The Front Burner
Cybersecurity

Office of the Chief Information Officer
Office of Cyber Security
Issue No. 19, October 2014

National Cyber Security Awareness Month

Please join the Office of the Chief Information Officer (OCIO) during October 2014 for the Annual DOE National Cybersecurity Awareness Month (NCSAM) events to be hosted at the Forrestal and Germantown locations. NCSAM is a collaborative effort between government and industry to engage and educate the public, private, and Federal sectors about cyber risks in an effort to increase the resiliency of the Nation against cyber incidents.

The 2014 DOE NCSAM theme is ***"Securing the Internet of Things***." This theme focuses on the multi-faceted use of the Internet and how it has become the main source of all things to all users, requiring the shared responsibility of all computer users in securing their personal and professional cyberspace. This event will continue to focus on the overarching NCSAM concept of Stop.Think.Connect (STC).

On October 8, 2014, in the Forrestal Cafeteria, and on October 23, 2014, in the Germantown Cafeteria, the OCIO will be hosting cyber awareness days, including a cybersecurity awareness fair and vendor expo.

The kickoff day, Oct 8th, will also include two guest speakers in the Forrestal Auditorium (with multiple viewing and audio options) sharing their perspectives on securing the Internet of Things through safe online practices and emphasizing that securing the Internet is ***our shared responsibility***.

A hearty DOE welcome to Mr. John Pescatore, who will be speaking on "Securing the Internet of Things - Separating Hype from Reality." This topic addresses the latest Internet evolution: billions of "things" connecting to users, businesses, and other "things" using mixtures of wired and wireless connectivity.

Wednesday, October 8, 2014
11:00 am – 12:00 noon

Mr. Pescatore, SANS Director of Emerging Security Trends, joined SANS in January 2013 with 35 years of experience in computer, network, and information security. He was Gartner's lead security analyst for 13 years, working with Global 5000 corporations and major technology and service providers. Prior to joining Gartner Inc. in 1999, Mr. Pescatore was Senior Consultant for Entrust Technologies and Trusted Information Systems, where he started, grew, and managed security consulting groups focusing on firewalls, network security, encryption, and Public Key Infrastructures. Prior to that, Mr. Pescatore spent 11 years with GTE developing secure computing and telecommunications systems. Mr. Pescatore began his career at the National Security Agency (NSA), where he designed secure voice systems, and the United States Secret Service, where he developed secure communications and surveillance systems. He holds a Bachelor's degree in Electrical Engineering from the University of Connecticut and is a NSA Certified Cryptologic Engineer.

DOE also welcomes Dr. Karen Paullet. Dr. Paullet will be speaking on "Opening the Digital Pandora's Box: Mobile Device Security Awareness." She will share how cell phones have become ubiquitous within our society, and many now consider them a necessity rather than a convenience. Because of mobile devices, people are staying "plugged-in" and connected to what has become an "always on" world.

Wednesday, October 8, 2014
1:30 p.m. – 2:30 p.m.

Dr. Paullet, a faculty member at American Public University System, holds a Bachelor of Science, a Master of Science, and a Doctor of Science in Information Systems and Communications from Robert Morris University. In addition, Dr. Paullet has spent over 13 years working with law enforcement preparing cases using digital evidence for trial. She has spoken at over 100 engagements throughout Pennsylvania and Maryland on the dangers of social network sites and has applied her research interests to educate students, organizations and law enforcement. She brings her professional experience in law enforcement and teachings to serve and educate others in the community.

National Cyber Security Awareness Month

Securing the Internet of Things: It's Our Shared Responsibility

Please Join Energy's Cybersecurity Community in October for Cybersecurity Events.

2014 NCSAM Event Agenda

Forrestal Building • Wednesday, October 8, 2014 Sponsored by the OCIO	
Forrestal Cafeteria	
9:30 am – 1:00 pm	**Cyber Awareness Fair and Vendor Expo**
Forrestal Large Auditorium Meet-Me #: 202.287.5318 U-stream: http://energy.gov/live VTC: Germantown Auditorium and Nevada*	
11:00 am – 12:00 pm	****Securing the Internet of Things – Separating Hype from Reality** Mr. John Pescatore Director, SANS Institute
1:30 pm – 2:30 pm	****Opening the Digital Pandora's Box: Mobile Device Security Awareness** Dr. Karen Paullet Faculty, American Public University System
Germantown Building • Thursday, October 23, 2014 Sponsored by the OCIO	
Germantown Cafeteria	
9:30 am – 1:00 pm	**Cyber Awareness Fair and Vendor Expo**

*Other sites requesting VTC connectivity, contact Tim Smith at 301-903-4555
**Certificate of Attendance will be provided for attending this event.

For more information or additional options to participate, contact **cybsectrn@hq.doe.gov** or search **cyber awareness** on Powerpedia.

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

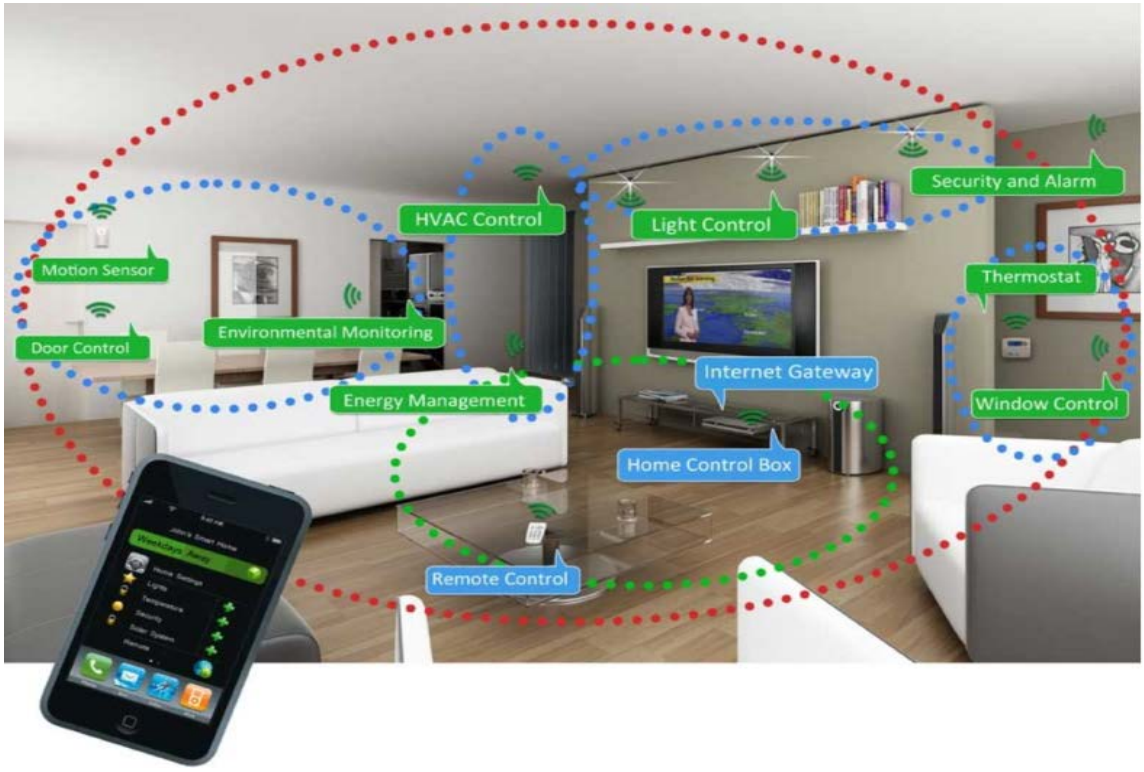
Please join us for this informative cyber awareness event and learn what you can do to be a responsible online citizen – securing cyberspace is our shared responsibility.

Everything is Connected: Securing the Internet of Things

In an increasingly interconnected world, everything from televisions, thermostats, airplanes, cell phones, medical equipment to smart meters, refrigerators, and automobiles, are connected to the Internet, have unique Internet identifiers, and are considered "smart" devices that continuously collect and transmit data via the publicly-accessible, unsecure Internet. The ability to connect embedded computing-like devices across the Internet infrastructure opens new horizons in automation in nearly every field and enables many advanced applications such as remote monitoring and the Smart Grid. The sheer number and ubiquitous nature of connected objects is staggering.

While this connectivity brings convenience and opens a world of opportunities, it also creates challenges. The smart devices use sensors that can measure and transmit information about location, temperature, speed, or even your home's electricity usage on demand. The exact features that make this connectivity appealing and functional make these smart devices vulnerable to hacking and malware attacks. By and large, manufacturers of "Internetable" devices aren't too concerned with cybersecurity features of their products, trading the convenience and benefits of a relatively unintelligent technology for security. Also, most of the embedded chips and other devices (essentially microcomputers) are manufactured all over the world and have geographically dispersed supply chains, so the possibility of the insertion of malware or tainted products increases and creates even more risk. All this put together creates the potential for product malfunction and may also put you at risk of having your personal information intercepted.

Hackers no longer have to limit themselves to your individual personal computer to access the information they want or steal your identity; they're looking at all of your personal property – everything that has that connectivity. Whether you are streaming a video on your tablet, downloading applications to your smartphone, remotely changing your air conditioning settings, or allowing your cable modem and router to be turned into a public Wi-Fi hotspot, there are precautions you should take to protect yourself.



1. Put your smart devices on their own network(s), not one that is shared with your PC.
2. Password-protect your wireless network, and use complex passwords (alphanumeric, upper case, lower case, special characters).
3. Password-protect your smart phone. Securing your mobile devices is even more critical now because all of the applications there that control your life. (Statistics show that more than 80 percent of people don't even put a PIN or password on their phones.)
4. Make sure you know if any device you buy has intended transmission capability, and buy from a reliable source.
5. When you make device purchases, disable any remote accessibility features and change the default password right away.
6. Choose a known and reliable technician to service smart devices.
7. Turn off mobile devices when not in use.

While smart devices have the potential to save time and energy and improve safety and health, the benefits come with significant risks. The data collection and potential sharing of that information with others are significant concerns.

The ability to connect, communicate with, and remotely manage an incalculable number of automated smart devices through the Internet is a significant challenge in fending off the adversary given the expanded footprint. Remember we must protect the information and systems we rely on everyday whether at home, work, or school.

Concerns over Facebook's New Messenger Application

Don't you love your smartphone and Facebook. Just be careful how you use them both.

The Facebook Messenger smart phone application grants Facebook access to the smartphone camera and photos, microphone, and contacts. Through the application, you can take pictures and videos, record audio, directly call phone numbers, receive text messages, and synchronize contacts. Facebook requires users to download the application to message through its platform on smartphone devices. That's great, but if Facebook were hacked, this application on your phone increases exposure to the loss of personally identifiable information (PII).

Once you give Facebook access, you lose control over the security of your PII. Through the application, Facebook has massively expanded access to huge amounts of PII resident on each smartphone that has the app downloaded. An August 2014 article in The Guardian reported that the application had been downloaded 500 million times on Android devices, alone.

Being that you can control only what you give Facebook access to, downloading Facebook Messenger may not be a wise choice. Think carefully before you download anything that links to your personal information.

Be a cyber hero!
Always STOP.THINK.CONNECT

Contractor Training Site (CTS) Upgrade

The OCIO is pleased to announce the availability of the upgraded Contractor Training Site (CTS) https://contractortraining.energy.gov for delivery of Cybersecurity and other training courses to contractors throughout the Department of Energy (DOE). The CTS offers free, online training courses for DOE contractors only*. DOE Federal employees will continue to use the Online Learning Center (OLC) for Headquarters-sponsored training*. The CTS has successfully been used in the past to offer other Departmental training and has now been expanded to provide a variety of cybersecurity courses such as the Annual Cybersecurity Awareness Training and other cyber courses to include:

- Authorizing Official (AO)/AO Designated Representative (AODR)
- Security Risk Management
- System Authorization
- Supply Chain Risk Management (SCRM) for the Information Technology (IT) Professional
- Incident Management (Available in FY2015)
- Enterprise Supply Chain Risk Management (eSCRM) for Program Managers (Available in FY2015)

These optional courses are highly recommended for DOE contractors who fulfill a Cybersecurity or IT role and can be completed at the employee's convenience.

First time users will be required to establish a new account by providing your official DOE e-mail address and creating a password. For all technical questions or issues with CTS, please contact the CTS Help Desk at (202) 558-2203 or toll free at (888) 804-4510, from 8:30 am to 6:00 pm EST, Monday through Friday, excluding holidays. A description of these training courses is available on the Cybersecurity Awareness & Training (CSAT) Warehouse at http://energy.gov/cio/training/cybersecurity-awareness-training-warehouse.

Cybersecurity Online Learning Center (COL)

The Cybersecurity Online Learning (COL) is a free web based, online learning program offered by the Department of State (DoS) to anyone (Federal employee and contractors) with a .mil or .gov email address and Adobe Connect software. To register for a workshop or review the workshop list, visit https://colcqpub1.connectsolutions.com/content/connect/c1/7/en/events/catalog.html. Additional information is available on Powerpedia, search ***cybersecurity***.

Books 24x7

The Office of Human Capital (HC) has just launched Books24x7 for DOE Federal Employees. It is a free online resource providing access to electronic books covering technical and business topics, including cybersecurity. Books24x7 offers on-demand, instant access to text of thousands of best-in-class online books, book summaries, audiobooks, research reports and best practices. Books24x7 has been added to Federal users' Online Learning Center (OLC) learning plans as "Books24x7 Referenceware" or by searching Books24x7 on Powerpedia

Cybersecurity Resources:

CDC Website - http://www.stopbullying.gov/ features several articles on awareness of cyber bullying and ways of preventing bullying before it starts.

Cybersecurity Online Learning Program (COL) - https://colcqpub1.connectsolutions.com/content/connect/c1/7/en/events/catalog.html. Attendance can be used for CPE credit.

***Updated*:** http://niccs.us-cert.gov/home/cybersecurity-education-and-training-catalog-update Cybersecurity Education and Training Catalog

UPCOMING EVENTS:

2015 Cybersecurity Conference

It's back! The OCIO is pleased to announce the return of the DOE Cybersecurity Training Conference. The conference is a good opportunity for networking and learning from today's cyber professionals. Watch for additional details.

2015 OCIO Cybersecurity Achievement Awards

Requests for nominations for the 2015 Cybersecurity Achievement Awards will be distributed in November 2014. Program Information can be found by searching cybersecurity on Powerpedia.

*For questions regarding these articles or any Cybersecurity issue, search **cybersecurity** on Powerpedia or send an e-mail to cybsectrn@hq.doe.gov.*