Input to the Commission on Enhancing National Cybersecurity

Michael Kaiser
Executive Director
National Cyber Security Alliance
michael@staysfaeonline.org
202-570-7430

Public Awareness and Education

1. Current and future trends and challenges:

Cybersecurity education and awareness efforts have grown tremendously in the last decade. Concerns about the safer and more secure use of the Internet by all computer users has emerged as a national priority for government and industry with an emphasis on protecting critical infrastructure, intellectual property, financial assets, and citizens and customers. Individual Internet users have begun to take the steps to protect themselves and their families. Faced with an ever-evolving technology platform, they have had to learn to protect increasingly complex home networks and mobile devices, and raise children in the digital age to use the Internet safely, securely and responsibly. Just as companies face real and daily cybersecurity treats from a variety of sources, home and individual Internet uses face identity theft and an environment rampant with scams.

There are many challenges in cybersecurity education and awareness including:

- Scale of the problem: With cybersecurity, we face a similar predicament as we do with public health. Virtually every organization and every individual using the Internet is a risk in some way. The possibility exists that any device anywhere could be compromised, and compromised devices put other devices at risk. Suppression of risk requires knowledge about potential harm, signs that something is wrong and mitigation. Unlike public health, where we have sophisticated methods for tracking instances of disease outbreaks, we have no "true" risk collection and analysis entity in cybersecurity equivalent to the Centers for Disease Control that can identify clusters of impacted populations and gear up with meaningful

interventions. We do have an emerging decentralized risk infrastructure via ISACs and other groups but no top down method of intervening down to the end user with the correct information on protection mechanisms.

- Scale the size of the landscape: To be effective, cybersecurity education and awareness needs to reach and educate every Internet user (including businesses, government and nonprofit organization) in the country with the correct information, applicable to the risks they face and with simple but impactful advice to fix problems or mitigate risk. Since nearly all Americans and American organizations use the Internet, we need to teach basics to everyone and keep them informed.
- Technology and attack surfaces change: Unlike other issues of universal public concern, such as traffic safety or disease suppression where the environment changes slowly and remediation efforts can be constant (e.g., "buckle your seatbelt" can easily be taught to every new generation), cybersecurity challenges emerge off a platform of unparalleled change. Never have we seen that full adoption of transformative technology at the breakneck speed we have seen with connected devices. It took forty years for the telephone to reach 40% adoption. It took only seven years for the smart phone to surpass 50% adoption and closed the gap to near 100% in an even shorter time horizon. Even while we struggle to get everyone educated on devices that we have been using awhile (PC's and laptops), along comes a new platform-- mobile --with its own risks and procedures for maintaining the security and safety of the device. The situation is becoming much more complicated with the explosion of the Internet of Things (IoT). Millions and millions of new devices will be coming online in the next decade. Businesses and consumers will need to be fully educated on the risks and methods for maintaining the safety and security of these devices over time. We don't yet know how this ecosystem will fully evolve. Will there be standardization that will facilitate universal education and awareness or will be dealing many proprietary environments all needing specialized education and awareness efforts?
- Cybersecurity education and awareness needs to be a lifelong learning pursuit. With the rapid changes in devices and systems we will need a method to ensure that citizens receive access to the correct information over their lifetimes and at different developmental stages (such as children and seniors). There needs to be a continuous saturation program so all people receive the expanding scope of messages.

- There is a lack of rigor in messaging development: While it is easy to get security professionals to list the things that would make people safer—stronger authentication, malware protection, protecting personal information, etc.—it is much harder to create messages that people will actually respond to. Most cybersecurity messaging, with the exception of the way it is approached by NCSA and a few others, is based on creating new advice for people on the fly. Often, that advice is created in reaction to a breaking event or news story about a hack or breach. That is not the way public service campaigns typically g work toward behavior change, so while it may be contextually relevant to the moment and even correct, it is unknown if those message will actually resonate with target audiences. Knowing audience resonance and if a message can actually lead to the desired behavior change can only be done through a message testing process. NCSA has engaged in extensive messaging testing in cybersecurity since 2009. The STOP. THINK. CONNECT. message was tested with consumers and many sub-messages—Keep a Clean Machine, Personal Information is like Money. Value it. Protect it, etc.—have been tested with American consumers and computer users. For the new campaign NCSA is creating with the White House and industry, NCSA has used extensive message testing to find a message (to be released late September) that will capture the attention and engage people in the topic.
- There is a tremendous lack of consistency in messaging: One of the greatest challenges in the education awareness space is the lack of consistency in messaging. For example, when you ask several experts about best password practices you are likely to get several different answers around key issues such as password length, whether it should be a phrase or include symbols, numbers and uppercase letters and the frequency for password changes. The plethora of advice, some of which is incorrect, causes confusion about what behaviors actually keep people safer, making them less likely to implement them. In the worst case scenario, the advice is actually wrong, and adopting those behaviors will not in fact make people safer. Furthermore, since cybersecurity is an emerging field, even best advice can rapidly change over time, and infusing the entire ecosystem with the new advice can be difficult. This challenge is further exacerbated by the fact that some purveyors of messaging have a self-interest in specific messaging (including about potential risk) that may benefit a product or policy that they hope to advance.

- The diverse media landscape: Gone are the days when a PSA Campaign on network television could guarantee reaching the vast majority of Americans with safety or security messaging. Reaching the vast majority of Americans today requires leveraging all forms of traditional and social media using a variety of tactics from PSAs on TV, radio and the web to user-generated and shared content from friends and family.
- Timeframes must be long: Broad sweeping education and awareness programs are by their nature long-term . Smokey Bear has been a campaign for more than seventy years. Click it or Ticket for seat belts was founded in 1993 and is still going strong. It takes time and continued presentation of the message across a variety of settings to secure the message and the actions we want taken in the public's consciousness.
- Agreements need to be made about what success looks like and vehicles for measuring need to be put into place: Metrics are critical to understanding campaign effectiveness and whether goals are being met. However, campaign impacts can be difficult to determine for several reasons; tracking behavior change can be expensive and difficult, and self-reporting of changed behavior is not always reliable. Further, there is currently no national data to compare a campaign against. In other areas, there are existing benchmarks. For instance, in public health, it is be easier to track reductions in new cases of diseases, With traffic safety, the reduction in physical injuries in accidents can be tracked when seatbelts were used vs. when they were not used. Success also needs to be charted over a continum that starts with recognition of the campaign, followed by recognition of advice (what people can do to be more cyber secure), followed by behavioral change—did the preferred behavior actually get implemented? This needs to be viewed over a significant period of time.

2. Progress being made to address the challenges:

The most significant progress to date in cybersecurity education and awareness is the public private partnership under the leadership of NCSA and DHS. Founded in 2001, right after 9/11, NCSA was created with the sole mission of cybersecurity education and awareness for home users and small and medium sized businesses, and to reach young people. From the start, the visionary industry founders (Microsoft, Symantec, Intel Security (then McAfee) and CISCO,

among others), wanted to create an environment where industry and government could work together to help everyone do their part to build a safer, more secure and trusted Internet. Immediately, NCSA began working with Commerce and the FTC conducting awareness activities. When DHS was stood up, it become the Federal funder of NCSA along with private-sector contributions. The collaborative effort led to the creation of National Cyber Security Awareness Month (called for by the President) starting in 2004. In 2009, coinciding with the President's call for a campaign for cybersecurity in his Cyber Space Policy Review with a reach like Smokey the Bear, NCSA along with the Anti-Phishing Working Group established a collaborative effort with the 25 companies and seven Federal agencies. This led to the creation of the STOP. THINK. CONNECT. campaign.

National Cyber Security Awareness Month

Since 2004, NCSA and DHS have co-led National Cyber Security Awareness Month (NCSAM), and it has emerged as the pre-eminent education and awareness effort on the yearly cybersecurity calendar. NCSA and DHS have built a far-reaching campaign involving many thousands of stakeholders with solid messaging and themes that represent the all corners of the cybersecurity ecosystem, from home users and schools to cybersecurity careers, business security and critical infrastructure to cutting-edge technology like the Internet of Things.

The month has experienced year over year growth since its founding. Sample metrics from 2015 follow:

Total Estimated Reach[1]: 28,226,898,748 (2014 = 5,371,602,127) an increase of 425%

- Exposure of the Brand (total traditional and social media including #CyberAware Twitter estimated reach, online circulation and broadcast viewership): 28,232,486,392 - an increase of 415% (2014 = 5,486,086,538)

[1] This number includes additional pickups, meaning the same articles may have appeared in different publications.

- Unique Articles: 1737 **-** an increase of 74% (2014= 998 online articles/print articles/blogs written)
- Broadcast Reac**h:** 59,956,383 (2014 = 31,189,239)
- Online/Print Impressions[2]: 3,585,355,236 (2014 = 5,522,254)

Increasing Number of Champions: NCSA generated a significant increase in the number of Champions who joined the effort – that is, companies, schools, municipalities and non-profit institutions that pledged their support to NCSAM. Numbering 714 by the end of the month, their commitment to keeping people safe online was well-illustrated by an over 78% increase from 2014.

Social Media Success: NCSAM 2015 and the new NCSAM hashtag (#CyberAware) achieved tremendous recognition during the month, with the use of the #CyberAware hashtag increasing by 44 percent over the use of #NCSAM in 2014—rising from 43,000 in 2014 to 61,804 in 2015.

International success: NCSAM currently being used as a major awareness activity during October in the EU, Canada, Australia (one week only in October), and we expect to see more involvement from Latin America countries in the next few years. There will be a Latin American launch for the month on September 30 in Columbia organized by the Organization American States.

Awareness Month has become institutionalized across broad swaths of industry as many companies now have internal awareness staff and NCSAM is a natural fit for their activities. The themes also fit with many of the themes they promote within the workplace. NCSAM has also been well-established on college campuses through partnerships with Educuase and others. Partnerships in other industry segments such as HIMMS in the healthcare sector and the Council of Better Business Bureaus with the business community have helped to accelerate the adoption of NCSAM.

STOP. THINK. CONNECT.

[2] Impressions are the number of people who have seen/viewed/heard the article as provided by the media outlet.

In late 2009 through early 2010, NCSA convened a multi-sector stakeholder, public private partnership of twenty-five companies and seven Federal agencies working group operating by consensus to find through research with American consumers, a message that would resonate across the ecosystem and could be used as a banner to conduct numerous kinds of campaigns relevant to the many ways people were using the Internet. The research indicated that Americans were seeking common sense message that provided advice about taking steps that was within their control. The clear winner in the research effort was STOP. THINK. CONNECT.. It was a simple message: take security precautions, understand the consequences of your behaviors and actions online and then connect and enjoy the Internet with more peace of mind. The message is simple, instructional, non-technical and follows with other broad sweeping security and safety messaging that has been cemented into the public consciousness, such as Stop, Drop and Roll (fire safety), Stop, Look and Listen (railroad crossings), Look Both Ways Before Crossing (traffic safety).

The President launched the STOP. THINK. CONNECT. campaign in his National Cyber Security Awareness Month proclamation(https://www.whitehouse.gov/the-press-office/2010/10/01/presidential-proclamation-national-cybersecurity-awareness-month) by stating:

"Together with businesses, community-based organizations, and public- and private-sector partners, we are launching a National Cybersecurity Awareness Campaign: "Stop. Think. Connect." Through this initiative, Americans can learn about and become more aware of risks in cyberspace, and be empowered to make choices that contribute to our overall security."

Since its inception, the STOP. THINK. CONNECT. campaign has become the rallying point for the Federal Government, private sector and civil society efforts around cybersecurity education and awareness. STOP. THINK. CONNECT. was designed as a distributed grass roots campaign. The belief is that people change behavior more quickly if the message and advice come from someone they know and trust. The source could be a company they do business with, a nonprofit they are associated with or federal, state or local government agency. This approach provides numerous benefits: it allows for quicker access to individuals and organizations; campaign participants can offer customized tips and advice to

their constituency (such as a bank providing the best ways to bank safely online or a social network showing how to use their site more securely); and it offers a low-cost model of engagement by reaching the computer users through familiar partners and existing channels.

NCSA has periodically polled adults in the U.S. about campaign recognition:

- Roughly a third of Americans recognize a campaign is underway and when asked to name the campaign, 40% of them selected STOP. THINK. CONNECT. and another 30% selected "Oure Shared Responsibility," which is the theme for National Cyber Security Awareness Month and is heavily promoted by NCSA, DHS and many others. No other possible campaign names receive more than 10% recognition. Since these alternative names were in fact not messaging in use it shows that core messages are getting into the public consciousness.
- The campaign promotes other behavioral messages such as Keep a Clean Machine, Own your Online Presence and Personal Information is like Money. Value it. Protect it. In a recent NCSA study sponsored by Microsoft, 70% of teens 13-17 years old could recognize a STOP. THINK. CONNECT. advice message (Keep a Clean machine, Share with Care, etc.) and 50% of parents of teens could recognize the advice as well. NCSA demonstrated similar results in a survey in 2015 that showed nearly 50% recognition of at least one tip or advice by adults 18 and over in the U.S. Clearly, these messages are being heard.

Select metrics about the STOP. THINK. CONNECT. campaign also include:

- More than 700 partners participate in the STOP. THINK. CONNECT. campaign in over 20 countries (https://stopthinkconnect.org/get-involved/our-partners).
- President Obama called for the creation of an education campaign on stronger authentication organized by NCSA under the STOP. THINK. CONNECT. campaign as part of the Cybersecurity National Action Plan (anticipated launch September 2016) and has included STOP. THINK. CONNECT. in international agreements.

- Several important partnerships have been forged under the STOP. THINK. CONNECT. banner with leading organizations such as HIMMS in the healthcare sector, the Council of BBBs and Educause.
- STOP. THINK. CONNECT has been integrated as the lead message in National Cyber Security Awareness Month since 2010.

3. The most promising approaches to addressing the challenges;

The most promising approaches to addressing the problem are: building the public private partnership to expand cybersecurity education and awareness efforts, continued rigor in the development of messaging, investing in broader and more far-reaching campaign efforts, targeting messaging and activities within industry segments and populations to make it contextually relevant, building an education and awareness infrastructure to develop and disseminate new messages as needed, and developing measurable goals along with methods and a proper infrastructure to track progress.

- Building the public private partnership to expand cybersecurity education and awareness efforts: It is a universal truth that no single organization or entity (including government) is solely responsible for cybersecurity education and awareness. The education awareness effort to help create a safer, more secure and trusted Internet is a shared self-interest of government, industry and civil society. As such, all should be playing a role in ongoing education and awareness efforts. Partnerships play a vital role in education and awareness -- they bring new resources, leverage trusted relationships to deliver messages that are more quickly received, help tailor messages to industry sector or demographic-specific audiences, and provide insight into risk and vulnerabilities that exist for their constituencies as well as the correct advice for mitigation and remediation. Perhaps most importantly, partnerships demonstrate the shared responsibility for securing the Internet and serve as a model for how the public/private sector collaboration.
- Rigor in messaging development: The STOP. THINK. CONNECT. campaign brought, for the first time, message development research into the

cybersecurity education and awareness efforts. By using research guided by multi- stakeholder involvement, it was possible to craft campaign messages that would have impact but also be acceptable to government and industry. Traditionally, cybersecurity messaging efforts had focused on implementation of advice from experts without any effort to find out beforehand what would motivate people to participate. Using research encourages a greater potential for success from the outset. Furthermore, research has proven to be an effective tool for recruiting new partners for campaign efforts. It is easy to explain and show new partners that they are participating in an effort designed to be successful because it's based on research. NCSA has continued the process of extensive message development and testing in subsequent campaign efforts. Many of NCSA's messages have been tested for effectiveness with the public, for example, for the upcoming stronger authentication campaign with the White House (to be launched shortly after the RFI deadline). NCSA tested several messages and logo designs around adopting stronger authentication, asking respondents to react to messaging based on its relationship to adopting better account security. The questions were as follows:

    - I believe this logo/tagline is simple and easy to understand
    - This logo/tagline is effective at getting my attention
    - This logo/tagline makes me want to learn more about how I could protect my online accounts
    - This logo/tagline makes me want to adopt stronger security for my online accounts
    - I believe this logo/tagline will motivate Americans to take action, prevent identity theft and secure our digital lives
    - This logo/tagline is important to me
- Investing in broader and more far reaching campaign efforts: While existing campaigns are showing some early success, investments in education and awareness have not been equal to the importance of the efforts. DHS developed television PSAs in 2014 that NCSA was able to distribute to stations across the country. And over the years, many great materials have been developed (posters, tip sheets, infographics, etc.). However, there has never been adequate funding to deploy a robust campaign coordinated across all media platforms that is sustained over a long period of time. Because the landscape is so broad and reaching every

American is so critical, the deployment of the campaign has to be equal to the task. This is an achievable objective with a well-funded and thoughtful campaign that takes advantage of a variety of tactics, including using senior government officials, industry luminaries and celebrities as message purveyors, coordinating the resources of partners to help fill in gaps, encouraging the participation of brands with a large reach to carry and promote the campaign and refreshing messaging and approach as needed.

- Targeting messaging and activities within specific verticals and populations to make them contextually relevant: Effective education campaigns in cybersecurity must address the challenge that not every threat or risk or response to threat or risk is universal. Some sectors and populations could have increased risks depending on the threat and some may have no risk at all. Therefore, making awareness and education efforts relevant to target groups is critical. Partnerships play a critical role in effectively creating targeted campaigns for specific sectors not only because of the trusted role some groups play with those verticals (e.g., trade or membership organizations), but also because of the expertise those groups have in determining the relevance of specific information to their constituencies as well as the cultural understanding they have in knowing how to best present information or make it meaningful. NCSA has used these kinds of partnerships with great success to make cybersecurity education and awareness a priority. For example, almost since its inception, NCSA has worked with Educause, an association of IT professionals on college campuses who in most cases are the people on campus tasked with awareness. Working in partnership, Educause has been able to help NCSA understand the kinds of materials that would be helpful to their members and cybersecurity issues they are dealing with on campuses. Educause has been actively encouraging and recruiting college campuses to participate in awareness activities, such National Cyber Security Awareness Month and Data Privacy Day. Collectively, we have enhanced each other's ability to be effective.
- Building an education and awareness infrastructure to develop and disseminate new messages as needed: Since no one wants cybersecurity messaging become stagnant, and new technologies and vectors of attack will likely require specialized messaging to help keep people and businesses safer and more secure, there need to be ways to craft messages responsive to these changes and then get them deployed across

the ecosystem. In NCSA's experience, sometimes this means deploying messaging in short time frame, such as providing sound advice after an event like HeartBleed, or taking a longer approach such as with the Internet of Things (IoT). With IoT, NCSA is working in advance of the broad roll-out of this area to (including as theme of National Cyber Security Awareness Month) explore and understand what the role of people and business will be in securing this expanded infrastructure and crafting and deploying messaging as the ecosystem grows and known best practices emerge. We believe that messages should be created through research and consultation with subject matter experts. Creating the messages is not enough. There needs to be a network of trusted sources ready to adopt and disseminate the messaging. That is why NCSA and DHS have created the network around education and awareness that includes thousands of stakeholders from National Cyber Security month and STOP. THINK. CONNECT. who are ready to accept and use the messaging. This network should be continually expanded. Additionally, mechanisms should be developed between ISACs and other organizations knowledgeable about risks and threats and education and awareness groups to better align messaging and remediation methods in a timely fashion. And increasingly, companies are investing resources in internal awareness efforts, including hiring dedicated staff and investing in additional resources and training. This is an important and promising trend and should be encouraged. This community of awareness professionals is growing to be a vital component of the education and awareness ecosystem. The SANS Institute maintains an online community of around 600 such people and holds an annual Summit to share best practices. This community is a major consumer of existing efforts including National Cyber Security Awareness Month and STOP. THINK. CONNECT.

- Developing measurable goals and methods and infrastructure to track progress: building an infrastructure to track the impact of education and awareness efforts needs to be a continuing priority. We can't track progress unless we have systems in place to measure success. Since the inception of STOP. THINK. CONNECT., NCSA has been polling people to track message recognition. There are many efforts around tracking other efforts in cybersecurity such as reports on phishing produced by APWG and informative reports on risks such as the Verizon Data Breach Report.

These are all helpful efforts but we need a more coordinated approach based on widely accepted goals for progress

4. What can or should be done now or within the next 1-2 years to better address the challenges;

NCSA makes the following recommendations for goals in the short term (first few months of the new administration) and longer term (over the first several years of the administration):

Short-Term

- Clearly designate someone in the White House Cybersecurity Coordinator's Office with responsibility for cybersecurity education and awareness to help keep the issue a priority within the White House. This person would work across agencies to ensure a continued and coordinated focus on the issue.
- Establish a White House-led interagency working group of executive branch and independent agencies on cybersecurity education and awareness to expand and facilitate the continued dissemination of harmonized messages on cybersecurity education and awareness across all government agencies and ensure high levels of coordination on education and awareness efforts, including how every government agency will participate in STOP. THINK. CONNECT. and National Cyber Security Awareness Month (planning for the following October starts winter of the same year).
- Continue momentum on existing efforts—the stronger authentication campaign, STOP. THINK. CONNECT., National Cyber Security Awareness Month—by having the new President and key administration officials—DHS, Commerce, Federal Trade Commission and others—speak out early on the need for individuals and businesses to maintain and take steps to be safer and more secure online.

Long-Term

- Take a multi-generational approach to cybersecurity education and awareness, provide funding at the same levels that are invested in other broad-sweeping, high-profile societal safety education and awareness campaigns (e.g. If You See Something, Say Something, Smokey the Bear, Click It or Ticket) and lead with harmonized messaging under a recognizable core message (e.g., STOP. THINK. CONNECT.). The campaign goals should include:
    - Establishing online safety and cybersecurity as a societal norm that everyone has a role in achieving
    - Connecting the contextual application of best cybersecurity practices in everyday life, from shopping and banking to travel to family and home safety and security
    - Establishing the need for a culture of cybersecurity throughout the workplace from the boardroom to the breakroom.
    - Establishing the inclusion and institutionalization of basic cybersecurity education for America's youth – including an overview of cybersecurity career opportunities – in schools, after-school programs and with civic groups working with young people
    - Using and maintaining messaging discipline around core messaging as the highly recognizable umbrella so that new messaging can be created to address specific cybersecurity issues that evolve over time.
    - Facilitating the continued success of existing public-private partnerships that leverage trust relationships to disseminate messaging as a critical component of the cybersecurity education and awareness effort, including the continued expansion of key activities such as National Cyber Security Awareness Month, the STOP. THINK. CONNECT. campaign and Safer Internet Day
    - Creating mechanisms through working with nonprofits, industry and government to quickly translate new or emerging threat activity, where relevant, into consumer and business friendly action items that are distributed via trusted sources and traditional and social media.

    - Engage in continuous exploration of new ways to use traditional and social media to keep the campaign fresh and use existing and emerging platforms in creative ways, including finding and engaging influencers (celebrities, leading authorities, etc.) as voices of the campaign.
- Convene industry, government, researchers and NGOs to establish consensus targets for behavioral change, outcomes, metrics, benchmarks and methodologies to determine the impact of awareness and education efforts with the goal of establishing and institutionalizing the most effective ways to increase cybersecurity and measure campaign effectiveness.

5. What should be done over the next decade to better address the challenges: continue to build infrastructure for developing and disseminating cybersecurity information for computer users and businesses. Build an expand the public private partnership to engage a broad range stakeholder in the effort. Encourage increased research on education and awareness. Recognize that a continuous cybersecurity education and awareness efforts are critical part of the overall cybersecurity strategy.

6. Future challenges that may arise and recommended actions that individuals, organizations, and governments can take to best position themselves today to meet those challenges.

It is very hard to predict exactly where the future challenges will lie. We can expect a continually expanding technology landscape with many more connected devices and tremendous volumes of data that will need to be protected and secured. Cybersecurity may change from being about protecting devices and infrastructure, as technology advances, to a focus on maintaining data integrity. How we will know the data being generated by machines is not corrupted and can be trusted?

The best way to position ourselves for the future is to continue to build strong public/private partnerships, create meaningful best practices that can be broadly implemented, establish measurable goals and use research and subject

matter experts to develop accurate and actionable messaging for cybersecurity. If we build this infrastructure, we can develop the flexible yet solid cyber aware community able to keep all Americans armed with knowledge to use the Internet safely and securely.

The Commission also seeks input on the following:

In the area of education and awareness:

1. Emerging technology trends and innovations; the effect these technology trends and innovations will have on the digital economy; and the effect these technology trends and innovations will have on cybersecurity. From our perspective we have seen a positive trend as technology around cybersecurity improves. We are hopeful that new technology will continue to make cybersecurity practices easier and more robust. We have moved a long way from to teach people to manually keep things like security software up-to-date. We see a great deal of promise in areas of stronger authentication that will provide significantly increased account security. Since for most users, unauthorized account access and identity theft is a significant concern and risk, these technologies should have a significant impact on cybersecurity.
2. Economic and other incentives for enhancing cybersecurity. Incentives should always be part of the discussion. They can be critical when efforts need to be brought to scale. One area where incentives should be explored is encouraging companies to implement internal awareness programs. This is a growing trend but more broad adoption of these efforts would be extremely beneficial to cybersecurity ecosystem.

Small and Medium Size Business

The RFI did not specifically call out Small and Medium Size Businesses (SMBs) as a critical area. However, this sector, we believe, deserves special attention because of the importance of this sector to the American economy and the need to make concerted efforts to reach this community with a actionable cyber security advice and information.

1. Current and future trends and challenges:

Increasingly over the last several years, SMBs have become target for cybercriminals. SMBs are targeted because they have valuable data, ca be gateways to larger businesses and they have other resources—intellectual property and money—that can be stolen. Trends and challenges in the SMB sector are as follow:

- SMBs may not sense they are at risk: even with the continuous news about breaches, threats and risks many SMBs may feel they have no valuable assets and will therefore not be a target.
- SMBs may have no dedicated staff overseeing technology. Often the business owner wears many hats and cybersecurity can become a low priority.
- The SMB community is fractured there are few central respected voices that can reach the whole community.
- The landscape is huge: According the Small Business Administration there are than 4 million small businesses in the country with less than 500 employees, another 22 million with no employees and 18,500 with more than 500 employees. Assuming that every business needs at least some kind of information on maintaining cybersecurity, it is a tremendous challenge to reach them all.
- All threats are not created equally SMBs are not monolithic: Not every threat applies to the same to every SMB. It can be difficult to determine the ones most significant to a specific company. SMBs can therefore be overwhelmed by threats and risks making it hard to act. There are many different types of SMBs in the country from retail and consumer facing services to manufacturing and agriculture and more. While there may be some generalities by sector or even size, each business will need a cybersecurity approach tailored to their situation.
- SMBs can put other businesses at risk: many SMBs are vendors to larger businesses and if they are compromised that could compromise their customers. Many do businesses with critical infrastructure, which could put critical sectors at risk.
- SMBs can be disempowered by overwhelming risk and threat information: There is so much negative information and so many larger organizations have been breached and hack, some businesses may be uninspired to act because they feel that if larger organizations can't protect themselves what can they do.

- Cybersecurity maybe viewed as a cost center and it can be unclear what investments will make the business most secure: It can very unclear about what kind of investments and how much SMBs need to spend to maintain cybersecurity. It can be extremely confusing about want SMBs actually need to purchase and implement that will give them the best return on investment in cybersecurity.

2. Progress being made to address the challenges;
    - The most significant progress made to date has the been the creation of the NIST Cybersecurity Framework. The framework has created an excellent starting point for SMBs to approach cybersecurity. By getting businesses to first focus on assets needing protection and taking that through to recovery and response, we now have an easy way to help businesses focus resources on their most important assets and build protection and detection schemes that directly build resistance around key assets. The focus on recovery and resistance also gets SMBs focused beyond protection to resilience. Give the fragile nature of many SMBs this holistic approach is an important change in the cybersecurity environment for SMBs.
3. The most promising approaches to addressing the challenges;
    - While the NIST Framework provides an excellent starting point, providing assistance to SMBs to act on and implement the framework is essential. NCSA has developed a highly interactive, scenario based training for SMBs based on the NIST Cybersecurity Framework. To date NCSA has field tested the training several time and refined it into a product that can be easily delivered. The focus of the training is like 101 on cybersecurity for SMBs. It is non-technical and helps SMBs begin the process of identifying key assets and protection schemes. The goal of the training is to get SMBs to engage directly in cybersecurity as it applies to their specific situations. The training is abed on adult learning principals that include interactivity, providing opportunities of participants to relay and legitimize their own experiences and hear from the experiences of their peer, which can significantly influence SMB leaders.

4. What can or should be done now or within the next 1-2 years to better address the challenges;
    - Build partnerships to reach SMBs: To bring any efforts to scale will require substantial partnerships between the many stakeholders in the public and private sectors concerned about the cybersecurity of SMBs.
    - Create a continuous flow of reliable information for SMBs: There needs to be high quality consumable information available to all SMBs, this could either be via a central hub or syndicated out through key stakeholders or trusted sources.
    - Fund efforts to reach and train SMBs.
    - Create a cross agency working group to provide a coordinated approach to cybersecurity for SMBs.
    - Explore possible incentives for SMBs to invest in cybersecurity.