Top Tips on Cybersecurity to share during NCSAM

• **Keep a clean machine**. Keeping your internet-connected devices free from malware and infections makes the internet safer for you and more secure for everyone. Regularly scan your personal and office devices for viruses and spyware along with keeping your software up to date. For additional ways to protect your devices please visit: https://www.stopthinkconnect.org/campaigns/keep-a-cleanmachine-campaign

• **Avoid oversharing online.** As a young professional, it may be very exciting to share what you do at work with others. Remember your organization's security standards and be careful what you say, especially in public settings. You never know who may be overhearing your conversations. Also, put away your work identification or badge when out in public and when using public transportation.

• **Protect your password.** Create a password with eight characters or more and a combination of letters, numbers, and symbols, and don't make it easy to guess. Additionally, always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email, medical files, or bank accounts.

• **Stay protected while connected.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, or café – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi.

• **Play hard to get with strangers.** Cyber criminals will often offer a financial reward, threaten you if you don't engage, or claim that someone is in need of help. Don't fall for it! Keep your personal information as private as possible. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

• **Report any cybersecurity incident.** Report computer or network vulnerabilities to the National Cybersecurity Communications and Integration Center (NCCIC) at 1-888-282-0870, or at www.us-cert.gov/report. Forward phishing emails or websites to NCCIC at mailto:phishing-report@us-cert.gov.

• **Do your part in protecting critical infrastructure**. Our nation's critical infrastructure runs on the Internet. The systems that enable us to live our daily lives—the electrical systems, financial institutions, transportation systems, and more—are all dependent upon a digital ecosystem. As cybersecurity breaches continue to rise in frequency and scale, it is critical for all Americans to understand their role and take steps to protect our critical infrastructure.