NASCIO 2015

STATE CYBERSECURITY RESOURCE GUIDE

AWARENESS, EDUCATION AND TRAINING INITIATIVES

Securing Government in a Digital World

Background

In support of the 12th annual National Cybersecurity Awareness Month, the National Association of State Chief Information Officers (NASCIO) has partnered with the Department of Homeland Security's Office of Cybersecurity and Communications, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the National Cybersecurity Alliance (NCSA), to promote government's commitment to securing cyberspace and protecting the citizens who rely on Internet technologies in their daily activities.

Each of these organizations has developed extensive security awareness resources and toolkits that are available through their websites, and links to those and other resources are provided on NASCIO's Cybersecurity Awareness page.

State CIOs and the programs they administer have supported cybersecurity awareness month from its inception, and states address IT security and privacy awareness, education, and training on a year-round basis.

For the 2015 observance, NASCIO has updated its Resource Guide for State Cybersecurity Awareness, Education, and Training Initiatives. The guide includes new information from our state members, who provided examples of state awareness programs and initiatives. This is an additional resource of best-practice information, together with an interactive state map to allow users to drill-down to the actual resources that states have developed or are using to promote cyber awareness. It includes contact information for the CISO, hyperlinks to state security and security awareness pages, and information describing cybersecurity awareness, training, and education initiatives.

The Resource Guide is a modifiable work that should provide a valuable reference resource for Cybersecurity Awareness Month, as well as the ongoing planning of security awareness and training efforts state programs may undertake thereafter.

NASCIO
2015 National Cybersecurity Awareness Month Champions
Password:
*****
CHAMPION
National Cyber Security Awareness Month

Table of Contents

Alabama 1
Alaska 2
Arizona 3
Arkansas 4
California 5
Colorado 6
Connecticut 7
Delaware 8
Florida 10
Georgia 11
Hawai'i 12
Idaho 13
Illinois 14
Indiana 15
Iowa 16
Kansas 17
Kentucky 18
Louisiana 19
Maine 20
Maryland 21
Massachusetts 22
Michigan 23
Minnesota 24
Mississippi 26
Missouri 27
Montana 28
Nebraska 29
Nevada 30
New Hampshire 31
New Jersey 32
New Mexico 33
New York 34
North Carolina 35
North Dakota 36
Ohio 37
Oklahoma 38
Oregon 46
Pennsylvania 47
Rhode Island 49
South Carolina 50
South Dakota 51
Tennessee 52
Texas 53
U.S. Virgin Islands 54
Utah 55
Vermont 56
Virginia 57
Washington 59
West Virginia 60
Wisconsin 62
Wyoming 63

Alabama

Alabama CISO: Brad Bird; brad.Bird@isd.alabama.gov; 334.353.3373
Alabama Cybersecurity Webpage: www.cybersecurity.alabama.gov

Alabama's focus on Cybersecurity can be seen in several initiatives this year:

- Development of Statewide Security Program Management Plan
    - Focus on Policy and Standards alignment with NIST RMF
    - Establishment of centralized Governance, Risk, and Compliance management
    - Establishment of centralized Plan of Action and Milestones
- Expansion of Awareness & Training initiative
    - End User Security Awareness training
    - Specialized Role based Security Training
- Expansion of Incident Response capability
    - Event and Incident Correlation
    - Event and Incident Management

Alabama is working to mature security at all levels within the state: security program, personnel, systems, agencies, etc. Also, Alabama plans to widen communication channels with internal and external entities (i.e. Alabama Fusion Center, etc.) in order to broaden the information and intelligence sharing that goes on in Alabama state government.

Alaska

Alaska CISO: Chris Letterman; Chris.Letterman@alaska.gov
Alaska Cybersecurity Operations: Jay Druyvestein; Jay.Druyvestein@alaska.gov
Alaska Security Awareness Webpage: security.alaska.gov/SA_Bulletins/index.html
State Security Office: security.alaska.gov/
SOA Security Training: security.alaska.gov/training/index.html

- Cybersecurity Awareness and Training Resources and Initiatives for 2015:
- Governor Bill Walker will be approached to issue a Proclamation of October 2015 as Cyber Security Awareness Month. Alaska's Governors have shown support for Cybersecurity by issuing this proclamation annually.
- Alaska's Security Office and Enterprise Technology Services will take steps in observance of National Cyber Security Awareness Month by hosting contact events throughout the month of October addressing information security topics. In addition to focusing on managers and security practioners, a new Cybersecurity Awareness Training curriculum is planned for launch during October with the objective of advancing cyber-safety skills of our end users. This is the state's first step to mandatory Cybersecurity Training for all Executive Branch employees.
- October is the target month for completion and release of its internal security policy refresh which will largely incorporate the NIST Cybersecurity Framework. Begun in March 2015, the effort was a collaborative project between Alaska's Security Office and several agency representatives who served on the review committee.
- The MS-ISAC Cybersecurity toolkit materials will be distributed throughout state government offices during the month of October.

Arizona

Arizona CISO: Mike Lettman; mike.lettman@azdoa.gov; 602.542.0030
Arizona CPO: Darrell Davis; Darrell.davis@azdoa.gov; 602.542.5409
Arizona Cybersecurity Awareness Coordinator: Ed Yeargain; ed.yeargain@azdoa.gov; 602.542.1837

The state of Arizona will be hosting the following events for National Cybersecurity Awareness Month:

- Cybersecurity Presentations available to the Agencies during October
- Agencies conducting CBT cyber awareness training during October
- Creating Cybersecurity Awareness webpage for Agencies, business and citizens
- Information Security Policy awareness training
- Distribution of MS-ISAC cybersecurity awareness toolkit
- Conducting Kids Cyber Awareness Poster contest for K – 12 during October/November
- Begin new marketing campaign for Cybersecurity Awareness
- Conduct an Industrial Control System (ICS) Cyber Exercise for public and private partners
- Conduct lunch and learns at agencies on different days
- Conduct a half day cyber awareness seminar for State Employees to attend

Arkansas

Arkansas CISO: Frank Andrews; franklin.andrews@arkansas.gov
Arkansas IT Security Homepage: www.dis.arkansas.gov/security/Pages/default.aspx
Arkansas Cybersecurity Toolkit: www.dis.arkansas.gov/security/Pages/CyberSecurityToolkit.aspx

Arkansas has several activities planned in preparation of National Cyber Security Awareness Month:

- Kick off for new monthly online cybersecurity training
- Handing out cybersecurity educational materials
- Governor’s Proclamation for National Cybersecurity Awareness Week

California

California CISO: Michele Robinson; Michele.Robinson@state.ca.gov ; 916.445.5239
California Information Security Office: www.infosecurity.ca.gov
California Cybersecurity Symposium: www.pspinfo.us/psp-events/css2015
California Security Awareness Webpage: www.cio.ca.gov/OIS/Government/library/default.asp
California Department of Justice, Office of the Attorney General, Privacy Enforcement and Protection Unit: www.privacy.ca.gov/

Colorado

Colorado CISO: Deborah Blyth; deborah.blyth@state.co.us
Office of Information Security website URL:
www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1249667675596
Cybersecurity Awareness Resources:
www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408776
Information Security Toolkit:
www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408811

The State of Colorado will be hosting the following events for National Cybersecurity Awareness Month:

- CyberGirlz: Regis University will be conducting workshops to prepare middle-school and high-school girls for careers in cybersecurity, during the months of September and October – this program is called CyberGirlz, and will culminate in a cyber event on October 24. The Governor's Office of Information Technology (OIT) will be providing mentors and coaches during the weekly training workshops and the October 24 event.
- School Security Presentations: We will be conducting presentations at various middle schools throughout the month of October and ongoing throughout the year. These presentations will be intended to help middle school students understand risks related to the use of social media, while providing guidance on how to use social media safely and securely.
- Daily Security Tips: We will utilize Twitter to tweet various security tips throughout the month of October. Our hashtag will be: #cocyberhelp

Security Videos: We will be creating and featuring 2 Security videos on our State of Colorado website: www.colorado.gov/oit/cyber. We will also be promoting the Stop.Think.Connect website.
Employee Security Awareness: We will be kicking-off our annual Security Awareness training for all state employees, and we will be utilizing posters to remind employees to take the training.
Governor's Proclamation: Lastly, the Governor of the State of Colorado is expected to issue a proclamation declaring October to be Cyber Security Awareness Month in the State of Colorado.

Connecticut

Connecticut CISO: David Geick; david.geick@ct.gov
CT DAS/Bureau of Enterprise Systems and Technology:
www.ct.gov/best/site/default.asp
CT Cybersecurity Awareness Webpage:
www.ct.gov/doitservices/cwp/view.asp?a=4063&Q=476440&doitservicesNav=|
CT Cyber Safe:
www.ct.gov/doitservices/cwp/view.asp?a=4063&Q=476440&doitservicesNav=|

For National Cyber Security Awareness Month, the State of Connecticut will be conducting SANS Awareness Training for state employees.

Delaware

Delaware CSO: Elayne Starkey; elayne.starkey@state.de.us; 302.739.9631
Delaware Security Home Page: dti.delaware.gov/information/cybersecurity.shtml

2015 National Cyber Security Awareness Month Delaware Campaign:

- Information Security 101 Training
    - When: October, 2015 Office of Management & Budget
- State of Delaware CISSP Boot Camp
    - When: November 2, 2015 through November 6, 2015
    - Target audience—ISOs, IRMs, Systems Administrators, and Web Developers, DTI employees, other IT staff from State organizations. (Class size is limited to 20 attendees)
- Elementary School Internet Safety Presentations
    - When: October 1, 2015 – December 13, 2015
    - Target Audience: 7,000 Delaware 4th grade students
    - Will promote a 4th & 5th grade poster contest which will run outside of this project's timeline
- National Cybersecurity Poster Contest
    - When: Delaware contest October 1, 2015 – December 15, 2015
    - Target Audience: Delaware 4th & 5th grade students
    - Publish Delaware-specific calendar using 2014 winning posters
- Statewide Cybersecurity Exercise
    - When: October 27, 2015
    - Venue: Remote Exercise
    - Target Audience: State Agency and School District IT Staff, Executive Leadership, Management, and Public Information Officers; and Community Partners
- Statewide Cybersecurity Workshop
    - When: September 29, 2015
    - Venue: Rollins Conference Center, Dover, DE
    - Target Audience: State Employees, Higher Education, Small Business Community, Armed Forces, Public
- State and Local Cybersecurity Proclamation Adoption
    - Governor of Delaware signing proclamation for Cybersecurity Awareness
    - Various municipalities signing proclamations for their jurisdiction

- Information Security Officer Meeting
    - When: September 23, 1:00 – 4:00pm
    - Venue: Polytech Conference Center
    - Target Audience: Information Security Officers for all state agencies and school districts
- Marketing Campaign
    - Awareness advertising to potentially include: News Journal post it note, PR items or news column, promotional items pending sponsorship
    - Continuation of social media with goal of at daily tweets, targeted Face Book ads, and an awareness campaign with targeted participation by local elected officials
- Internal Awareness Campaign (DTI only)
    - "Thank you Thursdays" email campaign. Example – "Thanks for not sharing your password…ever."
    - Cybersecurity Scavenger Hunt – Employees search on internal SharePoint site for clues related to each department's role in security

Florida

Florida CISO: Danielle Alvarez; danielle.alvarez@ast.myflorida.com; 850.412.6049
Agency for Enterprise Information Technology, Office of Information Security:
www.secureflorida.org/

Georgia

Georgia CISO: Mark Reardon; mark.reardon@gta.ga.gov
Georgia Technology Authority – Office of Information Security Website: gta.georgia.gov/

The State of Georgia has the following planned for National Cyber Security Awareness Month:

- Governor's Proclamation for National Cybersecurity Awareness Week. Governor Deal to sign official proclamation recognizing October as Cyber Security Awareness Month in Georgia
- In collaboration with GEMA, a tool kit from the STOP.THINK.CONNECT campaign will be sent to all state agencies in October
- Cybersecurity awareness materials will be distributed to State agency information security officers for distribution to state employees
- Promote cybersecurity awareness throughout State Government by sending a Cyber Security Awareness Month announcement email to state employees
- Daily Security Tips: We will utilize Twitter to tweet various security tips throughout the month of October

Hawai'i

Hawai'i Acting CISO, IT Development Officer:
Michael E. Otsuji; michael.e.otsuji@hawaii.gov
Cybersecurity Website: ags.hawaii.gov/icsd/cyber-security/
State Cybersecurity Resources:
ags.hawaii.gov/icsd/cyber-security/cyber-security-resources/
State Cybersecurity Toolkit: ags.hawaii.gov/icsd/cyber-security/cyber-security-toolkit/

Recent Updates:
In April 2015, Gov. David Y. Ige appointed Todd Nacapuy as the State of Hawaii's Chief Information Officer, leading the Office of Information Management and Technology (OIMT) and overseeing the Information and Communication Services Division (ICSD) of the Department of Accounting and General Services. Nacapuy was confirmed by the State Senate on April 22 and formally stepped into the role on May 4. He has since identified security as his top priority.

Several advancements have been made in recent years to improve Hawaii's cybersecurity posture and ensure protection of valuable information and data assets. In fiscal years 2014-2015, OIMT:

- Established the state's first Security Operations Center (SOC), which conducts continuous monitoring and response to cyber threats to departments and agencies. The state also aligned its cybersecurity approach with the National Cybersecurity Framework.
- Implemented an enterprise-wide Incident Response (IR) program with numerous critical components necessary to properly respond to all natural hazard and cyber threats. This initiative has placed processes, procedures, reporting, and a highly structured workflow around this essential function. As IR is the first line of response to a cyber threat, adopting a proven and organized approach is critical.
- Formed a partnership with the U.S. Department of Homeland Security's Cyber Hygiene program, which provides network vulnerability scanning of external-facing public IP addresses to help the state understand how it appears to attackers on the Internet.
- Deployed additional security tools to increase protection against network-based threats.

October 2015 Activities:

- Governor Ige will proclaim October "Cyber Security Awareness Month" in Hawai'i.
- OIMT and ICSD, under the leadership of the State Chief Information Officer, will launch an educational campaign among State of Hawai'i employees and citizens on the topic of cybersecurity to promote best practices.

Idaho

Idaho CISO: Thomas Olmstead; thomas.olmstead@cio.idaho.gov; 208.332.1951
Idaho Cybersecurity Awareness Website: cybersecurity.idaho.gov/
Idaho Cybersecurity Identity Theft Prevention Website: cybersecurity.idaho.gov/identity_theft.html

Promotion of National Cybersecurity Awareness Month

- Notify state agencies that the NCSM toolkit is available for download
- Conduct cybersecurity workshops with state agencies and universities
- Participate in the Idaho Cybersecurity Interdependence workshop, October 8, 2015

Illinois

Illinois CISO: Kirk Lonbom; kirk.lonbom@illinois.gov 217.557.0429
Illinois Bureau of Communication and Computer Services Security Awareness Webpage:
www.illinois.gov/bccs/services/catalog/security/assessments/Pages/default.aspx
Illinois Bureau of Communication and Computer Services Disaster Recovery Webpage:
www.illinois.gov/bccs/services/catalog/security/DRS/Pages/default.aspx
Ready Illinois Web Page
http://www.illinois.gov/ready/Pages/default.aspx

Illinois Cybersecurity Awareness plan includes:

- Expansion of online cybersecurity training for state employees
- Statewide distribution of Cybersecurity awareness materials to more than 100 Agencies, Boards and Commissions
- Weekly topics throughout the month to state employees and the general public via the Ready.Illinois website
- Online access to the Cybersecurity Awareness Toolkit for Statewide usage

Indiana

Indiana CISO: Tad Stahl; tstahl@iot.IN.gov
Indiana Office of Technology Security Website: www.in.gov/iot/2284.htm

The State of Indiana will be hosting the following events for National Cybersecurity Awareness Month:

- Launch of the Indiana Information Security and Analysis Center SOC
- Governor's Proclamation of Cybersecurity Week for a yet to be determined week
- Distribution of MS-ISAC Cybersecurity Tool Kit to agencies
- Enterprise wide distribution of cybersecurity awareness messages (various topics and timing throughout the month)

Iowa

Iowa Deputy CIO & CISO: Jeff Franklin; jeff.franklin@iowa.gov; 515.281.4820
Iowa Information Security Office Website: secureonline.iowa.gov/
Iowa ISO Security Awareness & Training Webpage:
secureonline.iowa.gov/security-awareness-training
Cyber Iowa: secureonline.iowa.gov/cyber-iowa

Our vision is to lead state government in protecting information technology resources and data and our mission is to promote the secure use of information technology resources and effectively manage the associated risks.

How we promote cybersecurity awareness during October:

- Governor's Proclamation for Cyber Security Awareness Month
- Cybersecurity Awareness announcement sent to all state employees
- Engage state agencies during the month of October to promote Cybersecurity Awareness through:
    - Web based security training to state and local governments
    - Distribution of a variety of cybersecurity awareness materials across state, county and city governments, schools, community colleges, libraries and the public
    - Host special events such as secure media disposal, awareness booths, and cybersecurity speakers

The remaining months of the year, we actively promote cybersecurity awareness through:

- Implementation of enterprise security initiatives; some of which include, Anti-Malware, Vulnerability Management, SIEM, Configuration and Patch Management
- Presentations to agencies and agency directors providing education on current threats and protection
- Security partnerships and collaboration with Iowa counties, schools, and city government
- Promotion and sponsorship of public/private cyber events

Kansas

Kansas Deputy CISO: Robert Vaile; Robert.vaile@ks.gov; 785.296.8434
Kansas Information Technology Security Council (ITSC) Webpage:
oits.ks.gov/kito/it-security-council
Cybersecurity Awareness Training Resources:
oits.ks.gov/info-security/awareness-training

Kentucky

Kentucky CISO: Katrina LeMay; Katrina.lemay@ky.gov; 502.564.6361
Kentucky Commonwealth Office of Technology Website: technology.ky.gov
Kentucky Office of CISO: technology.ky.gov/ciso
Kentucky Security Services: technology.ky.gov/services/Pages/SecurityServices.aspx
Security Awareness Page (includes video): technology.ky.gov/ciso/Pages/CyberSecurity.aspx

Kentucky's Cybersecurity Awareness and Training Resources and Initiatives for 2015:

- Governor Steve Beshear will be approached to issue a Proclamation of October 2015 as Cybersecurity Awareness Month. He has issued this proclamation annually since holding the office of Governor.

- Kentucky's Commonwealth Office of Technology (COT) observes National Cybersecurity Awareness Month annually by hosting seminars for state government staff during the month of October. The focus for 2015 will be to provide practical security guidelines for protection of personal information.

- The MS-ISAC Cybersecurity toolkit materials will be distributed throughout state government offices.

- Kentucky has made significant progress in implementation of NIST standards including the addition of mandatory security awareness and compliance-focused training for staff. Office of the CISO security staff members have individual plans for their continuing education which begin with a basic security course and certification.

- COT Office of the CISO has provided a security awareness video for use by all of state government. The video is available on the COT website as well as Kentucky Personnel Cabinet's website.

- COT reaches out to schools through the Kentucky Department of Education to encourage involvement in the MS-ISAC Annual K-12 National Poster Contest.

Louisiana

Louisiana CISO: Dustin Glover; dustin.glover@la.gov; 225.773.6719
Louisiana IT Security Home Page: doa.louisiana.gov/oit/IT_Security_Index.htm

Maine

Maine Enterprise Architecture, Security & Policy: B. Victor Chakravarty;
Victor.Chakravarty@Maine.Gov
Maine Security Site: maine.gov/oit/security/

Maine has consolidated I.T. throughout the Executive Branch in the Office of Information Technology (OIT). OIT Security is a ten-person team, spanning devices, apps, physical access, and hardened perimeter. Strong security can be accomplished only by baking security into the architecture (as opposed to bolting it on post-fact), and enforcing it through policy. Therefore, OIT Security rolls up to a consolidated Architecture-Security-Policy unit, which reports to the CIO.

No asset, either hardware or software, is deployed into production without security certification. All information assets undergo periodic vulnerability scans, and remediation. There exists a strict policy regime, with exceptions granted only through a CIO waiver. OIT Security does regular outreach to Agency Commissioners and the Governor’s Office. There exists an aggressive user education program, with mandated annual re-certification. Instituted Cyber Liability Insurance for both on-premises hosting as well as remote/cloud hosting. The perimeter monitoring is provided by Federal Homeland Security. We have also established an active cybersecurity collaboration with Homeland Security, the National Guard, Emergency Management, the University of Maine, and local industries.

Upcoming Initiatives:

- Incident Response Exercises
- Log Analysis
- Automated Intrusion Detection & Protection

Maryland

Maryland Cybersecurity Webpage: doit.maryland.gov/support/pages/securityservices.aspx
Maryland Cybersecurity Resource Center: doit.maryland.gov/cybersecurity/Pages/default.aspx
Maryland Governor's Cybersecurity Dashboard:
doit.maryland.gov/cybersecurity/Documents/Gov_cybersecurity_dashboard.pdf
Maryland Cybersecurity Law (enacted July, 2014):
mgaleg.maryland.gov/2013RS/Chapters_noln/CH_304_sb0676t.pdf
Maryland Cybersecurity Multimedia Center:
doit.maryland.gov/cybersecurity/pages/multimedia.aspx
Maryland Commission on Cybersecurity Innovation and Excellence: umuc.edu/legal/cyber
Maryland Cybersecurity Center (MC2), University of Maryland: cyber.umd.edu/education
University of Maryland (Baltimore County) Center for Cybersecurity: cybersecurity.umbc.edu

Massachusetts

Massachusetts CSO: Kevin Burns; kevin.burns@state.ma.us; 617.619.5696
Massachusetts Cybersecurity Website: www.mass.gov/cybersecurity
Massachusetts Cybersecurity Twitter Account: @MassCyberAlerts

The mission of the Security Office, in close collaboration with the Enterprise Security Board, is to ensure the security of the Commonwealth's information technology enabled service delivery systems by constantly assessing and improving upon our cyber education & awareness, vulnerability prevention, and exploit detection & response capabilities.

The Commonwealth of Massachusetts is planning the following National Cyber Security Awareness Month activities:

- Cybersecurity Awareness Day event for State Agencies, Cities, Towns, and schools at the State House on October 7
- Continue distributing cybersecurity awareness tips via email
- Governor sign proclamation declaring October Cyber Security Awareness Month
- Distribute cybersecurity awareness materials to State Agencies, Cities, Towns and Schools
- Publicize Cyber Security Awareness Month on highway billboards

Michigan

Michigan CSO: Christian Kopacsi; kopacsic@michigan.gov
Michigan Department of Technology, Management & Budget (DTMB)
Cybersecurity Homepage: www.michigan.gov/cybersecurity
Cybersecurity Awareness Month Toolkit:
www.michigan.gov/cybersecurity/0,4557,7-217-51788---,00.html
Michigan DTMB – Internet Security for Citizens and Government – Video Resources: www.michigan.gov/cybersecurity/0,4557,7-217-52357_51219---,00.html
Michigan DTMB – Michigan Online Security Training (MOST) Webpage: www.mi.gov/cybersecurity/0,4557,7-217-51788-192552--,00.html
Michigan Cyber Disruption Response Strategy: www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf

Michigan has recently raised awareness and conducted several exercises related to cybersecurity in 2015:

Leading up to National Cybersecurity Awareness Month, Michigan published the Michigan Cyber Initiative 2015 outlining the State’s cybersecurity goals and objectives from 2015 through 2018. Additionally, Michigan held a number of highly-successful cyber exercises in Lansing and Grand Rapids with participants from the State of Michigan, Michigan Cyber Range, Cyber Civilian Corps, Western Michigan Cybersecurity Consortium, and private industry. Michigan will conclude Cyber Security Awareness Month with the North American International Cyber Summit at Cobo Center in Detroit, MI.

Minnesota

Minnesota CISO: Chris Buse; Chris.Buse@state.mn.us
Minnesota Office of Enterprise Technology – Cybersecurity Awareness Website:
mn.gov/oet/programs/security/
Minnesota Office of Enterprise Technology – Cybersecurity Toolkit:
mn.gov/oet/programs/security/security-res/

Minnesota has several activities planned in preparation of National Cyber Security Awareness Month:

- Minnesota, along with the MS ISAC, has requested that Governor Dayton declare October Cyber Security Awareness Month. Minnesota has successfully obtained a declaration for the past 9 years.
- In Minnesota we plan to have weekly email messages go out to staff about cybersecurity topics and we will post helpful awareness tips on our Facebook and Twitter pages.
    - www.facebook.com/MN.ITServices
    - twitter.com/MNIT_Services
- We have planned several public forums for our staff and the general public. Visitors will be able to have a conversation with security professionals and use some the hands on tools available. Minnesota's security team will be going out to various government agencies across the state to reach as many of our 33,000 state employees as possible. The events are planned for Minnesota state employees and in some locations they do serve the state's general public as well. The security awareness events will include a display booth with the following types of materials:
    - Promote and explain the new Enterprise Security Policies and Standards
    - Printed materials on cybersecurity
    - Visuals to reinforce best practices for an individual work space security
    - Computers for visitors to check their password strength
    - Cybersecurity video modules
    - Promote our updated annual security awareness training
- On October 20 & 21 the Cybersecurity Summit will be held at Minneapolis Marriott Northwest in Minneapolis, MN: www.cybersecuritysummit.org/
    - MN.IT Services is a supporting partner of the Summit
    - Chris Buse, State CISO, serves on the Advisory Board for the Summit

- The Summit's mission is to establish a multi-stakeholder consortium that brings together industry, government and academic interests in an effort to improve the state of cybersecurity on both a domestic and international level. We believe that cybersecurity cannot be contained and outsourced to any one sector. Due to the vast scope of cyber threats, it requires active engagement of all stakeholders, including entities and organizations – large and small - across every industry.
- Finally, in October the state will once again participate in the Kids Safe Online poster contest as part of the larger national program sponsored by the MS ISAC. The contest is open to all public, private or home-schooled students in Kindergarten – 12th grade. MN.IT Services has sponsored the contest for the past 6 years. The primary emphasis of the contest is to raise awareness of cyber issues for our student population. As student utilize technology and mobile devices more and more, in school and socially, the risks increase. The contest strives to educate students about safe use of technology, curb cyber bullying and raise awareness about cybersecurity.

Mississippi

Mississippi CISO: Jay White; jay.white@its.ms.gov
Mississippi Department of Information Technology Services: www.its.ms.gov/security/

Tentative plans for October:

- Work with the Governor's Office to get the Governor to sign a proclamation proclaiming October 2015 as National Cybersecurity Awareness Month.
- Create an October Security Awareness Month web page which will be featured on the ITS website. The awareness month web page will contain security awareness information and promotion information for National Cyber Security events.
- Promote the MS-ISAC 2016 Kids Safe Online Poster Contest that is designed to increase the cybersecurity awareness of children across the state. All public, private or homeschooled students in Kindergarten - 12th grades in Mississippi are eligible to participate in the contest. The winning posters from the Mississippi contest will be entered in the national contest sponsored by the Multi-State Information Sharing and Analysis Center (MS-ISAC) division of CIS.
- Promote cybersecurity awareness throughout State Government by creating a messaging campaign of cybersecurity-themed information. Cyber awareness information will be distributed to the security contacts at each agency throughout the month and the security contacts will be encouraged to spread the information to all employees of their respective agency.
- Cybersecurity awareness information (MS-ISAC toolkit, posters, calendars, bookmarks,etc.) will be provided to state agencies.
- ITS will partner with the MS Office of Homeland Security and the Office of the State Auditor to host a Cybersecurity Summit on October 8. Recognizing that October is National Cyber Security Awareness Month, this Summit will focus on current cybersecurity challenges facing state, local governments, and educational institutions.

Missouri

Missouri CISO: Michael Roling; michael.roling@oa.mo.gov
Missouri Cybersecurity Awareness Website: www.cybersecurity.mo.gov/
Missouri Cybersecurity Portal: portal.cybersecurity.mo.gov
Missouri Cybersecurity Tools: cybersecurity.mo.gov/tools/
Internet Safety section on MO.gov: www.mo.gov/safety/internet-safety/
Missouri Cybersecurity Blog: cybersecurity.mo.gov/blog/
Missouri Cybersecurity Twitter Account: @mocybersecurity
Missouri Cybersecurity Facebook Page:
www.facebook.com/pages/Missouri-Cyber-Security/140114041959

The State of Missouri has the following planned for National Cyber Security Awareness Month:

- The Governor will declare October to be Cyber Security Awareness Month in Missouri in an official proclamation
- Cybersecurity training will be provided to all state employees during the month of October.
- Employee awareness will be assessed through exercises
- Computer security tips will be emailed to all state employees
- 31 Days of Cybersecurity
    - Utilizing social media and our website, tips will be shared online
- Approved banners, posters, and other educational material will be made available to state employees

Montana

Montana CISO: Lynne Pizzini; lpizzini@mt.gov
Montana Information Technology Services Division Webpage: sitsd.mt.gov/
Montana Information Systems Security Office Webpage: sitsd.mt.gov/MontanaInformationSecurity
Montana Information Security Advisory Council Webpage (MT-ISAC): sitsd.mt.gov/Governance/ISAC

Cybersecurity awareness plans:

- By Governor Bullock's executive order the Montana Information Security Advisory Council (MT-ISAC) was created in August, 2015. The Montana CISO and the Enterprise Security Program will be working with the MT-ISAC to promote information security awareness throughout Montana's state and local governments and the university system.
- Work with Governor's office to have him sign a proclamation in support of National Cyber Security Awareness Month.
- By Governor's proclamation all State of Montana employees will be required to take SANS Securing the Human awareness training. Agencies can begin this training in September 2015.
- Promote National Cyber Security Awareness month by keeping the new Information Systems Security Office Website fresh with information about current information security threats, security awareness events conducted by the Enterprise Security Program, cybersecurity tips and resources, and information about professional information security training through local vendors and reputable online providers.
- Hold four events during the month of October with educational activities, handouts, prizes, promotional items, and treats. The theme for National Cyber Security Month 2015 will be "Stay Safe on the Information Highway". Additional events will be held every month through September 2016.
- Distribute monthly posters using the 2015 theme throughout state buildings and make these posters also available to other agencies for use in their locations.
- Distribute a monthly security newsletter and materials to the security officers in all state agencies, as well as to county and city security contacts. Each monthly communication will focus on an area of information security with activities, educational materials, and posters for use by the security contacts in their organizations.
- Promote the Multi-State Information Sharing and Analysis Center (MS-ISAC) K-12 Computer Safety Poster Contest.
- Conduct eight security-related sessions at the 2015 Montana Information Technology Conference December 7-11, 2015. Facilitate a cybersecurity tabletop exercise at the conference in addition to the educational sessions. The Information Systems Security Office will also have a booth at the vendor showcase with informational handouts.

Nebraska

Nebraska CISO: Chris Hobbs; chris.hobbs@nebraska.gov
Nebraska Cybersecurity Homepage: www.cio.nebraska.gov/cyber-sec/index.html

Nevada

Nevada Dept. of Information Technology – Office of Information Security Webpage:
it.nv.gov/Security-Home/

New Hampshire

DoIT CISO: Leslie Williams; leslie.williams@doit.nh.gov; 603.223.5752
DoIT Commissioner and CIO:
Denis Goulet; denis.goulet@doit.nh.gov; 603.223.5703
Public Cybersecurity Webpage: www.nh.gov/doit/cybersecurity/
NH Department of Information Technology Webpage: www.nh.gov/doit/

The New Hampshire Department of Information Technology (DoIT) formed a Cybersecurity Advisory Committee (CAC) in 2011 to improve cybersecurity across state government and its stakeholders by promoting information-sharing and awareness; consistent application of policies, procedure and standards; collaborative partnerships; and consensus building for enterprise initiatives. The committee Chair is the DoIT Chief Information Security Officer (CISO); members include agency Information Security Officers (ISO) and representatives from Emergency Management (EM) including the NH National Guard and Law Enforcement (LE). The CAC's mission is to improve cybersecurity across state government by strengthening the business, IT, EM and LE partnerships required to collectively address cybersecurity.

As part of the National Cyber Security Awareness Month, the New Hampshire Department of Information Technology will:

- Coordinate with the Governor's Office to have a Cybersecurity Awareness Proclamation issued
- Distribute the Center for Internet Security, Multi-State Information Sharing and Analysis Toolkit materials for display and dissemination in state agencies and schools
- Send a Cyber Security Awareness Month message to DoIT IT Leaders and Agency ISOs for distribution to state employees
- Conduct a special CAC session for Toolkit material review/pickup and interactive discussions on cybersecurity topics
- Post cyber awareness notifications and Toolkit materials/links on the NH public-facing and Agency Intranet Cybersecurity webpages
- Provide Cyber Security Awareness Month information to the NH Information Sharing and Analysis Center (IAC) for inclusion in their bi-weekly All Hazards Digest
- Display the signed proclamation and Toolkit material samples at DoIT headquarters

New Jersey

New Jersey CISO: John Essner; John.Essner@oit.nj.gov
New Jersey Office of Information Technology: nj.gov/it
New Jersey Office of Homeland Security and Preparedness: njhomelandsecurity.gov
New Jersey Cybersecurity & Communications Integration Cell (NJCCIC): cyber.nj.gov
New Jersey Security Awareness: cyber.nj.gov/citizens
New Jersey Resources: cyber.nj.gov/resources

12th Annual National Cybersecurity Awareness Month, October 2015:

During the month of October, the public sector and the State of New Jersey will highlight the importance of cybersecurity preparedness. Each state and local government will plan to get the word out to the citizens, businesses, government and schools that in a digital age we are all connected, the actions of one can impact many. It is important they understand their role in securing cyber space.

This campaign will not just be limited to state and local government; it will be a collective effort among the Multi-State Information Sharing and Analysis Center (MS-ISAC), the U.S. Department of Homeland Security's National Cyber Security Division, the National Cyber Security Alliance, the National Association of State Chief Information Officers (NASCIO) and other public and private sector organizations.

Governor Chris Christie's Proclamation - every governor in the nation endorses Cybersecurity Awareness Month through the issuance of a proclamation or letter of support. Such recognition at the highest levels of state government is an important component in ensuring all Americans have the opportunity to learn more about cybersecurity and how to safeguard themselves from cyber-based threats. For the past few years, all 50 governors signed a proclamation or letter of support; the Governor and Lieutenant Governor will sign the proclamation and present it on the State's one-stop website for cybersecurity.

State of New Jersey's Website – spotlight section highlighting Cybersecurity Awareness Month. The link in the spotlight is directed to cyber.nj.gov. The website is branded, managed and operated by the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC.) The NJCCIC is the State's one-stop shop for cybersecurity information sharing, threat analysis, and incident reporting.

Cybersecurity Seminar - the State of New Jersey Office of Homeland Security and Preparedness, the Office of Information Technology, and the Regional Operations and Intelligence Center plan to have a ½ day seminar about cybersecurity threats and best practice. The seminar will be open to NJCCIC members.

New Mexico

New Mexico Security Contact: Darryl Ackley (CIO); darryl.ackley@nm.us; 505.827.0016
New Mexico Dept. of Information Technology Webpage: www.doit.state.nm.us/
New Mexico Dept. of Information Technology Office of Security:
www.doit.state.nm.us/securityoffice.html

New York

Office of Information Technology Services, CIO: Maggie Miller
Enterprise Information Security Office, Acting CISO: Peter Bloniarz; eiso@its.ny.gov
NYS Enterprise Information Security Office: www.its.ny.gov/eiso
Cybersecurity Awareness Resources: www.its.ny.gov/awarenesstrainingevents
Cybersecurity for Kids: www.its.ny.gov/keeping-kids-safe
Cybersecurity for Local Government: www.its.ny.gov/local-government
NYS Office of Information Technology Services on Facebook: www.facebook.com/nystatecio
NYS Office of Information Technology Services on Twitter: @NYStateCIO

As part of the 2015 National Cyber Security Awareness Month (NCSAM) this October, the New York State Office of Information Technology Services Enterprise Information Security Office (NYS ITS EISO) will participate in the following activities:

- Work with the Office of the Governor to issue a Cybersecurity Awareness Proclamation
- Develop cybersecurity awareness articles to be published through local government organizations for distribution throughout New York State
- Participate in the United States Department of Homeland Security's (DHS) STOP.THINK. CONNECT. campaign
- Distribute outreach material to schools and clubs for children
- Exhibit and present to various state, local, and education communities
- Distribute the Multi-State Information Sharing and Analysis Center Toolkit to state agencies.
- Post awareness material and the New York State Cybersecurity Awareness Toolkit on the NYS ITS EISO website for citizen download
- Coordinate the 2015-2016 Student Poster contest.
- Send NCSAM announcements to our various distribution lists (e.g., state agencies, local government, schools)
- Post cyber awareness activities and messages on the NYS ITS Facebook and Twitter sites
- Promote state agency and local government participation in the Nationwide Cyber Security Review
- Promote use of DHS grant funding for local government cybersecurity projects

In addition to website posted awareness materials, the NYS ITS EISO website provides newsletters that you can brand, policies that can be used as best practice, booklets to get you started with a cybersecurity program, links to national high school and college cyber security competitions, training opportunities, and information on special events.

North Carolina

North Carolina CISO: Maria Thompson; maria.s.thompson@nc.gov; 919.754.6578
North Carolina State CIO Homepage: it.nc.gov/
North Carolina Enterprise Security and Risk Management Homepage:
it.nc.gov/statewide-resources/cybersecurity-and-risk-management
North Carolina Enterprise Security and Risk Management Awareness and Training Program:
it.nc.gov/statewide-resources/cybersecurity-and-risk-management/cybersecurity-awareness

The State of North Carolina will kick off National Cybersecurity Awareness Month with the Governor of North Carolina's Cybersecurity proclamation. The goal for this year is to focus on strengthening the training and awareness program. In order to do so, North Carolina will be using a multi-phased approach. The initial steps will be to deliver the mandatory annual cyber awareness training/refresher to all authorized state employees via our NC Learning Management System and onsite training for SLTT members. The second phase will include conducting training exercises to validate the effectiveness of the training being provided. During this phase, North Carolina hopes to identify areas of improvement, capture lessons learned and update the State's Cyber Awareness Training Program. The last phase will include outreach to academia that may not have an established program or need assistance in the development of one.

North Dakota

North Dakota Acting CIO: Mike Ressler; mressler@nd.gov
North Dakota Enterprise Information Systems Security Administrator/Architect: Art Bakke; ambakke@nd.gov
North Dakota IT Security Home Page: www.nd.gov/itd/services/it-security/

North Dakota has the following activities planned in preparation of National Cyber Security Awareness Month:

- The Governor will declare October to be Cyber Security Awareness Month in North Dakota in an official proclamation
- Statewide Information Security Awareness Training will be provided to all state employees during the month of October utilizing the SANS Securing the Human computer-based training
- Cybersecurity Toolkit materials provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC) will be distributed to all State agencies
- Messages on pertinent cybersecurity issues will be routinely sent to all state workforce members

Ohio

Ohio CISO: David Brown; david.allen.brown@das.ohio.gov; 614.728.2037
Ohio Chief Privacy Officer: Daren Arnold; chief.privacy.officer@oit.ohio.gov
Ohio IT Security-Privacy Home Page: privacy.ohio.gov/
Ohio Privacy and Security – Education and Awareness Webpage:
privacy.ohio.gov/EducationAwareness.aspx

Awareness activities will begin with a request that the Governor sign a proclamation, officially making October the State's Cyber Security Awareness Month. Following the proclamation signing, the Ohio Department of Administrative Services' Office of Information Technology will sponsor Ohio's annual Cybersecurity Day event on October 15, 2015. The Cybersecurity Day event is held in conjunction with National Cyber Security Awareness Month; and is promoted to state/ local government, and higher education employees to provide no-cost opportunities for lectures, training, and collaboration in the area of cybersecurity.

Ohio uses the SANS Securing the Human (STH) cybersecurity awareness training throughout the year to educate approximately 53,000+ state employees, contractors, temporary personnel and other agents of the State. The training provides extensive security awareness education that targets today's weakest link in enterprise security - the human. STH goes beyond just compliance and addresses the most common risks using a proven framework based on the Twenty Critical Security Controls for Effective Cyber Defense.

Ohio sponsors the State of Ohio's Kids Safe Online poster contest. The contest is part of a national contest held in collaboration with the Multi-State Information Sharing and Analysis Center to promote safe and secure internet usage among young people.

Additionally, Ohio distributes a monthly newsletter containing content from the Multi-State Information Sharing and Analysis Center which covers a wide variety of topics pertinent to the user community. The newsletter highlights many issues that could be important to users, as well as information to help people understand different ways to keep our technology safe from various attacks.

Oklahoma

Oklahoma CISO & CyberCommand Director: Mark Gower; mark.gower@omes.ok.gov
Oklahoma Cybersecurity Webpage: www.ok.gov/homeland/Cyber_Security/index.html

Oklahoma Cybersecurity Initiative - Secure Oklahoma - 2015 National Cyber Security Awareness Month Action Plan

State Goals and Objectives:
The consolidation of the Information Technology infrastructure, data and, computer systems presents unique possibilities and challenges for the State of Oklahoma. As a result of this consolidation effort, a new advanced information ecosystem has developed that requires new approaches to Cybersecurity. This information ecosystem must be secured. State agencies and employees must be made aware of personal accountability and vulnerability when operating in this information ecosystem. Previously, assumption of Cybersecurity risk by an individual agency was under the sole province of that single agency; however, in the consolidated environment, what affects one, impacts all. The decisions and information provided to agency management and Information Technology experts must include processes for Cybersecurity and balance the risks of current business practices with the need for preservation of the Confidentiality, Integrity, and Availability of the systems and data which are integral to agency business functions.

The impact to citizens and the economy of Oklahoma and the nation depend on the Cybersecurity posture of the State's Information Technology infrastructure and computer systems. A poor or mismanaged Cybersecurity posture of a single state agency could compromise the entire State information ecosystem. The threats are very real. Attacks such as malicious code attacks, directed attacks by hackers, and foreign governments, Advanced Persist Threats, criminal enterprise, espionage, and employee misconduct have advanced to the realm of technically proficient attackers and those with the motivation to succeed at all costs.

Cybersecurity is central to the top critical concerns to State, Federal, local government and private businesses. These threats have even been declared by the Whitehouse as "the most serious economic and national security challenges we face." The State of Oklahoma is uniquely positioned to lead the Cybersecurity initiatives for the Public and Private sectors in Oklahoma, bridging the gap between these two sectors to build a better Cybersecurity posture for strength, resiliency, and continuity to the citizens of Oklahoma.

It is the goal of the Oklahoma Cybersecurity Initiative - Secure Oklahoma to participate in the

National Cybersecurity Awareness Campaign. The State of Oklahoma and its citizens are using the internet to conduct business and enrich our daily lives. It is imperative that Cybersecurity awareness be a top priority for the Oklahoma CyberCommand.
There are three main objectives for the 2015 awareness campaign of Oklahoma Cybersecurity Initiative - Secure Oklahoma activities:

1. Develop a State of Oklahoma Cybersecurity awareness campaign
2. Launch cybersecurity.ok.gov with resources for cybersecurity awareness that will evolve to meet the needs of the OCSI "Cyber Portal" goal.
3. Kick off the 12 month cybersecurity awareness campaign for the OCSI, providing a platform and framework for monthly cybersecurity awareness that focuses on citizens and state agencies.

Themes:

- National Theme: #CyberAware
- State of Oklahoma Theme: Secure Oklahoma #SecureOklahoma

Timeframe:

- Preplanning: July 15th through the 30th
- Production and Development: July 15th through September 30th
- Main Campaign Go Live - October 1st through the 31st and monthly goals there-after for 12 months of Cybersecurity awareness programs.

Weekly National and State level Topics:

- October 1-2 -Week 1: General Cybersecurity Awareness: Celebrating 5 Years of Stop.Think. Connect.™
  www.staysafeonline.org/ and www.stopthinkconnect.org/ (National Topic)
  - (State Topic -National Content)Main Topic 1: Keep a Clean Machine and Protect your Personal Information
  - (State Topic -National Content)Main Topic 2: Connect with Care and Be Web Wise
  - (State Topic -National Content)Main Topic 3: Be a Good Online Citizen
- October 5 -9 - Week 2: Creating a Culture of Cybersecurity at Work (National Topic)
  - (State Topic)How cyber threats enter the workplace
  - (State Topic)What should you do to protect your work systems from cyber threats
  - (State Topic)When to report a cybersecurity concern and who to report to

- October 12-16 -Week 3: Connected Communities: Staying Protected While Always Connected (National Topic)
  - (State Topic)The dangers of "Free" Wi-Fi hotspots and how to protect yourself when using them.
  - (State Topic)Social Media and the dangers presented to individuals
  - (State Topic)Mobile Devices and staying safe and secure when using online services and applications
- October 19-23 -Week 4: Your Evolving Digital Life (National Topic)
  - (State Topic)The Internet of Things and protecting devices and your privacy
  - (State Topic)Best practices for personal use of Mobile devices
  - (State Topic)The connected world, the look ahead
- October 26-30 -Week 5: Building the Next Generation of Cyber Professionals (National Topic)
  - (State Topic)The growing demand for cybersecurity skills in the workforce
  - (State Topic)Highlight a Cyber Program at a 2 year Oklahoma College
  - (State Topic)Highlight a Cyber Program at a 4 year Oklahoma University

Program Needs / Plans:

- A new web presence : Cybersecurity.ok.gov
- Plan and provide cybersecurity content development for subject matter per week for the month of October with no more than three main points to circulate during a given week on the current national weekly topical subject.
  - The content to be delivered via a social media campaign, E-Mail Campaign, Website and Public Media.
- Build a PowerPoint Templates with canned Content and speaker notes, that have presentations that correspond to the national weekly topics and the subtopics for Oklahoma found in the Schedule of Activities Section Below.

Social Media Campaign

- Have OMES Communications use the OMES Social Media Presence or create and secure a State Cybersecurity or CISO Twitter Account and HashTags #SecureOklahoma and Facebook presence to provide for the Social Media components that will kick off in October, but have a monthly venue to deliver Cyber Awareness messages to the public and state entities.

Materials

- Obtain the material for posters and flyers for the National Cyber Security Awareness Month campaign to use as materials - will need OMES Print Shop support for a small printing of the materials in the items below - See "Lobby Days"

OMES Office of Communications Support

- OMES Communications / e-Government Create and Roll out the new Oklahoma Cybersecurity Website cybersecurity.ok.gov/ based on the CISO vision and research (research almost done on the type of content and capabilities for the design and building consulting to begin-modeling best of, from other states, cities, and organizations with a Cybersecurity focus) - Cybersecurity.ok.gov - maps back to NIC
- Enroll Oklahoma cybersecurity.ok.gov as a STOP. THINK. CONNECT national Partner. stopthinkconnect.org/get-involved/partner-program/
  - Co-Brand with the NCSAM www.staysafeonline.org/ncsam/get-involved/promote-ncsam
- Consult OMES Communications PIO for a Media Out Reach to provide possible media releases for the Media to carry a one time or weekly story about Cybersecurity Awareness, incorporating subject matter experts from the state, high education institutions, etc.
- OMES Communications support and to identify appropriate venues and mechanisms for communications ideas include:
  - E-mail blasts via GOV Delivery (Timed per week)
    - Also Promote the State Wide Free Training Security Education and Awareness Training Program for SANS Securing the Human - highlight modules and training through simple, quick short messages.
  - Pre-defined and created OMES and a formal CISO Twitter and Facebook Content Delivery (Timed per week with the outlined pre-scripted content).
  - Governor Twitter support and content delivery for citizen focused tips for #CyberAware and #SecureOklahoma
  - Pre-developed Web Content for weekly topics to link to (Timed per week and for a landing page that builds the Oklahoma Cybersecurity Initiative - Secure Oklahoma as a public service component sponsored by the Oklahoma CyberCommand / OMES-whatever works best for the branding) which also support the Social Media Postings, Email Blasts and Planned Outreach.
- Creation of a PIO / Organizational Toolkit for the Oklahoma Cyber Security Awareness Month for other state agencies, Higher Education Institutions, and K-12 School Systems, and Law Enforcement Entities to use that have the weekly e-mail blasts and timing so that they can use them as templates, and if they wish to be part of the social media outlets, they can follow or time their postings based on the main postings for the #SecureOklahoma messages. Provide in Digital Format the National Cyber Security Awareness Month posters to agencies for printing and digital signage. State Agency Focused #Security tips for Directors, Managers and Supervisors to discuss with staff www.staysafeonline.org/ncsam/resources/

- Engage with OETA to talk about programming or Ad's that can run for the month that have the provided content and voice overs for #SecureOklahoma. If OMES Communications, the CISO, and OETA can agree on a plan to support it then a cross development can occur to provide the content based on the weekly messages.

Governor and Official Support

- Governor Proclamation of Cyber Security Awareness Month for Oklahoma
- Cabinet Secretary / State Superintendent of Education Twitter and E-mail support for teacher, student, and parent focused content delivery focused tips for #CyberAware and #SecureOklahoma: www.staysafeonline.org/ncsam/resources/internet-safety-and-security-tips-for-parents
- Speaking engagements for the state CIO and CISO to have short topical discussions with organizations about #SecureOklahoma and the National Awareness Month.
- Oklahoma Cybersecurity Summit of Appointed and Elected Officials ½ day with the State CIO, CISO, and a guest speaker from the FBI OKC Office that relates the CyberSecurity issues that high level profile individual needs to be aware of and how to leverage the Oklahoma CyberCommand services and OMES IT. Roll out cybersecurity.ok.gov and the platform it can support for their agencies in cybersecurity awareness.

State Agency and Internal Focus

- Tech Talk Tuesdays should have a guest security speaker for no more than 10 minutes per week to present a high level topic and push #SecureOklahoma and the content that is developed for that week to statewide IT staff.
- Security Staff Volunteers to speak at Schools, and local group organizations about Online Safety and Stop. Think. Connect.
- Provide 4 online events through the State's Abode Connect platform capabilities to highlight an appropriate topic and information for the appropriate week. This should use the templates created for the speaking engagements and follow the weekly e-mail blasts from GovDelivery.
- Coordinate "Lobby Days" where OMES Communications will assist Security staff in planning and arranging a "Lobby Day" with key agencies to setup a booth space in their front lobbies or foyers with Security Posters, Flyers, and a message for Cybersecurity Awareness. This will be in the mornings only from 7:45 to 9:00 AM.

Schedule of Activities:

- October 1-2- Week 1: General Cybersecurity Awareness: Celebrating 5 Years of Stop.Think. Connect.™ www.staysafeonline.org/ and stopthinkconnect.org/
    - Celebrating the fifth anniversary of the Stop.Think.Connect. Campaign, week one focuses on cybersecurity as a shared responsibility, and provides simple online tips to empower all Americans to be safer online.
    - Main Topic 1: Keep a Clean Machine and Protect your Personal Information
        - Keep security software current: Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
        - Automate software updates: Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
        - Protect all devices that connect to the Internet: Along with computers, your smartphones, gaming systems and other web-enabled devices also need protection from viruses and malware.
        - Plug & scan: USBs and other external devices can be infected by viruses and malware. Use your security software to scan them
    - Main Topic 2: Connect with Care and Be Web Wise
        - When in doubt, throw it out: Links in email, tweets, posts and online advertising are often the ways cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.
        - Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
        - Protect your $$: When banking and shopping, check to be sure the sites is security-enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "Http://" is not secure.
        - Connect with Care
        - When in doubt, throw it out: Links in email, tweets, posts and online advertising are often the ways cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or, if appropriate, mark as junk email.

        - Get savvy about Wi-Fi hotspots: Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.
        - Protect your $$: When banking and shopping, check to be sure the sites is security-enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "Http://" is not secure.
    - Main Topic 3: Be a Good Online Citizen
        - Safer for me, more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
        - Post only about others as you have them post about you.
        - Help the authorities fight cybercrime: Report stolen finances, identities and cybercrime to http://www.ic3.gov (the Internet Crime Complaint Center) and http://www.onguardonline.gov/file-complaint (the FTC).
- October 5 -9- Week 2: Creating a Culture of Cybersecurity at Work
    - Highlights the common threats businesses and employees are exposed to and provides resources for business and employees to stay safer online and enhance their existing security plans.
    - How cyber threats enter the workplace
        - Malware through E-mail
        - Malware and other malicious code on Websites
        - Removable Media
    - What should you do to protect your work systems from cyber threats
        - Responsible cyber hygiene practices
            - SCAM Awareness Tips
            - Password Tips
            - E-mail Tips
            - Saving data to your Network drive instead of the local system
            - Report unusual system behaviors
    - When to report a cybersecurity concern and who to report to
        - Contact the OMES-IS Service Desk
        - Report that you have a Cybersecurity concern / issue and the details
- October 12-16 - Week 3: Connected Communities: Staying Protected While Always Connected
    - Emphasizes the importance of protecting ourselves when connecting to the Internet while on the go. Week two provides best practices for using mobile devices and social

media, and encourages us all to become better digital citizens in our communities.

  - The dangers of “Free” Wi-Fi hotspots and how to protect yourself when using them.
    - Beware of WiFi Hotspots (why)
    - Tips for Protecting yourself when using them
  - Social Media and the dangers presented to individuals
    - Malware through Social Media
    - Cyberstalking and Over-Communicating
  - Mobile Devices and staying safe and secure when using online services and applications
    - Free Applications aren’t always free
- October 19-23 - Week 4: Your Evolving Digital Life
  - Highlights the “smart world” we live in and the importance of educating all citizens on cybersecurity as more and more of the devices we use – from phones and tablets to homes and medical devices – become connected to the Internet. Week four provides a current snapshot of technology and where we envision technology taking us in the future.
    - The Internet of Things and protecting devices and your privacy
      - Understanding the risk of a connected world
    - Best practices for personal use of Mobile devices
      - When to say “No Thank you”
    - The connected world, the look ahead.
      - How the world is changing through technology
- October 26-30 -Week 5: Building the Next Generation of Cyber Professionals
  - Week five looks to the future of the cybersecurity workforce, focusing on cybersecurity education and awareness in schools at all levels, and emphasizing the need for properly trained cybersecurity professionals.
  - The growing demand for cybersecurity skills in the workforce
    - The growing demand for a cybersecurity workforce
  - Highlight a Cyber Program at a 2 year Oklahoma College
    - Rose State
    - Cyber Camps for Kids
  - Highlight a Cyber Program at a 4 year Oklahoma University (OU, OSU)

Oregon

Oregon CISO: Stefan Richards stefan.richards@oregon.gov
Oregon Enterprise Security Office Webpage:
www.oregon.gov/DAS/CIO/ESO/Pages/index.aspx
Oregon Information Security Resource Center:
secureinfo.oregon.gov/

Pennsylvania

Pennsylvania CISO: Erik Avakian; eavakian@pa.gov; 717.722.4240
Pennsylvania IT Security Homepage: cybersecurity.state.pa.us
Pennsylvania Cybersecurity Awareness Webpage:
www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494
Pennsylvania Cybersecurity Best Practices Webpage:
www.cybersecurity.state.pa.us/portal/server.pt/community/best_practices/495
Pennsylvania Security Awareness Resources and Tips:
www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/resources_and_tips/203340
Pennsylvania Security Awareness Posters:
www.cybersecurity.state.pa.us/portal/server.pt?open=512&objID=494&&PageID=205259&mode=2
Pennsylvania Cybersecurity Toolkit:
www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/security_awareness_toolkit/203338
Pennsylvania Security Awareness Cyber Quiz:
www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/cyber_quiz/203342
Cybersecurity for Kids:
www.cybersecurity.state.pa.us/portal/server.pt/community/cyber_security_for_kids/496

Information Security Awareness Training is offered for state employees through the Commonwealth's Human Resources Office.

2015
The Commonwealth of Pennsylvania will participate in National Cybersecurity Awareness Month, a national campaign to encourage everyone to protect their computers and our nation's critical cyber infrastructure. This month-long effort is supported by federal, state and local governments; industry groups and the private sector. This year's theme focuses on our shared responsibility for cybersecurity. With the increasing use of technology in government, educational institutions, businesses, and homes, as well as the increased use of mobile devices such as smart phones and tablets, we must ensure that our individual actions have a collective impact on cybersecurity and protecting the Internet. Throughout October, we will be working with state agencies, law enforcement, businesses, educational institutions and others to promote awareness and the use of standard practices and technologies to enhance computer security in the commonwealth.

This year, the Commonwealth of Pennsylvania is encouraging everyone to take the "Cyber Pledge," a national campaign organized by the Multi-State information Sharing and Analysis Center (MS-ISAC) which aims to raise awareness to citizens about staying safe online and encourages all individuals to confirm their commitment to doing their part to keep cyber space safe. Everyone is encouraged to sign the Cyber Pledge and demonstrate the commitment to taking cybersecurity seriously. OA/OIT will be distributing cybersecurity calendars, security awareness bookmarks, posters and brochures to agencies. In addition, the governor will issue a proclamation to declare October as Cyber Security Awareness Month.

OA/OIT will be kicking off our annual cybersecurity awareness training for all employees and contractors throughout the month. Additionally we will follow up the training with social engineering exercises to test employees' awareness against online attacks and phishing threats. We will also be hosting a Cybersecurity Awareness Event on October 19th featuring a wide array of educational presentations at the PA State Museum during the Best Practices Exchange annual event.

Rhode Island

Rhode Island CIO: Kurt Huhn; kurt.huhn@doit.ri.gov; 401.222.4444
Rhode Island IT Security Home Page: www.doit.ri.gov/security/infosec/index.php

South Carolina

South Carolina CISO: Marcos Vieyra; marcos.vieyra@admin.sc.gov
Division of Information Security:
www.admin.sc.gov/technology/information-security

South Dakota

South Dakota CISO: Jim Edman; jim.edman@state.sd.us
South Dakota Bureau of Information & Telecommunications: bit.sd.gov/

South Dakota's plans for National Cyber Security Awareness Month include:

- Distributing the MS-ISAC cybersecurity bookmarks, posters, and calendars to schools & government offices
- Distributing the MS ISAC cybersecurity newsletter
- Governor to potentially sign a proclamation designating October as Cyber Security Awareness Month
- Posting security tips via a splash screen when our internet browsers are launched.
- Having a special presentation at the Governor's monthly Cabinet meeting focusing on cybersecurity
- Planning a security presentation to staff from an industry expert
- Having an expanded distribution of our monthly cybersecurity report

Tennessee

Tennessee CISO: Curtis Clan; curtis.clan@tn.gov; 615.741.9109
Tennessee Chief Data Privacy Officer: Peter Gallinari; peter.gallinari@tn.gov; (615) 253-8563
Tennessee Office for Information Resources Webpage:
tn.gov/finance/section/office-for-information-resources

Tennessee's plans for National Cyber Security Awareness Month include:

- A Governor's Proclamation declaring October to be Cyber Security Awareness Month
- Renewal/Kickoff of annual security awareness training
- Poster/flier campaign – posting materials in State office buildings
- Sending weekly Cyber News e-mails following the themes of the campaign
- Business Impact Analysis engagements with Agencies
- Quarterly Security meetings with Agencies
- Phishing exercises

Texas

Texas CISO: Eddie Block; eddie.block@dir.texas.gov; 512.463.8807
Texas Department of Information Resources (DIR) Webpage: www.dir.texas.gov

Events planned for National Cybersecurity Awareness Month for Texas include:

- Governor Greg Abbott has been asked to proclaim October 2015 to be Texas Cybersecurity Awareness Month
- The State OCISO will continue the statewide cybersecurity education program, "Texas Infosec Academy"
    - The Academy includes an education platform of courses from the National Initiative for Cybersecurity Careers and Studies (NICCS), industry standard certification preparation, custom courses for professional development and Texas specific Information Security Officer courses
    - The Academy also includes incident response aids such tabletop scenarios and facilitated exercises
- The State OCISO will continue working with state organizations to implement SANS 'Securing the Human' security awareness tool
- The State OCISO will be available for Security Awareness presentations at state organizations
- The State OCISO will be supporting agency events throughout the month of October, and will host a security awareness event

U.S. Virgin Islands

U.S. Virgin Islands CISO: Jesus Caban; jesus.caban@bit.vi.gov; 340.774.1013 ext. 5700
U.S. Virgin Islands webpage: www.vi.gov

Utah

Utah CISO: Phil Bates; pbates@utah.gov; 801.538.3298
Utah Enterprise Information Security Office Webpage: dts.utah.gov/security/
Security Awareness Training: http://securityawareness.utah.gov

Vermont

Vermont CISO: Jack Green (interim) Jack.Green@vermont.gov
Vermont Information Security Webpage: itsecurity.vermont.gov/
Vermont Security Tools: itsecurity.vermont.gov/security-tools

Virginia

Virginia CISO: Michael Watson; michael.watson@vita.virginia.gov; 804.416.6030
Virginia State IT Security Webpage: www.vita.virginia.gov/security/
Virginia – Information Security Awareness Toolkit Webpage: www.vita.virginia.gov/security/toolkit/

Pre-Cybersecurity Awareness Month Activities

- Sept. 15 – Feature a leadership message from Chief Information Security Officer Mike Watson in the VITA employee e-newsletter (The Link)
- Sept. 30 – Oct 1 – The Commonwealth of Virginia Cybersecurity Unmanned Systems Technology Showcase

Week 1 Theme: Cybersecurity: It's Our Shared Responsibility

- Oct. 1 – Feature cybersecurity in CIO's message in monthly e-newsletter (Network News) to state and local government IT and business representatives and others who subscribe
- Oct. 1 – Brown bag lunch and learn session featuring a security family feud game to test employees' knowledge of cybersecurity etiquette
- Cybersecurity games, videos and informational links will be emailed to employees
- Kick-off of the MS-ISAC's annual "Kids Safe Online" poster contest for school kids K-12
- Setup a cybersecurity information table in the hallway
- Publish the governor's Cyber Security Month proclamation
- Post Security Awareness Toolkit online
- Post weekly Cybersecurity Awareness Blog
- Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week

Week 2 Theme: Social Media – Be Careful What You Post

- Social media-related security games, videos and informational links will be emailed to employees
- Cybersecurity information table in the hallway
- Oct. 7 – Information Security Officers Advisory Group (ISOAG) monthly meeting; security awareness posters and pamphlets will be distributed to all attendees
- Post weekly Cybersecurity Awareness Blog
- Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week

Week 3 Theme: Securing Our Work Environment (If You See Something, Say Something)

- Securing Our Work Environment games, videos and informational links will be emailed to employees
- Oct. 13 – Employee popcorn social to celebrate “National Cybersecurity Awareness Day”
- Oct. 14 - Brown bag lunch-and-learn session on “Protecting Our Infrastructure” presented by the Department of Homeland Security
- Oct. 15 – Information regarding cybersecurity awareness will be highlighted in the VITA employee e-newsletter (The Link).
- Oct. 15 – Tabletop intrusion exercise with members of the Governor’s Cabinet, agency heads.
- Cybersecurity information table in the hallway
- Post weekly Cybersecurity Awareness Blog
- Twitter Thursdays – Invite employees to tweet security awareness tips based on the theme of the week

Week 4 Theme: Protecting Your Privacy Online – Know the Risk

- Privacy-related games, videos and informational links will be emailed to employees
- Cybersecurity information table in the hallway
- Oct. 21 - A brown bag lunch-and-learn session presentation by Special Agent James LaMattina, United States Secret Service in conjunction with Capital One, on “ATM Skimming”
- Post weekly Cybersecurity Awareness Blog
- Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week

Week 5 Theme: Keeping Children Safe Online

- Keep children safe online security-related games, videos and informational links will be emailed to employees
- Oct. 28 – Brown bag lunch-and learn session presentation by Captain Robert P. Chappell, Virginia State Police, author of the book “Child Identity Theft: What Every Parent Needs to Know.”
- Oct. 29 – Cybersecurity bake sale and cyber games for donations to benefit the Commonwealth of Virginia Charities
- Post weekly Cybersecurity Awareness Blog
- Twitter Thursday – Invite employees to tweet security awareness tips based on the theme of the week

Washington

State of Washington CISO: Agnes Kirk; agnes.kirk@cts.wa.gov
State of Washington Cybersecurity Information: soc.wa.gov
Follow us on Twitter: @WaTechSOC

Events planned for National Cyber Security Awareness Month include:

- A National Cyber Security Awareness Month kickoff presentation on October 1st
  - Keynote from Michael Cockrill, State of Washington CIO
  - Target audience of Agency CIO's, CISO's, and System Administrators
- State Office of Cybersecurity Open House
  - Legislative stakeholder tour of the Security Operations Center (SOC)
- Executive Tabletop Incident Response Exercise
  - Executive leadership from the State Auditor's Office will participate in an incident response scenario developed by the Office of Cybersecurity
- School Presentations
  - Joint venture of Washington State Patrol, Intel, and Office of Cybersecurity staff to promote cybersecurity awareness at area schools, ranging from grade school through high school
  - Presentations include the promotion of the MS-ISAC poster contest for participation eligible schools
- Multimedia Campaign
  - Participation in the MS-ISAC Cyber Pledge contest
  - Daily Tweets on cybersecurity topics from the Office of Cybersecurity SOC Twitter account
  - Local print advertising of the MS-ISAC posters in regional newspapers
- Print Material Campaign
  - Distribution of the MS-ISAC toolkit to all State of Washington Agencies and several municipalities
  - Governor Proclamation
- Governor Jay Inslee will sign a proclamation recognizing October as Cyber Security Awareness Month

West Virginia

West Virginia CISO: Joshua D. Spence; Joshua.D.Spence@wv.gov
West Virginia Office of Information Security Controls & Compliance:
www.technology.wv.gov/security/

The mission of the OISC is to support the goals of the State by assuring the availability, integrity and appropriate confidentiality of information. Primary objectives include the development and implementation of proactive measures to prevent security problems, as well as an effective response to security incidents when those prevention methods are defeated. The OISC encompasses three main categories: information security management, risk management, and incident handling.

Policies and Procedures:
www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx
Policies are issued by the West Virginia Office of Technology Chief Technology Officer under the authority granted by the Legislature in WV Code Section 5A-6-4a, effective July 1, 2006, and the Governor's Executive Order 6-06, signed August 16, 2006. These policies apply to all Executive Branch Departments, Agencies and Commissions within the Governor's organizational structure.

West Virginia Security Training and Awareness: www.technology.wv.gov/security/awareness/
It is important to have security awareness training in every type of industry. Whether from inside or outside, malicious or criminal attacks can have devastating effects on your company, or your personal life. Effective training can help you become proficient at spotting suspicious activity, which in turn can reduce the opportunities for harm to occur.

Available Outreach/Presentations: www.technology.wv.gov/security/PresentationOpportunities
The Office of Technology wants to assist citizens in maintaining the availability, integrity and confidentiality of their professional and personal information. With that goal in mind, we offer a Public Outreach Program. Our office offers free presentations to organizations or groups.

Resources
For Families: www.technology.wv.gov/security/awareness/Pages/Resources.aspx
Technology is a daily part of a child's life, and it is essential that children, their parents, and their teachers be knowledgeable about the dangers lurking online. Use the links on this page to find local support centers and organizations, parent forums, educational resources, and more!

For Students: www.technology.wv.gov/security/Students
The importance of spreading the message about safe online behavior has never been more important. The majority of today's youth are online, and the risks for cyber bullying, identity theft and other serious incidents are increasing.
For Technicians: www.technology.wv.gov/security/ArticlesNews/Pages/default.aspx
Articles and newsletters can help you keep informed on the ever-changing world of cybersecurity.

Forms
Risk Reporting Form: www.technology.wv.gov/security/Pages/risk_reporting.aspx
For users to help stop issues before they happen
Security Incident Report Form: www.technology.wv.gov/security/PresentationOpportunities
For reporting immediate security risks that have occurred.
Contact Us: www.technology.wv.gov/security/Pages/contact_information.aspx
Questions and inquiries can be submitted here.

Wisconsin

Wisconsin CISO: Bill Nash; Bill.Nash@wisconsin.gov
IT Security Webpage & Awareness Information:
doa.wisconsin.gov/Divisions/Enterprise-Technology/Bureau-of-Security
Ready Wisconsin/ Cybersecurity Awareness:
ready.wi.gov/cyber/default.asp

Wisconsin is preparing for several cybersecurity events that include:

- A new and improved cybersecurity awareness training program for all WI state employees geared toward creating a security awareness culture
- A Governor's declaration being sent out on Cyber Security Awareness Month in October 2015.
- Cyber response team training/exercises for the Wisconsin cyber response teams (State and local government members) and the Wisconsin National Guard Computer Network Defense Team
- 2015 Wisconsin Cyber Summit on October 28
- 2015 Cyber awareness media campaign following the National Cyber Security Awareness Month themes from the Department of Homeland Security/National Cyber Security Alliance for each week in October, which includes PR, Radio and TV

Wyoming

Wyoming Information Security Officer: Rick Imbrogno; rick.imbrogno@wyo.gov
Wyoming Cybersecurity Homepage: www.wyo.gov/cyber-security

The following actions for the State of Wyoming shall be taken:

- The Governor will declare October to be Cyber Security Awareness Month in Wyoming via official proclamation
- Statewide Security Awareness Training will be provided to all state employees during the month of October utilizing the SANS Securing the Human computer-based training
- Cybersecurity Toolkit materials provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC) will be distributed appropriately
- Incident Response plans will be updated
- Targeted marketing messages on pertinent cybersecurity issues will be routinely transmitted.

NASCIO

2015

STATE CYBERSECURITY
RESOURCE GUIDE

FOLLOW US