STATE CYBERSECURITY RESOURCE GUIDE

Securing Government in a Digital World

Background

The National Association of State Chief Information Officers (NASCIO) supports National Cybersecurity Awareness Month, now in its 13th year. 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 2016 observance, NASCIO has updated its Resource Guide for State Cybersecurity Awareness, Education, and Training Initiatives. This guide includes:

- Updated information on state awareness programs, initiatives and best-practice information;
- Contact information for state chief information security officers (CISOs);
- Hyperlinks to state security and security awareness pages; and
- Information describing cybersecurity awareness, training, and education initiatives.

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

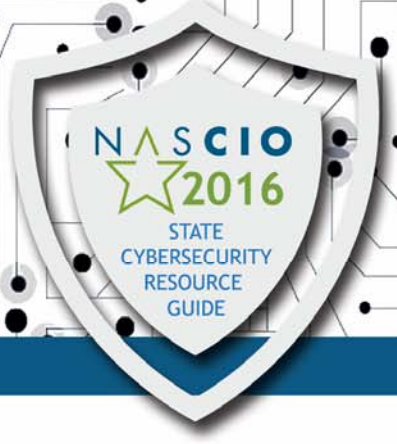

Table of Contents

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 2016:
- Governor Bill Walker has Proclaimed October 2016 as Cyber Security Awareness Month.

Alaska's Security Office will take the following steps in observance of National Cyber Security Awareness Month:

- Partnering with Stop, Think, Connect campaign, hosting weekly WebEx "Lunch and Learn" session. Each week will highlight the weekly STC theme. These will also be recorded and hosted on the State's Security Training website for future viewing. Target audience is end users.
- Arranging technical level presentations for Department Security and IT Staff throughout the month capitalizing on NCCIC, US Cert, and Vendor Partner relationships.
- Highlight a Cybersecurity Awareness Training course each week; staff who complete the training that week will be entered into a drawing for a prize.

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 Cyber Security 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
- Conducting four statewide cyber exercises for locals, tribes and private sector in outlying regions of the state
- Conducting Kids Cyber Awareness Poster contest for K – 12 during October/November
- Begin new marketing campaign for cybersecurity awareness
- Conduct a statewide cyber exercise for agencies and significant 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 Cyber Security Awareness Month

California

California CISO: Scott MacDonald; scott.macdonald@state.ca.gov; 916.319.9223
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: http://www.oit.state.co.us/ois
Cybersecurity Awareness Resources: http://www.oit.state.co.us/ois/resources
Information Security Toolkit: http://www.oit.state.co.us/ois/cyber-security-help

The state of Colorado will be hosting or participating in the following events for Cyber Security Awareness Month:

- CyberGirlz: Regis University will be conducting workshops to prepare middle-school and high-school girls for careers in cyber security, during the months of October through February. This program is called CyberGirlz, and will kick-off with a cyber event on October 11. The state of Colorado will be providing speakers, mentors, and coaches to assist as needed with CyberGirlz events.
- School Security Presentations: The state of Colorado 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.
- Security Tips: We will utilize Twitter to tweet various security tips throughout the month of October. Our hashtag will be: #cocyberhelp
- Security Blogs: Colorado's Office of Information Security will be creating and featuring a couple of Security blogs on our state of Colorado Office of Information Security blog site: http://www.oit.state.co.us/ois/cyber-security-help. We will also be promoting the Stop.Think.Connect website.

Governor's Proclamation: Lastly, the Governor of the State of Colorado has issued a proclamation declaring October to be Cybersecurity 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.

Arthur House has been named as Connecticut's first Chief Cybersecurity Risk Officer. Connecticut also is developing a state Cybersecurity Strategy with a coalition of public and private sector representatives.

Delaware

Delaware CSO: Elayne Starkey; elayne.starkey@state.de.us; 302.739.9631
Delaware Security Home Page: https://digiknow.delaware.gov
Twitter: @DeldigiKNOW

2016 National Cyber Security Awareness Month Delaware Campaign:

- State of Delaware CISSP Boot Camp, November 14, 2016 through November 19, 2016
  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, October 1, 2016 – December 13, 2016
  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, October 1, 2016 – December 31, 2016
  Target audience: Delaware 4th & 5th grade students
  Publish Delaware-specific calendar using 2015 winning posters

- Statewide Cybersecurity Exercise, October 27, 2016
  Venue: Remote Exercise
  Target audience: State agency and school district IT staff, executive leadership, and management

- Statewide Cybersecurity Workshop, September 7, 2016
  Venue: Rollins Conference Center, Dover, DE
  Target audience: state employees, higher education, small business community, Armed Forces, public; https://digiknow.dti.delaware.gov/pages/cyberworkshop/2016/

- Food For Thought Cyber Security Awareness Food Truck Rally, October 4, 2016
  Venue: Silver Lake Blvd., Dover, DE
  Target audience: state agency staff, local businesses, residents, other members of the public

- Cyber for Seniors, October 27, 2016 Venue: Dover Modern Maturity Center
  Target audience: Delaware seniors

- State and Local Cybersecurity Proclamation Adoption: Governor of Delaware signing proclamation for Cybersecurity Awareness

2016 NCSAM Events:

- Secure Delaware Conference
- 4th grade cyber safety presentations
- Information security officer meeting
- CSAM kickoff event
- Food truck rally: 500 attendees, 8 food trucks
- Cyber for seniors
- Governor Markell declares October CSAM
- Enterprise disaster recovery test
- Statewide cyber security exercise

Florida

CISO: Danielle Alvarez; danielle.alvarez@ast.myflorida.com; 850.412.6050
CISO Home Page: http://www.ast.myflorida.com/ciso.asp
Secure Florida: http://www.secureflorida.org/

2016 National Cyber Security Awareness Month Campaign:
Kickoff: October 1

- Governor signs Proclamation

  Audience: Florida citizens, visitors and businesses

- National Cybersecurity Poster Contest

  Audience: 67 counties, kindergarten through 12th graders

Week 1: October 3-7 – Every Day Steps Towards Online Safety with Stop.Think.Connect.™

Cybersecurity 101, http://www.pbs.org/wgbh/nova/labs/video_popup/5/31/

Safe online surfing: https://sos.fbi.gov/

Video series: Savvy Cyber Kids: http://raisingsavvycyberkids.org/

Cyber Tips:

https://www.dhs.gov/sites/default/files/publications/stc-tipcard-cyber%20for%20kids.pdf

https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20and%20Older%20Americans.pdf

Week 2: October 10-14 – Cyber from the Break Room to the Board Room

Resources:

https://staysafeonline.org/re-cyber/ (Audience: CEO/board)

https://www.us-cert.gov/ccubedvp/smb (Audience: small & midsize businesses)

Tools:

Custom Cyber Planning Guide, https://www.fcc.gov/cyberplanner (Audience: small & midsize businesses)

Protect your Workplace, https://www.dhs.gov/sites/default/files/publications/Protect%20Your%20Workplace%20Materials_3.zip (Audience: businesses)

Week 3: October 17-21 – Recognizing and Combating Cybercrime

A Cyber Privacy Parable, http://www.pbs.org/wgbh/nova/labs/video_popup/5/34/ (Audience: child/young adult)

Resources:

Scams, https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors/seniors (Audience: seniors)

Protect your information, https://www.consumer.ftc.gov/features/feature-0038-onguardonline (Audience: adults)

Federal Trade Commission Tips and advice, https://www.ftc.gov/tips-advice/business-center/privacy-and-security (Audience: adults)

Week 4: October 24-28 – Our Continuously Connected Lives: What's Your 'App'-titude?

Cyber codes, http://www.pbs.org/wgbh/nova/labs/video_popup/5/32/ (Audience: child/young adult)

Tool: https://www.fcc.gov/smartphone-security (Audience: mobile users)

Tips: https://www.dhs.gov/sites/default/files/publications/Cybersecurity%20While%20Traveling.pdf (Audience: travelers)

Week 5: October 31 – Building Resilience in Critical Infrastructure

What is Critical Infrastructure: https://www.dhs.gov/publication/stopthinkconnect-government-resources

Resources:

Multi-State ISAC, https://msisac.cisecurity.org/ (Audience: states & critical infrastructure owners/operators)

US CERT, https://www.us-cert.gov/government-users (Audience: Government, industry & cybersecurity professionals)

Cybersecurity framework, https://www.nist.gov/cyberframework (Audience: cybersecurity decision makers and professionals)

Framework Industry Resources, https://www.nist.gov/cyberframework/industry-resources (Audience: cybersecurity professionals)

Information Security Manager (ISM) Meetings
Audience: ISMs and security staff from all state agencies.
Dates: Monthly
User Group Meetings (SIEM, incident response, identity, other topics)
Audience: IT staff from state agencies.
Dates: Ongoing
Audience: The public, state agency staff, etc.
Dates: Ongoing, monthly

Outreach Activities – Webinars, Podcasts, Newsletters, and more:

Domestic Security Oversight Council Meetings
Audience: state, local, municipalities, private sector partners
Dates: Quarterly

Security, Governance Trends & Best Practices
Audience: ISMs from state agencies.
Dates: May 17, 2016

Gartner CISO Peer Forum: Lessons Learned on the Cyber Range
Audience: private & public sector CISOs
Dates: March 23, 2016

E-Waste Webinar – Challenges & Solutions for Recycling Electronics in Florida
Audience: Open
Dates: February 29, 2016

Cyberattacked! Lessons Learned About Cyber Security (panel discussion)
Audience: Tampa Port Authority
Dates: February 19, 2016

Middle School Cyber Safety Presentations
Audience: Certain 6th graders in technology classes
Dates: February 10, 2016

Florida Cyber Sunrise 2016 (Cyber Range Exercise)
Audience: IT staff from state agencies.
Dates: January 25-29, 2016

Georgia

Georgia CISO: Stanton Gatewood; stan.gatewood@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 Cyber Security Awareness Month. 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
- Cybersecurity Awareness Fair scheduled for all state employees

Hawai'i

Hawai'i 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, 2015. 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.

OIMT has:

- 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.

NCSAM October 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 Cyber Security 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

Illinois

Illinois CISO: Kirk Lonbom; kirk.lonbom@illinois.gov; 217.557.0429
Department of Innovation and Technology Cybersecurity Awareness Public Web page:
https://www.Security.illinois.gov
Department of Innovation and Technology Web page:
https://www2.illinois.gov/sites/doit/Pages/default.aspx
Ready Illinois Web Page:
http://www.illinois.gov/ready/Pages/default.aspx

The state of Illinois is currently undergoing a major transformation in cybersecurity. An entire new agency has been created to accomplish this. The Department of Innovation and Technology (DoIT) was created on July 1, 2016 to transform the information and cybersecurity capabilities of the state of Illinois. DoIT is aligning all cybersecurity efforts with the NIST Cybersecurity Framework, the National Cybersecurity Workforce Framework, MS-ISACS and other leading groups who promote an enterprise wide training program.
DoIT has proposed an entire Cybersecurity Awareness Program.

To promote cybersecurity for all residents of the state, the Illinois Cybersecurity Awareness plan includes:

- Creating a new cybersecurity website for the public to access (Security.illinois.gov). This is a work in progress that the state hopes to build on over the coming months. This website will provide resources, newsletters, presentations and videos from a variety of sources to help families, business and school be more informed about cybersecurity best practices.
- Placing the new webpage within DoIT's webpage (with a vanity URL) will enable all state of Illinois employees to be able to access this website while at work and use as a resource.
- Creating videos produced by our own video production crew at the Department of Innovation and Technology. The first video in the "Ask a Hacker" series will be unveiled at the Digital Summit meeting in early October.
- Proclaiming October, Cyber Security Awareness month by Governor Bruce Rauner. Illinois Governors have shown support for Cybersecurity by issuing this proclamation annually.
- Distributing the Cybersecurity Awareness Toolkit materials online for statewide usage.
- Creation of topical tip sheets/factsheets for upload to security.illinois.gov website and distribution between all State agency CIOs.

To promote better cybersecurity strategies and best practices amongst the state's 50,000+ employees, DoIT will:

- Conduct half day seminars on the NIST Cybersecurity Framework for state of Illinois Agency representatives to attend. This idea came from a DHS provided course, which state agencies were invited to attend. This training would emphasize the collaborative nature of cybersecurity and the importance of building a combined cybersecurity vision with the business and IT sides of governmental agencies.

- Conduct Risk Assessments for the each state agency based upon the NIST Cybersecurity Framework. Provide a Cybersecurity Awareness Training curriculum for all state employees.

- This curriculum has been utilized ad hoc by some state agencies but will be provided on a much larger scale this year to all State of Illinois employees to advance the cyber-safety skills of our end users. Distribute the MS-ISAC Cybersecurity toolkit materials throughout state government offices during the month of October.

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 Cyber Security 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/
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 CISO: Joe Acosta; joe.acosta@ks.gov; 785.296.3463
Kansas Information Technology Security Council (ITSC) Webpage: oits.ks.gov/kito/it-security-council

Kentucky

Kentucky CISO: David Carter; davidj.carter@ky.gov
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:

- Governor will be approached to issue a Proclamation of October as Cyber Security Awareness Month. He has issued this proclamation annually since holding the office of Governor.
- Kentucky's Commonwealth Office of Technology (COT) observes National Cyber Security Awareness Month annually by hosting seminars for state government staff during the month of October. The focus for NCSAM 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 IT 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 US Department of Homeland Security (DHS). 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 CISO: Charles Ames; Charles.ames@maryland.gov; 443.787.9683
Maryland Cybersecurity Resource Center: doit.maryland.gov/cybersecurity/Pages/default.aspx

Massachusetts

Massachusetts CSO: Dennis McDermitt; dennis.mcdermitt@mass.gov; 617.626.4403
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 to 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: Rajiv Das; dasr@michigan.gov; 517.373.1004
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: http://www.michigan.gov/cybersecurity/0,4557,7-217-52357_51219---,00.html

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

- Leading up to NCSAM, Michigan published the Michigan Cyber Initiative, outlining the State's cybersecurity goals and objectives from 2015 through 2018.
- 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 IT Services – Cybersecurity Awareness Website: http://mn.gov/mnit/programs/security/
Minnesota IT Services – Cybersecurity Toolkit: http://mn.gov/mnit/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 and received a proclamation from Governor Dayton declaring October Cyber Security Awareness Month. Minnesota has successfully obtained a declaration for the past 10 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.

https://www.facebook.com/MN.ITServices
https://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 11 & 12 the Cybersecurity Summit will be held at the JW Marriott Minneapolis – Mall of America: http://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.

Mississippi

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

Mississippi's planned activities for National Cyber Security Awareness Month:

- Work with the Governor's office on signing a proclamation proclaiming October 2016 as National Cyber Security 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 Awareness Month events.
- Promote a 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 (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 13. 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: http://sitsd.mt.gov/
Montana Information Systems Security Office Webpage: http://sitsd.mt.gov/MontanaInformationSecurity
Montana Information Security Advisory Council Webpage (MT-ISAC): http://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 October 2016.
- 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 Awareness Month 2016 will be "It's a Jungle out there." Additional events will be held every month through September 2017.
- Distribute monthly posters using the 2016 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 201 Montana Information Technology Conference December 12-16, 2016. 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 Information Technology Commission website: http://nitc.ne.gov/

Nevada

Nevada CISO: Brian Wilcox; brian.wilcox@admin.nv.gov; 775.684.7322
Nevada Department 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
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: Michael Geraghty; mgeraghty@cyber.nj.gov; 609.963.6900
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

13th Annual National Cybersecurity Awareness Month, October 2016:

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 Department of Information Technology Webpage: www.doit.state.nm.us/
New Mexico Department of Information Technology Office of Security: www.doit.state.nm.us/securityoffice.html

New York

Enterprise Information Security Office: Jim Garrett, Chief Information Security Officer
Email: eiso@its.ny.gov
NYS Enterprise Information Security Office: www.its.ny.gov/eiso
Cyber Security Awareness Resources: www.its.ny.gov/awarenesstrainingevents
Cyber Security for Kids: www.its.ny.gov/keeping-kids-safe
Cyber Security 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

The New York State Office of Information Technology Services Enterprise Information Security Office (NYS ITS EISO) will be participating in the following activities as part of National Cyber Security Awareness Month (NCSAM) this October:

- Work with the Office of the Governor to issue a cyber security awareness proclamation.
- Develop cybersecurity awareness articles to be published through local government organizations for distribution throughout New York State.
- Participate in the U.S. Department of Homeland Security's (DHS) STOP.THINK.CONNECT. campaign.
- Distribute outreach material to schools, state agencies, local government and community groups.
- Exhibit and present to various state agencies, local government and community groups.
- Distribute the Multi-State Information Sharing and Analysis Center Toolkit to state agencies.
- Post awareness material and the New York State Cyber Security Awareness Toolkit on the NYS ITS EISO website for citizen download.
- Coordinate the 2016-2017 Kids Safe Online NYS 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.

In addition to website posted awareness materials, the NYS ITS EISO provides policies and standards that can be used as best practice, booklets to get you started with a cyber security program, cyber advisories, resources for small-medium businesses, phishing awareness resources, training opportunities, and information on special events.

North Carolina

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

The State of North Carolina will kick off National Cybersecurity Awareness Month (NCSAM) with the Governor of North Carolina's Cybersecurity proclamation. The theme for this year was "Making Yourself a Hard Target vs. Soft Target."

As part of the NCSAM campaign, the state will conduct the following list of activities:

- The state will kick off its Disabled Veteran Cyber Apprenticeship Program. Selected Veterans will be embedded into state agencies for a period of two years, and will obtain training and mentorship to further their advancement in cybersecurity.
- Weekly tweets from the Stop, Think, Connect program, CISecurity, and the National Cybersecurity Alliance - #NCDIT #StopThinkConnect #CyberAware
- Calendar of cyber events including webinars that state employees may participate in
- The state's Enterprise Security and Risk Management Office (ESRMO) will conduct phishing exercises on state agencies in order to strengthen the knowledge and reduce the risks of phishing attacks
- ESRMO will sponsor a Cybersecurity Training Day on October 12, 2016. Guest speakers include private and public organizations who will focus on global, federal and state threats and mitigations
- The state has an ongoing Cyber Awareness Training program using Security Mentor's ten minute modules that are delivered to state employees every other month
- Distribution of monthly newsletters on the state agencies on various cybersecurity topic and tips.

North Dakota

North Dakota CISO: Sean Wiese; swiese@nd.gov; 701.328.1985
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: Russ Forsythe; russ.forsythe@das.ohio.gov; 614.995.1534
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 in October.

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: cybersecurity.ok.gov

Oklahoma Cybersecurity Initiative - Secure Oklahoma - Cyber Security Awareness Action Plan

State goals and objectives: The consolidation of the Information Technology infrastructure, data and, computer systems present 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 develop and deliver a 12-month program for Cybersecurity Awareness. This program began in 2015 and continues today.

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:

State of Oklahoma Theme: Secure Oklahoma #SecureOklahoma

Program Timeframes:

•Preplanning and Program updates: July 15th through the 30th

•Production and Development of new materials for the upcoming year: 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.

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/

NCSAM 2016:

- Governor's Proclamation was signed by Governor Brown.
- Weekly security awareness emails (based off of national Campaign) including newsletters, posters, links to security awareness topics were sent to all agencies.
- Distribute MS-ISAC awareness material to agencies.
- Security mystery game. The game consists of four emails to staff, providing increasing amounts of information around the potential causes of a data breach in order to allow them to identify the culprit. The game highlight multiple risks to data security and make staff think about whether or not the highlighted organizational controls are effective – and whether their own processes involve risk of human error which could lead to a data breach.
- Spot the Security Game - The game consists of a picture of a cubicle with several "security gaps." Staff emailed their list of security gaps to our security staff. Each response received a Security Awareness Certificate and staff were eligible to win prizes.

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.

NCSAM 2016:

- The commonwealth of Pennsylvania will participate in National Cyber Security 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, Governor Wolf will issue a proclamation to declare October as Cyber Security Awareness Month. The proclamation by Governor Wolf highlights the importance of protecting data and devices from online threats. To raise awareness, Office of Administration and Harrisburg University will also be jointly hosting the 2016 Cybersecurity Awareness Summit for state and local governments on October 20, 2016 in Harrisburg.

This year's summit will provide agency leaders and program managers with the latest information on IT security risks and steps they can take to mitigate them. In addition to top experts from the private sector, we will also have representatives from the Governor's Office of Homeland Security and state agencies to provide valuable input on cybersecurity and continuity of operations. Government leaders and program managers are on the front lines of safeguarding sensitive data entrusted to them. This 2016 Security Summit will provide government leaders and their teams with the knowledge and awareness of security risks to sensitive data and systems and discuss steps state government leaders and program managers can take to mitigate the risks.

Rhode Island

Rhode Island CIO: Kurt Huhn; kurt.huhn@doit.ri.gov; 401.222.4444
Rhode Island Division of Information Technology: http://www.doit.ri.gov/

South Carolina

South Carolina CISO: Marcos Vieyra; marcos.vieyra@admin.sc.gov
Division of Information Security: www.admin.sc.gov/technology/information-security
South Carolina Chief Privacy Officer: Theo Wills; theodora.wills@admin.sc.gov
Enterprise Privacy Office: www.admin.sc.gov/technology/enterprise-privacy

The South Carolina General Assembly created the South Carolina Department of Administration's (Admin) Division of Information Security (DIS) in 2014. Through Governor Nikki Haley's leadership and the General Assembly's funding, Admin is able to make protecting citizens' data and information associated with conducting state business a major priority. During National Cyber Security Awareness Month and throughout the entire year, DIS focuses its efforts on people, process and technology to reduce information security risk.
DIS continually works with other Admin divisions to further develop career paths for information security and privacy positions in state government, and to offer advanced information security and privacy trainings to employees in those positions and state agencies. In November, DIS will conduct a six-day, hands-on course in incident response, which will focus on identifying hacker techniques.

DIS provides regular assistance and feedback to state agencies to ensure compliance with the State's 13 policies related to information security and privacy. Assistance includes helping agencies conduct internal risk assessments of information security capabilities and to plan for implementation of security enhancements.

DIS has deployed stronger network monitoring capabilities for all Cabinet agencies such as 24-hour a day monitoring, intervention, and interruption of unusual events and viruses, and has installed new firewall technology and security infrastructure technology designed to protect the state's network and perimeter.

South Dakota

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

South Dakota's 2016 plans for National Cyber Security Awareness Month include:

- Governor signed proclamation designating October as Cyber Security Month
- Presentation from the CISO & CTO on ransomware and cybersecurity at the Governor's October cabinet meeting
- Presentation from the MS ISAC to the state's Working Group on Cyber Security
- Regular distribution of the MS ISAC cyber security newsletter
- Update of the state's cyber security web site
- Expanded distribution of the monthly cyber security report
- Weekly distribution of email message to all state government employees on cyber tips for work and home
- Distributing the MS ISAC materials of bookmarks, posters and calendars to schools and government offices
- Revamping our employee cyber education program to include the new SANS online training course
- Distribution of the BIT-designed cyber posters
- Individual cyber meetings with client agencies

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's plans for National Cyber Security Awareness Month include:

- 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 Acting CISO: Claudia Escobar; Claudia.escobar@dir.texas.gov; 512.463.8249
Texas Department of Information Resources (DIR) Webpage: www.dir.texas.gov

Events planned for National Cyber Security Awareness Month for Texas include:

- Governor Greg Abbott has been asked to proclaim October to be Texas Cyber Security 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 Acting CIO/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: Glenn Schoonover; glenn.schoonover@vermont.gov; 802.828.0911
Vermont Information Security Webpage: itsecurity.vermont.gov/
Vermont Security Tools: itsecurity.vermont.gov/security-tools

Events planned for National Cybersecurity Awareness Month for Vermont include:

- Governor Phil Shumlin has proclaimed October 2016 to be Vermont Cybersecurity Awareness Month
- The State CISO will continue the statewide cybersecurity education program, "Securing the Internet One Person at a Time"
- The State CISO is rolling out the SANS 'Securing the Human' security awareness training to all state agencies.
- The State CISO is providing cyber security awareness articles for the State HR October newsletter

Virginia

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

NCSAM 2016 Activities:

Week 1 Theme: Cyber Security Awareness Month Kick Off (Oct. 3-7)

Oct 3 – 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; cybersecurity games, videos and informational links will be emailed to employees

Oct. 5 – Information Security Officers Advisory Group (ISOAG) monthly meeting; security awareness posters and pamphlets will be distributed to all attendees to display in their offices

- Kick-off of the MS-ISAC's 2017 "Kids Safe Online" poster contest for school kids K-12
- Cybersecurity awareness security games, videos and informational links will be emailed to employees
- Setup a cybersecurity information table in the hallway
- Publish the governor's Cyber Security Month proclamation and PSA video
- Post MS ISAC Security Awareness Toolkit online
- Post weekly Cyber Security Awareness Blog on the CyberVa website.
- Twitter Thursday – Invite employees to participate in the STOP.THINK.CONNECT twitter chat Series.

Week 2 Theme: From the Break Room to the Board Room: Creating a Culture of Cybersecurity in the Workplace (Oct. 10 -14)

- Cybersecurity in the workplace security games, videos and informational links will be emailed to employees
- Cybersecurity information table in the hallway

Oct. 11- Brown bag lunch-and-learn session on "Active Shooter Training" presented by members of the Chesterfield County Police Department.

- Post weekly Cyber Security Awareness Blog on the Cyber VA website
- Twitter Thursday –Invite employees to participate in the STOP.THINK.CONNECT twitter chat series

Week 3 Theme: Recognizing and Combating Cybercrime – (Oct 17 – 21)

- Preventing Cybercrime games, videos and informational links will be emailed to employees

Oct. 18 - Brown bag lunch-and-learn session on "Has Your Bank Account Been Hacked" presented by Chris Woodbury of the Virginia Credit Union.

Oct. 15 – Information regarding cybersecurity awareness will be highlighted in the VITA employee e-newsletter (The Link).

- Cybersecurity information table in the hallway
- Post weekly Cyber Security Awareness Blog on the Cyber Virginia website
- Twitter Thursdays – Invite employees to participate in the STOP.THINK.CONNECT twitter chat series

Week 4 Theme: Our Continuously Connected Lives: What's Your Appitude? (Oct. 24 – 28)

- Cyber and Cutting Edge Technology videos and informational links will be emailed to employees
- Cybersecurity information table in the hallway

Oct. 28 – Cybersecurity bake sale and cyber games for donations to benefit the Commonwealth of Virginia Charities

- Post weekly Cyber Security Awareness Blog on the CyberVA website
- Twitter Thursday – Invite employees to participate in the STOP.THINK.CONNECT twitter chat series

Week 5 Theme: Building Resilience in Critical Systems (Oct. 31 – Nov. 4)

- Protecting our Infrastructure games, videos and informational links will be emailed to employees
- Post weekly Cyber Security Awareness Blog on the CyberVA website
- Twitter Thursday – Invite employees to participate in the STOP.THINK.CONNECT twitter chat series

Washington

State of Washington CISO: Agnes Kirk; agnes.kirk@ocs.wa.gov
State of Washington Cybersecurity Information: www.cybersecurity.wa.gov
Follow us on Twitter: @Wa_OCS

Highlights for October 2016:

- State CISO Agnes Kirk was part of a panel at the 2016 annual NASCIO conference in Florida in September. The panel discussed the results of a NASCIO cybersecurity survey.

- More than 230 people attended a two-day National Cyber Security Awareness Month kickoff in Bellevue hosted by the Washington State Office of CyberSecurity, the National Cyber Security Alliance and the U.S. Department of Homeland Security. An additional 1,200 people tuned in to a livestream feed of the event carried on Facebook.

- Speakers included U.S. Chief Information Security Officer Gregory Touhill, Jeanette Manfra, the senior counselor for cyber and critical infrastructure for the secretary and deputy secretary at the U.S. Department of Homeland Security, and Michael Cockrill, Washington State's Chief Information Officer.

- The event included panels covering the privacy and cybersecurity concerns around drones, autonomous vehicles and the "internet of things." In addition, college students, educators and industry representatives talked about the rapidly growing cybersecurity job sector. Former students who attended Whatcom Community College's Cybersecurity Center talked about how that program helped them in their careers. And a workforce panel highlighted the Microsoft Software Systems Academy, which trains military veterans for cybersecurity jobs.

- A separate kickoff event was held in Spokane, which included a discussion on smart grids and the next generation power system, and a session on how small businesses can protect themselves from cyberattacks. Additional presentations also were provided by speakers from Department of Homeland Security and the National Cyber Security Alliance.

- Governor Jay Inslee signed a proclamation recognizing October as Cyber Security Awareness Month.

- The Office of CyberSecurity, OCS also launched its first ever Hacktober, a game aimed at increasing cybersecurity awareness among all state employees. The event has gotten tremendous response. State employees participate by viewing tips and answering questions. They can win prizes, including two roundtrip airline tickets.

- In addition, OCS launched a redesigned web page, with additional content and cybersecurity tips for viewers.

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: 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: 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: 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: 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: 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: Articles and newsletters can help you keep informed on the ever-changing world of cybersecurity.

Forms Risk Reporting Form: For users to help stop issues before they happen

Security Incident Report Form: For reporting immediate security risks that have occurred.

Contact Us: 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.
- 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
- Wisconsin Cyber Summit
- 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: http://cybersecurity.wyo.gov

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

- The Governor will declare October as Cyber Security Awareness Month in Wyoming via official proclamation
- Web-based Statewide Security Awareness Training will be provided to all state employees during the biennium
- Cybersecurity Toolkit materials provided by the Multi-State Information Sharing and Analysis Center (MS-ISAC) will be distributed appropriately
- Refreshed web content with resources will be released
- Additional security tools to increase protection against network-based threats will be deployed
- Incident response plans, training, exercises policies and procedures will be current with best practice and security trends
- Information sharing and collaboration will be enhanced with our partners
- Collaborative relationships with government and critical infrastructure partners will continue to be forged at all levels
- Regular public awareness presentations will occur on the Cyber Response and Infrastructure Support Program (CRISP) and Center for Internet Security (CIS) Top 20 content
- Targeted marketing messaging on pertinent cybersecurity issues will be routinely transmitted