



### **Background:**

In its 11<sup>th</sup> year, National Cyber Security Awareness Month (NCSAM) is a collaborative effort between the Department of Homeland Security and its public and private partners, including the National Cyber Security Alliance (NCSA), to raise awareness about the importance of cybersecurity and individual cyber hygiene.

### **NCSAM 2014 Themes:**

Each week in October is dedicated to a specific cybersecurity theme with corresponding messaging. The themes listed below offer the opportunity for all stakeholder communities 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. More information about locations will be shared shortly. Details on the weekly themes are as follows:

- 1. Week 1: October 1-3, 2014 – Promote Online Safety with the Stop.Think.Connect.™ Campaign*  
The kickoff will be held in conjunction with the 2014 National Association of State Chief Information Officers (NASCIO) Conference, where the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Public Technology Institute are also holding their big annual events in **Nashville, TN**.
- 2. Week 2: October 6-10, 2014 – Secure Development of IT Products*  
Building security into information technology products is key to enhanced cybersecurity. Security is an essential element of software design, development, testing, and maintenance. The software we use everyday on our phones, tablets, and computers may have vulnerabilities that can compromise our personal information and privacy. This week will target these stakeholders and educate others about what to do and look for in products.
- 3. Week 3: October 13-17, 2014 – Critical Infrastructure and the Internet of Things*  
The Internet underlies nearly every facet of our daily lives and is the foundation for much of the critical infrastructure that keeps our Nation running. The systems that support electricity, financial services, transportation, and communications are increasingly interconnected. The Internet of Things—the ability of objects and devices to transfer data—is changing the way we use technology. Week four highlights the importance of protecting critical infrastructure and properly securing all devices that are connected to the Internet.
- 4. Week 4: October 20-24, 2014 – Cybersecurity for Small and Medium-Sized Businesses and Entrepreneurs*  
Small and medium-sized businesses are an important part of our Nation's economy, but they often do not see themselves as a target for a cyber attack. Strong cybersecurity practices are vital within these organization. Entrepreneurs are recognizing the cybersecurity field as a burgeoning marketplace. This week will focus on what emerging and established businesses can do to protect their organization, customers, and employees, as well as cybersecurity as a business opportunity using tools such as the DHS C<sup>3</sup> Voluntary Program.
- 5. Week 5: October 27-31, 2014 – Cyber Crime and Law Enforcement*  
The event will coincide with the International Association of Chiefs of Police (IACP) Annual Conference in **Orlando, FL**. The goal is to help draw awareness to and educate law enforcement officers about how to assist their communities in combating cyber crime. In addition, we will provide information to the general public with ways to protect themselves from becoming a victim of identity theft, fraud, phishing, as well as what to do if their personal or financial information has been stolen.

**For more information, please contact:** Kristina Dorville, Deputy Branch Chief of Cybersecurity Education and Awareness at the Department of Homeland Security, [kristina.dorville@dhs.gov](mailto:kristina.dorville@dhs.gov).