SAMPLE TALKING POINTS

Introduction

- Good [morning, afternoon, evening] everyone.
- I'm glad you have taken the time to discuss this important issue with me and members of your community.
- Before I begin, let me tell you a little bit about myself.

About the Campaign

- The reason I am here today is to talk about cybersecurity awareness and to motivate you to become involved in the National Cybersecurity Awareness Campaign.
- In May 2009, President Obama issued the *Cyberspace Policy Review,* which recommends the Federal government "initiate a national public awareness and education campaign informed by previous successful campaigns."
- The Department of Homeland Security launched the Stop. Think. Connect.™ (STC) Campaign in October 2010 in conjunction with National Cybersecurity Awareness Month.
- Stop. Think. Connect. is part of an unprecedented effort among Federal and State governments, industry, and non-profit organizations to promote safe online behavior and practices.
- Together we are working to combat threats and raise awareness across this country.
- Now, we want to get you to become an active member of the campaign to help us raise cybersecurity awareness with your family and friends and in your community.

Issues Affecting You and Your Family

- To understand the importance of cybersecurity, we have to talk about the risks and threats that exist online and their impact at a national and personal level.
- Cyber risks and threats are real and endanger our national security. For example:
    - Every 3 seconds an identity is stolen- so for the length of this discussion over [enter # depending on length of remarks] identities may have been stolen;
    - Cybercrime has surpassed illegal drug dealing as the #1 criminal moneymaker worldwide; and that

- Without security, your unprotected computer can become infected within four minutes of connecting to the Internet.

- Threats to our Nation's cybersecurity are truly threats to our national security. We all have a role to play in understanding and preventing these threats.
- We need to understand the who, the how, and the what in order to be able to understand and deal with cyber risk.
  - The who is simple. There are two types of attackers that can cause harm to the Internet: hostile and non-hostile attackers. The difference is based on their intent. Hostile actors intend to cause harm, like cybercriminal organizations or hackers, while non-hostile actors accidentally cause harm, like an employee, who accidentally downloads malware into a key system.[1]
  - The how are the methods threat actors use to cause the harm. These methods can range in sophistication and complexity from botnets to viruses.
  - The what are the vulnerabilities that actors exploit, such as our inherent trust in software that we use on a daily basis. We expect that the software we buy and use is what it says it is and does not contain anything that can harm our computer or the Internet.
- Kids today are growing up with the technological revolution.
- They will use the Internet to do everything- from socializing to applying for college to managing their finances.
- The Internet is a great resource for them and gives them access to resources you and I never had growing up.
- However, with this accessibility comes great risk.
- Securing cyberspace starts with you-[the parents, teachers, community leaders, mentors, etc.] of these students.
- There are four issues significantly affecting your families, your schools, and your community including identity theft, fraud and phishing, cyber bullying and ethics, and cyber predators.

Identity Theft

- Identity theft is prevalent, regardless of age.
- A child's credit can be ruined before she or he is even old enough to have their own credit card.

[1] *Information Technology Sector Baseline Risk Assessment*. Department of Homeland Security. August 2009.

- It is imperative that we teach our children what is ok to share on the Internet, and more importantly, what is not.
- Social Security numbers, account numbers and passwords are examples of information to keep private.
- If you have a child that is old enough to set his or her own password, help them choose a password that is easy to remember, but hard to guess.
- Most teens (and adults for that matter) choose passwords based on "20 questions".
- They use the same 20 questions to come up with their passwords, like their middle name, their pet's name, the town they live in, their birthdate, the college they want to attend, etc.
- The problem is that these passwords are pretty easy to guess.
- You should set a password that means something to you and you only. Get creative.
- Many kids don't understand that identity theft if real and it can happen to anyone.
- The reality is that it can happen to anyone.
- Simple things like locking computers and cell phones; not sharing specific information about yourself online—full name or birthdate; setting proper privacy settings on social networking sites.
- These are common sense tips that many of you know, but it is a matter of actually practicing these tips and teaching them to your kids.
- I want to encourage you to lead by example and proactively apply and share with those around you what we are discussing today.

Fraud and Phishing

- Phishing is becoming more and more of an issue.
- Phishing scammers use email or malicious websites to solicit personal information by posing as a trustworthy source.
- For example, an attacker may send an email seemingly from a reputable news organization with links to pictures from a current news event.
- These links may take you to a malicious website or download harmful viruses onto your computer and may be used to elicit your personal information.
- Look for "teachable moments"- if you get a phishing message, show it to your kids and help them understand that messages on the Internet aren't always what they seem.
- These attacks are not going away; they are only growing.

- You cannot prevent your kids from receiving such e-mails, but you can help teach them what these type of e-mails look like and what they can do if they receive one.
- Teach them not to reply to texts, emails or pop-up messages that ask for personal information and don't click on any links in the message.
- And, educate your neighbors and friends about the types of phishing scams that are out there and what they can do to protect themselves.

Cyber Bullying and Ethics

- Over the last year, there have been a number of high-profile cyber bullying incidents that have exploded across the Internet.
- These incidents remind us that whatever anyone posts online can go viral and can have very serious consequences.
- How can you tell if your child is being bullied online?
- Look for changes in behavior- do they suddenly shy away from the computer?
- Also, talk to them about what to do if they witness someone else who is being bullied online?
- Tell the bully to stop.
- The mean behavior usually stops pretty quickly when somebody stands up for the person being bullied.
- I would suggest reminding your kids of "golden rule": be nice.
- Don't say or do anything online that you wouldn't do in person.
- Words that they write and the images that they post have consequences offline.

Cyber Predators

- The final issue I would like to talk about is cyber predators.
- Cyber predators are real.
- Social networking sites make it easy for these predators to find your kids, as we all share a lot of information about ourselves on these sites.
- Help your kids use privacy settings to restrict who can see and post on their profile.
- Many social networking sites, chat rooms and blogs have privacy settings.
- Find out how to turn these setting on, and then do it.
- Help your kids understand that people on the Internet are not always what they seem.

- Most IM programs allow parents to control whether people on their kids' contact list can see their IM status, including whether they're online.
- Some IM and email accounts allow parents to determine who can send their kids messages, and block anyone not on the list.
- Also, ask your kids who they're in touch with online
- Just as you want to know who your kids' friends are offline, it's a good idea to know who they're talking to online.
- Simply put- trust your gut.
- If you even think your child is talking to someone they shouldn't be, investigate.
- Ask them questions and help them understand the dangers of cyber predators.

Call to Action

- Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe.
- And, when we all take simple steps to keep our families safer online, it makes being online a more secure experience for everyone.
- If we each do our part online, we are protecting ourselves and helping to make the Internet safer for everyone.
- Ultimately, each of our efforts helps to enhance the nation's cybersecurity.
- You can help us spread the word and become a source of information for your family and friends and your community.
- We want the Stop. Think. Connect. Campaign to effectively reach parents and community members like you. You can help us spread the word:
    - The Campaign is hosting **Cyber Citizen Forums** just like this one in collaboration with national youth serving organizations across the country to generate dialogue and prompt action to support the nationwide campaign
    - We have created a **Friends Program** to help make an impact in local communities as a part of the larger national effort. You can become a *Friend* of the Campaign and help us mobilize efforts in your community or schools by organizing Internet safety events, handing out Stop.Think.Connect. Campaign resources or volunteering to help others in your community understand how they can be safer online.
- And, in your day-to-day life, apply what we've discussed today.

- Continue to innovate. Children are the future of our country and can take a stand against cyber threats, helping to keep America safe.

Conclusion

- **So, let me leave you with the campaign's intent so you can pass it along:**
  - **Stop:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.
  - **Think:** Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.
  - **Connect:** Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.
  - **STOP. THINK. CONNECT**. Protect yourself and help keep the web a safer place for everyone.