NSTAC Cybersecurity Moonshot FAQ

Q: What is NSTAC?

A: NSTAC was created by President Reagan in 1982 to provide the President with advice, expertise and recommendations concerning telecommunications, network services, information technology and other relevant technological issues. It consists of thirty chief executives or high-level executives from a broad spectrum of companies. Its charter is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the U.S. Government maintain a reliable, secure, and resilient national communications posture.

Q: What companies participated in the subcommittee efforts?

A: NSTAC is represented by a broad array of communications and technology companies. Some of the biggest names in cyber, as well as some smaller companies that specialize in securing networks and infrastructure.

Q: Whom did you consult to develop this plan?

A: Our subject matter experts (SMEs) represented government, industry, and academia, and included a former head of the NSA, a former National Security Advisor, researchers, authors, and the person largely credited for developing the protocols that led to the Internet. We can provide you a complete list.

Q: The Apollo program was a one-time event, with a concrete, definable objective, while this one is open-ended. How does this qualify as a moonshot?

A: The underlying principles apply to both scenarios: An audacious-yet-achievable, time-based measurable objective that can be accomplished using existing tools and solutions but that will require significant coordination and effort on the part of government, industry, and academia. Moonshots can only occur at specific moments. Apollo was deemed necessary not just as a scientific accomplishment, but to demonstrate that the US had not only caught up to the Soviet Union in space technology, but would surpass them. In 1961, the US was losing the Space Race. Likewise, in 2018, the cost and damage wrought by cyber crime has reached a point where the average consumer now has legitimate concerns about credit card fraud, disclosure of personal information, privacy violations on social media, and even terrorist activities accomplished via the Internet.

Q: Is your goal for the Internet to be 100% secure?

Our goal is to create a secure Internet for critical infrastructure, financial transactions, and any other activity that needs 100% security. This can be accomplished with some existing tools and practices, plus a dedication of government, industry and academia to

enforce new standards to ensure 100% accountability and identification of users and endpoints.

Q: We have seen other Executive Orders, Commissions, and even Presidential summit on cybersecurity. How do you differentiate this effort from the others?

A: Just as Apollo built upon Gemini, and Gemini built upon Mercury, and Mercury built upon the high-altitude testing conducted by the Air Force, this Moonshot will hardly stands alone; it will acknowledge, coordinate, and build upon the considerable volume of material, knowledge and expertise already developed. It will break down the silos of cybersecurity activity and bridge the gaps between them. The Apollo program could not have succeeded just as a government process, nor as a commercial program. Nor can we solve Internet security issues with one EO, one commission, one summit, or even one incremental technology. Instead, we need to "work backwards," from an aspirational goal, leverage the existing research, and find the gaps between them, all while strictly coordinated and effectively directed.

Q: What sort of aspirational statements were considered?

A: The subcommittee began discussions with a clean slate and an open mind. Working from our basic charter, we engaged with industry, government, and academia experts to listen, not dictate. We noted similarities and common themes, held healthy debates, and then brought everyone together for a one-day facilitated meeting, which was managed by a technology expert with no prior knowledge of our previous meetings. We came out with a variety of ideas, which varied from the extremely ambitious (Make the entire Internet safe in ten years) to the more incremental (adopt IPV6 nationwide), to the "somewhere in-between" approach that we have recommended.

Q: Why Ten years?

A: The U.S. Government has adopted a "Defend today, secure tomorrow" approach, and the National Cyber Moonshot is intended to primarily address the "secure tomorrow" aspect. While the report clearly calls out, respects, and supports the nation's past and current efforts on defending today, our task was to come together as a nation to envision a dramatically more secure future state and recommend pathways to achieve it. Additionally, while focused on the aspirational goal, the report has defined these pathways fully intending a series of early benefits to the nation that will help improve both the risk and economic posture of the nation along the way.

Q: Why did the efforts of previous administrations fail to create a safe Internet?

A: While there has been a history of dedicated efforts and beneficial intentions from many components of government, international norms, industry associations, and individual organizations, the National Cyber Moonshot has proposed to solve these vexing problems as a single, coordinated, and funded whole-of-nation approach. The report calls for the President or Vice President to be the top-level sponsor of the effort,

but not the owner or operator. An ecosystem of all aspects of Federal, state, and local government is called to contribute, as well as industry, academia, associations, and individuals, in order to make this truly a whole-of-nation endeavor. Collectively, we have the passion, expertise, and wherewithal to succeed, and it is the report's recommendation that working together gives our country its best chance to truly trust in the delivery of its critical services on the Internet.

Q: In terms of Global Grand Challenges, is a cybersecurity moonshot the kind of thing that Bill and Melinda Gates (or other tech billionaires) should be funding?

A: The NSTAC was briefed by the heads of several grand challenges from a variety of critical issues, including space exploration, cancer prevention, mapping DNA, and even potential planetary extinction. A common thread of their expert advice was that the funding, while critical, was not the key determinant of success. Rather the consensus of these experts was to focus on how best to define the questions, how broadly to extend the reach, and how collaborative to make the process. While the report does not stipulate the source of prize money, it has been historically true that patriotic Americans will rise to any challenge they truly believe in, and a chance to make the Internet safe and secure is certainly in that category. Of course, we are happy to hear from the Gates, or other philanthropists.

Q: How does this effort differ from incremental, best practice standards that are already in place?

A: The report calls out many of these existing efforts, supports them, and expects them to continue to provide benefit to society. These efforts are good, are making progress, and should continue. The report also posits a goal that goes beyond incremental improvements and recommends a whole-of-nation effort to get us to a more secure steady state to work from in the future. The report recommends that as a society we need both done- defend today and secure tomorrow.

Q: Since the bad guys evolve faster than the responses from the Good Guys, how will this initiative respond to that dynamic?

A: Our national adversaries have multiple tactics that they employ successfully, including leveraging new technology faster on offense that we do on defense. With so much new transformational technology becoming available within the moonshot's time window, the report recommends that the US must change that dynamic for our national defense. By instilling closer corporate collaboration within an ecosystem, leveraging governmental adoption, matching education and funding priorities, fostering entrepreneurial spirits, and honing the wide variety of policies to be all targeted toward this new national mission, the country should be able to level the playing field and make the Internet safe and secure for the delivery of critical services.

Q: Why didn't the US sign on to the recent Paris Call for Trust and Security in Cyberspace?

A: Unisys was an early signatory, and along with many other global companies and organizations proudly support the goals called for in the Paris Call for Trust and Security in Cyberspace.

Q: How does the NSTAC committee plan to articulate the challenge in a way that incentivizes collective action?

A: When the NSTAC looked at recommending a framework to success, we focused on six critical pillars that would need to be established. They are Technology, Privacy, Eco-system, Policy, Education, and Behavior. It is within this behavioral change section that we most fully recognize that the issues facing the country are not simply technology issues, but rather we must fully embrace all aspects of human behavior. We were briefed on several successful efforts to convey highly technical issues in a way that most humans could understand and get behind. These briefs included "Don't be like the dinosaurs" when talking about avoiding asteroid collisions, "Only you can prevent forest fires" to protect our lands, and "Buckle up for safety" to reduce highway deaths. We believe that this behavior pillar, to include grand challenges and human behaviors, will be one of the six key areas that must be successful for the country to achieve its goals.

Q: The report mentions quantum computing, AI/ML, and 5G as benefits to cybersecurity. Won't the Bad Guys use these same technologies for attacks?

A: You cannot put new technology genies back into their bottles, nor should we want to. Further, we cannot ignore the fact that our adversaries – both military and economic- will be working to use these new technologies to their own advantage. The National Cyber Moonshot recommends that the US must accelerate efforts to leverage these technologies for our national defense, and suggests ways including increasing pure and directed research funding, fostering corporate collaboration, and launching a series of grand challenges. An example is a report assumption that adversaries will have access to a quantum general-purpose computer within the ten-year time frame of the moonshot, and that computer will have the ability to decrypt, alter, or steal the encrypted information that makes our economy run. To counter that, the report recommends that we must accelerate the development and deployment of what is called "quantum resistant encryption" in a trusted fashion in advance of these coming adversarial abilities.

Another example is the coming roll out of 5G communications, which offers the US the ability to significantly improve our overall national communications security posture, if that is instilled as a national priority by all.

Q: The report mentions federal funding. How much?

A: Funding security has always been a “pay me now or pay me later” proposal, but at this national level, where the result of a successful cascading cyber-attack against entire sectors of our economy like finance, transportation, healthcare, energy, government services, and more will have truly catastrophic effects on our country, the costs will go up. The report provides a playbook to get to the answers of how much and by whom, but the authors did not want to sugarcoat the issue of funding. The report also indicates that working toward these goals should provide long-term economic benefits that help to offset early costs.

Q: Who will plan the goals for the Moonshot project?

A: The report recognizes the importance of quantifiable goals, and made these suggestions as a way to foster discussion on this key factor. The report recommends the formation of a Cybersecurity Moonshot Council that is chaired by the President or Vice President, but made up of representatives from across government, industry, academia, professional organizations, cyber and privacy experts, and representative users groups. That council will be charged with collectively and transparently developing a system of measures and measurements.