USNIC Wraps Up National Cybersecurity Awareness Month!

October 31, 2017, Suitland, MD – U.S. National Ice Center (USNIC) wrapped up Cybersecurity Awareness Month this week with an all-hands message from the USNIC Information Technology (IT) Department reminding everyone of increasing cyber security threats and the need for greater cybersecurity awareness.

" I would like to talk to you all about some recent attacks that have happened and remind everyone that cybersecurity is not just the responsibility of a few people, it takes a team effort said Information Systems Technician 1st Class (IT1) Mitchell Starbard, USNIC's Information Systems Security Manager (ISSM). IT1 Starbard gave some examples of notable recent, cybersecurity attacks:

1. The Equifax data breach which potentially compromised confidential information of over 143 million Americans is a recent example of the impact of a cybersecurity attack.
2. The WannaCry ransomware attack in May, affected over 150,000 computers in over 150 countries worldwide within the first 24 hours of the attack.
3. The 2016 U.S. presidential elections were subject to cybersecurity attacks focused on data thefts and disclosures.
4. The 2015 Office of Personnel Management hack resulted in the loss of 21.5 million personnel records.

IT1 Starbard continued to say "what we can do is remain aware and keep alert at all times. Remember, any electronic device used for storing and processing data is at risk, regardless of whether it's connected to the Internet or not. Cybersecurity attacks are employing innovative tactics to reach systems not connected to the Internet. Things like thumb drives are not exempt. In a related incident, thumb drives loaded with damaging software were used to spread the Stuxnet virus."

Chief of Naval Operations (CNO), Admiral John Richardson, summed s up the current cybersecurity threat environment in an interview last month by stating, "The threats reach well beyond what you would consider a traditional computer or information technology network into the control systems and indeed almost every aspect of our lives and of our mission."

Although National Cybersecurity Awareness Month has come to a close, cybersecurity remains an everyday task and everyone's responsibility. IT1 Starbard reminded personnel that they can make a difference by adhering to cybersecurity policies, directives, and best practices. Simple actions such as reporting suspicious email activity to the ISSM can help keep USNIC systems secure. These best practices do not just apply to the office but should be applied to protect command members and families while online, or outside of work. Remember, always be vigilant. Be safe!