



STATE CYBERSECURITY

RESOURCE GUIDE

AWARENESS, EDUCATION AND TRAINING INITIATIVES

October 2013

SECURING GOVERNMENT IN A DIGITAL WORLD.

Background

In support of the 10th annual National Cyber Security Awareness Month, the National Association of State Chief Information Officers (NASCIO) has again partnered with the Department of Homeland Security's National Cybersecurity Division (NCSA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the National Cyber Security 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 2013 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 work-in-progress that should provide a valuable reference resource for Cyber Security Awareness Month, as well as the ongoing planning of security awareness and training efforts state programs may undertake thereafter.



10TH ANNIVERSARY

National Cyber Security
Awareness Month

Table of Contents

Alabama	5
Alaska	6
Arizona	7
Arkansas	8
California	9
Colorado	10
Connecticut	11
Delaware	12
District of Columbia	14
Florida	15
Georgia	16
Guam	17
Hawai'i	18
Idaho	19
Illinois	20
Indiana	21
Iowa	22
Kansas	24
Kentucky	25
Louisiana	26
Maine	27
Maryland	28
Massachusetts	29
Michigan	30
Minnesota	31
Mississippi	32
Missouri	33
Montana	34
Nebraska	35
Nevada	36
New Hampshire	37



Table of Contents (continued)

New Jersey	38
New Mexico	39
New York	40
North Carolina	41
North Dakota	42
Ohio	43
Oklahoma	44
Oregon	45
Pennsylvania	46
Puerto Rico	49
Rhode Island	50
South Carolina	51
South Dakota	52
Tennessee	53
Texas	54
Utah	55
Vermont	56
Virginia	57
Washington	59
West Virginia	60
Wisconsin	62
Wyoming	63

Alabama

Alabama Director of Security Services: 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:

- To strengthen its overall Cybersecurity posture with the proper implementation of more up to date security technology
 - Border Security - next-gen firewalls, more robust intrusion prevention technologies, etc...
 - Patch management
 - Security Event Incident Management
 - Secure Email Gateway
 - Fault Tolerance - Mainframe and Server DR, Firewall High Availability, etc...
- To increase communication with internal agencies as well external agencies
 - Federal DHS and MS-ISAC information sharing
 - Alabama Law Enforcement information sharing - ABI, Alabama Fusion Center, etc...
 - Local and Tribal entities information sharing - cities, counties, etc...
 - User groups - Security User's Group, Mobile User's Group, etc...
 - User Security training
- To increase adherence to state policies and industry best practices
 - Vulnerability Assessments - host and application
 - Zoned network architectures
 - MDM, BYOD, device provisioning

Alabama has been in the process of building a more security focused awareness within State Information Technology groups and agencies for the past two years. Redefining our Security groups as well as architecting a new Security Services team are just two steps in an increasingly large overhaul of Alabama's Cybersecurity plan.

Alaska

Alaska CSO: Darrell Davis; darrell.davis@alaska.gov; (907) 269-6733

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

Arizona

Arizona CISO: Mike Lettman; mike.lettman@azdoa.gov; (602)542-0030

Arizona CPO: Mary Beth Joubanc; mbjoubanc@azgita.gov; (602) 364-4537

Arizona Strategic Enterprise Technology: aset.azdoa.gov/security

Arkansas

Arkansas Security Officer: Kym Patterson; kym.patterson@arkansas.gov

Arkansas IT Security Homepage: www.dis.arkansas.gov/security/Pages/default.aspx

Cybersecurity Toolkit: www.dis.arkansas.gov/security/Pages/CyberSecurityToolkit.aspx

Arkansas has several activities planned in preparation of Cybersecurity Awareness Month:

- Hosting a state security working group meeting during October with a presentation on security.
- Handing out cyber educational materials.
- Governor's Proclamation for National Cybersecurity Awareness Week.

California

California CISO: Michele Robinson; Michele.Robinson@state.ca.gov; (916) 431-5058

California Information Security Office: www.infosecurity.ca.gov

California Cybersecurity Symposium: pspinfo.us/events/css2013/

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/

Some of the key initiatives California has scheduled for this year include:

- Annual Cybersecurity Awareness Event on October 9 & 10.
 - Link to Event: www.cio.ca.gov/Public/events_meetings.html and pspinfo.us/events/css2013/
- Requested that Governor issue a proclamation recognizing October as National Cybersecurity Awareness Month.
- Continue to be a Stay Safe Online and Stop.Think.Connect Champion, promoting the message and visit to their website resources from our website, email messaging, etc. Link to our homepage: [www.cio.ca.gov/OIS /](http://www.cio.ca.gov/OIS/)
- Promoting Cyber Pledge participation through October 31.
- Promoting and supporting other cybersecurity awareness events in our state through the month of October.

Additionally, our Library of resources is located at: www.cio.ca.gov/OIS/Government/library/default.asp

Colorado

Colorado CISO: Jonathan Trull; jonathan.trull@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

On October 1 Cyber Awareness Month kicks off with a formal proclamation by Governor John Hickenlooper made in state Legislative House in support of Cyber Awareness month and its importance.

On October 8 there will be a joint meeting of state, county, city, higher education, and private partners surrounding the “Secure Colorado” initiative.

Throughout the month of October the Office of Information Security will be sending out helpful awareness tips and tricks and alerts to known threats.

Connecticut

Connecticut CISO: Steve Casey; steve.casey@ct.gov

Connecticut Bureau of Enterprise Systems and Technology: www.ct.gov/best/site/default.asp

Connecticut Cybersecurity Awareness Webpage: www.ct.gov/best/cwp/view.asp?a=3938&Q=464498&bestNav=1

Connecticut Cyber Safe: www.ct.gov/best/cwp/view.asp?a=3938&Q=301858

The governor will proclaim October Cybersecurity Month in Connecticut.

The State of Connecticut is also starting their second year of Security Awareness Training for all state employees in the Executive Branch.

Delaware

Delaware CSO: Elayne Starkey; elayne.starkey@state.de.us; (302) 739-9631

Delaware Security Home Page: dti.delaware.gov/information/cybersecurity.shtml

Delaware is planning the following activities for Cybersecurity Awareness Month:

- Information Security 101 Training
 - When: Friday, October 25th - Department of Services for Children Youth and their Families
- State of Delaware CISSP Boot Camp
 - When: September 23, 2013 through September 27, 2013 at Delaware State Police Training Academy
 - Target audience—ISOs, IRMs, Systems Administrators, and Web Developers, DTI employees, other IT staff from state organizations. (Class size is limited to 50 attendees)
- Elementary School Internet Safety Presentations
 - When: October 1, 2013 - December 13, 2013
 - Target Audience: 7,000 Delaware 4th grade students
 - A limited number of presentations will be made to 7th grade students as well
 - 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, 2013 through February 28, 2014
 - Target Audience: Delaware 4th & 5th grade students
 - Announce winners on March 15
 - Publish Delaware-specific calendar using 2012 winning posters
- Statewide Cybersecurity Exercise
 - When: October 24, 2013, Full day exercise
 - Venue: Remote Exercise
 - Target Audience: State Agency and School District IT Staff, Executive Leadership, Management, and Public Information Officers; Community Partners will also be invited to join the exercise play
- High School Video Contest
 - Target Audience: 9th through 12th Grade
 - Submissions accepted October 1, 2013 through December 31, 2013
 - The video should illustrate the safe use of the Internet and/or mobile devices

- 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 18, 1:00 - 4:00pm
 - Venue: Polytech Conference Center
 - Target Audience: Information Security Officers for all state agencies and school districts
- DTI Employee Involvement
 - One activity a week in October
 - Lunch and Learn Webinar, “What’s Wrong With This Cubicle?”, Lunch and Learn Cyber Movie, Scavenger Hunt
- Securing the Human
 - Statewide Information Security Awareness Training
 - When: August, 2013 - April, 2014
 - Mandatory Audience: Executive Branch state employees
 - Potential Audience: Municipal employees and school districts
- Marketing Campaign
 - Awareness advertising to include Delaware Department of Transportation bus wrap, News Journal post it note, Carmike Cinema preview ad, promotional items
 - Continuation of social media with goal of at least one tweet a week day

District of Columbia

DC Security Contact: Chris Bennett; christopher.bennett@dc.gov

Cybersecurity Page: octo.dc.gov/DC/OCTO/Agency+Support/Cybersecurity



Florida

Florida Acting CIO: Jason Allison; Jason.Allison@LASPBS.STATE.FL.US

Agency for Enterprise Information Technology, Office of Information Security: www.secureflorida.org/

Georgia

Georgia CISO: Mark Reardon; mark.reardon@gtg.ga.gov

Georgia Technology Authority - Office of Information Security Website: gtg.georgia.gov/

Georgia has several activities planned in preparation of Cybersecurity Awareness Month:

- Promotion of MS-ISAC National Cybersecurity Awareness Month Toolkit to state agencies and GTA publicly facing website.
 - GTA promotional banner: gtg.georgia.gov/egap/
 - Incorporated the Stop, Think, Connect public service announcement
- Cyber Work Force Development - Engaged with an educational partnership with a local university for research.
- Conduct Risk Management Workshops to facilitate implementation of the FISMA model for Risk Management in state government.
- Monitoring of other agency activities.



Guam

Guam Acting Chief Technology Officer: Joseph Manibusan; joseph.manibusan@doa.guam.gov

Guam Office of Technology: www.bit.guam.gov/



Hawai'i

Hawai'i CISO (Acting): Jeffrey Habrych; jeffrey.r.habrych@hawaii.gov

State of Hawai'i 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/

Idaho

Idaho Security Officer: Pam Stratton; Pam.Stratton@cio.idaho.gov; 208-332-1851

Idaho Cybersecurity Awareness Website: cybersecurity.idaho.gov/

Idaho Cybersecurity Identity Theft Prevention Website: cybersecurity.idaho.gov/identity_theft.html

Illinois

Illinois Acting CISO: Patrick Blair; Patrick.Blair@Illinois.gov; (217) 524-0429

Illinois Bureau of Communication and Computer Services new Cybersecurity Webpage: www.illinois.gov/bccs/services/catalog/security/assessments/Pages/default.aspx

Illinois Bureau of Communication and Computer Services Security Awareness Website: www.illinois.gov/bccs/communications/Pages/awareness.aspx

Illinois 2013 Cybersecurity Awareness plan includes:

- Statewide distribution of Cybersecurity awareness materials to more than 100 Agencies, Boards and Commissions.
- 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

Indiana has several activities planned in preparation of Cybersecurity Awareness Month:

- Provision of materials from the MS-ISAC National Cybersecurity Awareness Month Toolkit to state agencies.
- Governor's Proclamation for National Cybersecurity Awareness Week.
- Daily messages on pertinent cybersecurity issues to all state workforce members.
- Recognition of the State's MS-ISAC calendar drawing winner.
- Strategy setting session with state agency information security staff - Cybersecurity Strategic Planning Group.

Iowa

Iowa Security Officer: Jeff Franklin; jeff.franklin@iowa.gov; (515) 281-4820

Iowa Information Security Office Website: secureonline.iowa.gov/index.html

Iowa ISO Security Awareness & Training Webpage: secureonline.iowa.gov/security_awareness/index.html

- Cybersecurity Awareness Month proclamation signing by Governor.
- Cybersecurity Awareness Month announcement email to 20,000 state employees.
- Promoting web-based security training to 20,000 state employees for third year.
- Cybersecurity Executive Summary and Risk Assessment report to agency Directors.
- Kickoff of the Iowa Cybersecurity Strategy and Roadmap.
- 45,000+ Cybersecurity Awareness materials distributed to:
 - State
 - State agency information security officers
 - State institutions (17 institutions)
 - State agency public relations officers
 - Public K-12 Education
 - Area Education Agencies (9 AEAs)
 - Public school districts (349 district superintendents)
 - K-12 Tech coordinators (Iowa Technology Education Connection Conference)
 - County
 - County Clerks of Court (99 counties)
 - County Treasurers (99 counties)
 - Iowa Counties Information Technology (ICIT) information security committee

- City
 - Cities with population of 10,000+ (35 cities)
 - Community Colleges\Regents Institutions
 - Community colleges (15 technology coordinators)
 - University of Iowa
 - University of Northern Iowa
 - Iowa State University
 - Iowa Braille & Sight Saving School
- Public
 - Public libraries (544 libraries)
- Security Awareness Month information tables at state office buildings.
- Security Awareness announcements sent to Security News distribution list (1500+ members).
- Presentations and Education Events - Infragard, FBI
- Media Disposal Event - Onsite destruction event of hard drives and backup tapes
- Distribution of Safeguarding Your Child's Future identity theft booklet through the Department of Health, County Offices and Hospitals

Kansas

Kansas CISO: John Byers; john.byers@ks.gov; (785)296-8434

Kansas Information Technology Security Council (ITSC) Webpage: www.da.ks.gov/kito/itsc/default.htm

Computer Security Awareness and Training Policy; January 22, 2009: da.ks.gov/kito/itec/policies/ITECITPolicy7400.htm

Computer Security Awareness and Training Requirements; January 22, 2009: da.ks.gov/kito/itec/policies/ITECITPolicy7400A.pdf

IT Security Awareness Resources

www.eso.ks.gov/EmployeeResources/default.htm

IT Security Awareness Assessment

www.eso.ks.gov/assessment/

Provides Certificate upon successful completion of the examination

Kentucky

Kentucky CISO: Katrina LeMay; katrina.lemay@ky.gov; (502) 564-6361

Kentucky Commonwealth Office of Technology (COT) Website: technology.ky.gov

Kentucky Chief Information Security Office: technology.ky.gov/ciso

Kentucky Security Services: technology.ky.gov/services/Pages/SecurityServices.aspx

Kentucky Cybersecurity Awareness Month 2013 Page: technology.ky.gov/ciso/Pages/CyberSecurity-AwarenessMonth2013.aspx

2013 Cybersecurity Awareness and Training Resources and Initiatives

Governor Steve Beshear will be approached to issue a proclamation of October 2013 as Cybersecurity Awareness Month. Governor Beshear has issued this proclamation annually since holding the office of Governor of the Commonwealth of Kentucky.

Kentucky's Commonwealth Office of Technology (COT) observes National Cybersecurity Awareness Month annually by hosting free seminars throughout the month of October addressing information security topics. The seminars are attended by managers and IT professionals from state and local governments and universities. Presenters include experts and leaders in IT security from both the public and private sector.

In addition to the seminars, COT distributes the MS-ISAC cybersecurity toolkit materials to state agencies for distribution throughout state government offices.

Security Awareness Training for all Commonwealth Office of Technology (COT) staff is being implemented. The training will coincide with ongoing efforts toward full NIST compliance. Individual plans for security training are reviewed and established annually within the Office of the CISO for security staff members.

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: Michael Gusky; security@la.gov; (225) 219-9475

Louisiana IT Security Home Page: doa.louisiana.gov/oit/IT_Security_Index.htm

Louisiana Security Newsletters: doa.louisiana.gov/oit/Security_Newsletter.htm

Maine

Enterprise Security Officer: Daniel Durgin; daniel.durgin@maine.gov

State of Maine Cybersecurity Website: www.maine.gov/oit/security/

State of Maine Office of Information Technology: www.maine.gov/oit/

The State of Maine is a consolidated IT state. The Maine Office of Information Technology (OIT) services the Executive Branch and other agencies. The Enterprise Security Group within OIT is responsible for securing the IT Infrastructure and Data of the State of Maine. In 2012, the State of Maine hired a new Enterprise Security Officer. Since then, the Enterprise Security Officer has re-staffed and retooled the Enterprise Security Group. The Enterprise Security Officer is currently focusing on remediating Social Engineering, Configuration and Software Vulnerabilities.

Cybersecurity Initiatives:

- Creation of a Cybersecurity Incident Response Team to respond to emergencies.
- Upgrading and standardizing the state's security tools.
- Increased Security Awareness Training for Executive Branch Employees.
- Implemented Content Filtering for malicious and inappropriate sites.
- Developed Phishing training for employees to recognize it and what to do.

Maryland

Maryland Director of Cybersecurity and CISO: Elliot Schlanger; Elliot.Schlanger@maryland.gov; (410) 767-9805

Maryland Cybersecurity Webpage: doit.maryland.gov/support/pages/securityservices.aspx

Maryland Cybersecurity Resource Center: doit.maryland.gov/cybersecurity/pages/cybersecurityhome.aspx

Maryland Cybersecurity Multimedia: doit.maryland.gov/cybersecurity/pages/multimedia.aspx

Maryland Commission on Cybersecurity Innovation and Excellence: www.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

The Commonwealth of Massachusetts is planning the following Cybersecurity Awareness Month activities:

- Kicking off Cyber Awareness Month in Massachusetts.
- Visit to local school to educate computer A+ certificate students on Security.
- Training seminar for Massachusetts Government Information Systems Association (MGISA).
- Cyber Awareness Training for our Internal Agency Information technology Division.
- Dissemination of Security Awareness Material to all of the Commonwealth Agencies, Cities & Towns in Massachusetts.
- Hanging of Awareness Posters in Commonwealth buildings.

Michigan

Michigan CSO: Dan Lohrmann; LohrmannD@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 has recently done several things regarding cybersecurity:

- New cybersecurity awareness training is being rolled out to 50,000 state employees.
- A Governor's declaration is being sent out on Cybersecurity Awareness Month in October 2012.
- 2013 Michigan Cyber Summit is scheduled for October 25, 2013.
See: www.michigan.gov/cybersecurity
- Implementation of the Michigan Cyber Range. See: www.michigan.gov/cybersecurity

Minnesota

Minnesota CISO: Chris Buse; chris.buse@state.mn.us

Minnesota Office of Enterprise Technology - Cybersecurity Awareness Website:
mn.gov/oet/support/cyber-security-awareness/

Minnesota Office of Enterprise Technology - Cybersecurity Toolkit:
mn.gov/oet/support/cyber-security-awareness/cyber-toolkit.jsp

Minnesota plans to have weekly email messages go out to their staff about Cybersecurity and they have planned several public forums so their staff and the general public can take part in a conversation with security experts and use some hands on tools.

Minnesota's security team will be going out to various state agencies for security awareness events, which will include the following:

Display Booth

- Printed Materials on Cybersecurity
- Computers for staff to check their password strength
- Cybersecurity Video modules showing

The events are planned for all Minnesota state employees and in some locations they do serve the state's general public as well.

Scheduled dates include both local and greater Minnesota locations:

- October 3, 8, 9, 15, 16, 17, 24, 28, 30

On October 4 Mark Mathison, one of Minnesota's security managers, will be participating in the Metropolitan Library Service Agency (MELSA) annual meeting focusing on Information Security and PCI Compliance.

On October 22 & 23 the Cybersecurity Summit is being held at the Minneapolis Convention Center: www.cybersecuritysummit.org/. MN.IT Services is a supporting partner of the Summit. Chris Buse, State CISO, serves on the Advisory Board for the Conference.

Furthermore, in October the state will once again launch our "Kids Safe on Line" 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 through 12th grade. MN.IT Services has sponsored the contest for the past 5 years. The primary emphasis of the contest is to raise the awareness of cyber issues for our student population. As students 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. In 2013 the State of Minnesota received 226 posters from students in grades 3 - 8. Our goal is to increase the number of poster entries from all across Minnesota for the 2013/2014 contest.

Mississippi

Mississippi CISO: Jay White; Jay.White@its.ms.gov

Mississippi Department of Information Technology Services: www.its.ms.gov/security/

Here is a list of proposed activities for Cybersecurity Awareness Month:

- **Waiting on Governor's Approval:** Mississippi's Governor signed a proclamation proclaiming October 2013 as Cybersecurity Awareness Month.
- **Creating an October Security Awareness Month webpage** featured on the Mississippi Department of Information Technology Services' (ITS) website.
- **Promoting the National Cyber Pledge contest** sponsored by the Multi-State Information Sharing and Analysis Center (MS-ISAC) division of CIS, which aims to raise awareness about staying safe online and encourages individuals to confirm their commitment to doing their part to keep cyber space safe.
- **Promoting the State of Mississippi 2014 Kids Safe Online Poster Contest** that is designed to increase the cybersecurity awareness of children across the state. All public, private or home-schooled 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 MS-ISAC.
- **Promoting cybersecurity awareness throughout State Government** by providing awareness information (posters, bookmarks, newsletters, tips, etc.) to state agencies so they can be distributed to state employees.
- **ITS will be holding a Security Council Meeting** for state agencies in October. Meeting topics will include information about current cyber threats, emerging vulnerabilities and trends, and a spotlight on the latest trends with BYOD. The meeting will be held on October 8, 2013.
- **Mississippi partnered with the Department of Homeland Security** to conduct a Cyber Storm Exercise during August of 2013. Several state agencies participated in the two-day table top event designed to assess cyber response plans. During the October Security Council Meeting, an overview of the Cyber Storm Exercise and a review of the top findings will be provided.

Missouri

Missouri CISO: Michael Roling; michael.roling@oa.mo.gov

Missouri Cybersecurity Awareness Website: www.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](https://twitter.com/mocybersecurity)

Missouri Cybersecurity Facebook Page: www.facebook.com/pages/Missouri-Cyber-Security/140114041959

The State of Missouri has the following planned for Cybersecurity Awareness Month:

- The Governor declared October to be Cybersecurity Awareness Month in Missouri in an official proclamation.
- Cybersecurity training will be provided to all state employees during the month of October. The training will be tailored to specific agency functions and will include topics such as HIPAA, FERPA, Federal Tax Information, and PII.
- Computer security tips will be emailed to all state employees.
- 31 Days of Cybersecurity.
 - Utilizing social media and our website, a tip will be shared each day.
- 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: itsd.mt.gov/default.mcpX

The State of Montana has several events occurring during Cybersecurity Awareness month to promote security items. They are as follows:

- Governor Bullock will be announcing mandatory security training for all state employees that will be available beginning in October.
- Governor Bullock will also be communicating his support for Cybersecurity Awareness Month at the end of September.
- The state will be conducting its first disaster recovery test in the new backup data center during the month of October.
- The state will be promoting Cybersecurity Awareness month through other various activities such as games, posters, and other communications.

Nebraska

Nebraska CISO: Chris Hobbs; chris.hobbs@nebraska.gov

Nebraska will celebrate National Cyber Security Awareness Month in October with the following activities:

- Distributing posters and educational materials to 120+ Agencies and educational institutions across the state.
- Providing educational materials for on-line access to state, counties and cities.
- Governor's proclamation signing for Cyber Security Awareness Month.

The eighth annual Nebraska Cyber Security Conference was held on June 4 at the Southeast Community College 68th & "O" Street campus location. The conference is a single full day of security workshops and security information sessions that cover a wide variety of security topics. Two separate hands-on workshops were given on free tools that are used in security analysis and will focus on wireless and mobile device security.

We will continue to review and update existing Policies and Standards and currently have a revised password standard out for comment. This Standard has been rewritten to place the emphasis on data classification when it comes to the strength of the password.

We will begin discussions with our Security Architecture Workgroup to devise a state wide Security Awareness Program. This program will include information and input from all agencies and will include information in the form of Newsletters, E-Mails, Presentations, Blogs and updated web sites.



Nevada

Nevada CISO: Christopher Ipsen; cipsen@doit.nv.gov; (775) 684-5800

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

Acting DoIT Commissioner and CIO: Peter Hastings, peter.hastings@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) leads an active Cybersecurity Advisory Committee (CAC) that addresses cybersecurity risks to the state's data, information assets and technology resources. The council 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 and its stakeholders by promoting awareness, developing effective policies and standards, and obtaining supportive consensus for enterprise-wide initiatives that advance the security of information assets and technology resources. The CAC strengthens the business, IT, EM and LE partnerships required to collaboratively and proactively address cybersecurity and collectively respond to major cybersecurity incidents.

DoIT developed and maintains both public facing and State Intranet cybersecurity web sites. Once available, October Cybersecurity Awareness Month notifications and links to toolkit materials will be available on both sites. Printed materials will be distributed to schools statewide by the Department of Education. CAC members will coordinate the distribution of toolkit materials in their respective agencies. Various notifications such as the Cyber Pledge link will be distributed to state employees for response and to key partners for distribution outside of state government. In 2012, NH was the winner of the Cyber Pledge contest in the 'Highest Percentage in State' category. It is expected that the Governor will sign a proclamation which will be displayed at the Department of Information Technology (DoIT) headquarters along with samples of toolkit materials.

DoIT's Security Response Team (SRT) is a multi-organizational team comprised of management and subject matter technical experts, who identify, prioritize, implement, and oversee security-related efforts; this team also functions as the response team during an incident. DoIT, in partnership with Homeland Security and Emergency Management (HSEM) and the NH National Guard, participated in the National Level Exercise (NLE) 2012 to exercise and test the NH Cyber Catastrophic Disruption Plan (CDP).

Cybersecurity awareness training has been provided to all personnel involved in Payment Card Industry (PCI) environments. NH is currently evaluating the options for a statewide awareness training solution.

Creation of the first State Cybersecurity Strategic Plan is in progress.

New Jersey

New Jersey CISO: John Essner; John.Essner@oit.state.nj.us

New Jersey Office of Information Technology: nj.gov/it

New Jersey Statewide Office of Information Security: nj.gov/njinfosecure

New Jersey Security Awareness: nj.gov/njinfosecure/practices/

New Jersey Resources: nj.gov/njinfosecure/other/

The State of New Jersey plans to have five events for the month of October:

- The Governor will sign the Governor’s Cybersecurity Awareness Month Proclamation Letter.
- The state will spotlight Cybersecurity on the state’s main website page and one-stop cybersecurity website.
- The Office of Homeland Security and Preparedness will have a Cybersecurity panel discussion session during their annual New Jersey’s Homeland Security and Preparedness Conference.
- The state’s Fusion Center will have a Cybersecurity Exercise workshop; participants will consist of State and Federal partners.
- The state will have their 3rd annual Cybersecurity Conference.

During the month of October, the Statewide Office of Information Security will be distributing MS-ISAC National Cybersecurity Awareness Toolkit material to public and private sectors.

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

Chief information Security Officer: Thomas D. Smith; thomas.smith2@its.ny.gov

Enterprise Information Security Office: www.its.ny.gov/eiso/

Cybersecurity Awareness Resources: www.dhses.ny.gov/ocs/awareness-training-events/#awareness

Cybersecurity for Kids: www.dhses.ny.gov/ocs/awareness-training-events/children/

Cybersecurity for Local Government: www.dhses.ny.gov/ocs/local-government/

NYS Office of IT Services on Facebook: www.facebook.com/nystatecio

NYS Office of IT Services on Twitter: @NYStateCIO

As part of the 10th annual National October Cybersecurity Awareness Month (OCSAM), 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.
- Present to 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.
- Provide awareness training to our agency employees.
- Participate in the third annual National Cyber Pledge Campaign contest.
- Coordinate the 2013-2014 Student Poster contest.
- Send OCSAM announcements to our various distribution lists (i.e., state agencies, local government, schools).
- Host two cybersecurity courses sponsored by DHS/Federal Emergency Management Agency.
- Post cyber awareness activities and messages on the NYS ITS Facebook and Twitter sites.

In addition to 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 cybersecurity competitions, training opportunities, and information on special events.

North Carolina

North Carolina CISO: Chip Moore; chip.moore@nc.gov; (919) 754-6300

North Carolina State CIO Homepage: scio.nc.gov

North Carolina Enterprise Security and Risk Management Homepage: www.esrmo.scio.nc.gov

North Carolina Enterprise Security and Risk Management Awareness and Training Program:
www.esrmo.scio.nc.gov/initiatives/awarenessTraining.aspx



North Dakota

North Dakota Acting CIO: Mike Ressler (CIO); mressler@nd.gov

North Dakota IT Security Home Page: www.nd.gov/itd/services/it-security/

Ohio

Ohio CISO: David Brown; dabrown1@oit.ohio.gov; (614)728-2037

Ohio Chief Privacy Officer: Daren Arnold; daren.arnold@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 the Governor signing a proclamation, officially making October the State's Cybersecurity Awareness Month. Following the proclamation signing, The Ohio Department of Administrative Services' Office of Information Technology and The Ohio State University's Office of the Chief Information Officer will co-sponsor Ohio's annual Cybersecurity Day event on October 3, 2013. The Cybersecurity Day event is held in conjunction with National Cybersecurity 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.

Additionally, Ohio will conduct an October launch of the SANS Securing the Human (STH) cybersecurity awareness training for 50,000+ state employees. The training provides extensive employee 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 SANS Twenty Critical Security Controls for Effective Cyber Defense.

Oklahoma

Oklahoma CISO: Sarjoo Shah; sarjoo.shah@osk.ok.gov; (405)521-4803

Oklahoma Cybersecurity Webpage: www.ok.gov/homeland/Cyber_Security/index.html

Oregon

Oregon CISO: Theresa A. Masse; theresa.a.masse@state.or.us

Oregon Enterprise Security Office Webpage: www.oregon.gov/DAS/EISPD/ESO/index.shtml

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.

2013

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 Cybersecurity Awareness Month.

OA/OIT will be conducting a security awareness social engineering exercise throughout the month of October. Additionally, the month will kick off our annual Cybersecurity Awareness Training for all commonwealth employees and will also be hosting “Cybersecurity Awareness Day” featuring several security awareness and educational presentations at the Commonwealth Technology Center.

2012

The Commonwealth of Pennsylvania participated in National Cybersecurity Awareness Month, a national campaign encouraging everyone to protect their computers and our nation’s critical cyber infrastructure. The month-long effort was supported by federal, state and local governments; industry groups and the private sector. Last year’s theme focused 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 worked 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.

The commonwealth of Pennsylvania encouraged everyone to take the “Cyber Pledge,” a national campaign organized by the Multi-State information Sharing and Analysis Center (MS-ISAC) which aimed to raise awareness to citizens about staying safe online and encouraged all individuals to confirm their commitment to doing their part to keep cyber space safe. Everyone was encouraged to sign the Cyber Pledge and demonstrate the commitment to taking cybersecurity seriously. OA/OIT distributed cybersecurity calendars, security awareness bookmarks, posters and brochures to agencies. In addition, the governor issued a proclamation to declare October as Cybersecurity Awareness Month.

OA/OIT hosted several cybersecurity awareness and educational presentations as part of our “Cyber Fridays” series at the Commonwealth Technology Center throughout the month of October.

Cyber Friday themes and Awareness session topics included:

- The Emerging Cybersecurity Threat Landscape
- How Microsoft Secures its Network
- 21st Century Incident Response
- Imperva Threat Radar Web Application Firewall (WAF)

- Unfolding the GRC Roadmap
- Hacking 101
- The State of Cloud Security: Ready or Not
- Keep Yourself Safe from Phishing Scams



Puerto Rico

Puerto Rico Chief Security Officer (CIO): Giancarlo Gonzalez; ggonzalez@fortaleza.pr.gov

Rhode Island

Rhode Island CISO: Ernest Quaglieri; equaglieri@doit.ri.gov; 401-462-9202

Rhode Island IT Security Home Page: www.doit.ri.gov/security/infosec/index.php

South Carolina

South Carolina CISO: James MacDougall; macdoug@cio.sc.gov

South Carolina ISAC: sc-isac.sc.gov/

South Dakota

South Dakota CISO: Jim Edman; jim.edman@state.sd.us

South Dakota Bureau of Information Technology Website: bit.sd.gov/

Tennessee

Tennessee CISO: Sese Bennett; sese.bennett@tn.gov; (615) 741-7754

Tennessee Office for Information Resources Webpage: www.tn.gov/finance/oir/security/

As part of the National Cybersecurity Awareness Month, Tennessee will be working with the Governor's Office to issue the National Cybersecurity Awareness Month Proclamation. We will be distributing awareness materials to state agencies. We also will be delivering new awareness training to employees.

Texas

Texas CISO: Brian Engle; brian.engle@dir.texas.gov; (512) 475-4700

Texas Department of Information Resources Webpage: www.dir.texas.gov

Texas Cybersecurity, Education and Economic Development Council (TCEEDC):
www2.dir.state.tx.us/sponsored/SB988/Pages/overview.aspx

Events planned for Cybersecurity Awareness Month for Texas include:

- Launching the SANS Secure the Human End User Security Awareness Training for state agency personnel.
- Launching a pilot of the SANS Secure the Human Developer Awareness Training within an Application Development Special Interest Group.
- Conducting executive level briefings for business management of state agencies.
- Hosting CyberPatriot launch events in Austin, Dallas/Fort Worth, and Houston for area high schools.
- Participating in a statewide Cybersecurity Summit held in Fort Worth Texas on October 17th.

Utah

Utah CISO: Tim Hastings; thastings@utah.gov

Utah Cybersecurity Incident Response Team (CSIRT) Manager: Boyd Webb; boydwebb@utah.gov

Utah Enterprise Information Security Office Webpage: dts.utah.gov/security/

The State of Utah is partnering with the Department of Homeland Security to host a cybersecurity forum on October 16-17.

Vermont

Vermont Information Security Officer: Kris Rowley; kris.rowley@state.vt.us; (802) 828-0911

Vermont Information Security Webpage: itsecurity.vermont.gov/

Vermont Security Tools: itsecurity.vermont.gov/Security_Tools

The State of Vermont has the following plans for Cybersecurity Awareness Month:

- Kris Rowley will be doing a TV spot on WCAX TV in Burlington, VT.
- Norwich University is collaborating with the state of VT security team to travel to schools (K-12) to talk about cybersecurity and to encourage students to enter the MS-ISAC poster competition. A VT student was selected for this year's calendar. We are very proud of this school and student.
- Kris Rowley is setting up some talks at local libraries to help inform our citizens about cybersecurity and how important it is for them to do their part in protecting our cyber assets.
- VT will be competing in the MS-ISAC Cyber Pledge competition.
- Kris Rowley will also be distributing the posters and calendars to as many places throughout the state as she can.

Please visit Vermont's newly updated security web site and all feedback has been encouraged.

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/

The Commonwealth of Virginia has the following activities planned for Cybersecurity Awareness Month. Each week will focus on a different theme for the month:

Week 1 Theme: What is Cybersecurity?

- Cybersecurity game and video link will be emailed to all employees.
- October 4: Monthly meeting of the Information Security Officers Advisory Group will feature presentations on Password Cracking, Secure Coding and a special presentation by the U.S. Secret Service.
- We will kick off our annual Cybersecurity Poster Contest for school age kids K through 12.
- Setup a Cybersecurity Information table in the hallway.
- Publish the Governor’s Cybersecurity Month Proclamation.
- Post Security Awareness Toolkit on our website.
- Email Cybersecurity Pledge to all employees.

Week 2 Theme: The Security Risks of Social Media

- A Social Media security game and video link will be emailed to all employees.
- A brown bag lunch-and-learn will focus on End User Remote Access security.
- Setup a “What’s Wrong with this Picture?” information table to demonstrate improper employee work area practices.

Week 3 Theme: Privacy: Protect Your Privacy on the Internet

- A Privacy related security game and video link will be emailed to all employees.
- An information table on Identity Theft will be setup in the hallways.
- October 16: Peter Miller, Chief Privacy Officer with the Federal Trade Commission will address employees on privacy issues.
- October 16: Virginia State Police, the Department of Motor Vehicles and the Virginia Alcoholic Beverage Control will have Mobile Command Post vehicles parked at the Commonwealth Enterprise Solutions Center parking lot for employee tours.

Week 4 Theme: Mobile Device Security

- A Mobile Device Security related game and video link will be emailed to all employees.
- An information table related to mobile device security will be setup in the halls.
- A brown bag lunch-and-learn will focus on McAfee Host and Network Intrusion Detection Systems.

Week 5 Theme: Keeping Children Safe Online

- A Keep Safe online security related game and video link will be emailed to all employees.
- October 30: Special Agent John Houlberg with the Virginia State Police will address employees on Internet Crimes Against Children.
- October 30: Phishing for Spam game will be played for donations to benefit the Commonwealth of Virginia Charities.



Washington

Washington CISO: Agnes Kirk; agnesk@dis.wa.gov

Office of the Chief Information Officer: www.ofm.wa.gov/ocio/default.asp

West Virginia

West Virginia CISO: Jim A. Richards - jim.a.richards@wv.gov

West Virginia Office of Information Security Controls & Compliance:
www.technology.wv.gov/security/

The mission of the Office of Information Security Controls & Compliance 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 unsuccessful.

West Virginia Office of Technology: www.technology.wv.gov/

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.

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!

Student Section: 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.

Policies Issued by the CTO: 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.

Available Outreach: 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 each month to organizations or groups that meet our engagement terms.

Forms:

- Risk Reporting Form. Stop issues before they happen:
www.technology.wv.gov/security/Pages/risk_reporting.aspx
- Security Incident Report Form: www.technology.wv.gov/security/PresentationOpportunities
- Contact Us:
www.technology.wv.gov/security/Pages/contact_information.aspx

West Virginia plans to hold the following event for Cybersecurity Awareness Month:

Money, Sanity, Identity: What are you willing to lose?

- Description: The event will feature dynamic presentations delivered by experts in the areas of cyber threats, effective practices to safeguard systems and data, risk management, and privacy issues. The agenda will offer an energizing morning of highly informative sessions educating end-users on the dangers that exist at work and at home.
- Event Info/Speaker Link: www.wv.gov/services/Pages/Infosec-conference.aspx
- Registration Link: apps.wv.gov/OT/SCR/
- October 2, 2013, Charleston Civic Center
- 9:00 AM to 1:00 PM
- Attend in-person or streaming online

Wisconsin

Wisconsin CISO: Ron Last; ron.last@wisconsin.gov

Wisconsin IT Security Webpage: itsecurity.wi.gov/

Wisconsin IT Security Awareness Webpage: itsecurity.wi.gov/section_detail.asp?linkcatid=2907&linkid=1498&locid=89

Wyoming

Wyoming Enterprise IT Security Coordinator: Michael Crouch; mike.crouch@wyo.gov; (307)777-5000

Wyoming Cybersecurity Homepage: www.wyoming.gov/cybersecurity.aspx



201 East Main Street Suite 1405
Lexington, KY 40507
www.NASCIO.org