THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on a Cybersecurity Moonshot

November 14, 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY

"Make the Internet safe and secure for the functioning of Government and critical services for the American people by 2028."

The United States is at an inflection point: simultaneously faced with a progressively worsening cybersecurity threat environment and an ever-increasing dependence on Internet technologies fundamental to public safety, economic prosperity, and overall way of life. Our national security is now inexorably linked to cybersecurity. Therefore, the Nation must build on past efforts and current strategies to seize the opportunity to strategically reorient from a largely reactive, incremental cybersecurity posture to a proactive approach that boldly assures digital trust, safety, and resilience for all Americans. Achieving this audacious outcome will require strong national leadership, political will, and a sustained whole-of-nation investment over an extended period. The U.S. Government can take immediate actions that lay the foundation for this long-term shared cybersecurity vision for the Nation, while simultaneously yielding near-term benefits that ensure continued technological global leadership.

Leadership must start with a bold aspirational statement of strategic intent, as the United States has done just a few times historically when facing existential challenges. The President's National Security Telecommunications Advisory Committee (NSTAC) believes cybersecurity represents one of the 21st Century's greatest challenges, and one the United States simply must enduringly address as a matter of national strategic imperative. To communicate this, the Administration, at its most senior levels, must deliver a clear aspirational and inspirational vision as a catalyzing force for national activities. It must declare a national strategic intent to: *Make the Internet safe and secure for the functioning of Government and critical services for the American people by 2028.* Such a pursuit would assure societal trust in digital infrastructure, promote economic vitality, and reinforce American innovation leadership.

> "I believe we possess all the resources and talents necessary. But the facts of the matter are that we have never made the national decisions or marshaled the national resources required for such leadership. We have never specified long-range goals on an urgent time schedule or managed our resources and our time so as to insure their fulfillment."
>
> - President John F. Kennedy in his address to a joint session of Congress on May 25, 1961

The NSTAC adopted the term "Cybersecurity Moonshot" to describe this approach, named after the National Aeronautics and Space Administration (NASA) Apollo program's effort to send a man to the Moon following President John F. Kennedy's May, 1961, address to a joint session of Congress. The original moonshot oriented collective national action towards an ambitious goal to put a man on the moon and return him safely to Earth by the end of the decade. Importantly, President Kennedy clearly articulated this end goal without being prescriptive of the many individual innovations and actions required to achieve that outcome.

The differences between the characteristics of President Kennedy's moonshot vision and those anticipated of a moonshot for cybersecurity, however, are numerous. Principally, the success criteria for a Cybersecurity Moonshot Initiative will be less precise and measurable because its achievement will be a societal transformation rather than a singular, visual triumph. The NSTAC recognizes these analogy limitations but forcefully believes the Moonshot represents a powerful and highly applicable model for the national prioritization, collective action, and accelerated innovation needed for cybersecurity.

In order to realize its goal, the Cybersecurity Moonshot Initiative must pursue answers to several complex questions. To start: What does 'safe and secure' mean in the modern digital society? What 'critical services' are most fundamental to national security and public safety and must be nationally prioritized to realize a measurably safe and secure Internet? Beginning to publicly contend with these complex questions on a national basis and with a far more inclusive community of stakeholders is foundational toward realizing this more audacious and sustainable future. In some instances, the NSTAC seeks to answer these types of questions within this report. In others, these answers should be borne out of the longer-term national Cybersecurity Moonshot Initiative this report is proposing be launched.

Delivering an aspirational statement of intent alone is, of course, not enough. The Cybersecurity Moonshot Initiative must be deeply rooted in a clear strategic framework and shared principles that transcend individual strategies and emphasize true generational change. It must have a governance structure that enables distributed groups of stakeholders across the Government, private industry, academia, and civil society to focus their collective energies and activities towards the defined, higher order national objectives of the Cybersecurity Moonshot Initiative.

Throughout this report, the NSTAC endeavors to answer several fundamental questions, including what a Cybersecurity Moonshot Initiative is, why it is necessary, and how the Nation can effectively operationalize it. Section 1.0, *Introduction*, and Section 2.0, *Why Does Cybersecurity Require a Moonshot?* focus on why a Cybersecurity Moonshot Initiative is needed, why the current trajectory of incremental improvement in cybersecurity is inadequate, and why this challenge is worthy of a generation defining pursuit.

Section 3.0, *Cybersecurity Moonshot Initiative Action Plan*, provides strategic recommendations and actionable steps the U.S. Government can take to lead this initiative and use its unique authorities to strategically champion, organize, direct, resource, and empower whole-of-nation activities aligned to its objectives. Section 3.0 defines the beginning elements of a Cybersecurity Moonshot Initiative playbook, outlining recommendations related to the practical organization and operationalization of the initiative. This includes key considerations related to governance, objectives, milestones, funding, and an organizing framework referred to as the Strategic Pillars. A summary of Key Recommendations contained throughout this report includes:

Key Recommendations: Cybersecurity Moonshot Initiative Governance (*Section 3.1-3.3*)

- The President or Vice President should introduce and strategically champion a Cybersecurity Moonshot Initiative to clearly signal that addressing cybersecurity challenges in an enduring manner is a strategic imperative fundamental to the Nation's future. This proclamation should be made in a forum of historical significance, such as the State of Union or a special address to a joint session of Congress, to emphasize this level of national prioritization.

- The Cybersecurity Moonshot Initiative must engender a whole-of-nation approach, including a multi-tiered governance model spanning Government, industry, and academia that align their inherent capabilities and activities towards realizing a safe and secure Internet. This model could include a consortia-style business structure that facilitates cooperation, resource and reward sharing when appropriate and not harmful to competitive market dynamics that promise the most efficacious path to objectives. There should also be formal mechanisms for collaboration with Government and academic partners in achieving common goals.

- Within the U.S. Government, an Administration-led Cybersecurity Moonshot Council should lead and manage the initiative. The Council should be responsible for and empowered to: raise national visibility, advocate for sustained funding, develop national-level strategies, and create policies and processes that empower and incentivize non-governmental stakeholders to drive accelerated innovation in defined Cybersecurity Moonshot Initiative enabling fields. The Council's mandate should be oriented exclusively towards the achievement of long-term outcomes, distinct but complementary to existing Government cybersecurity leadership often naturally driven towards shorter-term and topical requirements.

- The President or Vice President should officially chair the Council, which should be comprised of Cabinet level officials from relevant departments and agencies. The Cybersecurity Moonshot Council should have formal mechanisms for appointed non-governmental entities to directly contribute to the Cybersecurity Moonshot Initiative strategy and policy development process. A Presidentially appointed Executive Director should operationally run the initiative and be responsible for, and empowered to maintain, visibility over all national Cybersecurity Moonshot Initiative activities and elevate activities that provide the greatest strategic impact towards realizing a safe and secure Internet environment.

- The Cybersecurity Moonshot Council should publicly articulate a Strategic Framework, after a period of internal and external consultation, to provide common structure that helps organize the Cybersecurity Moonshot Initiative's distributed, whole-of-nation activities. As a recommended starting point, the NSTAC proposes six Strategic Pillars, recognizing that achieving a more enduringly safe and secure Internet within the next 10 years will require a holistic and multi-disciplinary approach.

Key Recommendations: Cybersecurity Moonshot Initiative Strategic Pillars (*Section 3.4*)

Making meaningful progress towards a more enduringly safe and secure Internet within the next 10 years will not be the result of a singularly transformative solution. The complexity of the cybersecurity challenge will require strategic attention and an accelerated rate of innovation across matters of technology, people, process, and policy—as represented by the Strategic Pillars. Meaningful progress will require incentivization of existing and known solutions and pursuing the realization of new transformational solutions.

The NSTAC recommends six strategic pillars to guide this whole-of-nation distributed activity: (1) *Technology*; (2) *Human Behavior*; (3) *Education*; (4) *Ecosystem*; (5) *Privacy*; and (6) *Policy*. These pillars should not be considered independent work streams. They should be seen as critical interdependent elements of the overarching Cybersecurity Moonshot Initiative, including activities that are all complementary and reinforcing to the desired outcome of a safe and secure Internet.

1. Technology

Dramatic technological advances continue to broaden the digital landscape and create new cybersecurity risks that malicious actors actively seek to exploit. However, these same new and rapidly emerging technologies, if leveraged strategically, can enable more automated and effective defensive security capabilities. Many of these foundational technological underpinnings exist or are in development—but they will require a concerted national research and product development strategy to bring them to bear against the national cybersecurity challenge. Key desired outcomes within the Technology Strategic Pillar include:

- Strategic technologies deemed critical to the overall safety and security of the Internet environment are identified, prioritized, and invested in to accelerate their availability. Illustrative technology areas deemed critical based on the NSTAC's findings include:

    - Augmented intelligence which assists humans rather than replaces them, for automated threat prevention that can stay ahead of the pace of attackers;

    - Quantum communications and quantum resistant cryptography that can protect current cryptographic methods used for cybersecurity defense;

    - Behavioral biometrics to provide identity scores that reduce the reliance on traditional passwords and frequently compromised personally identifiable identification for authentication; and

    - 5G Communications and other next generation networks designed and architected at the outset with enhanced security, connectivity, and availability.

- National strategic plans to accelerate growth in these critical technology areas, including through targeted Cybersecurity Grand Challenges where appropriate, are implemented to outpace competitive international efforts.

- A policy framework is developed and regulatory obstacles are streamlined to both incentivize and reward private sector investment and innovation in the technologies underpinning the Cybersecurity Moonshot Initiative.

2. Human Behavior

Technology alone cannot address the Nation's core cybersecurity challenges. These challenges will demand the ingenuity of a much broader innovation community of multi-disciplinary experts inspired to devote their expertise to transformative objectives for cybersecurity. Citizens and companies must also understand their responsibility in preventing successful cyber attacks and be empowered with information and tools that incentivize them to make the right security decisions, by default. Effective behavioral change campaigns, like "Smokey the Bear" and anti-drunk driving initiatives aimed at increasing social pressure against risky, societally damaging behaviors, are one such tool.

3. Education

The Cybersecurity Moonshot Initiative must address the significant shortage of expertise and funding for key strategic research disciplines, including previously identified critical technologies. The initiative must promote highly distributed, exponentially scalable educational tools and expand the use of mentoring and apprenticeship as force multipliers in critical areas. Strategic cybersecurity educational planning must also consider how emerging technologies, such as augmented intelligence, will alter traditional cybersecurity workforce requirements.

4. Ecosystem Roles and Responsibilities

No single Government entity, company, or industry group is individually capable of designing, conceptualizing, building, or operationalizing the underpinnings of an assuredly safe Internet environment. The effort must be the result of a coordinated approach where stakeholders have a shared understanding of their respective roles and responsibilities and take actions that promote integration of complementary ecosystem capabilities. The Internet is comprised of billions of devices, software programs, services, and users. Enabling a fundamentally safe Internet environment for Government and critical services, while maintaining the ubiquity of Internet access, will require a conscious and coordinated effort to work with a wide variety of participants at various levels of trust.

5. Privacy

Privacy is a core principal that must permeate all aspects of the Cybersecurity Moonshot Initiative's development and will be paramount to engendering the trust of the American people. American citizens must be able to trust the information systems that provide critical services and have practical certainty that the Cybersecurity Moonshot Initiative will not create privacy vulnerabilities, but instead enhance privacy assurance and ensure that their personal data and transactions will remain protected, and in their control.

6. Policy

The Government must carefully assess and implement policies that empower and incentivize key stakeholders responsible for Cybersecurity Moonshot Initiative enabling innovations and implementation. Policies will need to be created, reformed, or ended to foster the creation of the fundamentally safe Internet environment. For example, the requirement for trusted identity and fully authenticated interactions to assure a safe Internet environment will necessitate a policy infrastructure of enhanced security, attribution, and accountability. Close coordination with lawmakers, the national and international community, and private partners on global norms of cyberspace behavior will also be critical to success.

Key Recommendations: Cybersecurity Moonshot Initiative- Grand Challenges (*Section 3.5*)

When proposing something as long-term and complex as the Cybersecurity Moonshot Initiative, the NSTAC believes it is critical to identify a discrete number of specific shorter-term focus areas to serve as representative models for the broader principles of the overall Cybersecurity Moonshot vision. The principles represented by the well-established 'Grand Challenges' community—audacious thinking, outcome-based incentivization, open innovation, solution crowdsourcing—closely fit this mold. This 'Grand Challenge' approach must be more robustly embraced by the cybersecurity community. The U.S. Government can lead this transformation by launching a series of Cybersecurity Grand Challenges that produce more immediate and momentum building breakthroughs towards realizing a safe and secure Internet environment.

- As a catalyst for the overall Cybersecurity Moonshot Initiative, the Cybersecurity Moonshot Council should lead the identification and launch of one or more Grand Challenges by conducting a six-month, collaborative process that formally engages stakeholders across the country. These Grand Challenges should be organized around critical areas of technology development where systemic intransigence and market failure has previously hampered progress. The U.S. Government can leverage various tools to incentivize and accelerate a whole-of-nation embrace of these Grand Challenge-aligned activities across all six Strategic Pillars.

- In evaluating potential Grand Challenge candidates, the Government should weigh several considerations and key questions, including: (1) Does the Government have a clear role in catalyzing activities aligned to the Grand Challenge where previous market-based drivers have proven insufficient; (2) Does the Grand Challenge require activities beyond the scope of Governmental authorities and/or strengths and would benefit from broader collaboration; (3) Would society, specifically non-cybersecurity experts, widely understand the strategic value and importance of the Grand Challenge; (4) Is the Grand Challenge both measurable and achievable; (5) Would realization of the Grand Challenge's objectives produce an outcome that is highly scalable; and (6) Does the Grand Challenge have a broad scope that is comprehensive enough to include activities across multiple Strategic Pillars?

The Administration has a unique opportunity in history. Decades of well-intentioned but disjointed activities have made the Internet progressively less safe for the critical services which depend upon it. The NSTAC believes we need to be bolder and proclaim, as a national strategic imperative, that our 10-year goal is to make the Internet safe for Americans' interactions with Government and critical services. The NSTAC is clear-sighted about the enormity of this goal and makes this recommendation fully grasping both the urgency of success and the critical issues that have caused prior, well-intentioned efforts to fall short.

History provides real precedent for the Nation overcoming seemingly impossible challenges. In these historical instances, leaders declared a strategic intent without a clear understanding of the means to the end. In these historical examples, like now, there was a clear goal, tangible first steps, and a whole-of-nation approach that U.S. Government leadership used to direct the effort and inspire success. A similarly imperative opportunity exists for the 21st Century. Our future prosperity and success as a Nation is now intrinsically dependent on our success in cybersecurity, and an inspiring Moonshot-like effort is needed to address it.

1.0 INTRODUCTION

The Internet, and the ongoing digital era it has ushered in, has been the source of immeasurable economic and societal benefit. The ability to use the open Internet and the freedom to use Internet-connected technologies has simply become a core and fundamental right. The United States must preserve this freedom by assuring that Americans can safely use these technologies, as a matter of national strategic imperative, while leading by example internationally.

Perhaps more than any 21st Century economic and national security challenge, cybersecurity demands a greater sense of shared responsibility and collective action.

On its current trajectory, the United States faces unequivocal risks to realizing this national and international imperative. Cybersecurity threats are becoming more frequent, more sophisticated, and more destructive—gradually eroding society's trust in digital infrastructure. As technology continues to advance and every facet of daily life becomes increasingly interconnected, both the likelihood and the cost of failure rise dramatically. Technologists and cybersecurity experts worldwide recognize this concerning trend, but it is still not widely understood by many Government leaders, business executives, or the general public. Perhaps more than any 21st Century economic and national security challenge, cybersecurity demands a greater sense of shared responsibility and collective action. Our age of hyperconnectivity now means that your risk is my risk, as attacks on the weakest links can now bear consequence for the broader digital environment.[1]

The complex nature of cybersecurity has created a multitude of challenges cutting across matters of technology, people, and processes. This complexity has led to a tendency to compartmentalize the challenge into its individual, more easily understood components. Further complicating the identification of enduring solutions is the fact that cybersecurity capabilities, authorities, and responsibilities are highly distributed across the ecosystem. No one stakeholder can address the challenge unilaterally. Often, the principal costs of a cybersecurity attack are not borne by the initial victim, leading to negative externalities and misaligned incentives to improve cybersecurity risk behaviors. These characteristics have too often led us to conceptualize solutions in ways that are too fragmented, reactive, or incremental in nature. As a result, discrete cybersecurity challenges tend to be addressed at the expense of proactively preventing cyber attacks and reducing systemic cybersecurity risk on a holistic basis.

The scale, severity, and complexity of the cybersecurity threat now pose an existential risk to the future of the Nation—demanding the exploration of a fundamentally new approach to identify bolder solutions for a more enduringly defensible and safe Internet. The President's National Security Telecommunications Advisory Committee (NSTAC) recognizes there are many known best practices and policies, if more judiciously followed, would measurably improve Internet safety and security. However, this report is focused on the pursuit of more transformational efforts that will fundamentally alter the default level of Internet safety and security. This pursuit will be a generation defining challenge and, like the space race before it, can serve to inspire and form the foundation of continued U.S. technological global leadership in the decades to follow. While the United States has not yet experienced a singular, Sputnik-like galvanizing event for

[1] Kirstjen M. Nielsen, "Remarks by Secretary Kirstjen M. Nielsen at the RSA Conference" (remarks, San Francisco, CA, April 17, 2018) Speeches, https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

cybersecurity, the Nation must demonstrate the fortitude and foresight to take bold and proactive steps before such a catastrophic, action forcing event occurs.

2.0 WHY DOES CYBERSECURITY REQUIRE A MOONSHOT?

The first phase of the NSTAC's research for this study intentionally focused on disciplines other than cybersecurity where the Nation, and in some instances the world, organized activities against the realization of a highly ambitious outcome. In the review of these historical 'moonshot-like' efforts, a common consensus emerged: Moonshot efforts have a distinct time and place in history. They require a unique convergence of political, societal, technological, and other forces to create the enabling environment necessary for success.[2] Ultimately, these forces come together in a way that leads to a societal consensus around two broad principles: (1) the challenge is of such significance that failure is not an acceptable outcome; and (2) a belief that failure is an inevitability on the current trajectory, absent a fundamentally new approach. These principles apply directly and completely to the current and future cybersecurity environment.

But significant work remains to foster a shared national understanding about the nature and severity of the cybersecurity challenge. This begins with articulating a clear and compelling answer to the question 'Why?' in order to justify the significant national investments, priority realignments, and even personal sacrifices that will be required to make real and enduring progress against this particularly complex challenge. Helping to catalyze a national plan of action that reframes and elevates cybersecurity as a near singular national security and economic challenge is one foundational goal of this report.

As a Nation, the United States has fundamentally failed to articulate the cybersecurity challenge in a way that incentivizes and ensures this level of collective action. Due to the complexity of cybersecurity, the Nation too often has compartmentalized the full scope of the challenge and characterized it in predominately technical terms. This approach has often excluded key stakeholders from the discussion, leaving them uninformed and believing that they have no responsibility or ability to help address the challenge. The U.S. Government must frame the cybersecurity challenge more broadly, making it clear that policy, educational, and human behavioral factors are as important as technological innovation towards a long-term solution and that a broader range of experts must be brought to bear.

Cybersecurity as a national challenge also has a clear and compelling answer to the question 'Why Now?' The American people seem to have accepted data breaches that compromise their personal information as the price of technology's convenience. However, they are not likely to tolerate future cyber attacks with direct and physical impact on their lives. In a digital environment where information increasingly exists as only bits and bytes, there is a narrowing line separating a smoothly functioning digital society built on a trusted digital foundation, and the chaotic breakdown of society that would result from the erosion of that trust.

On the current trajectory, it is highly likely that within the next 10 years, the United States will experience more severe and physically destructive cyber attacks than have been experienced to date. Preventing them will require a proactive, strategic, and systematic approach to defense that

[2] Lisa Goldman and Kate Purmal, "How to Launch a Successful Moonshot," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, February 20, 2018).

galvanizes the collective action of the American people. This approach must start with a statement by national leadership, supported at the highest levels of the U.S. Government, industry, and academia, that frames the cybersecurity challenge as no longer an acceptable risk, but an existential threat to the American people's fundamental way of life.

The Nation's leaders must articulate this "Why and Why Now" in an aspirational and optimistic manner. While it is important to be forthright about the negative consequences of inaction, national leadership should also espouse the positive and cascading effects of focused, accelerated, whole-of-nation action towards a fundamentally safe and secure Internet. These positive and cascading effects could be similar to the results of the national mobilization around the space program. During the original moonshot, massive investments in research and development (R&D) distributed across the U.S. Government, private industry, and the academic system led to dramatic engineering breakthroughs and unexpected innovations in medicine, material science, and GPS technologies that formed the bedrock of U.S. technological global leadership in the decades that followed.

The United States possesses much of the technological foundation in cybersecurity to make this pursuit more than an academic exercise. Recent and near-term technological breakthroughs (explored in depth in the NSTAC's *Report to the President on Emerging Technologies Strategic Vision*[3]*)* in areas such as quantum computing, artificial intelligence (AI) and machine learning, cloud computing, and 5G communications create the potential for more simplified and automated cybersecurity defenses, shifting more leverage and the overall balance of power to cybersecurity defenders.

Government and industry must consider these technological issues and the interdependent policy, process, and behavioral questions—so that they may effectively evaluate, prioritize, and incentivize action towards those innovations that provide the greatest amount of leverage, and ultimately advantage, against malicious cyber actors. This starts with an outcome focused, aspirational, and inspirational statement of strategic intent.

3.0 CYBERSECURITY MOONSHOT INITIATIVE ACTION PLAN

The United States is entrenched on a path of incrementalism in its approach to addressing cybersecurity. Forging a fundamentally new trajectory of progress is daunting to conceptualize, but the Nation simply must shift from its unsustainable and costly mindset around cybersecurity. This will demand the highest level of national leadership to galvanize resources and energies towards a bolder pursuit. To be successful, the initiative must become truly 'whole-of-nation', propelled by charismatic leadership, a comprehensive milestone driven plan of execution, and an engaged coalition of Government, industry, and academia experts.

This section, the *Cybersecurity Moonshot Initiative Action Plan*, details strategic recommendations related to the practical execution and operationalization of the Cybersecurity Moonshot Initiative. It details actionable steps the U.S. Government can take to lead this initiative by using its unique authorities and capabilities to strategically champion, organize,

[3] NSTAC. *NSTAC Report to the President on Emerging Technologies Strategic Vision*. (Washington, DC: NSTAC, July 14, 2017) 2017 NSTAC Publications, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

direct, resource, and empower whole-of-nation activities aligned to defined objectives. The overarching message here is simple: Although it may be hard to visualize and impossible to predict all the long-term actions required to realize a fundamentally 'safe and secure' Internet environment over the next 10 years, this Administration can demonstrate leadership by taking specific short-term actions that produce immediate gains and lay the foundation for a long-term, bolder vision for cybersecurity.

Because the NSTAC is chartered to advise the President, the balance of recommendations contained within this report are oriented towards specific actions the U.S. Government can take to move this initiative forward. The NSTAC recognizes and celebrates the globally interconnected nature of the Internet. Close partnership with like-minded partnerships will be essential. However, given the scope of the NSTAC's charter, our recommendations are focused on actions the U.S. Government can take to serve as model for like-minded nations. However, these recommendations should not be interpreted as actions the U.S. Government should take unilaterally, but rather actions the NSTAC recommends the U.S. Government take to empower the broader ecosystem. Often, this will require close and direct consultation with non-governmental stakeholders during the policy and initiative development process. Accordingly, many recommendations in this section make direct reference to the U.S. Government exercising its convening and mobilizing capabilities to lead this collaborative process.

Cybersecurity Moonshot Initiative
Recommended Actions: Timeline

• Announce Cybersecurity Moonshot Initiative/Deliver Aspirational Statement (*Section 3.1*)	At Launch
• Establish Cybersecurity Moonshot Council (*Section 3.2.1*)	At Launch
• Establish Non-Governmental Component of Council (*Section 3.2.2*)	Launch + 60 Days
• Define Strategic Framework and National R&D Priorities for Cybersecurity (*Section 3.4*)	Launch + 120 Days
• Launch Multi-Stakeholder Process to Define Grand Challenges (*Section 3.5*)	Launch +180 Days
• Launch First Cybersecurity Grand Challenge (*Section 3.5*)	Launch +1 Year

3.1 Deliver Aspirational Statement

Key Recommendation: The President or Vice President should introduce and strategically champion a Cybersecurity Moonshot Initiative to clearly signal that enduringly addressing the Nation's cybersecurity challenges is a singular strategic imperative. This proclamation should be made in a forum of historical significance, such as the State of the Union or a special joint address to Congress, to emphasize this national prioritization.

In reviewing historical messaging around wide-scale initiatives, including President Kennedy's original 'moonshot' speech, the NSTAC identified several common characteristics that must be engrained in a presidential or vice presidential-level cybersecurity proclamation. Key characteristics included:

- **A Clear and Compelling Goal:** The statement featured a succinct, outcome-based goal, articulated in a way that reduces complexity to something that can be widely understood across society.

- **An Aspirational Tone:** The statement framed the challenge and its expected solution in optimistic terms that promoted national objectives, as opposed to "selling fear" or the negative consequences of inaction.

- **A Compressed Timeline:** The statement featured a clearly articulated, set timeline—underscoring the urgency of resolution.

- **An Audacious and Non-Prescriptive Approach:** The statement was intentionally audacious in nature to generate skepticism and productive dialogue about its achievability.[4]

Key Recommendation: With these characteristics in mind, the NSTAC recommends that the President or Vice President deliver an aspirational statement of intent to: *"Make the Internet safe and secure for the functioning of Government and critical services for the American people by 2028."*

The NSTAC found this aspirational statement effective in that it was seen as specific in its intent but flexible in its interpretation. The term 'safe' was specifically chosen because societal conceptions of safety were determined to be more universally understood, instinctual, and identifiable—especially when compared to the more ambiguous, technical terms commonly associated with cybersecurity. 'Safe' was also deemed to be instructive in that it appropriately acknowledged cybersecurity threats now transcend the digital realm and pose real physical threats to public safety as society increasingly embraces a world of connected cars and Internet-dependent critical infrastructure systems.

The term 'safe' was also determined to carry a productive degree of ambiguity, critical in catalyzing a more robust national conversation. For example, to realize a 'safe' Internet; what core technologies does the Nation need to prioritize for long-term R&D investment? How does the United States need to reform its educational system to grow well-rounded cybersecurity experts and incentivize better cybersecurity practices among citizens? How do Information Technology supply chain policies need to adapt to more fundamentally assure safety?

The NSTAC does not profess to have all the answers to these difficult questions, many of which will be risk management tradeoffs and not binary in nature. Through its findings, the NSTAC hopes to catalyze a broader national dialogue that embraces these complex and, at times, difficult conversations—because they are challenges that simply must be overcome for the future of the Nation. Section 3.4, *Define Strategic Framework and Pillars,* further explores in greater depth these types of questions.

Perhaps even more critical than the substance of the aspirational statement, is who delivers the first message and where the individual delivers it. This individual must be a strong and

[4] Lisa Goldman and Kate Purmal *The Moonshot Effect: Disrupting Business as Usual* (San Carlos, CA: Wynnefield Business Press, 2016).

charismatic leader, someone viewed with legitimacy across multiple stakeholder sets and motivated by the broader national interest. The individual must articulate the vision to emphasize a commitment to continuity and sustained investment to the Cybersecurity Moonshot Initiative over the long-term—impermeable to Administration transitions and political partisanship. This will require a level of aspiration and unity of effort between and across the Executive and Legislative branches that has not been seen in some time.

The NSTAC's assessment is that only a Presidential or Vice Presidential level of emphasis can generate the appropriate national mobilization around this challenge with wartime-like urgency. When the President or Vice President first articulates the initiative, it should be done in close coordination with relevant Cabinet officials, Congressional leadership, chief executives, and academic leaders to demonstrate a real and symbolic unity of effort that expands across elements of society well beyond the traditional cybersecurity community. The location and forum of delivery must also be one of elevated historical stature; the U.S. Capitol for a State of the Union address or a special joint address to Congress are appropriate representative examples that would convey the strategic and historic importance of this national initiative.

3.2 Establish Governance for Whole-of-Nation Approach

Merely delivering an aspirational statement of intent, however, is not enough. The statement must be deeply rooted in a clear strategic framework and shared principles. It must be backed by a clear governance structure that enables distributed groups of stakeholders across the Government, private industry, academia, and civil society to contribute and focus their collective energies and activities towards the defined, higher-order national objectives of the Cybersecurity Moonshot Initiative.

Prior to the initiative being formally introduced to the public by the President or Vice President, the White House should lead an internal process to establish a governance structure for the Cybersecurity Moonshot Initiative. Broadly speaking, the NSTAC defines governance as the way the Cybersecurity Moonshot Initiative organizes participants, authorizes decision-making authorities, establishes objectives, and imposes accountability measures to ensure progress. A robust and comprehensive evaluation of appropriate governance and organizational models will be foundational to the long-term viability and effectiveness of a distributed national Cybersecurity Moonshot Initiative.

Key Finding: The Cybersecurity Moonshot Initiative will only be successful through a unity of effort that leverages both the unique authorities and capabilities of the whole-of-Government and harmonized efforts across the whole-of-industry and academia.

Cybersecurity is an inherently distributed challenge, with unique authorities, roles, and responsibilities that are shared across the broader public, private, and academic ecosystem. All these capabilities must be effectively leveraged in a collective security model to make meaningful progress. The Cybersecurity Moonshot Initiative's implementation and success will depend on a highly distributed system of stakeholder groups that are effectively empowered, resourced, and mobilized.

Based on a collation of findings across multiple briefings, the NSTAC developed the graphic below to conceptually visualize how a shared understanding of distributed roles, responsibilities, and strategic vision can help focus—not limit or stifle—targeted innovation towards defined areas that can lead to a more fundamentally safe and secure Internet. Conceptually, this includes top-down pressure from the highest levels of the U.S. Government to define strategic intent, and upward pressure from the operational engines of the private sector and academia that are actively defining innovation priorities and leading progress.

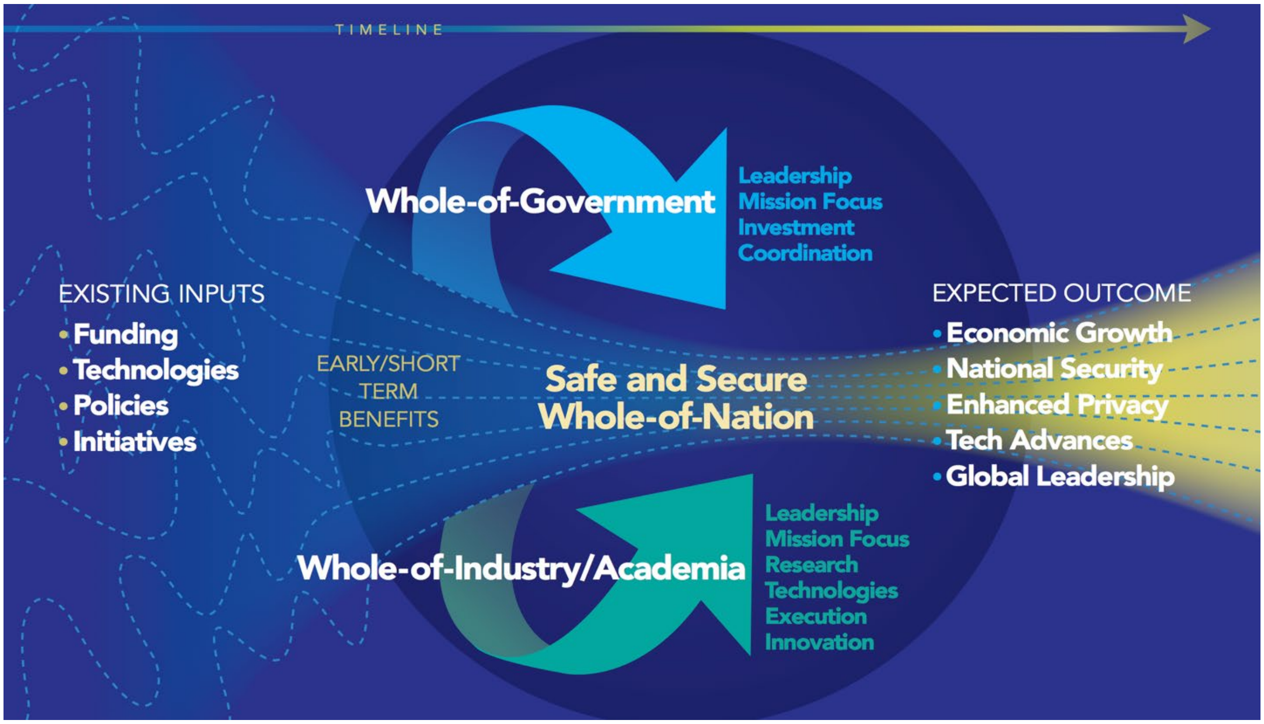


Figure 1: *Conceptual model of whole-of-nation focus towards defined Cybersecurity Moonshot Initiative objectives.*

3.2.1 Whole-of-Government

Key Recommendation: Within the U.S. Government, the White House should establish a Cybersecurity Moonshot Council ('Council') to strategically lead and oversee the initiative. The Council will be responsible for, and empowered to: establish strategic intent, raise national visibility, advocate for sustained funding, collaboratively develop national-level strategies, convene stakeholders, and create policies and processes that empower and incentivize non-governmental entities to drive accelerated innovation in defined Cybersecurity Moonshot-enabling fields.

The Council should be officially chaired by the President or Vice President and comprised of Cabinet level officials from relevant departments and agencies. New offices should be created within existing departments and agencies with the responsibility and authority for implementing and executing interagency policy directives from the Council. This must include department level entities with designated responsibility and authority to lead the private sector and academic engagement on Cybersecurity Moonshot Initiatives as identified throughout the report's recommendations. Based on the demonstrated capacity and Congressional authority to lead collaboration with the critical infrastructure community, the NSTAC recommends that the Department of Homeland Security (DHS) be empowered with primary responsibilities for this type of stakeholder engagement.

Further, the Council should have formal mechanisms for appointing non-governmental entities to directly contribute to the Initiative's strategy and policy development process within the official Council construct. The Council should have an official non-governmental component, comprised of representatives from critical entities across the private sector and academia. The President should determine the structure and authorities that govern non-governmental entity participation and the level of authority these representatives have with respect to overall Council decision making. However, the NSTAC strongly believes the responsibilities and authorities of non-governmental participants within the Council leadership structure must exceed those responsibilities traditionally afforded to non-governmental participants in Government advisory bodies.

Illustrative Model: Whole-of-Government
National Space Council

In June 2017, President Trump signed Executive Order 13803, *Reviving the National Space Council*, re-establishing the National Space Council as a U.S. Government-led, multi-stakeholder forum to coordinate the development and implementation of national space policies. The National Space Council provides a useful governance model, with many organizational attributes the NSTAC recommends the Cybersecurity Moonshot Council should embody, including:

- Chaired by the Vice President with Cabinet level representatives making up the Council.

- Non-governmental entities formally involved in the decision making process through the National Space Council Users Advisory Group, comprised of senior experts from private industry and academia.

- Corresponding department/agency level offices with responsibility for implementing National Space Council policies (including the Department of Defense, Department of Commerce and NASA)

- Ability to efficiently develop and issue Executive branch policies designed to lower barriers and empower the broader national space industry ecosystem. The National Space Council issued three National Space Policy Directives in its first year.

A presidentially appointed Executive Director should operationally run the initiative and be responsible for, and empowered to, maintain visibility over all national Cybersecurity Moonshot Initiative activities. The Executive Director should be responsible for:

- Elevating activities determined to provide the greatest strategic leverage towards the outcome of a safe Internet environment;

- Communicating the initiative's long-term strategic goals, breaking down the effort into its core components, communicating to stakeholders how each component fits into the overarching initiative, and directing its implementation;

- Recognizing and coordinating the value each stakeholder group can deliver to the overarching goal and how groups can create synergies to further optimize value; and

- Identifying stakeholders and making recommendations as to how to incentivize stakeholders to act in support of shared Cybersecurity Moonshot Initiative objectives.

3.2.2 Whole-of-Industry and Academia

The private sector and academia's leadership role in the broader Cybersecurity Moonshot Initiative cannot be limited to those formally appointed to serve within the official Council construct. Governmental entities cannot solely initiate, manage, or sustain the Cybersecurity Moonshot Initiative. The initiative's structure must reflect the highly distributed nature of the Internet and actively engender the enthusiastic commitment to and sustained participation in the Council by a diverse group of stakeholders with complementary roles, responsibilities, and authorities for cybersecurity.

In doing so, the governance for the Cybersecurity Moonshot Initiative must recognize the center of gravity of innovation in this country has evolved from predominantly U.S. Government funded to privately funded R&D. In the original moonshot, President Kennedy presented his aspiration as a national mandate, invoking the battle between freedom and tyranny and, in so doing, secured notable participation from private contractors and companies. The Cybersecurity Moonshot Initiative must depend even more heavily on a variety of private sector and academic stakeholder groups.

Key Recommendation: The Cybersecurity Moonshot Initiative must engender a whole-of-nation approach, including a cooperative governance model bridging Government, industry, and academia to align their inherent capabilities and activities towards realizing safe and secure Internet objectives. This should include a consortia style business structure that facilitates cooperation, shares resources and rewards, and works closely with partners in Government and academia to achieve common goals.

The Cybersecurity Moonshot Initiative leadership will emerge, by necessity, in many distributed forums. If effectively galvanized at a Presidential or Vice Presidential level, an ideal state would be the voluntary operationalization of a myriad of independent non-profit consortia, educational associations, and other joint efforts to execute against defined Initiative objectives. The U.S. Government's role, through the Cybersecurity Moonshot Council, would be to incentivize, publicize, or even selectively fund the achievements of these independent entities if aligned with the Cybersecurity Moonshot Initiative's strategic goals.

A number of historical examples illustrate this model. For example, in the late 1990s, the U.S. Government—through the White House, National Institute of Health, and Congress—provided significant funding and strategically championed large portions of the Human Genome Project. The project's ultimate achievement, however, was the product of largely independent activities from entities like the Celera Corporation and over 20 universities and research entities from around the globe that comprised the International Human Genome Sequencing Consortium.[5]

In the 1980s and 1990s, a number of multi-stakeholder efforts were launched to defend the United States' technological edge against foreign companies heavily subsidized by their

[5] "The Human Genome Project Completion: Frequently Asked Questions," October 30, 2010, National Human Genome Research Institute, https://www.genome.gov/11006943/.

governments. The result was the creation of business consortia such as the Semiconductor Manufacturing Technology Consortium (SEMATECH)[6], and the Microelectronics and Computer Technology Corporation (MCC). These consortia were congressionally chartered, privately owned, not-for-profit corporations designed specifically to help the Nation in specific research and commercial development areas. Ultimately, over 100 companies worked together to solve large scale technology issues of the day, leading to key breakthroughs in areas such as microchips and Internet infrastructure.

Illustrative Model: Whole-of-Industry/Academia
The Microelectronics and Computer Technology Corporation

Faced with losing American technology superiority to Japanese companies due to their enhanced level of governmental assistance, the Microelectronics and Computer Technology Corporation (MCC) was founded in 1982. Sponsored by the Reagan Administration, designed by former members of the U.S. Intelligence Community, enacted by Congress, and led by recent Government luminaries, MCC enlisted major computer and semiconductor manufacturers, elite technological schools representatives, and related groups to foster technological growth.

Under the *National Cooperative Research Act of 1984*, MCC was vital in developing AI technologies, reverse engineering tactics, and creating fundamental Internet search functions. It was one of the first companies to register a ".com" email address. MCC brought together disparate organizations to share scarce research personnel and investment funds, collaborate on common goals, and develop solutions to benefit the entire Nation.

* Source: The Microelectronics and Computer Technology Corporation[7]

3.3 Other Key Cybersecurity Moonshot Initiative Considerations

Launching a formal Cybersecurity Moonshot Initiative requires decisions on complex considerations related to governance, policy, budget, and many other factors to make the effort inclusive, enduring, and actionable. This section is focused on outlining a few initial considerations, as well as specific recommendations to inform key organizational decisions the Executive Director must make before the Cybersecurity Moonshot Initiative's launch.

3.3.1 Budgetary Considerations

History provides countless examples of commissions and advisory committees that *advised* the President on resource allocation but did not control any budgetary resources. In this case, it is critical for the Executive Director to have a formal role in budget planning and execution in support of the Cybersecurity Moonshot Initiative's process and recommendations, including activities pertaining to non-governmental entities. The President and the Executive Director must articulate Federal budget resources needs, match resources with specific Cybersecurity Moonshot Initiative objectives, and ensure outcomes justify the investments. The level of U.S. Government funding and investment in cybersecurity should exceed current levels by orders of magnitude and must be sustained at wartime-like levels for the decade timespan of the initiative.

[6] Robert Hof, "Lessons from Sematech," *MIT Technology Review*, July 25, 2011, https://www.technologyreview.com/s/424786/lessons-from-sematech/.

[7] David V. Gibson and Everett M. Rogers, *R&D Collaborations on Trial* (Boston: Harvard Business School Press, 1994), , Introduction, 15.

Key Recommendation: The Cybersecurity Moonshot Initiative Executive Director should be given a robust role in budget planning, formulation and execution. The President should consider designating the Executive Director as the co-lead to the Director of the Office of Management and Budget on developing the Administration's annual budget proposal. The President should also consider requiring the Executive Director to certify the annual budget fully supports the Cybersecurity Moonshot Initiative objectives. Finally, the Executive Director must have a regular and direct line of communication to the Committees on Appropriations and the pertinent U.S. Senate and U.S. House of Representatives authorizing committees.

3.3.2 Measuring Success, Defining Progress Milestones, and Building Momentum

Key Finding: The Cybersecurity Moonshot Initiative's overall success will be dependent on the Council's ability to clearly articulate the strategic end goal, identify significant progress milestones, and develop metrics to demonstrate success. How the Government articulates and measures the Cybersecurity Moonshot Initiative's success is paramount to its eventual impact and how Americans remember and feel about the Initiative.

Like the original space moonshot, the Government must identify concrete milestones the public can easily grasp, even if the underlying details are complex. President Kennedy's publicly broadcast speech in May 1961 implicitly laid out a steady and visible path forward: Suborbital flight, the multi-orbit flights of the Mercury program, engineering docking maneuvers and Extra-Vehicular Activities during the Gemini program, development of three-man Apollo capsule, longer manned orbital flights, unmanned lunar flights, and, finally, the July 1969 lunar landing.

Beneath these important, publicly broadcasted events, engineers accomplished a steady stream of development triumphs: larger boosters, more power, development of new fuels, higher reliability, and better nutrition and waste elimination systems. Similarly, communicating Cybersecurity Moonshot Initiative progress is essential to keep the public focused on the effort and to serve as intermittent, if not continuous, reminders of its national significance.

The difficulty and complexity of the overarching goal and the intensity and pace of action demand that the Government observe, measure, and to some extent, enforce both progress and completion of the Cybersecurity Moonshot Initiative. The governing Cybersecurity Moonshot Council, in coordination with identified stakeholders, should be responsible for developing the Cybersecurity Moonshot Initiative's milestones and metrics. There are several notional metrics that are illustrative of how the Cybersecurity Moonshot Initiative might measure achievement of sub-goals over a 10-year horizon, including:

- Cybersecurity no longer named the top threat in the Office of the Director of National Intelligence's Worldwide Threat Assessment;
- Repeated, measurable demonstration by operators of critical infrastructure, both large and small, of the ability to maintain continuity of service during cyber attacks;

- Department of Labor or industry associations' measures of cyber workforce vacancies and deficits decrease;

- Improvements in public polling regarding perceived safety and trust of Internet infrastructure and Internet-connected technologies;

- A marked decrease in the number of material cybersecurity incidents reported to state and Federal regulatory bodies, including the Securities and Exchange Commission; and

- A decrease in the time to remediate known vulnerabilities ("time to patch") by critical infrastructure providers that are required to report such data.

3.4 Define Strategic Framework and Pillars

Key Recommendation: As one of its first actions, after a period of internal and external consultation, the Cybersecurity Moonshot Council should publicly articulate a Strategic Framework, to provide common structure to help organize the Cybersecurity Moonshot Initiative's distributed, whole-of-nation activities. As a recommended starting point, the NSTAC proposes six Strategic Pillars: *Technology, Human Behavior, Education, Ecosystem, Privacy, and Policy*; recognizing that achieving a more enduringly safe and secure Internet within the next 10 years requires a holistic and multi-disciplinary approach.

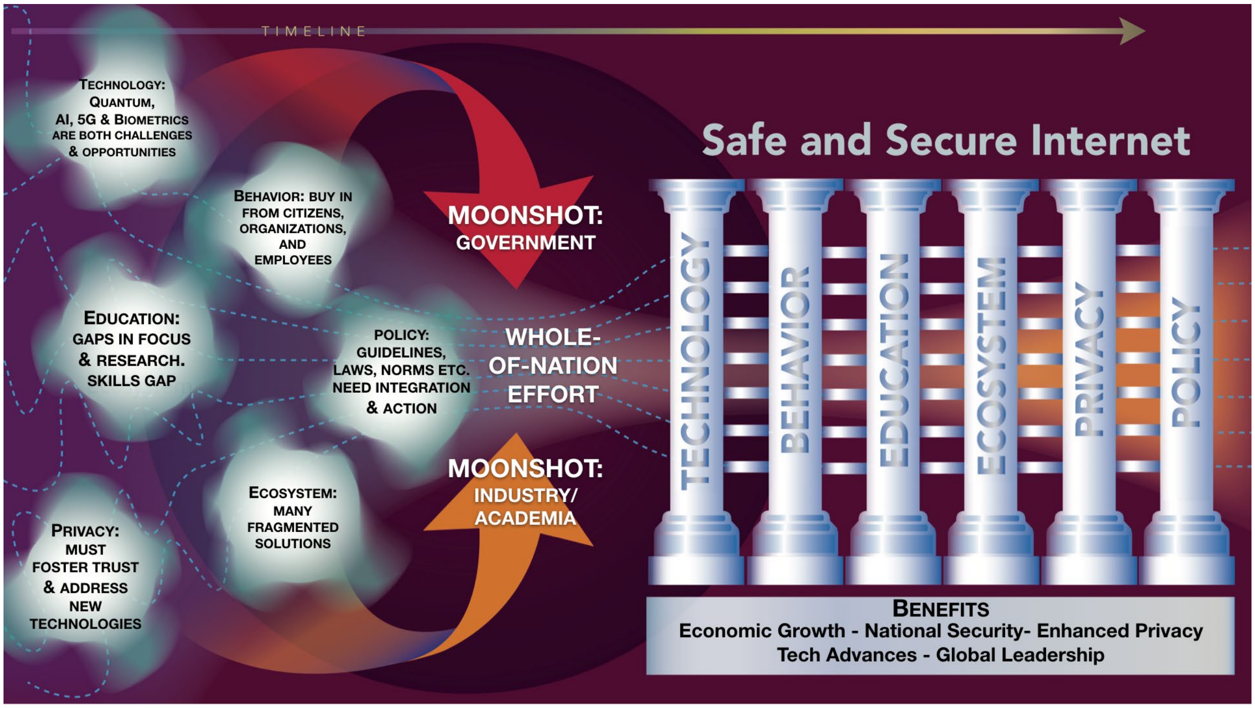

TIMELINE
Technology: Quantum, AI, 5G & Biometrics are both challenges & opportunities
Behavior: Buy in from citizens, organizations, and employees
Education: Gaps in focus & research. Skills gap
Policy: Guidelines, laws, norms etc. need integration & action
Ecosystem: Many fragmented solutions
Privacy: Must foster trust & address new technologies
MOONSHOT: GOVERNMENT
WHOLE-OF-NATION EFFORT
MOONSHOT: INDUSTRY/ ACADEMIA
Safe and Secure Internet
TECHNOLOGY
BEHAVIOR
EDUCATION
ECOSYSTEM
PRIVACY
POLICY
Benefits
Economic Growth - National Security- Enhanced Privacy
Tech Advances - Global Leadership

Figure 2: *The NSTAC's recommendation for the Cybersecurity Moonshot Initiative's Strategic Pillars—a proposed organizational construct for the broad but interdependent categories of activities required.*

The NSTAC used the Strategic Pillars construct to describe broad categories of activity where whole-of-nation, multi-disciplinary action must be organized in pursuit of realizing a fundamentally safe and secure Internet environment that assures trust and resiliency for digitally-connected Government and critical services at a fundamentally superior level relative to the status quo. The Strategic Pillars should be interpreted as reinforcing and cross-dependent rather than separate, independent work streams. Indeed, some Strategic Pillars, such as the Policy Pillar, are primarily focused on direct enablement of other Pillar objectives. These interdependent, enabling relationships are explored in the Inter-Pillar dependencies section.

The NSTAC recommends the pursuit of a safe and secure Internet environment on the existing, open Internet in order to assure safe interaction with critical services in a more resistant and resilient manner. Key characteristics to realize this outcome include:

- Endpoints and actions will be attributable;
- Malicious behavior will have consequences;
- Identities will move beyond passwords and PII;
- Privacy and trust will be enhanced and enforced; and
- A voluntary, opt-in process to realize the full spectrum of benefits.

The NSTAC believes this needs to be accomplished by 2028, as a whole-of-nation effort, before the challenges become more difficult and complex.

This is the optimal time to move the country to more effectively leverage emerging technological capabilities to achieve a fundamentally safe Internet environment—with the coming advancements in fifth generation (5G) communication technology for vastly increased connectivity and a defensible infrastructure, breakthroughs in artificial and augmented intelligence for more automated cyber threat prevention, behavioral biometrics that can deliver an entirely new way to identify people, and new capabilities in quantum encryption that can resist advanced attacks far into the future. While all of these advancements are coming—both to the United States and our adversaries—without a national framework to steer their research, development, and deployment toward the common good, we risk losing this generational opportunity.

To be clear, the NSTAC is not advocating for Internet balkanization, the creation of an entirely separate Internet infrastructure, nor prescribing any specific type of technical architecture. The NSTAC is advocating for a fundamentally safe and secure Internet for critical services, characterized by the harnessing of significant technological advances, more strongly aligned incentives and consequences for user behaviors that promote secure choices, cybersecurity policy and education reforms, and a clearer understanding about ecosystem roles and responsibilities in building and operating within this fundamentally safe environment for specific critical services. Other desired elements identified included:

- Resilience to attacks;
- Guaranteed availability of services;
- Fully attributable actions of users, for specific critical service functions;
- Consequences for malicious actions;
- Assured protection of private information;

- Consumer and business confidence in systems;
- Primary delivery channel for lifeline services; and
- Accessible by all who need it.

When referring to 'critical' and 'lifeline' services throughout this report, the NSTAC uses a definition informed by well-established U.S. Government policy. Through a series of policies spanning the current and previous three Administrations, the U.S. Government has coalesced around a cybersecurity risk management strategy that prioritizes the protection of Internet-connected critical infrastructure. In furtherance of Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, DHS and relevant Sector-Specific Agencies annually identify and maintain a list of 'Section 9' entities, which are defined as "*critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security*."[8] In the *National Cybersecurity Strategy* published in September 2018, the Administration further defined seven priority areas to identify critical functions and focus risk reduction activities around: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation. But the NSTAC's conception of lifeline services is not defined on a purely sector-specific basis. The NSTAC fully supports emerging critical infrastructure risk management prioritization efforts, including those advocated by DHS's National Risk Management Center, that seek to identify and prioritize protection of cross-sectoral functions deemed most critical to a safe and secure Internet.

Achievability Framework

The NSTAC found value in broadly considering and categorizing initiatives based on their assessed likelihood of achievement within the Cybersecurity Moonshot Initiative's 10-year timeline. Some initiatives have been categorized within this report as an example. These categories are based on direct expert briefings and research, are subjective and are used as general guidance only. Such a framework would prove valuable for use by the Cybersecurity Moonshot Council in assessing proposed initiatives. These categories include:

A: Expected to be addressed based on the current trajectory, including the predicted pace of technological innovation and development.

B: Expected to be addressed with increased investment, national level focus, and collaboration towards key technological developments, and innovative applications of the other five Strategic Pillars.

C: Not expected to be addressed without a targeted Grand Challenge that uses various incentivization tools to dramatically accelerate whole-of-nation innovation.

D: No known reasonable approach (Note: The NSTAC did not include any "D" initiatives, so that what is being proposed within this report is possible within the 10-year timeline of the Cybersecurity Moonshot).

[8] Exec. Order. No. 13800, 82 FR 22391 (May 11, 2017), https://www.dhs.gov/sites/default/files/publications/EO-13800-Section-9-Report-Summary-20180508-508.pdf.

3.4.1 Technology Pillar

Strategic Pillar Goal: Strategically leverage developments in emerging technologies to deliver a safe and secure Internet environment, accessible to average citizens; businesses; and federal, state, and local governmental entities, for conducting critical service transactions without fear of compromise.

Introduction and Background

The United States increasingly relies on the Internet and digitally connected technologies for its national security, public safety, and economic prosperity. The Cybersecurity Moonshot Initiative aspires to identify, prioritize, coordinate, and accelerate development of technologies that will lead to the creation of an Internet environment that is more trustworthy and capable of meeting the safety, security, and privacy needs of a modern, hyper-connected critical infrastructure environment.

Representative examples of these technologies include augmented intelligence, quantum communications and quantum resistant cryptography, biometrics, 5G communications, and authentication technologies. These technologies will provide the technological foundation for realizing a safer and more secure Internet. The NSTAC understands that adversaries are pursuing these same technologies toward their own goals. Therefore, the Cybersecurity Moonshot Initiative must include strong defensive implementations of these new technologies, including guarding against training data poisoning in augmented intelligence, hardware-based vulnerabilities introduced within ecosystem supply chains, and quantum general purpose computers capable of decrypting existing data.

Identity Paradigm Shift

For online identities, we need to move beyond IDs, passwords, and personally identifiable information--all of which can be compromised—toward a more safe and secure means to identity users. The NSTAC recommends leveraging technological advances in behavioral biometrics, augmented intelligence, and new sensor data available with the rollout of 5G communications, to provide a real-time identity score (from 1 percent to 99 percent) when an identity credential is required. This method provides transparency for friction-free transactions, much greater identity assurance based on many data points, and significantly reduces online identity risk.

NSTAC History: Previous and Future Studies Related to Emerging Technologies

The 2017 *NSTAC Report to the President on Internet and Communications Resilience* focused primarily on short-term recommendations related to existing, known best practices and technologies that, if implemented more broadly, could have an immediately tangible impact on reducing the threat of automated and distributed cyber attacks. The report also reinforced the findings and recommendations of the *NSTAC's Report to the President on Emerging Technologies Strategic Vision* (2017) and concluded that emerging technology landscape, including significant advances in AI, cloud computing, quantum computing, biometrics, and authentication provide the requisite foundation to achieve a dramatic transformation in cybersecurity. The NSTAC is currently developing a report on advancing resiliency and fostering innovation in the information and communication technology (ICT) ecosystem, which will examine technology capabilities that are critical to U.S. national security and emergency preparedness (NS/EP) and how the Government can manage near-term risks, support innovation, and enhance vendor diversity for NS/EP-critical capabilities. The NSTAC intends to complete this report in Spring 2019.

Within this report, the role of the NSTAC is not to prescribe specific technology related initiatives as singular solutions to achieving the desired outcomes of the Cybersecurity Moonshot Initiative. Identifying the highest priority focus areas—those that provide the greatest amount of strategic leverage towards achieving a safe and secure cybersecurity environment for critical services—will need to be born out of a more distributed process. However, there are broad categories of technologies that are fundamental to the realization of a safe cybersecurity environment in the future. The following are illustrative examples only. As the Cybersecurity Moonshot Initiative is launched, U.S. Government leadership can use a variety of policy levers to incentivize and empower the private sector and academia to accelerate research and development of these critical, paradigm shifting technologies:

- **5G Communications and Next Generation Networks:** Provide a 5G communications network (wireless and wired) designed with enhanced security, interconnectivity, privacy, and availability. This will provide a much more resilient infrastructure, expand secure connectivity for the Internet of Things (IoT), industrial control systems, mobile, healthcare, and more, with dramatically greater bandwidth and near real time latency.[9]

- **Artificial Intelligence**: Ensure development of machine learning and AI to augment (rather than replace) humans, while minimizing risks such as data poisoning of AI systems. Allowing for near autonomous response to cyber threats at machine speed to achieve self-healing computing environments that identify flaws, prevent exploitation of those flaws, and mitigate impacts of failures.

- **Behavioral Biometrics for Identity:** Behavior biometrics combined with AI capabilities can reduce the reliance on easily compromised personally identifiable identification, allowing for the creation of identity scores that render passwords obsolete and give greater transparency and confidence in identifying users.[10]

- **Quantum Communications and Quantum Resistant Cryptography:** Provide a trusted encryption and communications platform, leveraging quantum technologies, that is resistant to quantum general purpose (QGP) computers, tamper-resistant, and available to all services. This needs to be in place before the advent of QGP computers that can decrypt existing sensitive data.

- **Common Resilience:** Assure access and availability for required functionality of critical services by automating and simplifying the consumption model of threat prevention-oriented cybersecurity tools and capabilities.[11]

- **Micro-segmentation:** Implementing cryptographically assured microsegments within distributed networks can reduce attack surfaces, limit lateral reconnaissance, and dramatically lessen impacts of malware, to help support both operational resilience and zero-trust methodologies.

[9] William O'Hern, "AT&T NSTAC Moonshot Briefing," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 18, 2018).

[10] John M. Poindexter, "Internet Accountability," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 22, 2018).

[11] Samuel Visner, "Cybersecurity Moonshots," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 29, 2018).

Expected Outcomes

While the NSTAC does not seek to prescribe specific technological solutions, it does define desired end states as an organizing challenge to innovators who will leverage the technologies previously outlined. The Nation must develop a greater trust model that enables stronger authentication and other security mechanisms and ensures a timely reaction to new security and privacy challenges. Expected outcomes include:

- Enhanced trust and confidence for critical infrastructure owners and operators;
- Ensure resiliency of critical infrastructure systems;[12]
- Ensure users' privacy through data controls that strengthen trust through transparency, while acknowledging the complexities of shared information ownership and derived information;
- Ensure users can count on devices and infrastructure to work properly; and
- Ensure information and devices are reasonably protected against evolving threats.

More specific requirements will be necessary in fully leveraging potential advances in technology to provide fundamental safety and security. These requirements include:

- Promoting identity scores based on behavioral biometrics (Category B);
- Developing AI-based network and computing defenses (Category B);
- Providing IoT data management with 5G (Category C);
- Encouraging quantum resistant encryption and key management research and development which are enhanced to match developments in quantum computing (Category C);
- Promoting citizen focused, safe, online operations, such as voting and filing taxes, followed by other critical infrastructure functions (Category C);
- Enabling the ability to conduct a transaction(s) between two entities with confidentiality, integrity, and resilience (Category B);
- Managing relationships of physical and virtual devices connected to the Internet (Category B);
- Enabling the ability to prevent, defend against, operate successfully despite incursion, and remove malicious code autonomously (Category B); and
- Prevent, identify, track, and remediate data corruption and compromise across all aspects of a critical infrastructure (Category C).

[12] Ibid.

Inter-Pillar Dependencies

This section includes references to outcomes, initiatives, and activities in other Strategic Pillars impacting technology, including those where the pace of technological development can be accelerated with the right support. For example:

- If education was more accessible and strategically focused on critical computer science areas, advances in critical enabling technologies may be expedited;

- Education of executive, legislative, and judicial branches of Government on technology could help ensure the Government provides the right policy framework to enable rapid advancements and ensure U.S. leadership in necessary technology advancements;

- Ensuring a policy framework and streamlining regulatory obstacles to both incentivize and reward private sector investment and innovation in technologies underpinning the Cybersecurity Moonshot Initiative;

- Developing a framework where the stakeholders in the ecosystem are incentivized to work together to deliver on technology objectives; and

- Developing technologies that abstract the complexity of security from the end user and enable humans to act more securely, by default.

3.4.2 Human Behavior Pillar

Strategic Pillar Goal: Achieving and sustaining a safe and secure Internet will require significant behavioral changes in all components of the cybersecurity ecosystem, including users, providers, and their employees. All parties will need to understand their specific roles and relationship to success, and the strong connection between cybersecurity and our national security. Progress towards this outcome will require action along several paths:

- Leveraging the intrinsic American innovation community by energizing and expanding interest in cybersecurity as a socially admirable pursuit beyond niche technologists to the mainstream;

- Providing tangible incentives for Internet users to make more secure decisions through the full spectrum of tools that reinforce the appropriate selection of security and authentication instead of the cheapest selection;[13]

- Demonstrating to citizens that good cybersecurity practices are part of national security by offering clear, compelling, minimally technical messaging to citizens; and

- Ensuring that an adequate set of security tools, options, and technologies are accessible to a broad range of the American public irrespective of technical acumen.

[13] New York Cyber Task Force, *Building a Defensible Cyberspace* (New York: Columbia University School of International and Public Affairs, September 28, 2017), https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Introduction and Background

Previous national cybersecurity efforts have failed to achieve widespread success, in part because they lacked an integrated human behavioral component. These earlier efforts, while offering significant benefits to the country, were often too siloed or compartmentalized to offer the holistic approach that the cybersecurity challenge requires.

Similar to the original moonshot effort, the 'citizen collective' must be recognized as a key stakeholder for the Cybersecurity Moonshot Initiative. The general public is often insulated from the serious cybersecurity threats facing the Nation and does not see the problem as one affecting the national well-being, much less national security.[14,15] Harnessing the energy and focus of the 'citizen collective' will be vital to facing and solving not just the technical challenges, but also navigating the political landscape that is paramount to the success of the Cybersecurity Moonshot Initiative.

Further, this initiative, like the original moonshot can drive innovations in other domains and leave a lasting legacy far beyond a trusted, resilient environment for critical services. The stability, safety, and security of the Internet is a key enabler for innovations in other critical, lifeline industries, such as health care, power, and transportation. It has proven impossible to engineer our way out of the challenges we face on the Internet today—there is no technological silver bullet to our core cybersecurity challenges. Additionally, there has been no meaningful progress toward making the difficult choices that result in a more simplified, safer, and secure environment. Wholesale changes in the behaviors of citizens, technology developers and operators, Government officials, and Internet users have been demonstrably and frustratingly elusive.

Expected Outcomes

Whole-of-nation activities related to the Human Behavior Pillar should focus on the following ideal outcomes:

- **Engaging the imagination and energy of the American public:** A safe and secure technological foundation for the provision of critical services will require engagement from more than just technology providers, network operators, and security professionals who have been traditionally focused on these challenges. Foundational changes in the way the environment operates, how users engage, the idea of online identity, and the roles of each individual will be required to support accomplishing this ambitious step forward. These changes can only be successful if we have a dedicated, informed, and engaged populace.

- **Energizing the innovation community:** Innovation must be recognized as a key cultural component of American life. The amount of overall funding for advanced research continues to be a declining percentage of the overall gross domestic product, which makes each

[14] Michael Daniel, Necessary Policy Foundations for a Cyber Moonshot," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 27, 2018).

[15] Dov S. Zakheim, "Structuring Government to Address the Cyber Challenge," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 27, 2018).

research dollar applied even more critical.[16] Universities have more to offer in this area as they are traditionally a key participant in the innovation community. Establishment and cultivation of a community aligned on common research goals has led to significant findings in the areas of physics and materials; this model needs to be adapted and accelerated in the cybersecurity domain.

- **Making the more secure decision the default choice:** All users, including employees, students, consumers, and citizens, need to consciously embrace cybersecurity as important for the societal good and understand their role in helping America through enhanced cybersecurity practices. At the same time, security choices must be made as transparent as possible to not add significant burdens or require advanced technical knowledge or sophistication so end users make the right security decisions. For example, studies have shown that some of the most impactful changes supporting security have occurred when security features are turned on by default and require no user action.[17, 18]

- **Incentives reinforce the appropriate selection of security and authentication requirements instead of just the cheapest selection:** The U.S. Government, through DHS, Department of Commerce, and Sector-Specific Agencies, has long supported and provided recommendations and voluntary guidelines in the area of encouraging secure outcomes. A necessary element of a successful Cybersecurity Moonshot Initiative will include directional influence over private actors that incentivize action. The Government can incentivize behaviors through financial incentives such as outcome focused procurement guidelines, running grand challenges or hosting prize competitions.[19] At the same time, public relations campaigns, with strong organizational outreach, can help consumers make the right decisions regarding security. Finally, the Government can promote security by establishing security requirements for public-Government Internet interactions.

In order to turn engagement into action, users must be provided with straightforward and low overhead methods to increase their security. These mechanisms must be readily understood and accessible to a broad range of the American public. Leveraging the innovations in machine learning, autonomy, and computing will establish and reinforce the choice of secure pathways for critical transactions, as well as managing the hyperconnectivity that 5G will help establish.[20,21]

[16] Jeffrey Mervis, "Data Check: U.S. Government Share of Basic Research Funding Falls Below 50%." *Science Magazine,* March 9, 2017, http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50.

[17] New York Cyber Task Force, Building a Defensible Cyberspace, https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

[18] Randy Sabett, "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 26, 2018).

[19] Paul Afonso, "Utility Regulation and Coordination with State-Level Agencies as it Relates to a Cybersecurity Moonshot Initiative," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 26, 2018).

[20] Bruce McConnell, "Make the [Global] Internet Safe and Secure . . . by 2028," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 22, 2018).

[21] O'Hern, "AT&T NSTAC Moonshot Briefing."

Inter-Pillar Dependencies

Ingenuity and the will of the American people will be a defining element of the Cybersecurity Moonshot Initiative's success. The establishment, sustainment, and application of this ingenuity and human will is measured through attention, action, and resources and will be impacted significantly by the other Strategic Pillars. For example, educational reforms, the protection of privacy rights, the evolution and adoption of technology, and policies that incentivize behaviors to drive exponential improvement in Internet safety will all require coordination and co-development across the Strategic Pillars.

3.4.3 Education Pillar

Strategic Pillar Goal: The Nation must dramatically increase the availability, quality, and diversity of cybersecurity talent for Cybersecurity Moonshot Initiative strategic focus areas, while also educating all citizens of their shared responsibilities in creating a safe and secure Internet environment. This includes a foundational understanding of the risks and positive incentives to perform their responsibilities safely and securely.

Introduction and Background

The development and implementation of safe environment enabling technologies will drive a greater demand for qualified practitioners to develop and operate its underlying cybersecurity infrastructure. Addressing this need will require an increase in the breadth and depth of K-12 Science, Technology, Engineering, and Math (STEM) programs that feed Cybersecurity Moonshot Initiative aligned strategic focus areas. The Nation must develop a concerted national strategy to rapidly increase the number of skilled cyber researchers and professionals. These cybersecurity professionals must be capable of fostering the transformative technological breakthroughs most critical to developing and sustaining the safe Internet environment. These breakthroughs must be accomplished in time to support the development, deployment, and cultivation of best practices, especially in the key identified areas such as quantum computing, AI, and 5G.

New incentives must be required to augment normal market supply and demand mechanisms to retain STEM graduates in academia and in government national security and infrastructure roles. These incentives can help attract and retain individuals in the Government cybersecurity workforce who might otherwise enter the private sector.[22] This will require additional funding and innovative collaborations between government, non-profit organizations, and private industry to develop new cybersecurity education initiatives.[23]

Robust STEM education at all ages will also be a foundational element to cybersecurity education and workforce development initiatives. Innovative cloud-based technology must be leveraged to improve the speed and quality of STEM education. For example, AI, big data, and augmented reality offer the potential to help address roadblocks in K–12 and higher education. Such programs can leverage gamification, media, and distributed platforms for learning. Efforts

[22] Richard Heimann, "State of the Discipline: Artificial Intelligence," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 6, 2018).

[23] Maughan, "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee."

must also be made to retain the best and brightest graduates of U.S. colleges and universities, many of whom are non-US residents, to remain in the U.S and join the U.S. workforce. In addition, ecosystem members should consider a rotation or exchange system, where Government employees are assigned, on a voluntary basis, to key commercial providers and vice-versa.[24] Though several cybersecurity education and workforce development initiatives are underway, the Nation faces a critical and thoroughly documented labor shortage.[25,26] Studies vary but indicate that by 2021 there will be at least 350,000 unfilled cybersecurity positions in the U.S. and up to 3.5 million cybersecurity-related vacancies globally.[27,28] This massive deficit still persists in an environment where cybersecurity salaries average three times the national median income, with private industry pay significantly outpacing government compensation.[29]

Finally, operating in a fundamentally safe cybersecurity environment may involve some level of personal inconvenience: a paradigm shift for the average user. End-users are often the weakest security link in a system, whether a result of malicious intent, lack of training, or negligence.[30] Government, academia, and the private sector must be engaged to help educate about this cultural transformation.[31]

Expected Outcomes

Whole-of-nation activities related to the Education Pillar should focus on the following ideal outcomes:

- National emphasis on education imperatives can be broken into two broad categories: (1) for professional careers in cybersecurity related science and technology; and (2) for the general population of users of safe and secure cybersecurity infrastructure;

- More university research community funding– both pure and applied research— to create and expand cybersecurity programs aligned to near-term development of enabling fields identified in the Technology Pillar;

- Creation of consortia-based structures for education, with job rotation and cross-pollination between government, industry, and academia;[32]

- Dramatic expansion of scholarships, fellowships, and grants to make STEM education more accessible; internships, apprenticeships, and post-graduate placement to help fill critical labor

[24] Zakheim "Structuring Government to Address the Cyber Challenge."

[25] "Meet the Millennials," 2017, Center for Cyber Safety and Education, https://iamcybersafe.org/research_millennials/.

[26] Center for Strategic and International Studies, *Hacking the Skills Shortage*, (Washington, DC: McAfee, 2016), https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

[27] Ibid.

[28] Douglas Maughan, "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee," Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 28, 2018.

[29] Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid, and Highly Selective," August 8, 2013, CIO, https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html.

[30] Robert Hinden and Russell Housley, "Challenges to Deploying Security on the Internet," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 25, 2018).

[31] Sabett, "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy."

[32] *Ibid.*

needs; early and sustained mentoring, especially for traditionally underrepresented populations in STEM;

- Evolved STEM education curriculums to introduce computer science topics in early childhood education through high school (including through cybersecurity Advanced Placement courses), so cybersecurity is seen as a clearly defined and socially admirable career track;

- By 2028, every K–12 student should have a basic awareness of cyber hygiene best practices and know the fundamentals of computer systems as outlined by the National Institute of Standards and Technology (NIST); and

- Citizenship opportunities through targeted visa quotas and financial incentives to retain in the U.S. workforce pipeline foreign born cybersecurity talent from the U.S. educational system.

Inter-Pillar Dependencies

Education outcomes have significant interdependencies with other Strategic Pillars. Representative examples include:

- **Human Behavior:** Both 'carrot' and 'stick'-type incentives will be required to achieve key educational outcomes, including public awareness campaigns to (1) drive students into Cybersecurity Moonshot Initiative aligned academic fields; and (2) significantly improve general populace cybersecurity behaviors.[33]

- **Ecosystem:** Countless more public and private sector cybersecurity professionals will need to be trained to build and operate the underlying infrastructure of a fundamentally safe Internet environment.

- **Privacy:** Informing Americans about the role of data privacy, their related responsibilities necessary to maintain that privacy, and the impacts national policies have on their actions is an essential education outcome.

3.4.4 Ecosystem Pillar

Strategic Pillar Goal: By 2028, the United States needs an integrated ecosystem of voluntary stakeholders working collaboratively to design, develop, and operate a safe environment for critical and lifeline services. Such an ecosystem is not something a single entity, even the Federal Government alone, can simply mandate. Instead, it requires a collection of representative organizations that have both a business and national security incentive, open to all parties at various levels of trust, and operating with a whole-of-nation approach, that embrace a 'secure to market' over a 'first to market' mentality.

[33] Craig Fields, "A National Cyber Initiative." (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 21, 2018).

Introduction and Background

Today, technology companies in large part offer commercially available competitive products and services that are generally trusted, resilient, accessible, and expected to continually evolve. Individually, these entities can effect little change, but working as part of a cohesive ecosystem, the collective can provide the more highly integrated security solutions required. This cybersecurity ecosystem includes components of governments (Federal, State and local), academia, and the private sector, with inherent inclinations for both competition and cooperation.[34]

The participants in the ecosystem include everyone who provisions or uses critical service infrastructure. In addition to researchers, manufacturers, operators, and users, this also includes the supply chains of manufacturers and operators. The ecosystem includes actors of private sector entities, all levels of government, citizens, standards organizations, foreign entities, non-profit organizations, the open source community and others. The physical and logical components of the ecosystem encompass devices, components, networks, services, and applied technologies that function together to create the Internet, critical infrastructure systems, and Government services.

In the context of the Cybersecurity Moonshot Initiative, Government services and critical infrastructure need higher assurances of authentication, integrity, security, privacy, accessibility, resilience, and attribution. While the Cybersecurity Moonshot Initiative charges the Government with ultimate strategic leadership, the private sector will commercialize technology as well as envision, build, and enable capabilities that assure a safe Internet environment on an ongoing basis. While the Cybersecurity Moonshot Initiative is proposed as a U.S.-based initiative, the U.S. Government should continue to coordinate closely with "Five Eyes" allies and other likeminded nations.

Today's ecosystem delivers products and services yielding immense convenience, increased resource utilization, and uncountable other benefits. Across these solutions there are varying levels of security, resilience, and durability in an ever-expanding legacy installed base. The U.S. marketplace for ICT products perpetually struggles to balance cost, usability, and customer visible features against (often) invisible security and resilient capabilities. Companies trying to provide above average security are displaced by those companies who bring products first to market or provide equivalent functionality at a lower cost than existing products.

Commercial off-the-shelf solutions with wide adoption deliver economies of scale that make attempting to build more secure custom solutions infeasible. At best, companies with strong brands try to reduce risk by allocating resources for risk management, security, resilience, or incident response. Standards or technologies that require widespread deployment to improve security but are not inherently intertwined with localized value, are often underemployed.[35]

Across all sectors, NSTAC briefers anticipated unprecedented transformative application of new technologies. Solutions are expected to relentlessly grow more integrated, interconnected, and

[34] Ibid.

[35] Hinden and Housely, "Challenges to Deploying Security on the Internet."

complex. Some examples cited by briefers were 5G applications for transportation infrastructure[36] and adding distributed energy resources[37] to the grid; increased threats to legacy encryption protocols from quantum computing; and the dual nature of AI, which can be used as a preventative security tool or as a cyber weapon.

Expected Outcomes

Ultimately, the Government needs engagement with all participants in the ecosystem to prioritize cybersecurity risk reduction and achieve a safe and secure environment for critical services by 2028. There are three fundamental ideal outcomes the U.S. Government needs to fulfill to empower whole-of-nation activities related to the Ecosystem Pillar:

- Lead and organize the ecosystem across sectors that unites voluntary stakeholders to achieve common objectives needed for a safe and secure environment, based on significant risk mitigation, standards, defensive technologies, shared infrastructure, and services. A public benefit organization, following in the successful footsteps of SEMATECH and MCC from the 1980s (explored in greater depth in Section 3.2.2*, Whole-of-Industry and Academia*) is a useful model for this type of voluntary consortia structure.

- Participate in the transition between design and execution phases of enabling a safe and secure environment, dedicated to spanning government and critical services, within 10 years. The core elements of security, resiliency, and accessibility needed for a safe and secure environment infrastructure should be identified across Government services, critical infrastructure, and other sectors that voluntarily participate. Barriers to implementation—whether financial, technical, regulatory, transparency—need to be collectively addressed through U.S. Government leadership.[38]

- Make all of the elements required for delivering Government and critical services in a safe and secure way available to other applications and business solutions. Elements include foundational resilient infrastructure, shared services, user authentication with biometrics, trusted identity providers that could replace traditional passwords, strong device and service identity, attribution, manufacturer incident response and patching, cybersecurity best practices, remote recovery mechanisms, software assurance, cyber response organizations, and authorities to investigate and remediate illegal activities.

Inter-Pillar Dependencies

By definition, the Ecosystem Pillar will include activities with inter-dependencies across all other pillars, as it represents the collection, aggregation, integration, and execution of the Cybersecurity Moonshot Initiative. This fundamental approach, that each Pillar is vital to the successful completion of the project, cannot be overstated.

[36] Terry Halvorsen, "5G Network Technology and Capabilities," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 5, 2018).

[37] Afonso, "Utility Regulation and Coordination with State-Level Agencies as it Relates to a Cybersecurity Moonshot Initiative."

[38] Jennifer Gustetic, "Designing and Implementing Grand Challenges: Learning from NASA's Experience," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 23, 2018).

3.4.5 Privacy Pillar

Strategic Pillar Goal: Privacy is a key component of delivering the trust needed to provide critical services to the Nation.[39] By 2028, American citizens must be able to trust the information systems that provide critical services and will demand with practical certainty that Cybersecurity Moonshot Initiative activities will not create privacy vulnerabilities but instead enhance privacy assurance and ensure that personal data and transactions are secure, will remain protected, and in their control. Privacy is a core principle fundamentally intertwined with the objectives of safety and security and must permeate all aspects of the Cybersecurity Moonshot Initiative.

Introduction and Background

Privacy in an assured safe Internet environment should be a right, echoing the 4th Amendment's rights that Americans will be "*secure in their persons, houses, papers, and effects, against unreasonable searches and seizures*." Alan Westin's pioneering definition that *"privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*", provides another foundational underpinning. [40] The Cybersecurity Moonshot Initiative design and directives must embody privacy principles extending to all interactions within the safe environment. A foundational element of the Privacy Pillar is that individuals, groups, and institutions will determine how and when personal information will be communicated.[41,] Finally, the architecture of a safe Internet environment must account for the significant exposure of personal data due to increased IoT and sensor connectivity driven by 5G implementation.[42]

Privacy in the digital world has faltered in part due to continual compromises of information and the proliferation of information-based business practices that, in some instances, have not been accompanied by appropriate security practices. Nearly every American has been affected by a data breach that adversely affects their personal privacy. On our current unaltered course, as the number of connected devices and data exchanges increase, the likelihood and impact of future privacy breaches increase exponentially. Given these challenges, the Cybersecurity Moonshot Initiative must establish a level of trust, transparency, and privacy to ensure optimal adoption within safe Internet environments.

When it comes to privacy, it is important to understand the interplay between anonymity and attribution. All users, regardless of their level of attribution or anonymity in online activities, have a valid expectation of privacy and choices about how their data will be used. While anonymity protects privacy, this does not mean that every Internet communication, including access to a critical infrastructure, should be anonymous; indeed, such anonymity has often resulted in a lack of deterrence with regard to harmful activity. At the same time, anonymity must be protected, particularly in areas where fear or the inability to exercise basic, fundamental human rights are at risk. In the current online environment there is little fear of consequence when undertaking malicious activity; the safe environment must address this reality and work to

[39] Poindexter, "Internet Accountability."

[40] Westin, Alan, *Privacy and Freedom,* New York: IG Publishing, 1967.

[41] "Book Review: Privacy and Freedom," November 24, 2004, Privacilla.org, http://www.privacilla.org/fundamentals/privacyandfreedom.html.

[42] O'Hern, "AT&T NSTAC Moonshot Briefing."

ensure attribution is absolute for specific critical services and thus consequences to an individual are not only possible but probable.

Expected Outcomes

The Privacy Pillar advocates for solutions to help solve challenges in many fundamental areas of privacy. Specific areas that must be addressed include: attribution and accountability, transparency, identity, encryption, sensor data, and augmented intelligence. Success will be demonstrated with transparency and will be based on objective and subjective outcomes, such as:

- All transactions within safe Internet environments will be fully accountable with positive identity and complete attribution;[43]

- Strong privacy governance, including input and oversight from leading privacy advocacy groups along with Government and industry stakeholders, is integrated throughout the Cybersecurity Moonshot Initiative;

- The general public's measured perception will be that critical services transactions are safe, secure, and trustworthy.

Attribution and accountability must be able to be enforced within safe environments, which have been nearly impossible to achieve today. Outside of the safe environment, lack of attribution and accountability is a moral imperative (e.g. supporting free speech without fear of retribution); however, this same environment has increasingly enabled activity and behavior that is a threat to our society. The asymmetry of risk and reward favors the malicious user.

To ensure privacy, there must be shifts in identity management, encryption, sensor data usage, and deployment of augmented intelligence. For example, identity must be context sensitive, pulling attributes necessary to positively confirm an entity's identity based on the specific need to know; encryption protocols must be quantum resistant; protections must be in place to prevent privacy infringing AI usage; and data from IoT devices and sensors must be managed and protected. Establishing and provisioning identity scores, instead of passwords, derived from real-time sensor and biometric data will devalue personally identifiable information while increasing privacy within the safe environment and extending into other aspects of online usage.

Inter-Pillar Dependencies

While Privacy is dependent upon the successful interaction of the other five pillars, three pillars have particularly strong codependence: a deep understanding of *Human Behavior* is critical to successfully implement privacy protections, *Policy* development that supports and incentivizes privacy innovations must be enacted and *Technology*, especially with the emergence of 5G and the maturation of AI for cybersecurity applications.

[43] Poindexter, "Internet Accountability."

3.4.6 Policy Pillar

Strategic Pillar Goal: The Nation must make focused, significant changes in policy, including laws, regulations, norms, rules, and standards to enable major advances in the other Strategic Pillars. These changes can be driven by incentives, national and international norms building, emerging threats, and new technologies—all sharing the common goal of facilitating a more enduringly safe and secure Internet. Policies will need to recognize, incentivize, and reward actors in this space for positive behavior as well as enforce accountability, attribution, and consequence for negative behavior.[44] Policies will have to evolve, as needed, to make the Cybersecurity Moonshot Initiative successful and be cognizant of the international scale of the challenge.

Introduction and Background

Today, the Nation is struggling to keep pace with sophisticated and increasing cyber threats, which fundamentally endanger the American way of life. The Nation's steadfast resolve in preserving and respecting the openness of society and freedom of all people creates opportunities for criminals and adversaries to exploit and harm us through cyber attacks. Akin to the law enforcement challenge to stop terrorism directed at soft targets, Internet policies have left critical systems vulnerable to the theft of private and sensitive data and to potential disruption or destruction. Perhaps more than any transformation in the Nation's history, cybersecurity policy must be adapted to exceed the current and future challenges posed by our digitally connected world.

Case Study: Policy and Automobile Safety

Lessons from the past regarding the use of broad policy reform to ignite change should be considered in this effort. In the late 1960s, the Government partnered with the automobile industry to meet the challenge of creating safer conditions for the increasing number of people and vehicles on the road. The Government instituted strict safety regulations starting with mandatory lap safety belts in 1968. In 1989, simple driver's airbags became mandatory— but today the market demands multiple front, side, and rear airbag systems to increase the likelihood of passenger survival in an accident. The Government also addressed the problem through regulations on road design, traffic controls, and mandatory speed limits as well as strict guidelines for drivers such as vehicle category specific licenses and strong consequences for breaking traffic laws. Today, industry is introducing new technologies like auto-braking to further reduce the likelihood of an accident. All of these changes were made for the perceived greater good of a society that was becoming increasingly dependent on automobiles. Although the number of traffic accidents, injuries, and deaths remain far too high, the vehicles and the infrastructure used by drivers today are significantly safer than they were 20 years ago.

Expected Outcomes

Neither Government, industry, nor academia can solve cybersecurity challenges holistically without policy reform. As can be learned from the multi-disciplinary approach taken to make automobile travel safer for all Americans, finding the right balance between promoting a cybersecurity environment that is safe for business, consumers, and the Government—while not stifling innovation and competition—will require a delicate application of various policy tools.

[44] Visner, "Cybersecurity Moonshots."

Domestic and international policies, which will include laws, standards, and guidance derived from a variety of bodies, including Congress, Government standards, industry and technology standards, as well as international Internet standards could include the following:

- Defining and investing in the necessary infrastructure to design and operate the Internet in a fundamentally safer and more secure manner;

- Defining the responsibilities and authorities for cybersecurity ecosystem stakeholders that incentivize proactive and voluntary action aligned to their specific roles and responsibilities;[45]

- Defining the boundaries of cybersecurity norms within the secure environment and promoting the public and private understanding of the role their decisions play in our national security;

- Defining decision paths for stakeholders (including encouraging market drivers or developing new non-technology resources) to encourage positive incentives and to avoid consequences for violating behavioral norms established for activities inside the safe environment. For example, defining "Underwriters Laboratory"-like certifications for cybersecurity products and services;

- Developing policies that encourage defining critical infrastructure resilience through use of high availability and redundant technology as well as service provider accountability to deliver promised services; and

- Defining rewards for cybersecurity research and innovation partnerships between industry, government, and academia to steer cybersecurity technology development towards the requirements defined in the Cybersecurity Moonshot Initiative and increase the volume and quality of both American cyber technology and cyber professionals in our future workforce.

Inter-Pillar Dependencies

Policy is the U.S. Government's enabler and primary tool in making sure the Cybersecurity Moonshot Initiative is successful. To that end, the *Policy* Pillar supports the *Technology* Pillar, specifically as technology roadmaps are defined that address security; *Behavior*, in which policies will drive and, in some instances, regulate user's activity; *Privacy*, as new laws and regulations are introduced ensuring the public's right to determine the use of their personal information; and *Education*, in which governmental efforts at increasing the pool of cyber professionals effects K–12 educational policies. These pillars help determine the Initiative's overall governance direction to create a trusted, resilient, and accessible safe environment. In support of the overall Cybersecurity Moonshot Initiative, policy reform should be:

- Based on positive incentives and the avoidance of negative consequences;

[45] For example, both enterprise users and critical infrastructure providers should have an expectation of implementing an accepted cybersecurity framework such as NIST or the SANS Institute, enforceable through existing sector channels of accountability.

- Considered from the beginning and throughout initiatives in other Cybersecurity Moonshot Initiative Strategic Pillars, not at the end as an afterthought or consequence; and

- Fair and just for the American common good, while being the example for the world and promoting where possible positive international outcomes and Internet freedom.

3.5 Cybersecurity Moonshot Initiative Grand Challenges

Key Recommendation: After defining the Cybersecurity Moonshot Initiative's Strategic Framework and related national cybersecurity R&D priorities, the Cybersecurity Moonshot Council and associated Department level entities should lead a national multi-stakeholder process to define, identify, and launch one or more Cybersecurity Grand Challenges. The Cybersecurity Moonshot Council can also play a critical role in raising visibility and incentivizing distributed action aligned to its objectives.

Throughout the study, experts repeatedly emphasized the importance of identifying one or two specific, initial areas where accelerated whole-of-nation focus could produce demonstrable progress over a three to five-year time horizon. These experts stressed the importance of this approach to produce more immediate breakthroughs, to help build momentum, and to establish a foundational model for the longer-term (10 year) vision of the overall Cybersecurity Moonshot Initiative. The NSTAC has adopted the well-established 'Grand Challenges' model to describe this approach for specific targeted focus. Briefers presented a variety of definitions for what constitutes a Grand Challenge, including the following:

- Bold but achievable science, technology, and innovation goals that demand an extensive number of activities across technical and non-technical disciplines;

- A 'North Star' for high impact, multi-disciplinary collaborations between Government, industry, universities, non-profits, and the Nation's elite scientists, engineers and citizens;

- A mechanism for organizations to leverage their unique skills and ability in solving problems larger than they can successfully address on their own; and

- A means to tackle many of the century's toughest problems, especially those that capture society's imagination, and thus political support.

The NSTAC heard from experts with direct experience in running 'Grand Challenge' initiatives within the Government, private industry and the non-profit community. These activities covered numerous disciplines, and were most prevalent in areas such as space, biomedicine, and public health. Our research also revealed a significant Grand Challenges community of interest across the Federal Government, with significant discipline agnostic best practice resources centrally provided through resources like Innovation.gov and Challenge.gov, administratively managed by the General Services Administration.[46,47] However, cybersecurity as a discipline has not

[46] "Challenges of Challenge," 2018, Challenge.gov, https://challenge.gov/list.

[47] "The Better Government Toolkit provides resources to build a better government through innovation," 2018, Innovation.gov, https://innovation.gov/toolkit/.

developed a similarly robust culture of open innovation and 'moonshot-like' thinking represented by the Grand Challenges community. The NSTAC believe this must change.

To this end, the NSTAC recommends the Cybersecurity Moonshot Council lead in the identification and launch of one or more targeted Cybersecurity Grand Challenges. To identify appropriate Grand Challenge candidates, the Council and associated Departmental entities should run a six-month, collaborative process that formally engages private sector and academic stakeholders across the country. Critically, this process should include citizens with no professional association or expertise in cybersecurity to inject new thinking into this dialogue.

3.5.1 Identification and Evaluation Criteria

A 'Grand Challenge' designation is appropriate for a specific priority development area where whole-of-nation progress is on an inadequate trajectory and would benefit from targeted national attention and strategic focus (Category 'C' in the Achievability Framework rubric first introduced at the beginning of Section 3.4, *Define Strategic Framework and Pillars*). In evaluating potential Grand Challenge candidates during this multi-stakeholder process, the Council should propose and weigh several evaluation criteria and key questions, including:

- **Clear Government Role:** Does the Government have a clear role in catalyzing whole-of-nation activities aligned to the initiative? Can Government strategic attention, barrier reduction, resourcing, or requirements incentivize action where previous market-based drivers have proved insufficient?

- **Benefits from Collaboration:** Does the initiative require activities beyond the scope of Government authorities or strengths? Would the initiative benefit from a more distributed, larger-scale effort that leverages a variety of sources of partnership and collaboration?

- **Societally Resonant:** Can the initiative be articulated in a way that is widely understood across society, especially to non-cybersecurity experts, as fundamentally important and strategic on a national basis?

- **Measurable and Achievable:** Are there demonstrable milestones and objectives that are achievable within the 10 year time span of the overall Cybersecurity Moonshot Initiative?

- **Highly Scalable:** Would realization of the initiative's objectives produce an outcome that is capable of being easily, even automatically, leveraged across cybersecurity defense environments?

- **Multi-Dimensional:** Does the initiative have a broad scope, comprehensive enough to include activities across multiple Strategic Pillars?

A careful consideration of these criteria and others, though a diversity of inputs from the six month multi-stakeholder process, should culminate in the identification of a specific outcome-based statement, along with activities aligned to achievement of that outcome across all six Strategic Pillars.

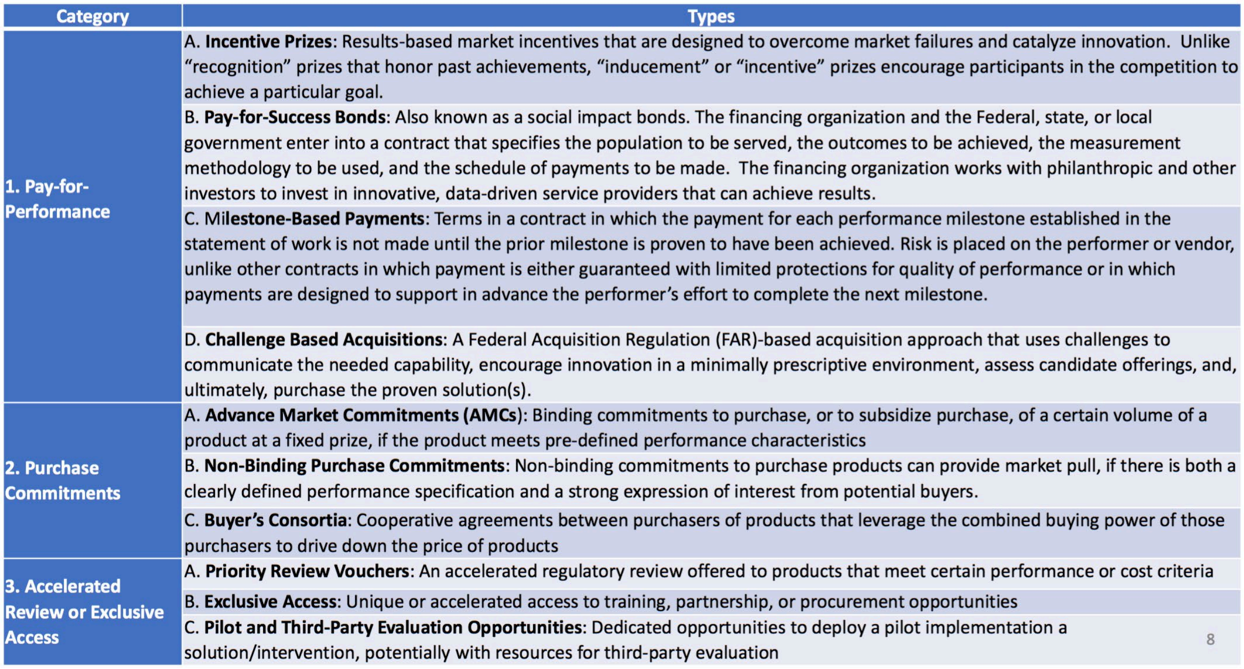
Illustrative Example of Grand Challenge Initiatives: AI for Cybersecurity

- White House-announced Prize to achieve Cyber AI technology 'Holy Grail' within 5 Years
- Crowd-sourced Competitions for algorithm development for automated threat prevention
- Policy Innovations/Communication Campaigns to make 'AI for Cyber' discipline as prestigious as 'AI for Autonomous Vehicles'
- Educational Consortia Models bridging academia and private industry to incent, grow and retain AI expertise for cybersecurity applications

3.5.2 U.S. Government Role in Incenting Action through Cybersecurity Grand Challenges

After the identification phase is complete, the U.S. Government can play a critical role in raising and sustaining visibility for the Cybersecurity Grand Challenges throughout its lifecycle. Representative examples include a Presidential or Vice Presidential level announcement of the Grand Challenge's launch or high profile celebrations of major breakthroughs related to the Grand Challenge. The U.S. Government can also raise and sustain interest on an ongoing basis by using various tools to incentivize and accelerate whole-of-nation activities aligned to achievement of the Grand Challenge. These include tools that predominately reward demonstration and achievement of outcomes, in a manner consistent with the principles of a 'moonshot' approach.

To be clear, the NSTAC is not proposing the U.S. Government unilaterally lead the development and launch of these Cybersecurity Grand Challenges and run all associated activities. Numerous non-governmental entities, such as XPrize and the Gates Foundation, have robust experience in successfully executing Grand Challenges and associated prize competitions to achieve ambitious, outcome-focused objectives. But the U.S. Government can play a critical role in kick-starting interest, scoping the challenge, and creating a pathway that allows for potential democratization and future commercial opportunities. By pairing an inspiring and impactful vision with organically emerging technologies, such as low-cost additive manufacturing, cloud applications, and AI, these Cybersecurity Grand Challenges can be naturally bolstered by corporate, academic and non-profit resources that serve their own priorities.



Category	Types
1. Pay-for-Performance	A. **Incentive Prizes**: Results-based market incentives that are designed to overcome market failures and catalyze innovation. Unlike "recognition" prizes that honor past achievements, "inducement" or "incentive" prizes encourage participants in the competition to achieve a particular goal.
	B. **Pay-for-Success Bonds**: Also known as a social impact bonds. The financing organization and the Federal, state, or local government enter into a contract that specifies the population to be served, the outcomes to be achieved, the measurement methodology to be used, and the schedule of payments to be made. The financing organization works with philanthropic and other investors to invest in innovative, data-driven service providers that can achieve results.
	C. Mi**lestone-Based Payments**: Terms in a contract in which the payment for each performance milestone established in the statement of work is not made until the prior milestone is proven to have been achieved. Risk is placed on the performer or vendor, unlike other contracts in which payment is either guaranteed with limited protections for quality of performance or in which payments are designed to support in advance the performer's effort to complete the next milestone.
	D. **Challenge Based Acquisitions**: A Federal Acquisition Regulation (FAR)-based acquisition approach that uses challenges to communicate the needed capability, encourage innovation in a minimally prescriptive environment, assess candidate offerings, and, ultimately, purchase the proven solution(s).
2. Purchase Commitments	A. **Advance Market Commitments (AMCs)**: Binding commitments to purchase, or to subsidize purchase, of a certain volume of a product at a fixed prize, if the product meets pre-defined performance characteristics
	B. **Non-Binding Purchase Commitments**: Non-binding commitments to purchase products can provide market pull, if there is both a clearly defined performance specification and a strong expression of interest from potential buyers.
	C. **Buyer's Consortia**: Cooperative agreements between purchasers of products that leverage the combined buying power of those purchasers to drive down the price of products
3. Accelerated Review or Exclusive Access	A. **Priority Review Vouchers**: An accelerated regulatory review offered to products that meet certain performance or cost criteria
	B. **Exclusive Access**: Unique or accelerated access to training, partnership, or procurement opportunities
	C. **Pilot and Third-Party Evaluation Opportunities**: Dedicated opportunities to deploy a pilot implementation a solution/intervention, potentially with resources for third-party evaluation

Figure 3: *There are a wide range of "pull mechanisms" available to the U.S. Government as tools for incenting outcome-focused action aligned to defined Grand Challenges.*[48]

4.0 CONCLUSION

This NSTAC report presented the case to establish a whole-of-nation Cybersecurity Moonshot Initiative with the fundamental goal of making the Internet safe and secure by 2028. This case is built on a strong historical precedent of collective achievement when facing a challenge with significant national risks.

This report lays out a path for a future state of the Internet that is resistant and resilient, values personal privacy and accountability, is available and accessible, and leverages emerging technological capabilities for good. This path will require dramatic changes in education and policy, the establishment of Grand Challenges that Americans can rise to meet, more strongly aligned incentives for secure behaviors and consequences for malicious ones, and a fundamental understanding of the global, interconnected nature of the Internet. The report presents a path where America can lead the world by example and should serve as both a guide and a warning, that when it comes to the preservation of trust and safety of the Internet and our digital way of life that depends on it, failure is not an option.

[48] Jennifer Gustetic, "Designing and Implementing Grand Challenges: Learning from NASA's Experience," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 23, 2018).

APPENDIX A: SUBCOMMITTEE STUDY METHODOLOGY

The President's National Security Telecommunications Advisory Committee (NSTAC) Cybersecurity Moonshot Subcommittee was comprised of representatives from over 20 Government, academia, and private industry entities from across the information technology, telecommunications, and cybersecurity ecosystem. In addition to representation from NSTAC member companies, the subcommittee appointed members from academia to ensure the group represented important perspectives of the whole-of-nation approach the Cybersecurity Moonshot Initiative championed. The NSTAC utilized several methods to gather information, including briefings from subject matter experts, examining numerous cybersecurity reports and articles, and conducting policy reviews. Specifically, the NSTAC:

- Received 27 official briefings from experts across industry, academia, and the public sector (Appendix E), plus numerous other unofficial interviews with external experts; and

- Conducted a review of private sector and Federal Government cybersecurity policies, regulations, reports, and best practice documents.

Over the course of the study period beginning in February 2018, the Cybersecurity Moonshot Subcommittee held approximately 50 meetings. In the first phase of the study, the subcommittee intentionally focused on receiving briefings from experts with direct experience or expertise in 'moonshot-like' efforts outside the cybersecurity domain. The intent of this approach was to identify domain-agnostics best practice models and methodologies for how whole-of-nation resources have been effectively leveraged in the past towards the realization of ambitious outcomes. The NSTAC believed this was critical to liberate thinking beyond the normal bounds that we believe have often limited our national dialogue around cybersecurity. Representative examples included briefings on the Human Genome Project, the creation of the Advanced Research Projects Agency Network /Internet, U.S. Agency for International Development's Grand Challenges for Global Public Health, and the Apollo program.

> "Whenever I run into a problem I can't solve, I always make it bigger. I can never solve it by trying to make it smaller, but if I make it big enough, I can begin to see the outlines of a solution."
>
> - President Dwight D. Eisenhower

In the study's second phase, the subcommittee heard from leading cybersecurity experts to begin identifying common organizing principles and desired outcomes for achieving a fundamentally safe and secure cybersecurity environment. Representative examples included briefings from experts on critical technologies, education, research and development, Grand Challenges and innovation policy, and governance models to inform the Cybersecurity Moonshot Initiative structure.

SUBCOMMITTEE MEMBERS

Mr. Peter Altabef, Unisys Corporation and Subcommittee Co-Chair
Mr. Mark McLaughlin, Palo Alto Networks and Subcommittee Co-Chair

Mr. Sean Morgan, Palo Alto Networks and Cybersecurity Moonshot Working Group Co-Lead
Mr. Thomas Patterson, Unisys Corporation and Cybersecurity Moonshot Working Group Co-Lead

Name	**Company**
Mr. Mark Bentley	Unisys Corp.
Mr. Christopher Boyer	AT&T, Inc.
Ms. Cherilyn Caddy	National Security Agency
Mr. John Campbell	Iridium Communications, Inc.
Mr. James Carnes	Ciena Corp.
Ms. Terri Claffey	Neustar, Inc.
Mr. Mark Cohn	Unisys Corp.
Ms. Kathryn Condello	CenturyLink, Inc.
Ms. Amanda Craig-Deckard	Microsoft Corp.
Mr. Michael Daly	Raytheon Co.
Mr. Darrell Durst	Lockheed Martin Corp.
Mr. Victor Einfeldt	Iridium Communications, Inc.
Mr. Patrick Flynn	McAfee, Inc.
Dr. Boaz Gelbord	Dun & Bradstreet, Inc.
Mr. William Gravell	Diogenes Group, LLC
Ms. Katherine Gronberg	ForeScout Technologies, Inc.
Mr. Dean Hullings	ForeScout Technologies, Inc.
Mr. Rodney Joffe	Neustar, Inc.
Ms. Ilana Johnson	Neustar, Inc.
Mr. Kent Landfield	McAfee, Inc.
Mr. Gregory Lebovitz	Equinix, Inc.
Mr. William Ryan	Department of Homeland Security

Mr. Jerry Scarborough	Raytheon Co.
Mr. John Scimone	Dell, Inc.
Mr. Robert Spiger	Microsoft Corp.
Ms. Roberta Stempfley	Software Engineering Institute
Mr. Kent Varney	Lockheed Martin Corp.
Mr. Milan Vlajnic	Communication Technologies, Inc.
Dr. Prescott Winter	Oracle Corp.

SUBCOMMITTEE MANAGEMENT

Ms. Helen Jackson	President's National Security Telecommunications Advisory Committee (NSTAC) Designated Federal Official (DFO)
Ms. Sandra Benevides	Alternate NSTAC DFO
Ms. DeShelle Cleghorn	Alternate NSTAC DFO
Ms. Kayla Lord	Department of Homeland Security NSTAC Support
Ms. Stephanie Curry	Booz Allen Hamilton, Inc.
Ms. Laura Karnas	Booz Allen Hamilton, Inc.
Mr. Barry Skidmore	Total Systems Technologies Corp.

APPENDIX C: ACRONYMS

AI	Artificial Intelligence
DHS	Department of Homeland Security
DOJ	Department of Justice
DSB	Defense Science Board
FDA	Food and Drug Administration
GPS	Global Positioning System
ICT	Information and Communication Technology
IoT	Internet of Things
MCC	Microelectronics and Computer Technology Corporation
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NS/EP	National Security/Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
QGP	Quantum General Purpose
R&D	Research and Development
SEMATECH	Semiconductor Manufacturing Technology Consortium
STEM	Science, Technology, Engineering, and Math

APPENDIX D: GLOSSARY

5G – A future, fifth generation mobile network, whose specification the International Telecommunications Union (ITU) has not fully defined. It is expected to support 10 gigabits per second data rates and higher. Commercial 5G deployments are not expected until around 2020. (Newton's Telecom Dictionary)

Additive Manufacturing – Is defined as the process of joining materials to make objects from three-dimensional (3D) model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies such as machining. (An Additive Manufacturing Test Artifact, Shawn Moylan, John Slotwinski, April Cooke, Kevin Jurrens, and M. Alkan Donmez, Journal of Research of the National Institute of Standards and Technology, Volume 119 (2014) http://dx.doi.org/10.6028/jres.119.017)

Artificial Intelligence – The intelligence exhibited by machines or software. A term popularized by Alan Turing, it historically describes a machine that could trick people into thinking it was a human being via the Turing Test. Recently, scientists within this field largely have abandoned this goal to focus on the uniqueness of machine intelligence and learn to work with it in intelligent, useful ways. (Newton's Telecom Dictionary)

Augmented Intelligence – An alternative conceptualization of artificial intelligence that focuses on AI's assistive role, emphasizing the fact that it is designed to enhance human intelligence rather than replace it. (whatis.techtarget.com/definition/augmented-intelligence)

Authentication – The process whereby a user, information source, or simply information proves they are who they claim to be; the process of determining the identity of a user attempting to access a network and/or computer system. (Newton's Telecom Dictionary)

Behavioral Biometrics – Behavioral traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. (NIST Biometric Standards Program and Resource Center)

Biometrics – The use of measurable biological characteristics, such as fingerprint recognition, voice recognition, and retina and iris scans to provide authentication. (Newton's Telecom Dictionary)

Cloud Computing – A model for enabling on-demand network access to a shared pool of configurable information technology capabilities/resources, (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. Both the user's data and essential security services may reside in and be managed within the network cloud. (Committee on National Security Systems Instruction (CNSSI) 4009, Adapted) (NSTAC Report 2016)

Critical Infrastructure – Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructure can be owned and operated by both the public and private sector. [*Critical Infrastructure Protection Act of 2001,* 42 U.S.C.519c(e)] (CNSSI 4009, Adapted)

Cyber Attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. (CNSSI 4009)

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks. (CNSSI 4009)

Industrial Control Systems – An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. (NIST SP 800-53A, Revision 4)

Information Technology – Equipment, processes, procedures, and systems used to provide and support information systems (computerized and manual) within an organization and those reaching out to customers and suppliers. (Newton's Telecom Dictionary)

Internet of Things – The total interconnected collection of device networks. (Newton's Telecom Dictionary)

Machine Learning – A type of artificial intelligence in which computers use huge amounts of data to learn how to do tasks rather than being programmed to do them. (Oxford Learner's Dictionary)

Material Cybersecurity Incident – an occurrence that actually or potentially results in adverse consequences to a company's information systems or data that would reasonably be expected to affect the value of (the company's) securities or influence investors' decisions. (SEC 33-10459).

Material Science – The scientific study of the properties and applications of materials of construction or manufacture (as ceramics, metals, polymers, and composites). (Merriam-Webster's Dictionary)

National Security/Emergency Preparedness (NS/EP) Communications – Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States (47 Code of Federal Regulations Chapter II, § 201.2(g)). NS/EP communications include primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international), to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal, and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications further include those systems and capabilities at all levels of Government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee based on Executive Order (EO) 13618, *Assignment of National Security and Emergency Preparedness Communications Functions* [2012])

Networks – Information system(s) implemented with a collection of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary of Information Security Terms – NIST IR 7298 – Revision 2)

Protocol – A set of rules and formats, semantic and syntactic, permitting information systems to exchange information. (NIST Glossary of Information security Terms – NISTIR 7298 – Revision 2)

Quantum Communications – A field of applied quantum physics closely related to quantum information processing and quantum teleportation. Its most interesting application is protecting information channels against eavesdropping by means of quantum cryptography. (www.picoquant.com/applications/category/quantum-optics/quantum-communication)

Quantum Computing – A developing computing technology that exploits the properties of atoms to create a radically different type of computer architecture through quantum physics. Quantum computing relies on the basic traits of an atom, such as the direction of its spin (left-to-right, right-to-left) to create a state, such as "1" or"0", as much as conventional computers use variations in electrical energy (positive and negative polarity). (Newton's Telecom Dictionary)

Quantum-Resistant Cryptography – Quantum-resistant encryption is a set of deployed public key encryption algorithms that are resistant to being broken by a fully functioning quantum computer (NSTAC Report to the President on Emerging Technologies Strategic Vision, 2017)

Software Assurance – The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle and that the software functions in the intended manner. (NIST SP 800-163)

Threat – Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-53, CNSSI 4009, Adapted)

APPENDIX E: BIBLIOGRAPHY

Afonso, Paul. "Utility Regulation and Coordination with State-Level Agencies as it Relates to a Cybersecurity Moonshot Initiative." Briefing to the President's National Security Telecommunications Advisory Committee (NSTAC) Cybersecurity Moonshot Subcommittee, Arlington, VA, September 13, 2018.

"The Apollo Program (1963-1972)." September 16, 2013. National Aeronautics and Space Administration (NASA). https://nssdc.gsfc.nasa.gov/planetary/lunar/apollo.html.

Bade, Gavin. "'Darknet' and quantum communications could enhance grid cybersecurity, scientists tell Senate." *Utility Dive*. October 27, 2017. https://www.utilitydive.com/news/darknet-and-quantum-communications-could-enhance-grid-cybersecurity-scie/508357/.

Bauer, Lujo. "Cybersecurity, AI and ML: Opportunities and Challenges." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee Arlington, VA, September 18, 2018.

"The Better Government Toolkit provides resources to build a better government through innovation." 2018. Innovation.gov. https://innovation.gov/toolkit/.

"Book Review: Privacy and Freedom." November 24, 2004. Privacilla.org. http://www.privacilla.org/fundamentals/privacyandfreedom.html.

Braga, Matthew. "In The Future, We'll Leave Software Bug Hunting to the Machines." *Motherboard.* June 16, 2016. https://motherboard.vice.com/en_us/article/mg73a8/cyber-grand-challenge.

Calvert, Kenneth and Gianchandani, Erwin. "NSF/CISE: An Overview and 'Moonshots.'" Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 15, 2018.

Center for Strategic and International Studies. Hacking the Skills Shortage. (Washington, DC: Sponsored by McAfee, 2016). https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

Cerf, Vinton. "The Future of the Internet of Things." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, April 5, 2018.

"Challenges of Challenge." 2018. Challenge.gov. https://challenge.gov/list.

The Communications Sector Coordinating Council. *Industry Technical White Paper*. Washington, DC: NTIA, July 17, 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

The Communications Security, Reliability and Interoperability Council. *Working Group 2A: Cybersecurity Best Practices Final Report*. Washington, DC: Federal Communications

Commission, March 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

Corbin, Kenneth. “Cybersecurity Pros in High Demand, Highly Paid, and Highly Selective.” August 8, 2013. CIO. https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html.

“Critical Infrastructure Sectors.” August 22, 2018. Department of Homeland Security (DHS). https://www.dhs.gov/critical-infrastructure-sectors.

Daniel, Michael. “Necessary Policy Foundations for a Cyber Moonshot.” Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 27, 2018.

Diamandis, Peter. “Massive Disruption Is Coming With Quantum Computing.” October 10, 2016. SingularityHub. https://singularityhub.com/2016/10/10/massive-disruption-quantum-computing/.

DHS. *Critical Infrastructure Partnership Advisory Council Charter.* Washington, DC: DHS, November 30, 2016. https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf.

“DHS Cyber Security Initiatives.” February 06, 2013. United States Computer Emergency Readiness Team. https://www.us-cert.gov/security-publications/dhs-cyber-security-initiatives.

Department of Justice (DoJ). “Justice Department Hosts Cybersecurity Industry Roundtable.” September 28, 2018. https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity-industry-roundtable.

DOJ. “Attorney General Sessions Announces Publication of Cyber-Digital Task Force Report.” July 19, 2018. https://www.justice.gov/opa/pr/attorney-general-sessions-announces-publication-cyber-digital-task-force-report.

Defense Science Board (DSB). *Cyber as a Strategic Capability–Executive Summary.* Washington, DC: Office of the Undersecretary of Defense for Research and Engineering (USD-R&E), June 2018. https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

DSB. *Cyber Deterrence*. Washington, DC: USD-R&E, February, 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

DSB. *Cyber Supply Chain–Executive Summary.* Washington, DC: USD-R&E, April, 2017. https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

The Economist. “The Big Data Breach Suffered by Equifax has Alarming Implications.” September 16, 2017. https://www.economist.com/finance-and-economics/2017/09/16/the-big-data-breach-suffered-by-equifax-has-alarming-implications.

"Enabling Distributed Security in Cyberspace." October 4, 2016. DHS. https://www.dhs.gov/enabling-distributed-security-cyberspace.

Ferguson, David and Kavanaugh-Ulku, Lorin. "USAID Grand Challenges for Development." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 1, 2018.

Fields, Craig. "A National Cyber Initiative." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 21, 2018.

Food and Drug Administration (FDA). *Post Market Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff.* Washington, DC: FDA, December 28, 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Frontain, Michael. "Microelectronics and Computer Technology Corporation." *Texas State Historical Association.* June 15, 2010. https://tshaonline.org/handbook/online/articles/dnm01.

Gallagher, Patrick. "Education and Research Programs Related to Critical Cybersecurity Technology Development." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 11, 2018.

Gibson, David V., and Everett M. Rogers. *R&D Collaborations on Trial*. Boston: Harvard Business School Press, 1994.

"Global Information Security Workforce Study." 2017. Center for Cyber Safety and Education. https://iamcybersafe.org/GISWS.

Goldman, Lisa and Purmal, Kate. "How to Launch a Successful Moonshot," Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, February 20, 2018.

Goldman, Lisa and Kate Purmal. *The Moonshot Effect: Disrupting Business as Usual*. San Carlos, CA: Wynnefield Business Press, 2017.

Greatwood, Duncan. "Making Compliance with Cybersecurity Regulations Easy for Critical Infrastructure." *CPO Magazine*. October 3, 2018. https://www.cpomagazine.com/2018/10/03/making-compliance-with-cybersecurity-regulations-easy-for-critical-infrastructure/.

Greenburg, Andrew. "The Untold Story of NOTPETYA, the most Devastating Cyberattack in History." *Wired.* August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

Gustetic, Jennifer. "Designing and Implementing Grand Challenges: Learning from NASA's Experience." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 23, 2018.

Gustetic, Jennifer, et al. "NASA's Asteroid Grand Challenge: Strategy, Results and Lessons Learned". Space Policy (2018). 10.1016/j.spacepol.2018.02.003.

Halvorsen, Terry. "5G Network Technology and Capabilities." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 5, 2018.

Halvorsen, Terry. "Incoming: We Must Anticipate 5G Consequences Now." *Signal*. March 1, 2018. https://www.afcea.org/content/incoming-we-must-anticipate-5g-consequences-now.

Hawkins, Derek. "The Cybersecurity 202: Congress poised to allow DHS to take the lead on federal cybersecurity." *The Washington Post*. September 25, 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/25/the-cybersecurity-202-congress-poised-to-allow-dhs-to-take-the-lead-on-federal-cybersecurity/5ba915ba1b326b7c8a8d162c/?utm_term=.706f4fe7dca5.
.

Heimann, Richard. "State of the Discipline: Artificial Intelligence." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 6, 2018.

Hinden, Robert and Russell Housley. "Challenges to Deploying Security on the Internet." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 25, 2018.

Hof, Robert. "Lessons from Sematech." *MIT Technology Review.* July 25, 2011. https://www.technologyreview.com/s/424786/lessons-from-sematech/.

"The Human Genome Project Completion: Frequently Asked Questions." October 30, 2010. National Human Genome Research Institute. https://www.genome.gov/11006943/.

Isaacson, Walter. "Building the Next Internet: A Moonshot to Make a Secure and Verified Identification System for Online Communications" Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 6 2018.

Kalil, Thomas. "Lessons Learned from White House and Private Sector Moonshots." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, February 27, 2018.

Lewis, James. "Cybersecurity Moonshot Issues." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 30, 2018.

Markoff, John. "Killing the Computer to Save It." *The New York Times.* October 29, 2012. https://nyti.ms/S91QbY.

Maughan, Douglas. "Acceleration Efforts Related to Critical Cybersecurity Technology Development." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 28, 2018.

McConnell, Bruce. "Make the [Global] Internet Safe and Secure . . . by 2028." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 22, 2018.

Mervis, Jeffrey. “Data Check: U.S. Government Share of Basic Research Funding Falls Below 50%.” *Science*. March 9, 2017. http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50.

NASA. *NASA Facts: Benefits from Apollo: Giant Leaps in Technology*. Houston, TX: NASA. July 2004. https://www.nasa.gov/sites/default/files/80660main_ApolloFS.pdf.

“National Emergency Communications Plan Goals.” May 17, 2018. DHS. https://www.dhs.gov/national-emergency-communications-plan-necp-goals.

NSTAC. *NSTAC Report to the President on Emerging Technologies Strategic Vision.* Washington, DC: NSTAC, July 14, 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

NSTAC. *NSTAC Report to the President on Information and Communications Technology Mobilization.* Washington, DC: NSTAC, November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Information%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf.

NSTAC. *NSTAC Report to the President on Internet and Communications Resilience.* Washington, DC: NSTAC, November 16, 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

NSTAC. *NSTAC Report to the President on the Internet of Things.* Washington, DC: NSTAC, November 19, 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

National Telecommunications and Information Administration (NTIA). *Catalog of Existing IoT Security Standards Draft Version 0.01*, Washington, DC: NTIA, July 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. *Fostering the Advancement of the Internet of Things*. Washington, DC: NTIA, January 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

NTIA. *Multistakeholder Process: Cybersecurity Vulnerabilities*. Washington, DC: NTIA, December 15, 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

New York Cyber Task Force. *Building a Defensible Cyberspace.* New York: Columbia University School of International and Public Affairs, September 28, 2017.

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Nielsen, Kirstjen M. "Remarks by Secretary Kirstjen M. Nielsen at the RSA Conference." Remarks, San Francisco, CA, April 17, 2018. Speeches. https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

O'Hern, William. "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee on 5G Networks and Standards." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee. Arlington, VA, September 18, 2018.

Office of Management and Budget (OMB). Guidance on the Use of Challenges and Prizes to Promote Open Government. March 2010. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-11.pdf.

Pence, Michael. Remarks by Vice President Pence at the DHS Cybersecurity Summit. July 31, 2018. https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-dhs-cybersecurity-summit/.

Perullo, Jerry. "Intercontinental Exchange/ NYSE" Briefing to the NSTAC Cybersecurity Moonshot Subcommittee. Arlington, VA, September 27, 2018.

Poindexter, John M. "Internet Accountability." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee. Arlington, VA, March 22, 2018.

Rosenblum, Todd. "Cybersecurity: A Whole-of-National Power Approach." *The Cipher Brief.* January 11, 2017. https://www.thecipherbrief.com/column_article/cybersecurity-a-whole-of-national-power-approach.

Rung, Anne E. and Tony Scott. "Acquisition Innovation Labs & Pilot for Digital Acquisition Innovation Lab." Memo from Anne E. Rung and Tony Scott to Chief Acquisition Officers, Senior Procurement Executives, and Chief Information Officers. March 9, 2016. https://www.dhs.gov/sites/default/files/publications/March%202016%20Memo.pdf.

Rutkowski, Kenneth. "Facilitated Session." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, April 10, 2018.

Sabett, Randy. "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy." Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 26, 2018.

"SANS Information Security Training." 2018. SANS Institute. https://www.sans.org/.

Seffers, George. "AFCEA: Whole-of-Nation Cybersecurity Approach Needed." *Signal.* https://www.afcea.org/content/afcea-whole-nation-cybersecurity-approach-needed.

Serbu, Jared. “Foreign cyber weapons ‘far exceed’ US ability to defend critical infrastructure, Defense panel says.” *Federal News Network*. March 17, 2017. https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber-weapons-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel-says/.

The Spark. “How Our Government Can Adapt to Evolving Cybersecurity & IT Infrastructure Needs.” July 2017. https://www.icf.com/blog/cybersecurity/how-government-can-adapt-to-evolving-cybersecurity-needs.

“Stakeholder Engagement and Cyber Infrastructure Resilience.” August 22, 2018. DHS. https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

Studeman, William. “Dialogue with the NSTAC Cybersecurity Moonshot Subcommittee.” Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 22, 2018.

U.S. Election Assistance Commission (EAC). *STARTING POINT: U.S. Election Systems as Critical Infrastructure*. Silver Spring, MD: EAC https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

Visner, Samuel. “Cybersecurity Moonshots.” Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 29, 2018.

Waldrop, M. Mitchell. “The Great Transition.” Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 8, 2017.

Westin, Alan. *Privacy and Freedom.* New York: IG Publishing, 1967.

Zakheim, Dov S. “Structuring Government to Address the Cyber Challenge.” Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 27, 2018.