For more information contact:
Jane Gervais, Adams County Emergency Management Director
608-339-4248

October 9, 2017
For Immediate Release

Cybersecurity Awareness Month begins

(FRIENDSHIP, WI) — We lead internet-connected, digital lives. From our homes to work, computers, notebooks, smart phones and other devices have made our lives easier. This has also made us vulnerable to cyber attackers. That's why Governor Scott Walker has designated October as Wisconsin's Cybersecurity Awareness Month.

"Cyber is part of our daily lives and impacts our entire economy and society," said Maj. Gen. Don Dunbar, Wisconsin's adjutant general and Homeland Security Advisor. "We need to understand cyber hygiene on a personal and organizational level, and practice it or accept the consequences of bad cyber actors intent on crime, theft, damage to reputations, and destabilization of routine operations."

"Simply performing basic cyber hygiene on a continual basis can dramatically reduce your chances of intrusions and attacks from impacting you, said David Cagigal, chief information officer with the Wisconsin Department of Administration's Division of Enterprise Technology.

Good cyber hygiene comes down to count, control, patch and repeat. These tips can help protect you from cyber attacks.

COUNT: Know what's connected to your network
- Identify authorized and unauthorized devices along with lost or stolen assets. You need to begin with an inventory.
- Knowing what IT assets you own will allow you to better manage your IT infrastructure and its security.
- Every piece of equipment has vulnerabilities and exposes you to risk. How you handle the risk will depend on what the equipment is and what purpose it has.
- You can't protect what you don't know exist.

CONTROL: Protecting your systems by properly managing accounts and limiting user and administrator privileges to only what they need to do their job.
- Properly controlling access to business information and systems reduces the risk of accidents, unauthorized access/use and security breaches.
- Failure to properly manage access can result in compromise and loss, damage or unauthorized disclosure of sensitive and private information.
- Special care must be taken with "privileged accounts" used by system administrators, since they have the ability to create accounts and change or by-pass security settings.
- Controlling access using good processes, including the use of strong passwords reduces the risk of accounts being compromised and used for unauthorized purposes.

PATCH: Protecting your systems by keeping current!
- Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.
- The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities.
- Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an attack has occurred.

REPEAT: Why is this step important?
- Reviewing your list will insure that each cycle of each individual priority has been appropriately met and that nothing falls through the cracks in your Cyber Hygiene.

Each week this October, ReadyWisconsin will highlight efforts to keep everyone in Wisconsin safe from cybercrime. Visit http://readywisconsin.wi.gov for more information. You can also follow us on Twitter, Facebook, and Instagram.

These and many other topics will be discussed at Wisconsin's 5th Annual Governor's Cybersecurity Summit, Monday, Oct. 16 at the Gordon Event Center, UW-Madison. Learn more about the Summit and register online at http://cybersummit.wisconsin.gov.

Current News Releases available at http://readywisconsin.wi.gov

Join us on Twitter at http://twitter.com/ReadyWisconsin
Facebook at http://www.facebook.com/ReadyWisconsin
and Instagram (www.instagram.com/readywisconsin).