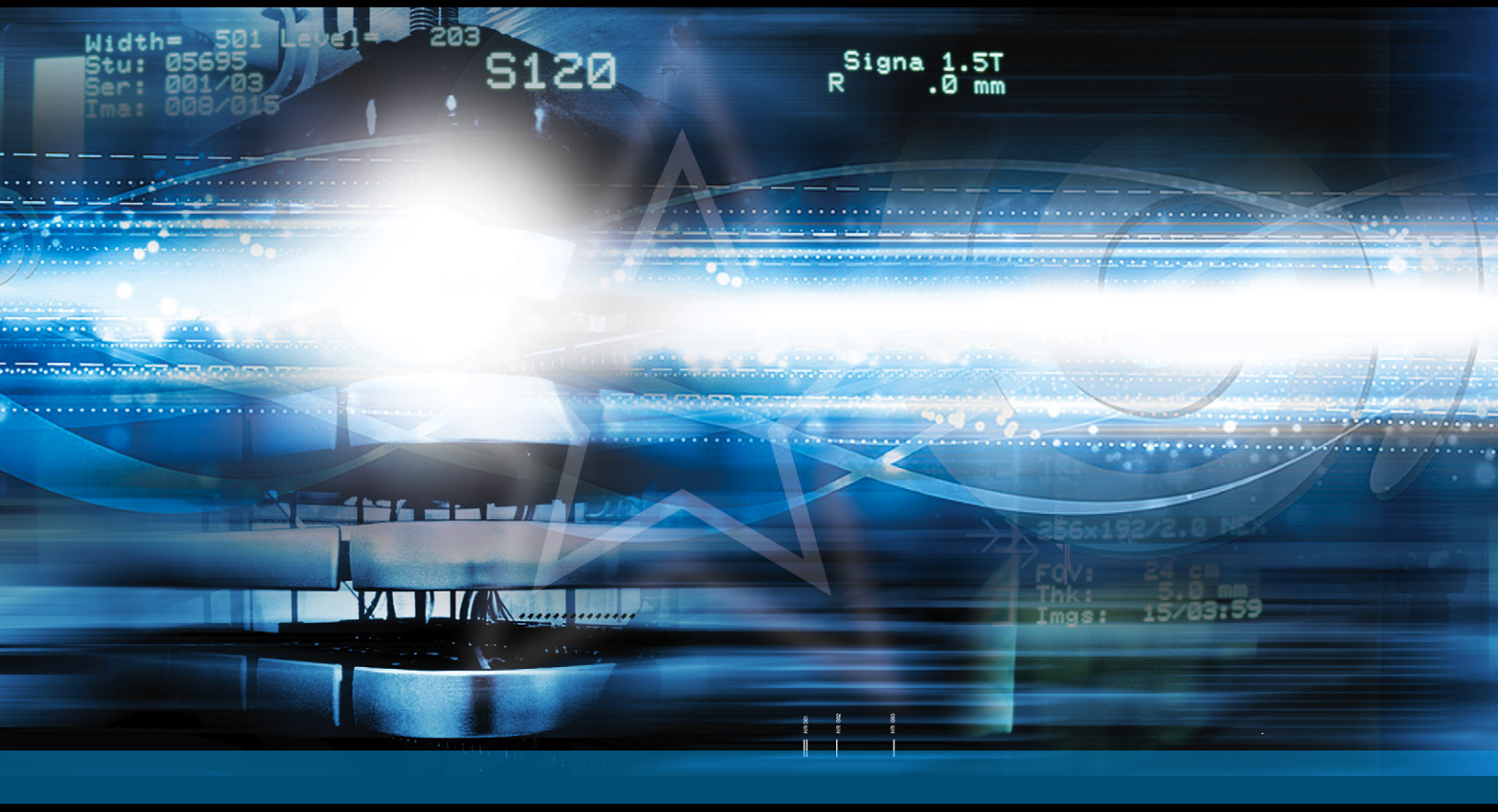
NASCIO
Representing Chief Information Officers of the States



STATE CYBER SECURITY

RESOURCE GUIDE

AWARENESS, EDUCATION AND TRAINING INITIATIVES

October 2011

SECURING GOVERNMENT IN A DIGITAL WORLD.

Background

In support of the 8th 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 Cyber Security Division (NCSD), 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 Cyber Security Awareness page.

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

For the 2011 observance, NASCIO has updated its Resource Guide for State Cyber Security 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 cyber security 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.

NASCIO
Representing Chief Information Officers of the States

TABLE OF CONTENTS

Alabama

Alabama CISO: Lee Styres; lee.styres@isd.alabama.gov; (334) 242-3044
Alabama Cyber Security Webpage: www.cybersecurity.alabama.gov

The State of Alabama participates in the annual October Cyber Security Awareness Month by signing and issuing of the Governor's Proclamation in collaboration with the Multi-State Information Sharing and Analysis Center, the Department of Homeland Security, the National Cyber Security Alliance, and the Federal Trade Commission.

Planned for October, 2011 - The State of Alabama Cyber Security Office in collaboration with and funded by the Federal Department of Homeland Security is hosting a cyber security awareness event in the Jasper/Tuscaloosa, Alabama area in order to further cyber education and awareness for grades K – 12 students. This presentation is an outreach developed via the StaySafeOnline.org and C-SAVE initiatives.

IT Security Assessments—State of Alabama: Alabama has enacted a training and awareness policy based on the standards of NIST (the National Institute of Standards and Technology). It applies to contractors and employees, and includes enforcement provisions and content and procedural guidance for awareness and training programs. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Baseline, p. 4)

Agency Head Awareness—State of Alabama: This state's policy requires that each agency have an awareness and training plan that is approved by each agency head. Through this requirement, agency heads are involved and ultimately responsible for plan implementation. Thus, responsibility can quickly elevate the importance of this issue for agency leaders. The state CIO's office also provides high-level security briefings for the upper management of agencies. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Awareness, p. 6)

Alabama provides a database and listserv for agency information security officers. The state's Information Security Officer in the CIO's Office provides updates on security-related information as it becomes available. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Use Agency CSOs, p. 8)

Employee Awareness/Training Mandated by Policy or Executive Order: (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Official Awareness/Training Mandate, p. 9)

Alaska

Alaska CSO: Darrell Davis; darrell.davis@alaska.gov; (907) 269-6733
Alaska CISO: Jay Druyvestein; jay.druyvestein@alaska.gov; (907) 465-2060
Alaska Security Awareness Webpage: http://security.alaska.gov/SA_Bulletins/index.html
State Security Office: http://security.alaska.gov/ (Link to MS-ISAC on this page).
SOA Security Training: http://security.alaska.gov/training/index.html

American Samoa

American Samoa Chief Security Officer (CIO): Easter Bruce; cio@as.gov; (684) 633-3648

Arizona

Arizona CISO: Jim Ryan; jryan@azgita.gov; (602) 364-4771
Arizona CPO: Mary Beth Joublanc; mbjoublanc@azgita.gov; (602) 364-4537
Arizona Information Security and Privacy Homepage: www.azgita.gov/sispo/
Arizona Government Information Technology Agency: http://www.azgita.gov/
Arizona Statewide Strategic IT Plan: http://www.azgita.gov/planning/2011StrategicPlan.pdf

Arkansas

Arkansas Security Officer: Kym Patterson; kym.patterson@arkansas.gov
Arkansas IT Security Homepage: http://www.dis.arkansas.gov/security/Pages/default.aspx
Cyber Security Toolkit: http://www.dis.arkansas.gov/security/Pages/CyberSecurityToolkit.aspx

California

California CISO: Keith Tresh; keith.tresh@state.ca.gov; (916) 323-7237
California Office of Information Security: http://www.cio.ca.gov/OIS/
California Security Awareness Webpage: http://www.cio.ca.gov/OIS/Government/library/awareness.asp
California Office of Privacy Protection: http://www.privacy.ca.gov/
State Employee Privacy Training
Protecting Privacy in State Government, Basic Training for State Employees

- PowerPoint Presentation (.ppt, 2.1mb)
- Presentation with Speaker Notes (.pdf, 2.8mb)
- Self-Training Manual (.doc, 860k)
- Guidelines for Self-Training Manual (.pdf, 94k)

This is described more fully in the Office of Privacy Protection's 2009 NASCIO Recognition Award Nomination.

Colorado

Colorado CISO: Travis Schack; travis.schack@state.co.us
Colorado Office of Information Security: http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1249667675596
Colorado OCS Resources Page: http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408776
Information Security Toolkit: http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408811

Connecticut

Connecticut CISO (Acting): Steve Casey; steve.casey@ct.gov
Connecticut Bureau of Enterprise Systems and Technology: http://www.ct.gov/best/site/default.asp
Connecticut Cyber Security Awareness Webpage: http://www.ct.gov/best/cwp/view.asp?a=3938&Q=464498&bestNav=|
Connecticut Cyber Safe: http://www.ct.gov/best/cwp/view.asp?a=3938&Q=301858

Delaware

Delaware CSO: Elayne Starkey; elayne.starkey@state.de.us; (302) 739-9631
Delaware Security Home Page: http://dti.delaware.gov/information/cybersecurity.shtml

2011 Cyber Security Awareness & Training Resources

1. **Executives/Public Officials**
   Delaware Cyber Brief 2011: Half day seminar on September 21 examining the latest tactics employed by cyber criminals and predators. Guest speakers are Karen Evans, Greg Shaffer, and Will Pelgrin. Governor Markell will attend to sign the proclamation declaring October as Cyber Security Awareness Month in Delaware. Immediately following the event, Governor Markell will receive a special classified cyber security briefing delivered by US-DHS.
   http://dti.delaware.gov/cyberbrief/

2. **State Workforce and IT/Security Staff**
   Cyber Security Exercise: On October 27, DTI will host "Operation End Game", the state's 7th annual cyber security exercise. IT staff, management, and public information officers from state agencies and school districts will come together to simulate a real world cyber attack on the State IT infrastructure. Approximately 125 attendees are expected. This will be a "hands-on" functional exercise, and the participants will have a chance to practice their incident and emergency response plans, and consider alternatives to the delivery of government services when their IT infrastructure is unavailable. Simulation exercise is to improve the State's overall readiness level to prevent and/or respond to a cyber incident.

   Cyber Terrorism Defense Initiative Training was held in August 2011 in Dover. 42 State and City employees earned a US-DHS certification in cyber terrorism defense, along with credits toward the Delaware ISO certification. www.cyberterrorismcenter.org/

   Information Security 101 Training is offered for State employees through the State Human Resources Office.

   Information Security Online Training requires all new State employees to complete the mandatory online MS-ISAC training within 30 days of their hire date.

   Security Scorecards
   - Information Security Scorecards were delivered to all Information Security Officers.
   - Each Agency and School District received a numerical score between 1-500, representing their information security maturity level.
   - The scorecards provide ISOs with data on how they are doing relative to their peer organizations, how they did compared to last year, and where there are opportunities to close gaps.

   Delaware Certified Information Security Officers (DCISO)
   Certification for a Delaware Information Security Officer (ISO) recognizes qualified and competent individuals and shows peers, managers and customers a commitment to the information security profession. A DCISO certification is earned by completing 4 core requirements and 20 electives over a 24-month period.

Delaware (continued)

3. Citizens

United States Cyber Challenge

- Delaware ran the second annual collegiate level US Cyber Challenge Camp in August.
- Delaware is participating in the high school Cyber Foundations competition again this year.

Community Cyber Security Maturity Model (CCSMM)

The Center for Infrastructure Assurance and Security (CIAS) announced that Delaware is the only state selected for Phase 2 of the CCSMM program. The goal of CIAS is to enforce the concepts of protecting essential cyber and physical assets while improving information sharing. The cyber security postures of local communities, states, and the nation are strengthened through community cyber security exercises and interactive training sessions.

Delaware DigiGirlz Day 2011 event had 153 girls in attendance. Delaware's First Lady was the keynote speaker. Media coverage included WBOC TV, and WDEL Radio, and the Delaware State News. Microsoft's DigiGirlz Day is a worldwide Microsoft program designed to introduce high school girls to careers in technology. During these events, Microsoft employees provide girls with career planning assistance, information about technology and business roles, thought-provoking exercises and compelling Microsoft product demonstrations.

MS-ISAC Cyber Security Poster Contest for all Delaware 4th and 5th graders. Delaware has had 11 national winners in the last 4 years.

Internet Safety and Cyber Bullying Presentations have reached over 11,000 4th and 5th grade students since inception.

Internet Safety and Cyber Bullying refresher training will be provided to 6th grade students throughout Delaware schools in 2011. This new venture will reaffirm and build on training provided in 4th grade.

Cyber Security messages posted on the electronic boards in all four Department of Motor Vehicles (DMV) locations targeting customers waiting in line.

Other promotions include online advertisements on Delaware.gov and delawareonline.com, twitter updates.

District of Columbia

DC Security Contact: Chris Bennett; christopher.bennett@dc.gov
DC Cyber Security Page: http://octo.dc.gov/DC/OCTO/Agency+Support/Cybersecurity

Florida

Florida CISO: Mike Russo; mike.russo@aeit.myflorida.com
Florida Agency for Enterprise Information Technology: https://aeit.myflorida.com/
Florida Office of Information Security: https://aeit.myflorida.com/aboutois
Security Awareness Webpage: https://aeit.myflorida.com/securityawareness
2010-2012 Florida Enterprise Information Technology Security Strategic Plan:
https://aeit.myflorida.com/sites/default/files/files/2010-2012 Florida Enterprise Informaiton Technology Security Strategic Plan.pdf

Policy
AEIT completed the promulgation of the State Security Rule 71A-1. Rule 71A-1 shall be known as the Florida Information Technology Resource Security Policies and Standards. The rule establishes a uniform methodology for applying reliable and consistent data protection techniques to protect Florida's information and data. Agencies are directed to implement policies compliant with AEIT guidelines, State and Federal laws, rules, or standards as stated in F.S. 282.318.

Training and Consulting
AEIT conducts monthly ISM meetings to discuss emerging cyber trends and threats, upcoming events and cyber security training initiatives. AEIT provides FREE IT cyber security training to State, City and County IT professionals. Newsletters are distributed to promote security awareness, webcast are offered by state partners, tools and technology training are provided to government ISMs.

AEIT coordinates and pays for certifications with Florida domestic security grants, the most common are the CISSP (Certified Information System Security Professional) course and certification and a CISA (Certified Information Systems Auditor) course and certification for the state's information security managers, IT professionals and the inspectors general community.

AEIT coordinates *Homeland Security funded* training events, the Cyberterrorism Defense Initiative (previously known as the *SENTINEL training*) a four day session where 60 state, city, county and private IT professional partners received annual training in the following areas:

- Comprehensive Cyberterrorism Defense (CCD) class stressed a proactive approach to providing computer, network, and infrastructure security. Solutions and methods taught are non-vendor-specific, which does not require participants to have specialized software when trying to implement class lessons at their own agencies.

- Incident Handling and Response (IHR) class educated and trained technical personnel in the proper actions and investigative procedures for dealing with critical incidents involving network infrastructure.

Individual State Agency Activities: Agencies use the annually distributed cyber security awareness tool kit and other resources to conducted training awareness activities within their agency. The tool kit is provided through our partnership with the *Multi-State Information Sharing* and *Analysis* Center (MS-ISAC) and is branded for Florida, the tool kits includes cyber awareness calendars, posters, bookmarks, training cds and materials to enhance cyber awareness.

Florida (continued)

The annual Florida Government Technology Conference and Cyber Summit, sponsored by Florida State University, in conjunction with the Agency for Enterprise Information Technology, Office of Information Security, presented the **FGTC and Cyber Summit (a free event); where locals and webcast viewers can participate**. Public sector IT and IT security professionals, as well as experts in the private sector, are invited to this two-day event. This is an excellent opportunity for **IT professionals** to congregate and exchange ideas and to discuss new solutions for today's issues that face technology and cyber security.

- The cyber security awareness tool kit and materials are on display along with other cyber security resources. Materials are distributed to the state agency's information security managers and our city and county partners. The tool kit is also available for branding and printing by any organization.

Georgia

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

Georgia Technology Authority – Office of Information Security:
http://www.georgia.gov/00/channel_title/0,2094,1070969_84340779,00.html

"October is Cyber Security Month" proclamation, resources, video:
http://gta.georgia.gov/00/article/0,2086,1070969_1074423_124268204,00.html

Guam

Guam Chief Security Officer (CIO): Ed Cruz; (671) 472-1229
Guam Bureau of Information Technology: http://www.bit.guam.gov/

Hawaii

Hawaii CISO: Todd Crosby; todd.m.crosby@hawaii.gov
State of Hawaii Cyber Security Website: http://hawaii.gov/dags/icsd/cst/view
State Cyber Security Resources, (Link to MS-ISAC): http://hawaii.gov/dags/icsd/cst/cyber-security-resources
State Cyber Security Toolkit: http://hawaii.gov/dags/icsd/cst/cyber-security-toolkit

Idaho

Idaho Security Officer: Pam Stratton; Pam.Stratton@cio.idaho.gov; 208-332-1851
Idaho Cyber Security Awareness Website: http://cybersecurity.idaho.gov/
Idaho Cyber Security Identity Theft Prevention Website: http://cybersecurity.idaho.gov/identity_theft.html

Illinois

Illinois CISO: Rafael Diaz; Rafael.Diaz@Illinois.gov; (312) 814-5477
Illinois Bureau of Communication and Computer Services (BCCS) Security Awareness Website :
http://www2.illinois.gov/bccs/security/Pages/awareness.aspx

Cyber Security Toolkit: http://www2.illinois.gov/bccs/security/Pages/Security_toolkit.aspx

Awareness Posters:
Keyboard_Hands: http://www2.illinois.gov/bccs/security/Documents/Keyboard_Hands.pdf
Security Survivors: http://www2.illinois.gov/bccs/security/Documents/SecSurvivorPoster.pdf
Global Security: http://www2.illinois.gov/bccs/security/Documents/GlobalSecPoster.pdf
Strong Passwords: http://www2.illinois.gov/bccs/security/Documents/Strong_Passwords_Poster.pdf

Indiana

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

Iowa

Iowa Security Officer: Jeff Franklin; jeff.franklin@iowa.gov; (515) 281-4820
Iowa Information Security Office Website: http://secureonline.iowa.gov/index.html
Iowa ISO Security Awareness & Training Webpage:
http://secureonline.iowa.gov/security_awareness/index.html

2011 Cyber Security Awareness & Training Resources

1. **Executives/Public Officials**
   The State of Iowa developed a video to promote information security awareness among agency administrators. The STARTS video is located at: http://secureonline.iowa.gov/PSAs/index.html

2. **State Workforce**
   The State of Iowa promotes security outreach by providing security awareness training to state agencies and distributing security awareness materials to state employees.

3. **Local Government**
   The State of Iowa distributes security awareness materials to counties, cities, and public K-12 schools.

4. **Citizens**
   The State of Iowa Information Security Office promotes information security awareness to Iowans via its website located at: http://secureonline.iowa.gov/index.html

5. **IT/Security Staff**
   The State of Iowa Information Security Office sponsors technical training for state IT/Security staff.

Kansas

Kansas CISO: Vacant

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

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

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

IT Security Awareness Resources
http://www.eso.ks.gov/EmployeeResources/default.htm

IT Security Awareness Assessment
http://www.eso.ks.gov/assessment/
Provides Certificate upon successful completion of the examination

IT Security Assessments—State of Kansas: During agencies' annual security self-assessments, they must identify training efforts that have taken place and opportunities for future training.

Kentucky

Kentucky CISO: Katrina LeMay; Katrina.Lemay@ky.gov; (502) 564-6361
Kentucky Commonwealth Office of Technology (COT) Website: http://technology.ky.gov
Kentucky Chief Information Security Office: http://technology.ky.gov/ciso/
Kentucky Security Services: http://technology.ky.gov/services/Pages/SecurityServices.aspx
Kentucky Cyber Security Awareness Page:
http://technology.ky.gov/ciso/Pages/CyberSecurityAwareness2011.aspx

The Kentucky Commonwealth Office of Technology will host seven free seminars on a wide range of information security topics during the month of October at the Commonwealth Data Center, starting on October 6th.

The seminars are being held in conjunction with National Cyber Security Awareness Month, an outreach effort led by the National Cyber Security Alliance (NCSA), the U.S. Department of Homeland Security (DHS) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) to raise awareness of IT security issues.

2011 Cyber Security Awareness & Training Resources

1. **Executives/Public Officials**
   Governor Steve Beshear will be approached to issue a proclamation of October 2011 as Cyber Security Awareness Month. Governor Beshear has issued this proclamation annually since he has held the office of Governor of the Commonwealth of Kentucky.

2. **State Workforce**
   In 2011, October Security Awareness Month will be promoted by the sponsorship of events including informational speakers provided by Kentucky's business partners and by the Kentucky Attorney General's Office. A web page is developed annually to promote October cyber security events and to highlight available resources. This is in addition to outreach efforts by email and agency contact memos.

   The Commonwealth Office of Technology distributes the MS-ISAC cyber security toolkit materials to representatives of numerous state agencies for distribution throughout state government.

3. **Citizens**
   Cyber security newsletters consisting of rebranded content provided by MS-ISAC are placed on the COT CISO website at http://technology.ky.gov/ciso along with external links to helpful cyber security information.

4. **IT/Security Staff**
   COT issues cyber security alerts and security awareness bulletins to state government security staff. These alerts and bulletins highlight current cyber security vulnerabilities and provide actionable guidance to agency security and IT staff. See: http://technology.ky.gov/Pages/alerts.aspx

Louisiana

Louisiana CISO: Michael Gusky; security@la.gov; (225) 219-9475
Louisiana IT Security Home Page: http://doa.louisiana.gov/oit/IT_Security_Index.htm
Louisiana Security Newsletters: http://doa.louisiana.gov/oit/Security_Newsletter.htm

Maine

Maine Security Contact: Kevin Jones; kevin.jones@maine.gov
Maine IT Security Homepage: http://www.maine.gov/oit/security/index.shtml

Maryland

Maryland CISO: Ron Witkowski; Ron.Witkowski@doit.state.md.us; (410) 260-6322

Maryland Cyber Security Webpage:
http://doit.maryland.gov/cybersecurity/Pages/CyberSecurityHome.aspx

Maryland Cyber Security Multimedia:
http://doit.maryland.gov/CYBERSECURITY/Pages/Multimedia.aspx

Maryland Cyber Challenge & Conference Webpage: http://www.mdc3.org

In conjunction with National Cyber Security Awareness Month, Maryland will be hosting their first ever Maryland Cyber Challenge & Conference October 21-22. This event will focus on advancing the field of cybersecurity across the public, private and academic sectors.

Massachusetts

Massachusetts CSO: Dan Walsh; dan.walsh@state.ma.us

Massachusetts Security Education and Awareness Webpage:
http://www.mass.gov/?pageID=afsubtopic&L=4&L0=Home&L1=Research+%26+Technology&L2=Cyber+Security&L3=Security+Education+%26+Awareness&sid=Eoaf

Massachusetts Cyber Security Website:
http://www.mass.gov/?pageID=aftopic&L=3&L0=Home&L1=Research+%26+Technology&L2=Cyber+Security&sid=Eoaf

Michigan

Michigan CSO: Dan Lohrmann; lohrmannd@michigan.gov
Michigan Department of Technology, Management & Budget (DTMB) – Cybersecurity Homepage:
http://www.michigan.gov/cybersecurity

Cyber Security Awareness Month Toolkit:
http://www.michigan.gov/cybersecurity/0,1607,7-217-51788---,00.html

Michigan DTMB – Internet Security for Citizens and Government – Video Resources:
http://www.mi.gov/cybersecurity/0,1607,7-217-51219---,00.html

Michigan DTMB – Michigan Online Security Training (MOST) Webpage:
http://www.mi.gov/cybersecurity/0,1607,7-217-48642---,00.html

Michigan Cyber Summit 2011 WebPage: http://www.michigan.gov/cybersummit
Press Release: http://www.michigan.gov/dmb/0,4568,7-150-9131_9352-260030--,00.html
Event Registration: http://events.esd.org/

The Michigan Cyber Summit 2011, hosted by Michigan Governor Rick Snyder, will be the national launch of the October 2011 National Cyber Security Awareness Month. This kick-off event is scheduled for October 6 and 7 at Eastern Michigan University's Marriott Eagle Crest Hotel and Convention Center. The Summit will bring together experts to address a variety of cyber security issues affecting business, education, information technology, economic development, law enforcement and personal use.

The Summit is a partnership between all levels of government, including local collaboration from groups such as the Washtenaw County Cyber Citizenship Coalition, State of Michigan Office of the Governor, US Department of Homeland Security-National Cyber Security Division, National Cyber Security Alliance and many private partners. The agenda for the event will feature recognized speakers and experts from around the country.

National-level speakers will be providing solutions during the following five featured tracks:

- Track #1: Business - Solutions for protecting data, networks, Wi-Fi, and employee accounts.
- Track #2: Education - Solutions for educators including cyberbullying, sexting, and using social media in the classroom.
- Track #3: Home Users/Families - Smart phone safety, online purchasing and banking, phishing scams, identify theft and protecting children online.
- Track #4: Law Enforcement - Solutions for preventing and responding to cyber crime, creating a local coalition to raise awareness and education residents on cyber safety.
- Track #5: Government - State, local and federal issues, challenges and solutions for government security professionals

Michigan (continued)

Business Case for Overall Security Program that Includes Training and Awareness—State of Michigan: Michigan's Department of Information Technology identified that citizens want web 2.0 transactions. However, a survey of Michigan citizens indicated that they were more afraid of identity theft than job or home loss or a terrorist attack. These findings supported Michigan's "Security 2.0: Next General Security" program that includes awareness and training efforts. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Business Case, p. 7)

Michigan Online Security Training (MOST) has four parts: at work, at home, government laws, and business issues. It can be taken anonymously by anyone, including citizens. State employees can register to take the training and receive a certificate if they obtain a sufficient score and can sign-up for notices of MOST updates. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Online training, p. 12)

Michigan coordinates CISSP training and certification of IT Security staff. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Training, p. 12)

Minnesota

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

Minnesota Office of Enterprise Technology – Cyber Security Awareness Website:
http://mn.gov/oet/support/training/cyber-security-awareness/index.jsp

Minnesota Office of Enterprise Technology – Cyber Security Toolkit:
http://mn.gov/oet/support/training/cyber-security-awareness/cyber-toolkit.jsp

Minnesota Cyber Security Awareness Website:
http://mn.gov/oet/support/training/cyber-security-awareness/

Mississippi

Mississippi CISO: Jimmy Webster; Jimmy.Webster@its.ms.gov; 601 359-2690

Mississippi Dept. of Information Technology - Information Security Page:
http://www.its.ms.gov/services_security.shtml

Mississippi Dept. of Information Technology – Cyber Security Training:
http://www.its.ms.gov/services_security_training.shtml

Missouri

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

Montana

Montana Security Officer: Lynne Pizzini; lpizzini@mt.gov
Montana Information Technology Services Division Webpage: http://itsd.mt.gov/default.mcpx

Nebraska

Nebraska CISO: Brad Weakly; brad.weakly@nebraska.gov
Nebraska Cyber Security Center Webpage: http://www.cio.nebraska.gov/cybersecurity/
Nebraska Cyber Security Conference Webpage: http://www.cio.nebraska.gov/cybersecurity/events/

2011 Cyber Security Awareness Month Activities

Security preparedness and awareness are of particular importance this year with additional focus on the use of social media sites and mobile device security. This year's theme is to get more value out of what we already have and a push toward more end-user Security awareness training and personal responsibility.

Past work on the State's personal mobile device use policy resulted in the approval of the Nebraska Information Technology Commission policy 5-204 "Linking a Personal Portable Computing Device to the State Email System".

The sixth annual Nebraska Cyber Security Conference was held on July 26th 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.

The State of Nebraska continues to make progress in securing information resources, reducing associated vulnerabilities and updating policy. Over the course of the last two years, the NITC Security Work Group has worked with the State Government council, the Technical Panel and Agencies in order to formulate new polices for emerging technologies and update existing policies. Work has also been done to unify our approach to federal audits and to reduce the individual Agency work along with providing a consistent and accurate response to audit requirements.

Nevada

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

Nevada Dept. of Information Technology – Office of Information Security Webpage:
http://infosec.nv.gov/

Nevada DIT-OIS Security Awareness and Training Webpage:
http://infosec.nv.gov/Security_Awareness.htm

New Hampshire

New Hampshire CISO: Leslie Williams; Leslie.Williams@doit.nh.gov
New Hampshire Dept. of Information Technology - Security Webpage: www.nh.gov/doit

DoIT established a Cybersecurity Advisory Council (CAC) to assist with the development of a strategy to address cybersecurity risks to the state's data, information assets and technology resources. The council Chair is the Chief Information Security Officer (CISO). The CAC's mission is to improve cybersecurity across State of New Hampshire government and its stakeholders by promoting awareness, developing effective policies and solutions, and obtaining supportive consensus for enterprise-wide initiatives that advance the cybersecurity of information assets and technology resources. The CAC strengthens the partnership between business and technology required to collaboratively address cybersecurity.

DoIT, in partnership with Homeland Security and Emergency Management (HSEM), participated in the Regional Catastrophic Preparedness Grant Program (RCPGP). This federally funded effort focused on strengthening local and regional abilities to restore essential government operations following a catastrophic event. Regions chosen for this grant effort included the Commonwealth of Massachusetts, the City of Boston, the City of Providence, and the State's of New Hampshire and Rhode Island. During this effort, NH identified critical infrastructure assets, provided information for capabilities and risk assessments, and developed a Cyber Disruption Plan which was tested by a state cyber drill then a regional exercise that included all disciplines of emergency response personnel.

NH recognizes the need and benefit of providing an externally facing Cybersecurity web site; this site is currently in the planning phase.

New Jersey

New Jersey CISO: John Essner; John.Essner@oit.state.nj.us
New Jersey Info Secure: http://www.state.nj.us/njinfosecure/about/
New Jersey Security Awareness: http://www.state.nj.us/njinfosecure/practices/
New Jersey Cyber Security Resources: http://www.state.nj.us/njinfosecure/other/

NJ Info Secure (www.state.nj.us/njinfosecure/) is New Jersey's website for computer and information security updates, alerts and advisories. Also included are security newsletters, educational resources for children/teens/parents, computer emergency links, federal and local government resources, glossaries, RSS news feeds, and other security resource links.

New Mexico

New Mexico State CISO: Vacant
New Mexico Dept. of Information Technology Webpage: http://www.doit.state.nm.us/
New Mexico Dept. of Information Technology Office of Security:
http://www.doit.state.nm.us/securityoffice.html

New York

New York State Office of Cyber Security – Director: Thomas D. Smith; tsmith@dhses.ny.gov
New York Office of Cyber Security Website: www.dhses.ny.gov/ocs/
New York State Division of Homeland Security and Emergency Services Website: www.dhses.ny.gov

October 2011 is National Cyber Security Awareness Month and this year's theme is "*Cyber Security is OUR Shared Responsibility*," one of the basic tenets of implementing security. If each of us does our part, together we can create strong defenses against cyber threats. To that end, the NYS Office of Cyber Security (OCS), in partnership with the Multi-State Information Sharing and Analysis Center, the U.S. Department of Homeland Security, the National Cyber Security Alliance and the National Association of State Chief Information Officers, offers free awareness materials "toolkit" to assist organizations in educating employees, partners, and citizens about cyber security.

The toolkit, which includes downloadable posters, calendars, bookmarks, guides, brochures, and other content, is designed to promote the delivery of a consistent cyber security awareness message by reinforcing core themes in practical, informative, and entertaining ways. Everyone is encouraged to use the information to promote cyber security awareness. The awareness "toolkit" and other free materials are available on the OCS website – www.dhses.ny.gov/ocs.

Also available on the OCS website are a wide variety of resources that can be used to support efforts to improve cyber security. These resources include advisories and information bulletins, policies that can be used as best practices, training videos and materials, newsletters and brochures, links to training opportunities, and information concerning national high school and college cyber security competitions and special events.

For more information on October Cyber Security Awareness Month, please visit: www.dhses.ny.gov/ocs/awareness-training-events/#awareness.

North Carolina

North Carolina CISO: Chip Moore; chip.moore@nc.gov; (919) 754-6300
North Carolina State CIO Homepage: http://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: http://www.esrmo.scio.nc.gov/initiatives/awarenessTraining.aspx

North Carolina Dept. of Justice – Consumer Homepage: http://ncdoj.com/Consumer.aspx

2011 Cyber Security Awareness Training & Resources

1. Executives/Public Officials
Working with the Office of the Governor of North Carolina, the Governor has issued proclamations to increase awareness of significant issues to North Carolinians and has declared October as Cyber Security Awareness Month. Each year, since 2006, the Governor has issued a proclamation in support of Cyber Security Awareness Month to ensure executive attention is given to this important issue. Additionally, the Governor has issued Executive Directives related to security and risk management, for example on December 16, 2008 Executive Directive No. 21 Establishing Guidelines for Encrypting Mobile Devices was sent to all Cabinet Secretaries. These and other measures raise the awareness of IT security to the highest levels of government.

2. State Workforce
Collaborating with Human Resources/Personnel Departments—State of North Carolina: The state CIO's office coordinated with the state's personnel department for IT security training as part of a larger executive assistants training course. Topics include spam, phishing, spyware and spam, security and online collaboration tools, and telephone communications. Security staff also make presentations on IT security at various events.

Focus is highlighted throughout the cyber security awareness website with security tips aimed at all levels of government and home users and for safe child Internet browsing (www.esrmo.scio.nc.gov/CyberSecurity.htm).

3. Citizens
Several departments/agencies offer targeted information for various groups. The NC Attorney General offers a comprehensive consumer protection website for state citizens. (http://ncdoj.com/Consumer.aspx).

4. IT/Security Staff
Cyber Security Awareness Initiatives: North Carolina's CIO's Enterprise Security and Risk Management Office (ESRMO) distributes security alerts and warnings throughout the state. ESRMO offers incident management training at no cost for executive branch agencies. Local governments and universities can also participate. In partnership with the Department of Homeland Security (DHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Enterprise Security and Risk Management Office (ESRMO) North Carolina Information Sharing and Analysis Center (NC-ISAC)

North Carolina (continued)

offers online training sessions to heighten awareness on various topics. Also offered are monthly and quarterly newsletters that augment the information provided.

Courses that focus on incident response training, risk management and state information security manual training are available through North Carolina's State CIO Office. Additionally, a wider more general array of cyber security topics are offered through online training funded by DHS and promoted by the NC-ISAC.

At the NC Office of Information Technology Services (ITS) all staff are required to complete online security training and sign policy compliance and non-disclosure forms annually. Mandatory new employee training includes security and risk management. The training program defines goals through employee work and training plans and supports staff efforts to obtain and maintain security certifications.

North Carolina has in-person and online training.

North Dakota

North Dakota CISO: Lisa Feldner (CIO); lfeldner@nd.gov
North Dakota IT Security Home Page: http://www.nd.gov/itd/services/it-security/

Throughout the year, the North Dakota Information Technology Department (ITD) provides Cyber Security Awareness to all state agencies. Specifically, ITD provides staff training through the State Enterprise Learning Management program. The current ELM training is computer based. The training is titled, "Securing the Human".

On a monthly basis, ITD sends unique cyber security awareness posters and corresponding newsletters to agency IT Security staff for staff education.

ITD notifies all designated agency IT Security staff of potential security risks through an early warning listserv. Once notified, the agency IT Security staff alerts their staff of the risks and how to report malicious activity.

In October 2010, North Dakota Governor John Hoeven signed a Proclamation declaring October as Cyber Security Awareness Month. Awareness activities included updating the State Cyber Security Portal; a presentation on cyber security during State Quarterly IT Directional Meeting; distribution of MS-ISAC Cyber Security Toolkit materials to agencies; distribution of Monthly Cyber Security Tips Newsletters to all designated agency IT Security staff for redistribution to agency personnel; Cyber Security Educational Booth at State Information Technology Department employee event; displayed Cyber Security Awareness posters in every conference room; provided tips and reminders that October is Cyber Security Awareness Month; the State Office of Attorney General utilized the branded Public Service Announcements from MS-ISAC to reach general public. Target audience included State and local government agencies as well as citizens of the State.

North Dakota is preparing to perform similar activities in October 2011.

Ohio

Ohio CISO: David Shaw; david.shaw@oit.ohio.gov
Ohio Chief Privacy Officer: Daren Arnold; daren.arnold@ohio.gov
Ohio IT Security-Privacy Home Page: http://privacy.ohio.gov/
Ohio Privacy and Security – Education and Awareness Webpage:
http://privacy.ohio.gov/EducationAwareness.aspx

Oklahoma

Oklahoma CISO: Ken Ontko; ken.ontko@osf.ok.gov
Oklahoma Cyber Security Webpage: http://www.ok.gov/homeland/Cyber_Security/index.html
Oklahoma IT Security Services Webpage:
http://www.ok.gov/OSF/Information_Services/ServiceCatalog/SecurityServices/index.html

Oklahoma Information Services Webpage: http://ok.gov/OSF/Information_Services/index.html

2011 Cyber Security Awareness & Training Resources

1. **Executives/Public Officials**
   An event for this group in October is being planned, but has not yet been scheduled.

2. **State Workforce**
   Oklahoma plays a leadership role in the Cyber Security Educational Consortium (CSEC)—a National Science Foundation Advanced Technological Education (ATE) Regional Center of Excellence dedicated to building an information security workforce who will play a critical role in implementing the national strategy to secure cyberspace. http://www.cseconline.org/

   Oklahoma is working with the State Board of Regents for Higher Education and the State Department of Education in support of the MS-ISAC and the Center for Internet Security for the U.S. Cyber Challenge (USCC)—a national competition for high school students to identify future cyber security experts. http://workforce.cisecurity.org/

   Oklahoma has made several proposals to provide Cyber Security Awareness Training and is currently working to obtain funding approval to implement the selected alternative.

3. **Citizens**
   No direct contact other than through involvement with organizations such as InfraGard, ISSA, ISACA, ACP and similar groups; additionally addressed with Web presence.

4. **IT/Security Staff**
   Activities include:
   a. Three Quarterly Cyber Security Focus Group 6 hour meetings;
   b. 7th Annual Cyber Security Awareness Seminar—a 2 day event scheduled for October 19th and 20th this year; we will again use a "Crawl, Walk, Run Approach" for our table top exercise and the theme for 2011 is Governance, Risk and Compliance in a Consolidated Environment.
      1) Crawl: Includes two primary course tracks -- one focusing on Technology Staff and Administrators and the second on Management and Supervisors;
      2) Walk: Provides a "Table Top Exercise" that focuses on "Incident Response", with specific scenarios taken from actual events during the year;
      3) Run: Provides a "Hands-on Lab" that leverages the use of mobile labs to support training and experience with actual malware and tools to identify and mitigate problem scenarios.

Oklahoma (continued)

Oklahoma's 2009 NASCIO Recognition Awards submission describes their extensive progress in developing cybersecurity training and education programs. E.g.,

> In 2008, Oklahoma worked to consolidate, leverage and advance its security initiatives with the formation of a comprehensive Information Security Training & Education Program (I-STEP), see Figure 1 on page 6. This program fuses together and builds upon the already established components of cross-organization teaming, synchronized communications, law enforcement partnerships, coordinated incident response, risk identification and mitigation, and information dissemination. The vision is to facilitate an increased conceptual awareness of information assurance issues and objectives while implementing effective planning and management practices to achieve compliance with State and Federal statutes. In short, I-STEP seeks to leverage and develop existing education and administration programs to ensure compliance with defined policies, procedures, standards and guidelines through effective governance and accountability.

Oregon

Oregon CISO: Theresa A. Masse; theresa.a.masse@state.or.us
Oregon Enterprise Security Office Webpage: http://www.oregon.gov/DAS/EISPD/ESO/index.shtml
Oregon Information Security Resource Center: http://secureinfo.oregon.gov/

Oregon is committed to improving information security awareness throughout state government. Eight security awareness training modules were developed focused on best practices all employees and contractors should understand and implement. The modules are accessible through the states online learning program so agencies can track and audit participation. Local government entities also can use the training courses. The modules are easy to customize so agencies can insert their policies and procedures.

The Enterprise Security Office (ESO) also provides a variety of forums and workshops for all agencies on timely information security and risk topics. ESO offers a wide variety of tools and templates agencies can use to develop their policies and plans along with resources for the public to access on The Information Security Resource Center.

The ESO is a key partner in the state's recent initiative to implement an Enterprise Risk Management (ERM) program.

Pennsylvania

Pennsylvania CISO: Erik Avakian; eavakian@pa.gov; (717) 722-4240
Pennsylvania IT Security Homepage: http://cybersecurity.state.pa.us
Pennsylvania Cyber Security Awareness Webpage:
http://www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494

Pennsylvania Cyber Security Best Practices Webpage:
http://www.cybersecurity.state.pa.us/portal/server.pt/community/best_practices/495

Pennsylvania Security Awareness Resources and Tips:
http://www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/resources_and_tips/203340

Pennsylvania Security Awareness Posters:
http://www.cybersecurity.state.pa.us/portal/server.pt?open=512&objID=494&&PageID=205259&mode=2

Pennsylvania Cyber Security Toolkit: http://www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/security_awareness_toolkit/203338

Pennsylvania Security Awareness Cyber Quiz:
http://www.cybersecurity.state.pa.us/portal/server.pt/community/security_awareness/494/cyber_quiz/203342

Cyber Security For Kids:
http://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.

2011
The commonwealth 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. Now in its seventh year, 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 cyber security. With the increasing use of technology in government, educational institutions, businesses, and homes, we must ensure that our individual actions have a collective impact on cyber security 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. In the coming weeks, OA/OIT will be distributing cyber security calendars, security awareness bookmarks, posters, and brochures to agencies. In addition, the governor will issue a proclamation and news release declaring October as Cyber Security Awareness Month. We will be promoting the new "Cyber Pledge" contest run 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

Pennsylvania (continued)

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 cyber security seriously. The Cyber Pledge Contest will run from September 1st to October 31st. The purpose of the contest will be to see which state and local government have the most "cyber secure" citizens, as illustrated by how many sign the pledge. OA/OIT will also be conducting an internal exercise in October to enhance overall security awareness. Additionally, we will host several cyber security awareness and educational presentations as part of our "Cyber Fridays" series at the Commonwealth Technology Center. Each Friday throughout the month of October, we will host two separate sessions daily on security awareness. All agency users all encouraged to participate in these events and share these opportunities with appropriate IT staff.

Cyber Friday themes and topics will include:

- Emerging Cyber Security Threat Landscape
- Computer Forensics and Incident Response
- Application Security
- Risk Management
- Network Security

Puerto Rico

Puerto Rico Chief Security Officer (CIO): Juan Rodriguez de Hostos; jerodriguez@fortaleza.pr.gov

Rhode Island

Rhode Island CISO: Ernest Quaglieri; equaglieri@doit.ri.gov; 401-462-9202
Rhode Island IT Security Home Page: http://www.doit.ri.gov/security/infosec/index.php

2011 Cyber Security Awareness Training & Resources

1. **Executives/Public Officials**
   Materials from MS-ISAC including a guide to firewalls, Internet and Acceptable Use templates, Local Government Cybersecurity and Guide to properly Disposing of Media.

2. **State Workforce**
   Specialized training is provided where required for users of federal or specialized systems. Cyber-Security posters are displayed throughout the state footprint.

3. **Citizens**
   There is no citizen training or awareness at this time.

4. **IT/Security Staff**
   IT Security Staff members have a number of industry recognized certifications, such as CISSP, MCSE, SANS GSEC, GCIH and GSNA. Also, two staff are Certified Computer Examiners.

South Carolina

South Carolina CISO: David O'Berry; doberry@ppp.state.sc.us
South Carolina ISAC: https://sc-isac.sc.gov/

Security Training, Awareness and Policy Services:
https://sc-isac.sc.gov/content/sans-security-awareness-training-0

South Carolina IT Security Homepage:
http://www.cio.sc.gov/productsandservices/securitymain.htm

South Dakota

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

This state's online security training system includes an Information Technology User Security Guide with IT security policies and procedures for state employees and contractors. All current state employees were required to take this course and each new state employee takes the course at his or her new employee orientation period. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Online training, p. 12)

Tennessee

Tennessee CISO: Jason Gunnoe; jason.gunnoe@state.tn.us

Tennessee Office for Information Resources Webpage:
http://www.state.tn.us/finance/oir/security/

Tennessee OIR Cyber Security Awareness Month Webpage:
http://www.state.tn.us/finance/oir/security/cybersecurity.html

Texas

Texas CISO (Acting): Doug Holt; doug.holt@dir.state.tx.us
Texas Dept. of Information Resources – SecureTexas Website:
http://www.dir.state.tx.us/securetexas/

Risk Assessments Regarding Social Engineering—State of Texas: The State's Department of Information Resources conducted penetration testing of many agencies to determine if agency employees were vulnerable to phishing and other types of attacks that use social engineering. This helped to identify agencies' training needs and build the business case for funding that training. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Baseline (?) p. 4)

[Texas] provides periodic cyber-security forums and conferences, including an Annual Cyber Security Forum, and information on security-related educational opportunities that might interest agencies' Information Security Officers. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Use Agency CSOs, p. 8)

Utah

Utah CISO: Boyd Webb; boydwebb@utah.gov
Utah Enterprise Information Security Office Webpage: http://dts.utah.gov/security/

In 2006, Utah initiated an online training program for state employees, in conjunction with Cyber Security Awareness Month. In that year, more than 16,000 state employees completed online awareness training (over 90% of Executive Branch employees). In addition, the Judicial and Legislative branches also had significant participation—resulting in more than 75% of all State employees completing the training. By the end of 2006, 96% of all Executive Branch employees had completed the training. Since that time, annual training has regularly exceeded 95%.

A record that employees have passed the online training is entered in employee's personnel records.

The 2011 program covers the following categories of information:

1. Authentication and Password Management
2. Security Threats and Menaces
3. Internet Security and Malicious Code
4. Awareness of Social Engineering
5. Identity Theft and Fraud

More detailed information can be found in Utah's 2009 Recognition Awards nomination at the following address: www.nascio.org/awards/nominations/2009/2009UT9-nasciosecurity2009.pdf.

Business Case for Online Training Tool—State of Utah: Utah has supported its business case for an enterprise online IT security training tool by citing the time that would be saved by employees in terms of travel time to in-person training and reduction of time spent by agency security personnel providing awareness and training and answering employee questions. In addition, online training saves costs in terms of travel, facilities and dedicated trainer costs. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Business Case, p. 7)

Forging New Partnerships—State of Utah: Through its new online training tool for IT security, Utah's CIO forged new relationships with the state's Risk Management and Surplus Property Departments, and the Bureau of Criminal Identification. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Partnering with other agencies, p. 8)

Vermont

Vermont CISO: Kris Rowley; kris.rowley@state.vt.us; (802) 828-0911
Vermont Information Security Webpage: http://itsecurity.vermont.gov/
Vermont Security Tools: http://itsecurity.vermont.gov/Security_Tools

Virginia

Virginia Acting 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/

Past awareness activities included information for agency heads to ensure they are meeting code requirements related to the security of electronic information held by the Commonwealth. Two of those relate to IT security audits and reporting breaches. Virginia had two first-place winners, two second-place winners and one third-place winner in MS-ISAC's 2010 poster contest. (***MS-ISAC After-Action Report, 2010***)

For the 2009 MS-ISAC poster contest, Virginia had three first-place winners, and two second-place winners. A Commonwealth Information Security Conference for state and local government attendees was held to assist in fulfilling our shared mission of securing information. "Information Security: Mission Possible!" was the theme of the conference held Nov. 2, 2009. Participants were from the executive (including higher education), judicial and legislative branches of state government, independent agencies and localities.

Virginia's Telly award-winning video, which is designed to promote simple changes in behavior that strengthen the security of Commonwealth information, was produced in-house by VITA staff and made available at no charge to any state entity. Agencies are encouraged to share the video with their staff. In addition to being posted online on the Commonwealth of Virginia YouTube channel, Commonwealth information security officers have been provided DVDs.

Watch the video: Duhs of Security (***MS-ISAC After-Action Report, 2009***)

Washington

Washington CISO: Agnes Kirk; agnesk@dis.wa.gov
Washington State IT Security Webpage: http://techmall.dis.wa.gov/sec.aspx

West Virginia

West Virginia CISO: Jim Richards; jim.a.richards@wv.gov
West Virginia Office of Technology: http://www.technology.wv.gov/

The West Virginia Office of Information Security and Controls is sponsoring a cyber-security awareness event on October 5, 2011, at the Culture Center Theatre at the State Capitol campus. The agenda will offer dynamic presentations delivered by world-class experts in the areas of cyber threats, effective practices to safeguard systems and data, with an emphasis on individual accountability, risk management, and privacy issues.

West Virginia Office of Information Security and Internal Control:
http://www.technology.wv.gov/security/
The mission of the Office of Information Security and Internal Controls 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.

West Virginia Security Training and Awareness:
http://www.technology.wv.gov/security/awareness/
It is important to have security awareness training in almost any type of industry. Whether inside or outside the organization, crime can have a devastating effect on your company or personal lives. Professional training will help you become proficient at spotting suspicious activity, which in turn can reduce the opportunities for crime to occur.

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

Policies Issued by the CTO:
http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

The 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.

Wisconsin

Wisconsin CISO: Mike Lettman; mike.lettman@wisconsin.gov
Wisconsin IT Security Webpage: http://itsecurity.wi.gov/
Wisconsin IT Security Awareness Webpage:
http://itsecurity.wi.gov/section_detail.asp?linkcatid=2907&linkid=1498&locid=89

Wyoming

Wyoming Security Contact: Michael Crouch; mike.crouch@wyo.gov
Wyoming Cyber Security Homepage: http://www.wyoming.gov/cybersecurity.aspx

Wyoming provides information for children, publications, bookmarks, calendars, and posters.