UNITED STATES CYBER COMMAND

CYBERSECURITY AWARENESS NEWSLETTER

National Cyber Security Awareness Month

Week 4

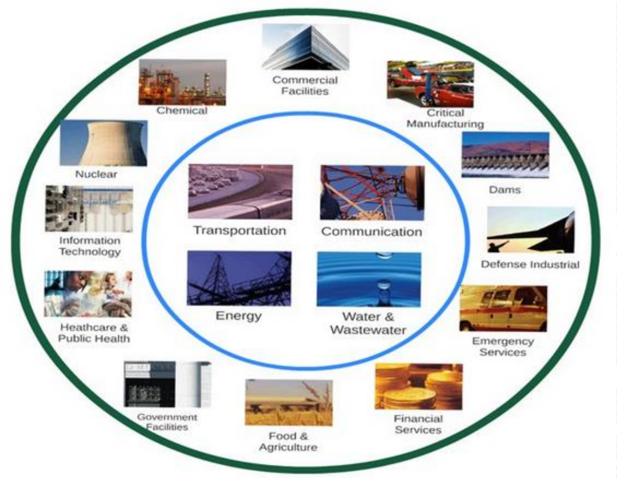
October 2018

Week 4: October 23-27

Safeguarding the Nation's Critical Infrastructure

Our day-to-day life depends on the country's 16 sectors of critical infrastructure, which supply food, water, financial services, public health, communications and power along with several other networks and systems. The Internet underlies nearly every aspect of our everyday lives and helps form our critical infrastructure, which keeps crucial systems like electricity, transportation and communications up and running. Week 4 emphasizes the importance of critical infrastructure and identifies the roles that the public can play in keeping it secure. This last week of October begins the transition to November, which is Critical Infrastructure Security and Resilience Month.

StaySafeOnline.org



https://twitter.com/NCSCgov/status/1055501526549098498

Our Critical Infrastructure

According the Department of Homeland Security, "Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." We depend on our critical systems to manage nearly all of our important installations like power stations and grids, pipelines, reservoirs, communications, and transportation. Almost all of our critical systems are connected to at least one cyber component.

Our Shared Responsibility

No individual, business or government entity is solely responsible for securing our critical infrastructure. All of us play an individual role in protecting our part of cyberspace. From our office computers to our home networks and devices our personal actions have a collective impact on the security of our critical infrastructure. If we all strive to do our part together we will be unified organization that is stronger, safer, resilient if an attack were to occur, and far more resistant from attacks.

The future of our nation depends on our ability build resilience in our critical systems. In order to do that we as a whole need to be diligent in contributing to our shared role.

Additional Government Resources and Useful Links

Cybersecurity Awareness Information: https://staysafeonline.org/

Critical Infrastructure Sectors: https://www.dhs.gov/critical-infrastructure-sectors

Critical Infrastructure Security**:** https://www.dhs.gov/topic/critical-infrastructure-security

What You Can Do

We are constantly connected to technology and information both at home and at work. Understanding what to protect can aid in securing our critical infrastructure. Simple steps like not discussing specifics of technology, routines, travel, property, and the particulars about service providers with others can frustrate a potential malicious actor. Take time with your friends, family and colleagues to learn what should and should not be discussed or shared with others. After defining what is critical, take a moment to evaluate what you can do to protect these vulnerable systems—malicious actors will look for any opportunity to circumvent security measures. Together we must do our part in order to help protect our critical infrastructure.

https://www.crises-control.com/news-blogs/cyber-security-is-threatening-our-critical-national-infrastructure.html

As NCSAM Comes to a Close

- *STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy the Internet.*
- *Initiate action to create a culture of cybersecurity at work.*
- *Take steps to protect yourself, your co-workers, and your family, when connecting to the Internet while on the go.*
- *Actively seek information to educate yourself on the dynamic and evolving Internet and cyber-connected world we live in.*
- *Be an active participant in our society's digital transformation by increasing your level of knowledge and understanding in cybersecurity.*

Next Month is Critical Infrastructure Security and Resilience Month!

USCYBERCOM OCIO

The Office of the CIO serves as the Information Assurance subject matter experts for U.S. Cyber Command. It is our mission to protect the confidentiality, integrity, and availability of Information Systems (IS) and networks throughout USCYBERCOM, while managing a customer-orientated IA organization capable of meeting the needs of all USCYBERCOM customers.

Additional Government Resources and Useful Links

Cybersecurity Awareness Information: https://staysafeonline.org/

Critical Infrastructure Sectors: https://www.dhs.gov/critical-infrastructure-sectors

Critical Infrastructure Security**:** https://www.dhs.gov/topic/critical-infrastructure-security