Special Report." Accessed 8 January 2019.  
<https://science2017.globalchange.gov/chapter/executive-summary/>
- Coats, Daniel. "Worldwide Threat Assessment of the U.S. Intelligence Community." Statement for the Record. Senate Select Committee on Intelligence. Washington, DC. January 29, 2019. Page 23.
- Commission to Review the Effectiveness of the National Energy Laboratories. 2015. *Securing America's Future: Realizing the Potential of the Department of Energy's National Laboratories, Volume 2*. Washington, DC: U.S. Department of Energy.
- Congressional Research Service. 2016. *Commercial Space Industry Launches a New Phase*. R44708. Washington, DC.
- . 2018. *Federal Research and Development (R&D) Funding: FY2019*. R45150. Washington, DC.

- . 2018. *Transatlantic Perspectives on Defense Innovation: Issues for Congress*. R45177. Page 6. Washington, DC.
- DARPA. "Clean-Slate Design of Resilient, Adaptive, Secure Hosts (CRASH)." Accessed March 1, 2019. <https://www.darpa.mil/program/clean-slate-design-of-resilient-adaptive-secure-hosts>
- Defense Microelectronics Activity. "Trusted Accreditation." Last accessed January 17, 2019. <https://www.dmea.osd.mil/trustedic.html>
- Denton, Sarah W., and Eleonore Pauwels. 2018. *There's Nowhere to Hide: Artificial Intelligence and Privacy in the Fourth Industrial Revolution*. The Wilson Center. Washington, DC. March 2018. <https://www.wilsoncenter.org/article/nowhere-to-hide-artificial-intelligence-and-privacy-the-fourth-industrial-revolution>
- Department of Defense. Office of the Under Secretary of Defense for Acquisition and Sustainment. 2019. *Report on Effects of a Changing Climate to the Department of Defense*. Page 2.
- Department of Homeland Security. "Sector-Specific Agencies." Accessed February 1, 2019. <https://www.dhs.gov/sector-specific-agencies>.
- . 2018. "Infrastructure Systems Recovery Support Function" as part of the National Disaster Recovery Framework. [https://www.fema.gov/media-library-data/1466718036457-e2026c3a5907bf0cb86e75b3a3c51757/RSF\\_Infrastructure\\_Systems\\_0623\\_508.pdf](https://www.fema.gov/media-library-data/1466718036457-e2026c3a5907bf0cb86e75b3a3c51757/RSF_Infrastructure_Systems_0623_508.pdf)
- . 2018. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. September 2018.
- Dietz, Thomas. 2013. "Bringing Values and Deliberation to Science Communication." *Proceedings of the National Academy of Sciences* 110, no. Supplement 3 (2013): 14081-14087.
- Executive Office of the President. 2017. *National Security Strategy of the United States of America*. Washington, DC. 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- . 2018. *National Biodefense Strategy*. Washington, DC. <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf>
- . 2018. *National Space Strategy Fact Sheet*. Washington, DC. <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/>
- Fischhoff, Baruch, and Dietram A. Scheufele. 2013. "The Science of Science Communication." *PNAS* 110 (Supplement 3): 14031-14032. doi:10.1073/pnas.1312080110.
- Funk, Cary, and Kim Parker. 2018. *Women and Men in STEM Often at Odds Over Workplace Equity*. Pew Research Center. Jan. 9, 2018.

- Gallo, Jason. 2017. "Translating Science into Policy and Legislation: Evidence-Informed Policymaking." *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017.  
<https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.27>
- GAO. 2017. *HIGH-RISK SERIES: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*. (GAO-17-317). Washington, DC. 2017.  
<https://www.gao.gov/assets/690/682765.pdf>
- . 2018. "GAO Adds Government-wide Personnel Security Clearance Process to 'High Risk List.'"
- . National Nuclear Security Administration. 2017. *Action Needed to Address Affordability of Nuclear Modernization Programs*. GAO-17-341. April 2017.
- Garg, Parie and Sam Glick. 2018. "AI's Potential to Diagnose and Treat Mental Illness." October 22, 2018. <https://hbr.org/2018/10/ais-potential-to-diagnose-and-treat-mental-illness>
- Gastañaduy, Paul A., Jeremy Budd, Nicholas Fisher, Susan B. Redd, Jackie Fletcher, Julie Miller, Dwight J. McFadden III et al. 2016. "A Measles Outbreak in an Underimmunized Amish Community in Ohio." *New England Journal of Medicine* 375, no. 14 (2016): 1343-1354.
- Gebelhoff, Robert. 2017. "China's on Track to Surpass Our Investment in Science." *Washington Post*, Jun. 20, 2017. [https://www.washingtonpost.com/news/in-theory/wp/2017/06/20/chinas-on-track-to-surpass-our-investment-in-science/?utm\\_term=.458a6ff9d350](https://www.washingtonpost.com/news/in-theory/wp/2017/06/20/chinas-on-track-to-surpass-our-investment-in-science/?utm_term=.458a6ff9d350)
- Hall, Victoria et al. 2017. "Measles Outbreak — Minnesota April–May 2017." *Morbidity and Mortality Weekly Report* vol. 66, 27 713-717. 14 Jul. 2017, doi:10.15585/mmwr.mm6627a1
- Howieson, Susannah V., Elmer Yglesias, Samuel L. Blazek, and Daniel E. Basco. 2013. *Federal Personnel Exchange Mechanisms*. IDA Document D-4906, November 2013.
- Howieson, Susannah V., Vanessa I. Peña, Stephanie S. Shipp, Kristen A. Koopman, Justin A. Scott, and Christopher T. Clavin 2013. *A Study of Facilities and Infrastructure Planning, Prioritization, and Assessment at Federal Security Laboratories (Revised)*. IDA Paper P-4916, Revised, February 2013.
- Howieson, Susannah V., Stephanie S. Shipp, Gina K. Walejko, Pamela B. Rambow, Vanessa I. Peña, et al. 2013. *Exemplar Practices for Department of Defense Technology Transfer*. Washington, DC: Science and Technology Policy Institute.
- Hughes, Mary E., Susannah V. Howieson, Gina K. Walejko, Nayanee Gupta, Seth Jonas et al. 2011. *Technology Transfer and Commercialization Landscape of Federal Laboratories*, Washington, DC: IDA Science and Technology Policy Institute.
- Intelligence Advanced Research Projects Activity. "Trojans in Artificial Intelligence." Accessed 10 January 2018.

[https://www.iarpa.gov/index.php?option=com\\_content&view=article&id=1142&Itemid=443](https://www.iarpa.gov/index.php?option=com_content&view=article&id=1142&Itemid=443)

- Intergovernmental Panel on Climate Change. 2013. *Climate Change 2013: The Physical Science Basis*. [Stocker, T.F., D. Qin, G.-K. Plattner, M. Tignor, S.K. Allen, J. Boschung, A. Nauels, Y. Xia, V. Bex and P.M. Midgley (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA.
- Jamieson, Kathleen Hall, Dan Kahan, and Dietram A. Scheufele. 2017. "Introduction: Why Science Communication?" *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017.  
<https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.1>
- Kahan, Dan M. 2017. "On the Sources of Ordinary Science Knowledge and Extraordinary Science Ignorance." *The Oxford Handbook of the Science of Science Communication*. Oxford University Press, 2017.  
<https://dx.doi.org/10.1093/oxfordhb/9780190497620.013.4>
- Lal, Bhavya, Asha Balakrishnan, Becaja M. Caldwell, Reina S. Buenconsejo, and Sara A. Carioscia. 2018. *Global Trends in Space Situational Awareness (SSA) and Space Traffic Management (STM)*. IDA Science and Technology Policy Institute. Washington, DC.
- Lapedus, Mark. 2018. "A Crisis in DoD's Trusted Foundry Program?" *Semiconductor Engineering*. October 22, 2018. <https://semiengineering.com/a-crisis-in-dods-trusted-foundry-program/>
- Luxton, David. 2016. "An Introduction to Artificial Intelligence in Behavioral and Mental Health Care." *Artificial Intelligence in Behavioral and Mental Health Care*, pp. 1-26.
- Martinich, Jeremy and Allison Crimmins. 2017. *Multi-Model Framework for Quantitative Sectoral Impacts Analysis: A Technical Report for the Fourth National Climate Assessment*. 10.13140/RG.2.2.14466.79045.
- McCright, Aaron M., and Riley E. Dunlap. 2011. "The Politicization of Climate Change and Polarization in the American Public's Views of Global Warming, 2001–2010." *The Sociological Quarterly*, 52:2, 155-194, DOI: 10.1111/j.1533-8525.2011.01198.x
- McNeil Jr., Donald. 2019. "Scientists Thought They Had Measles Cornered. They Were Wrong." *New York Times*. April 3, 2019.  
<https://www.nytimes.com/2019/04/03/health/measles-outbreaks-ukraine-israel.html>
- Memorial Sloan Kettering Cancer Center. "Watson Oncology." Accessed 28 January 2018. <https://www.mskcc.org/about/innovative-collaborations/watson-oncology>
- Miller, D. Douglas, and Eric Brown. 2018. "Artificial Intelligence in Medical Practice: the Question to the Answer?" *The American Journal of Medicine*, 131(2), 129-133.

- National Academies of Sciences, Engineering, and Medicine. 2015. *Report in Brief: Climate Intervention*. <http://dels.nas.edu/resources/static-assets/materials-based-on-reports/reports-in-brief/climate-intervention-brief-final.pdf>
- . 2016. *Attribution of Extreme Weather Events in the Context of Climate Change*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/21852>.
- . 2017. *Enhancing the Resilience of the Nation's Electricity System*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/24836>.
- . 2017. *Communicating Science Effectively: A Research Agenda*. Washington, DC: The National Academies Press. Page 7. <https://doi.org/10.17226/23674>.
- National Association of City Transportation Officials. 2018. "Blueprint for Autonomous Urbanism." Accessed February 1, 2019. <https://nacto.org/publication/bau/>
- National Conference of State Legislatures. 2018. "Autonomous Vehicles." November 7, 2018. <http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx>
- National League of Cities. 2018. "Autonomous Vehicles: Future Scenarios." Accessed January 28, 2019. <http://avfutures.nlc.org/>
- National Research Council. 2009. *Sustainable Critical Infrastructure Systems: A Framework for Meeting 21st Century Imperatives: Report of a Workshop*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/12638>.
- . 2012. *Disaster Resilience: A National Imperative*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/13457>.
- . 2012. *Using Science as Evidence in Public Policy*. Washington, DC: The National Academies Press. <https://doi.org/10.17226/13460>.
- National Science and Technology Council. 2016. *Federal Cybersecurity Research and Development Strategic Plan*. <https://www.nitrd.gov/pubs/2016-Federal-Cybersecurity-Research-and-Development-Strategic-Plan.pdf>
- Naval Facilities Engineering Command. 2017. *Climate Change Installation Adaptation and Resilience*. January 2017. [https://www.fedcenter.gov/\\_kd/Items/actions.cfm?action=Show&item\\_id=31041&destination=ShowItem](https://www.fedcenter.gov/_kd/Items/actions.cfm?action=Show&item_id=31041&destination=ShowItem)
- Nisbet, Matthew C., and Dietram A. Scheufele. 2009. "What's Next for Science Communication? Promising Directions and Lingering Distractions." *American Journal of Botany* 96, no. 10 (2009): 1767-1778.
- NIST. 2018. "NIST Cybersecurity Framework." <https://www.nist.gov/cyberframework>

- Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press, 2018.
- Office of the Director of National Intelligence. 2019. *National Intelligence Strategy of the United States of America*.  
[https://www.dni.gov/files/ODNI/documents/National\\_Intelligence\\_Strategy\\_2019.pdf](https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf)
- Omer, Saad B., Kyle S. Enger, Lawrence H. Moulton, Neal A. Halsey, Shannon Stokley, and Daniel A. Salmon. 2008. "Geographic Clustering of Nonmedical Exemptions to School Immunization Requirements and Associations with Geographic Clustering of Pertussis." *American Journal of Epidemiology*, Volume 168, Issue 12, 15 December 2008, Pages 1389–1396,  
<https://doi.org/10.1093/aje/kwn263>
- Pager, Tyler. 2019. "‘Monkey, Rat and Pig DNA’: How Misinformation is Driving the Measles Outbreak Among Ultra-Orthodox Jews." April 9, 2019.  
<https://www.nytimes.com/2019/04/09/nyregion/jews-measles-vaccination.html>
- Parker, Laura. 2015. "The Anti-Vaccine Generation: How Movement against Shots Got Its Start." *National Geographic* 6. February 6, 2015.
- Partnership for Public Service and Booz Allen Hamilton. 2009. *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce*. July 2009.
- Partnership for Public Service and the Volcker Alliance. 2018. *Renewing America’s Civil Service*. September 2018.
- Piscopo, Paul, Richard Hallion, Terrence Trepal, and Mark Lewis. 2014. *Study on the Ability of the U.S. Test and Evaluation Infrastructure to Effectively and Efficiently Mature Hypersonic Technologies for Defense Systems Development: Summary Analysis and Assessment*. IDA Report GR-74. Washington, DC: IDA Science and Technology Policy Institute.
- President’s Council of Advisors on Science and Technology. 2012. *Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Mathematics*.  
[https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-engage-to-excel-final\\_2-25-12.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/pcast-engage-to-excel-final_2-25-12.pdf)
- The White House. 2012. *National Bioeconomy Blueprint*.  
[https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national\\_bioeconomy\\_blueprint\\_april\\_2012.pdf](https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_bioeconomy_blueprint_april_2012.pdf)
- . 2018. *National Cyber Strategy of the United States of America*.  
<https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>
- U.S. Global Change Research Program (USGCRP). 2018. *Impacts, Risk, and Adaptation in the United States: Fourth National Climate Assessment, Volume II*. [Reidmiller, D. R., C.W. Avery, D.R. Easterling, K.E. Kunkel, K.L.M. Lewis, T.K.

Maycock, and B.C. Stewart (eds.)]. U.S. Global Change Research Program, Washington, DC, USA, 1515 pp. doi: 10.7930/NCA4.2018

United States Congress. House Subcommittees on Research and Technology and Energy, Committee on Science, Space, and Technology. 2018. *Artificial Intelligence Emerging Opportunities, Challenges, and Implications for Policy and Research. 26 June 2018*. (Statement of Timothy M. Persons, United States Government Accountability Office).

USDA. 2013. *Climate Change and Agriculture in the United States: Effects and Adaptation*. USDA Technical Bulletin 1935.

Veugelers, Reinhilde. 2017. "China is the World's New Science and Technology Powerhouse." *BRINK Asia*. August 30, 2017.

Weinberg, Alvin V. et al. 1963. *Science, Government, and Information: The Responsibilities of the Technical Community and the Government in the Transfer of Information*. The White House, Washington, DC. January 10, 1963, Page 1.

Woetzel, Jonathan et al. 2018. *Smart Cities: Digital Solutions for a More Livable Future*. McKinsey Global Institute.  
<https://www.mckinsey.com/~media/McKinsey/Industries/Capital%20Projects%20and%20Infrastructure/Our%20Insights/Smart%20cities%20Digital%20solutions%20for%20a%20more%20livable%20future/MGI-Smart-Cities-Full-Report.ashx>

World Economic Forum. 2017. *Shaping the Future Implications of Digital Media for Society: Valuing Personal Data and Rebuilding Trust*. January 2017.  
[http://www3.weforum.org/docs/WEF\\_End\\_User\\_Perspective\\_on\\_Digital\\_Media\\_Survey\\_Summary\\_2017.pdf](http://www3.weforum.org/docs/WEF_End_User_Perspective_on_Digital_Media_Survey_Summary_2017.pdf)

Xue, Yi, and Richard Larson. 2015. "STEM Crisis or STEM Surplus? Yes and Yes." *Monthly Labor Review*, U.S. Bureau of Labor Statistics, May 2015.  
<https://doi.org/10.21916/mlr.2015.14>.



**REPORT DOCUMENTATION PAGE**

*Form Approved  
OMB No. 0704-0188*

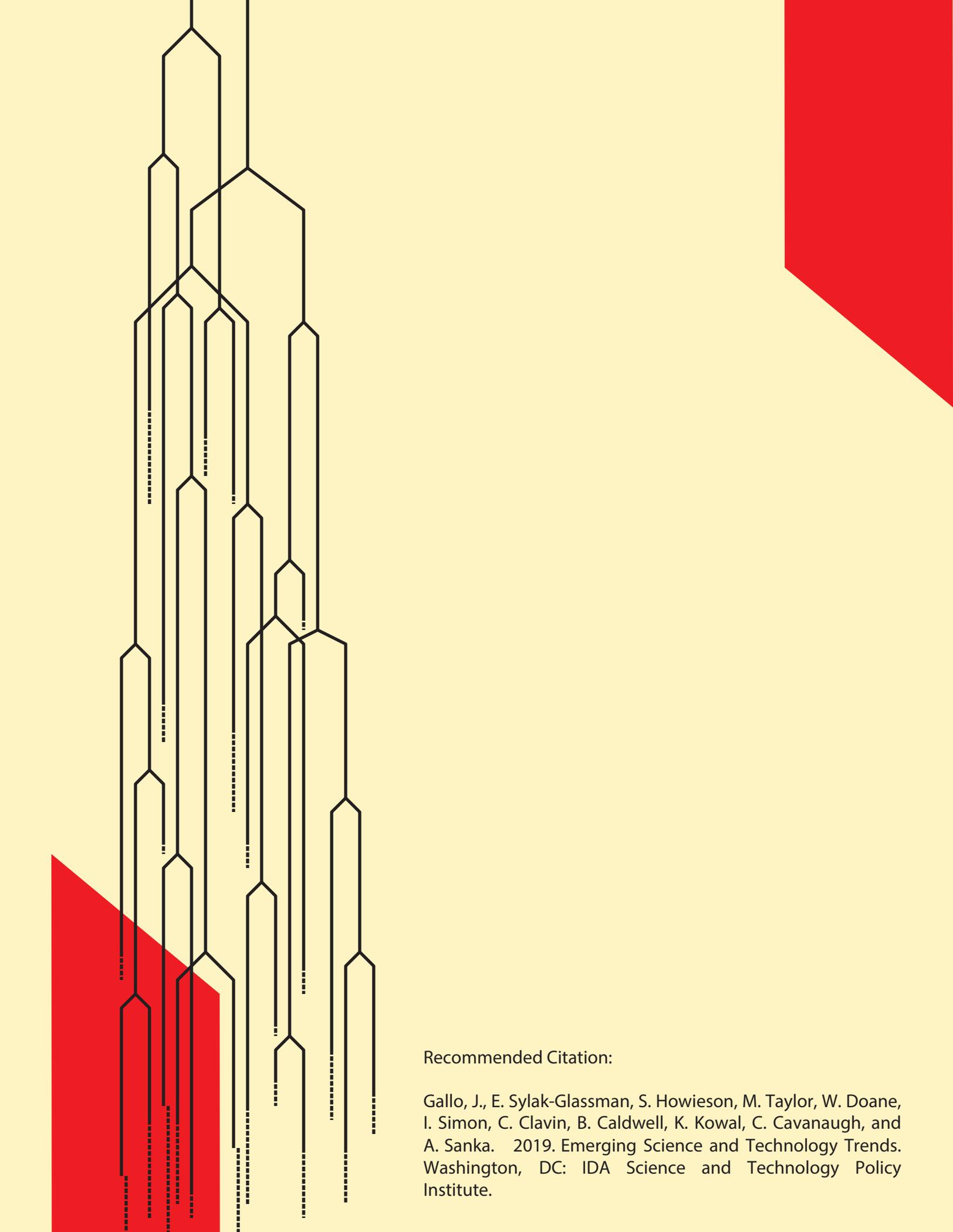
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b>		<b>2. REPORT TYPE</b>		<b>3. DATES COVERED (From - To)</b>	
<b>4. TITLE AND SUBTITLE</b>				<b>5a. CONTRACT NUMBER</b>	
				<b>5b. GRANT NUMBER</b>	
				<b>5c. PROGRAM ELEMENT NUMBER</b>	
<b>6. AUTHOR(S)</b>				<b>5d. PROJECT NUMBER</b>	
				<b>5e. TASK NUMBER</b>	
				<b>5f. WORK UNIT NUMBER</b>	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b>				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b>				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b>					
<b>13. SUPPLEMENTARY NOTES</b>					
<b>14. ABSTRACT</b>					
<b>15. SUBJECT TERMS</b>					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			<b>19b. TELEPHONE NUMBER (Include area code)</b>





An abstract graphic on a yellow background. It features several vertical black lines of varying lengths, some of which are connected at the top by thin horizontal lines, creating a series of vertical, elongated, somewhat irregular shapes. Some of these shapes have small gaps or breaks in the lines. In the bottom-left corner, there is a red shape that looks like a triangle pointing upwards. In the top-right corner, there is a red shape that looks like a triangle pointing downwards. The overall effect is a modern, geometric design.

Recommended Citation:

Gallo, J., E. Sylak-Glassman, S. Howieson, M. Taylor, W. Doane, I. Simon, C. Clavin, B. Caldwell, K. Kowal, C. Cavanaugh, and A. Sanka. 2019. Emerging Science and Technology Trends. Washington, DC: IDA Science and Technology Policy Institute.