National Cyber Security Awareness Month
October 2016

Background:
Recognizing the importance of cybersecurity awareness, President Obama designated October as National Cyber Security Awareness Month (NCSAM). Now in its 13th year, NCSAM is a collaborative effort between the U.S. Department of Homeland Security (DHS) and its public and private partners, including the National Cyber Security Alliance, to raise awareness about the importance of cybersecurity and individual cyber hygiene.

NCSAM 2016 Themes:
Each week in October is dedicated to a specific cybersecurity theme with corresponding messaging. The themes listed below offer the opportunity for government and industry to get involved in cybersecurity activities most relevant to them. To engage Americans across the Nation, key events will be coordinated in geographically diverse locations. We encourage you to align your NCSAM plans to the following weekly themes:

1. *Week 1: October 3-7, 2016 – Topic: Every Day Steps Towards Online Safety with Stop.Think.Connect.*™
   Cybersecurity is present in every aspect of our lives, whether it be at home, work, school, or on the go. Regardless of one's technical ability or background, there are simple steps everyone can take to be more cyber secure in their digital lives. Week 1 kicks off NCSAM 2016 and reinforces basic tips for everyone to be safer online, including more secure accounts through stronger authentication and keeping security updates current.

2. *Week 2: October 10-14, 2016 – Topic: Cyber from the Break Room to the Board Room*
   We are all part of protecting personal and organizational data in the workplace. From CEO to incoming entry-level employee, each organization's cybersecurity posture is reliant on a shared level of vigilance and awareness. Week 2 looks at how every employee can promote a culture of cybersecurity at work.

3. *Week 3: October 17-21, 2016 – Topic: Recognizing and Combating Cybercrime*
   As technology advances, the impact of cybercrime is becoming more costly and frequent. Law enforcement, government, industry, and individual citizens all play a vital role in mitigating adverse impact to our schools, communities, and personal well-being. Incidents ensue through every day 'phishing' emails masked behind trusted sources, in infected websites that unknowingly capture personal information when entered, and as persuasive links that lock files until a ransom is paid. Week 3 focuses on the signs of criminal intent through technology and what individuals can do to detect and prevent cybercrime.

4. *Week 4: October 24-28, 2016 –Topic: Our Continuously Connected Lives: What's Your 'App'-titude?*
   With compounding growth of connected technologies – cars, household appliances, finances, healthcare, and more being increasingly managed by smart devices – we are confronted with the need for increased awareness to secure cutting-edge, technical innovations. Week 4 looks to the future and discusses how cybersecurity is being built into advanced technology along with areas of opportunity for individuals to operate securely in a digital society.

5. *Week 5: October 31, 2016 – Topic: Building Resilience in Critical Infrastructure*
   The linkage between cyber and physical security is essential to the resiliency of critical infrastructure at both the local and national level. Resilience of essential systems and assets, from power grids to banking systems, is vital to our national security, economy, and public health and safety. Week 5 looks at the sustainment of the Nation's critical infrastructure, and facilitates the transition to November's Critical Infrastructure Security and Resilience Month (CISR).

The hashtag for NCSAM will be **#CyberAware** – we encourage you to use this both before and during the month of October to promote your organization's involvement in raising cybersecurity awareness.

For more information, please contact the Stop.Think.Connect.™ Campaign at stopthinkconnect@dhs.gov.