September 2009

NASCIO
Representing Chief Information
Officers of the States

STATE CYBER SECURITY RESOURCE GUIDE

AWARENESS, EDUCATION & TRAINING INITIATIVES

SECURING
GOVERNMENT
IN A DIGITAL WORLD

TABLE OF CONTENTS

NASCIO
Representing Chief Information Officers of the States

BACKGROUND

In support of the sixth annual National Cyber Security Awareness Month, the National Association of State Chief Information Officers (NASCIO) has 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. Their efforts have been documented previously in NASCIO briefs, most recently the 2007 publication, ***IT Security Awareness and Training: Changing the Culture of State Government,*** as well as through NASCIO Recognition Award submissions, many of which are available on NASCIO's website.

For this year's observance, NASCIO has created this Resource Guide of examples of state awareness programs and initiatives, as 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. The compendium augments previously gathered information with data from a just-completed, short survey of state CISOs. It includes contact information for the latter, hyperlinks to state security and security awareness pages, and information describing cyber security awareness, training, and education initiatives that target four categories: Executives/Elected Officials; Citizens; State Workers; and IT Security Personnel.

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.

ALABAMA

Alabama CISO: Lee Styres; lee.styres@isd.alabama.gov; (334) 242-3044
Alabama Cyber Security Awareness and Training Resources Webpage:
www.isdtraining.alabama.gov/Cyber_Security_Awareness.aspx

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 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)

2008
Proclamation signed by Governor Robert Riley. Awareness activities included the distribution of toolkit materials to all state agencies and some local schools; Target audience included all state employees, county and local governments and the general public. (***MS-ISAC After-Action Report, 2008***)

2007
Proclamation signed by Governor Robert Riley. (***MS-ISAC After-Action Report, 2007***)

ALASKA

Alaska CSO: Darrell Davis; darrell.davis@alaska.gov; (907) 269-6733
Alaska Security Awareness Webpage: http://security.alaska.gov/awareness.shtml

State Security Office: www.state.ak.us/local/akpages/ADMIN/info/security (Link to MS-ISAC on this page). Also links from this page:

SOA Security Awareness:
www.state.ak.us/local/akpages/ADMIN/info/security/awareness.shtml

SOA Training Awareness:
www.state.ak.us/local/akpages/ADMIN/info/security/training/home.shtml

Cyber Security Awareness Toolkit Instructions & Documentation:
www.state.ak.us/local/akpages/ADMIN/info/security/training/home.shtml

Identity Video:
www.state.ak.us/local/akpages/ADMIN/info/security/training/home.shtml

2008

Proclamation signed by Governor Sarah Palin. Awareness activities included the distribution of toolkit materials to all state agencies and some local schools; Target audience included all state employees, county and local governments and the general public. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Sarah Palin. Awareness month activities included the following: establishment of a quarterly Security Newsletter; enhancements to the security website, including on-line training materials available via streaming; distribution of a direct mailing of awareness and training materials to 226 communities in Alaska; presentations to the State Infragard, numerous corporations, and local agencies; and distribution of the MS-ISAC cyber awareness materials at six Governor events. (***MS-ISAC After-Action Report, 2007***)

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 Governor Signs Cyber Security Executive Order (Jan 08)
http://azgovernor.gov/dms/upload/EO%202008-10.pdf

Arizona Security Roundtable: www.homelandsecurity.az.gov/asrt

Proclamation: October 31st is Cyber Security Day in Arizona

Arizona Security Training and Awareness Standard:
www.azgita.gov/policies.../P800-S895%20Security%20Trng.pdf

2008

Proclamation signed by Governor Janet Napolitano. Awareness activities included multiple cyber security awareness sessions for staff and client agencies hosted by the Department of Administration Information Security; the State Infrastructure Protection Center (SIPC) promoted information and event awareness via weekly summary on-line reports statewide; the Government Information Technology Agency hosted a tailored awareness session for Group 2 Agencies, Boards and Commissions leadership and staff; and the Statewide Information Security and Privacy Office promoted information with Agency Information Security and Privacy Officers. Arizona's target audience consisted of: 120 executive branch agencies, boards and commissions and approximately 50,000 employees; Agency Information Security and Privacy Officers (including Deputy Directors); Statewide recipients of SIPC weekly summary notifications; and indirect audiences include the Courts, Legislature and Universities. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Janet Napolitano. Arizona's Department of Administration Information Security (AIS) department hosted multiple cyber security awareness sessions for staff and client agencies. On October 17th, AIS department hosted cyber security awareness day. IT standards compliance training session was held for 120 agencies. The primary target audience was the 120 executive branch agencies and their approximate 50,000 employees. Indirect audiences include the Courts, Legislature and Universities. MS-ISAC Toolkit materials were shared with CIOs of 120 agencies, boards and commissions. (***MS-ISAC After-Action Report, 2007***)

ARKANSAS

Arkansas Security Officer: Kym Patterson; kym.patterson@arkansas.gov
Arkansas IT Security Homepage: www.dis.arkansas.gov/security/index.htm
Arkansas Cyber Security Toolkit:
www.dis.arkansas.gov/security/cybersecurity_toolkit.htm
Security Newsletters: Arkansas' State Security Office. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Newsletters, p. 9)

2008

Proclamation signed by Governor Mike Beebe. Awareness activities included distribution of toolkit materials to schools, libraries, and state agencies, as well as posting toolkit items on the state security website. Other activities included rolling out a new cyber security awareness training program for the Department of Information Systems, "cyber security awareness" as the focus of the Arkansas Continuity of Operations Program monthly Newsletter, and including cyber security awareness tips in newsletters to state IT customers. Target audience included all state employees, K-12 school faculty, staff and students, and public library patrons. (***MS-ISAC After-Action Report, 2008***)

CALIFORNIA

California CISO: Mark Weatherford; Mark.Weatherford@OISPP.ca.gov; 916-323-7322
California Office of Information Security & Privacy Protection:
www.oispp.ca.gov/government/default.asp

California OISPP Security Awareness Webpage:
www.oispp.ca.gov/government/library/awareness.asp

California OISPP Security & Privacy Training Resources Page:
www.oispp.ca.gov/government/library/training.asp#ISLA

California Office of Privacy Protection Training Program (www.oispp.ca.gov/government/privacy/default.asp**):**

State Employee Privacy Training
Protecting Privacy in State Government, Basic Training for State Employees
PowerPoint Presentation (.ppt, 1344k)
Presentation with Speaker Notes (.doc, 14mb)
Self-Training Manual (.doc, 852k)
Guidelines for Self-Training Manual (.pdf, 94k)

This is described more fully in the Office of Privacy Protection's 2009 NASCIO Recognition Award Nomination (see: www.nascio.org/awards/2009awards/securityPrivacy.cfm).

2008

Proclamation signed by Governor Arnold Schwarzenegger. Activities included an Information Security Officer meeting in September where activities were discussed for October; posting and distribution of the MS-ISAC newsletter; email reminders regarding the campaign and ideas that state and local governments could use to reach their employees about cyber security awareness. Target audience included approximately 3,000 state and local government employees. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Arnold Schwarzenegger. On October 10th, California celebrated its first annual Cyber Security Symposium for government, calling it "Securing California: Exploring Cyber Security Solutions for California Government." It was a full day's celebration with over 300 attendees including top level directors, managers, and security professionals from state/local government. Presentation was also made at the data center's Security Fair on two topics: From Server Room to Board Room and ISO Roles and Responsibilities Three new products were developed and released: Information Security Program Guide, Information Security Officer Role and Responsibility in State Government and a Risk Assessment Toolkit. California issued a Pay Warrant cyber security message on all 225,000 state employees pay stubs announcing October as National Cyber Security month and providing some tips for them. The State also released a prepared message that state agencies could easily resend to their employees announcing October as National Cyber Security Month. (***MS-ISAC After-Action Report, 2007***)

COLORADO

Colorado CISO: Seth Kulakow; seth.kulakow@state.co.us;

Colorado Cybersecurity Website: www.colorado.gov/cybersecurity/

Colorado OCS Resources Page:
www.colorado.gov/cs/Satellite/Cyber/CISO/1207820731491?rendermode=preview

NASCIO 2009 SURVEY RESPONSE:

State Employee Security Awareness Project Description: The goal of the employee awareness campaign is for each attending State Employee to achieve a basic level of understanding of Information Security and (general) technology in their daily **home-computing lives**. By showing them how common home technologies work such as WIFI proper configurations and security best practices and how they can positively and negatively affect their home environments, then we are hoping to translate this new understanding into the work environment.

To do this, we enlisted Information Security and general technology personnel from various State Departments to develop content and share their information security and technology knowledge with other state employees, and be available to answer questions and provide assistance where needed, in a town hall or fair-like environment.

The on-going plan for the campaign will include events four times a year. We will survey a segment of recipients at least twice a year to measure the changes in Information Security Awareness.

Motivation & Benefits: Examples of what could be included in the Motivation & Benefits section are:

- Helping State employees recognize and respond appropriately to real and potential security concerns.
- To show State employees that the Office of Cyber Security is an effective team that includes individual State Department ISO's.
- Providing fresh, updated information to keep State employees current on new risks and what to do about them.
- Making State employees aware that the data on their computers and mobile devices (PDAs, thumb drives, smart phones, etc.) are valuable and vulnerable.
- Securing and answering questions regarding setting up technologies such as safe WIFI.
- Provide a face with a solution. Market security to all levels and backgrounds of State Employees.
- Providing information that is personally useful to State employees, such as how to avoid scams, fraud, phishing, and ID theft. Information on how to protect home PCs and how to use e-mail and the Internet safely lets State employees know that the Office of Cyber Security cares about them. Building good computing habits at home is as

important as building those behaviors at work. Secure computing habits will transfer across environments.

- Showing State employees that the Office of Cyber Security cares about protecting their information.
- Building a culture of security competence. Motivate State employees to improve their behaviors and incorporate security concerns into their decision making.
- Demonstrating a concern for security and a process for ensuring that the State's workforce will provide adequate protection for information assets entrusted to its care.
- ROSI statement

Project Plan Ideas:

1. Brief presentations on several security and general technology topics in a town hall format
2. Booths that have handout material
3. Brochures on presentations
4. Open discussions between State employees and ISO's

Established cyber training policy:
Enterprise Cyber Security Policy: Security Training and Awareness (P-CCSP-015)

Requirements:

- The Cyber Security Training Program details shall be outlined in the Agency Cyber Security Plan and support:
- All end users of systems must complete initial Cyber Security Training.
- All users must complete refresher training annually.
- Training content must be refreshed/reviewed annually.
- Training activities are to be recorded and kept in the employee's file for the duration of his/her employment.
- Annual reporting to the CISO of the Agency training completion statistics.
- Periodic delivery of security awareness training to the staff.
- Description of consequences for failure to comply with training requirements, to include the possibility of termination.

Cyber Security Training Content must include:

- The Agency's End User Acceptable Use Policy
- Colorado Cyber Security Plan overview
- The Agency Cyber Security Training Program must meet the following standards:
- Initial training is required prior to use of State or Agency systems.
- Be approved by an executive with the authority to enforce the sanctions for non-compliance.

2008

Proclamation signed by Governor Bill Ritter. Awareness activities included distribution of cyber security tips to all agencies via email; distribution of all toolkit items to state agencies as well as to area schools; posting of Governor's proclamation and distribution of awareness items at the National ISSA Conference; and a cyber threat presentation to state agency ISOs. Audience included State of Colorado employees, approximately 1,000 students, and approximately 300 ISSA Conference participants. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Bill Ritter. The following awareness activities were undertaken: released "CyberTips" statewide; a webcast with *SC Magazine* – CSO of Tomorrow; Colorado Cyber Security Council meeting – conducted security training and awareness; presented at the following: local ISSA meeting; MIS Institute Government Security Summit; Colorado CISO Lecture Series (a security training day for state and local governments); held three day Botnet/Forensics technical training course, in conjunction with Denver InfraGard; and Denver InfraGard Quarterly meeting. Several hundred individuals were reached through these events. The MS-ISAC Toolkit material has been distributed at numerous events, meetings and conferences. (***MS-ISAC After-Action Report, 2007***)

CONNECTICUT

Connecticut Department of Information Technology Cyber Security Website:
www.CT.Gov/Cybersafe

The Department of Information Technology (DOIT) launched an Information Security Awareness Program to educate employees and the public about basic information security issues and practices. The first issue had a special focus on identify theft, with resources and tips on how you can protect your own personal information.
www.ct.gov/doit/cwp/view.asp?a=1244&Q=331012

2008
Proclamation signed by Governor M. Jodi Rell. (***MS-ISAC After-Action Report, 2008***)

DELAWARE

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

NASCIO 2009 SURVEY RESPONSE:

1. **Executives/Public Officials**
   Delaware Cyber Brief 2009- a half day seminar examining the latest tactics employed by cyber criminals and predators. http://dti.delaware.gov/cyberbrief/

   Delaware's CSO is a member of the Governor's Homeland Security Advisory Council.

2. **State Workforce and IT/Security Staff**
   Delaware Cyber Brief 2009: There will be a half day seminar on October 1 examining the latest tactics employed by cyber criminals and predators.
   http://dti.delaware.gov/cyberbrief/

   Cyber Security Exercise: On October 29, DTI will host "Cyber Siege", the state's 5th 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 "hand-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 Training: Training was held in July in Dover. 54 State and City employees earned a US-DHS certification in cyber terrorism defense, along with credits toward the Delaware ISO certification. www.cyberterrorismcenter.org/

   "Cyber Ween" (That's what you get when you cross Cyber Month with Halloween!) celebration event for employees; potluck lunch and games on cyber security trivia

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

   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.

3. **Citizens**

   United States Cyber Challenge

   - Delaware has been selected as one of the three state partners that will help lead the new U.S. Cyber Challenge.
   - The goal of the Cyber Challenge is to identify and nurture America's top young people destined for careers in cyber security.
   - The program will encourage high school and college students to learn advanced skills to protect our critical infrastructure.
   - The University of Delaware and Wilmington University and Delaware Technical & Community College have been chosen as locations for the challenge.
   - We will also be working with the Department of Education to offer the program to 11th and 12th grade students. http://csis.org/uscc

   Delaware Money School—Cyber Security presentations will be conducted at the Delaware Money School during the month of October.

   Cyber Security Poster Contest for all Delaware 4th and 5th graders. Delaware has had 3 national winners in the last 2 years.

   Internet Safety and Cyber Bullying Presentations reached 2741 students in prior years, and the goal for 2009 is 3000 students.

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

   In addition, Delaware will feature:
   Governor's Cyber Security Month Proclamation signing ceremony
   Television Public Service announcements on local channels
   Cyber Security text crawl on the Weather Channel
   Advertisements on delaware.gov, delawareonline.com, and in 11 local newspapers
   Movie Theater Advertising—Cyber Security Month promotion at local Dover theaters.

4. **IT/Security Staff**

   See State workforce.

Further details about Delaware's awareness and training efforts are provided in the state's 2008 NASCIO Recognition Award submission.

2008

Proclamation signed by Governor Ruth Ann Miner. Awareness activities included a Bi-Monthly Information Security Officer Team Meeting on September 17th; October eSecurity Newsletter sent to 33,500 inboxes on 10/1; Poster Awareness Campaign, 940 posters were distributed to 81 organizations on 10/1; Cyber Security Subscription Service, scripted message sent out to 1,150 subscribers 10/3; MS-ISAC webcast facilitated, Phishing Scams: Don't Get Hooked! on 10/9; Held a Cyber Week celebration event for DTI employees on 10/23 including a potluck lunch and games on cyber security trivia; Held 1st Annual Statewide Cyber Brief, informative ½ day briefing to examine the latest tactics employed by cyber criminals and predators on 10/23. The Cyber Brief was attended by 140 State of Delaware employees; 96% of the survey respondents said the event exceeded or matched their expectations; 4th Annual Statewide Cyber Security Tabletop Exercise, "Web of Distrust" 10/29; the MS-ISAC toolkit material (posters, bookmarks, calendars) were posted on the ISO and DTI website throughout the month of October; Information Security 101 Training, scheduled for January 2009 for up to 40 students; Cyber Security Poster Contest was announced to all 4th and 5th graders statewide; 34 Presentations in 29 Schools (State, Parochial and Private), reaching 2741 students, 9 districts in all 3 counties. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Ruth Ann Miner. Delaware conducted its 3rd Annual Cyber Security Tabletop Exercise including a keynote by Assistant Secretary for Cyber Security and Communications for the Department of Homeland Security, Gregory T. Garcia. Delaware also coordinated TV Public Service Announcements. Two Delaware Transit Buses were wrapped with Cyber Security graphics and went into service on October 23. Cyber Security messages were posted on the electronic boards in all four Department of Motor Vehicles locations. A Cyber Security poster contest and commercial contest was unveiled. Flyers with a cyber security message were inserted in pay advice to all 30,000 state employees. Presentations were made to thirteen schools reaching an audience of over 2,000 students! A cyber security text crawl was placed with the Weather Channel. Advertisements with cyber security messages were placed on delaware.gov, delawareonline.com, and in 11 local newspapers. A booth was sponsored at the 2007 Delaware IT Conference on October 30 for State and School organizations; pamphlets, including MSISAC material, were offered to the 509 attendees. (***MS-ISAC After-Action Report, 2007***)

DISTRICT OF COLUMBIA

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

FLORIDA

Florida CISO: Mike Russo; Mike.Russo@aeit.myflorida.com

Florida Enterprise Information Technology Security Awareness Webpage:
www.myflorida.com/myflorida/cabinet/aeit/index.php?pg=ois_awareness

Participating with State Security Officials: The state of Florida's CISO is a member of the Florida Domestic Security Law Enforcement Terrorism Committee and has partnered with the state's Domestic Security initiative to build a business case for Cyber-funding that includes training on awareness and basic training for security managers. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Partnering with External Security Officials, p. 8)

Branding: SecureFlorida.org (Florida). (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Branding, p. 9)

Taking it to Those Who Want to Learn More—State of Florida: This state has developed the C-Safe in-person security awareness and training program that can be tailored to individual business' and organizations' needs. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Outreach, Training, p. 10)

Florida has in-person training. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Online training, p. 12)

2008

Proclamation signed by Governor Charlie Crist. Awareness activities included participation in the Florida Government Technology Conference in September, where the Agency for Enterprise Information Technology, Office of Information Security conducts a full day security track where experts in the field speak to the audience on arising threats and vulnerabilities to businesses and organizations including new and emerging technology solutions and best practices in the security area. We have been fortunate to have speakers from the FBI Cyber Division, National Cyber Security Division, US Dept. of Homeland Security and the SAIT Laboratory, Florida State University. During this event we distributed the tool kit along with other materials to the attendees. The audience included 37 State Agencies and the State Court System, their agency heads, Chief's of Staff, Inspector's General's, Chief Information Officers and Information Security Managers, Legislature and Auditor General, representatives from cities and counties, Information Technologists, private industry and Florida's citizens. The Florida Government Technology Conference had over 1,100 participants. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Charlie Crist. (***MS-ISAC After-Action Report, 2007***)

GEORGIA

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

Georgia Technology Authority – Enterprise Information Security Webpage:
http://gta.georgia.gov/00/channel_title/0,2094,1070969_84340779,00.html

Georgia Emergency Management Agency – Security Awareness Training Video:
www.gema.ga.gov/ohsgemaweb.nsf/64709FFF5B0306988525755B006E2829/E887C628DFEA3EED8525760E00562850

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

2008

Proclamation signed by Governor Sonny Perdue. (***MS-ISAC After-Action Report, 2008***)

2007

The MS-ISAC posters and materials were distributed to state agencies. Georgia also conducted the following activities: launched a refresh of the state employee security website; began pilot of in-house produced Security Awareness Video; launched inter-agency partnership for graduate level certificate in Information Assurance with follow-on Master's degree in Information Systems; and initiated inter-agency partnership for a statewide IT Security Awareness and IT security Training Program modeled after the federal guidelines. (***MS-ISAC After-Action Report, 2007***)

GUAM

Guam Security Contact: Jim Lacson (CIO); jim.lacson@bit.guam.gov

HAWAII

Hawaii Security Contact: Russ Saito (CIO); russ.k.saito@hawaii.gov

State of Hawaii Cyber Security—website (Resources, Videos, FAQ's, Monthly Newsletter):
http://hawaii.gov/dags/icsd/cst/

State Cyber Security Toolkit, Cyber Security Resources, (Link to MS-ISAC):
http://hawaii.gov/dags/icsd/cst/cyber-security-resources

IDAHO

Idaho Security Officer: Terry Pobst-Martin; terry.pobst-martin@cio.idaho.gov; (208) 332-1851

Idaho Cybersecurity Awareness Website: www.idaho.gov/cyber

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

2008

Proclamation signed by Governor C.L. "Butch" Otter. Awareness activities included a roundtable on Business Continuity, Disaster Recovery, and Risk Analysis at the Boise Information Systems Security Association Monthly Meeting; distribution of a news release distributed for media utilization describing the purpose of the Cyber Security Awareness Month, distributed throughout the state's media; presentation on software vulnerabilities at the Idaho Dept of Agriculture; participation in the National Cyber Security Awareness Webcast on Phishing; participation in the University of Idaho's annual Information Technology Service's Computer Security Awareness Symposium in the Idaho Commons Clearwater Room; Cyber Security Awareness Presentation; presentation on our vulnerability to Cyber threats, the current trends of security incidents, and what we can do to protect ourselves; distribution of security awareness posters and guides to state/local agencies and businesses; Info Sec Office's Cybersecurity Awareness Carnival, promoting awareness of IT Security for the BSU Student body and visitors; and Boise IT Service Mgt Forum (itSMF) Conference, Evolve '08, promoting excellence in IT Service Management, to include Security in IT. (***MS-ISAC After-Action Report, 2008***)

2007

Awareness activities in Idaho included the announcement of the Public Security awareness website (via Idaho.gov) that provides educational information related to identity theft, how to protect home and business computers, how to avoid on-line predators, and other cyber security related issues; MS-ISAC Cyber security awareness posters distributed to state/local agencies and businesses; Cyber Security Awareness presentations - Idaho State Controller's Conference for Accounting and Payroll Professionals (held at several locations across the State); University of Idaho's annual Computer Security Day; and a half-day seminar with all IT Security Coordinators to discuss statewide cyber security issues. More than 300 individuals were reached through these events. (***MS-ISAC After-Action Report, 2007***)

ILLINOIS

Illinois CISO: Rafael Diaz; Rafael.Diaz@Illinois.gov; (312) 814-5477

Illinois Bureau of Communication and Computer Services (BCCS) Security Awareness Website : http://bccs.illinois.gov/security/awareness.htm

Awareness Posters available at this link: http://bccs.illinois.gov/security/awareness.htm

2008

Proclamation signed by Governor Rod Blagojevich. Awareness activities included distributing the MS-ISAC cyber security awareness posters and toolkits to all state agency departments, boards and commissions (more than 50,000 employees); creating a batch of original slide shows for display on lobby kiosks. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Rod Blagojevich. Awareness month activities included distributing the MS-ISAC cyber security awareness posters and toolkits to all state agency departments, boards and commissions (more than 50,000 employees); creating an intranet state website for cyber security awareness; and a series of security awareness presentations were made targeting server administrators and application developers. (***MS-ISAC After-Action Report, 2007***)

INDIANA

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

IOWA

Iowa Security Officer: Alison Radl; Alison.radl@iowa.gov

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

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

NASCIO 2009 SURVEY RESPONSE:

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 general security awareness training to state agencies and distributing security awareness materials to state employees.

3. **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

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

2008

Proclamation signed by Governor Chet Culver. Awareness activities included distribution of cyber security materials to state agencies, area education agencies, and InfraGard chapter, holding informational tables in State office buildings; offering technical security training as well as security awareness training, and promoting the Information Security Office newsletters "Security News" & "Security Alerts." The audience included approximately 23,000 state employees. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Chet Culver. The MS-ISAC Toolkit materials were shared with state agencies (52 ISOs responsible for working with over 19,000 state employees) and educators (510 public elementary school principals and 10 Area Education Agencies – responsible for working with 364 public school districts). A press release promoting Cyber Security Awareness Month was sent to the media. Elementary school principals received an electronic copy of the Cyberbullies brochure and information regarding the *Cyber Citizens: Defenders of Cyberspace* webcast. Area Education Agencies received posters, bookmarks, calendars, the Cyberbullies brochure, FTC ID Theft booklets, and training CDs. (***MS-ISAC After-Action Report, 2007***)

KANSAS

Kansas CISO: Larry Kettlewell; Larry.Kettlewell@da.ks.gov
Kansas Information Technology Security Council (ITSC) Webpage:
www.da.ks.gov/ITEC/ITSec/

Computer Security Awareness and Training Policy; January 22,2009:
http://da.ks.gov/itec/Documents/ITECITPolicy7400.htm
Computer Security Awareness and Training Requirements; January 22,2009:
http://da.ks.gov/itec/Documents/ITECITPolicy7400A.pdf

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. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Baseline (?) p. 4)

KENTUCKY

Kentucky CISO: Richard Smothermon; richard.smothermon@ky.gov; 502-564-8074

Kentucky IT Security Home Page: http://technology.ky.gov/security/

Kentucky Cybersecurity Awareness Month Page:
http://technology.ky.gov/security/october_2008.htm

NASCIO 2009 SURVEY RESPONSE:

1. **Executives/Public Officials**
   Governor Steve Beshear issued a proclamation on August 22nd, 2008 proclaiming October 2008 as Cyber Security Awareness Month.

2. **State Workforce**
   In 2008, the Commonwealth Office of Technology (COT) sponsored two informational cyber security awareness events that were held at Kentucky's Commonwealth Data Center. The events were conducted with the assistance of two strategic business partners, Microsoft and Systems Design Group, who provided nationally recognized speakers for the events. These events focused on current and emerging cyber security threats and the ever increasing need for vigilance in IT and cyber security. All state agency Chief Information Officers and their staff were invited to participate in these events. Approximately 90 representatives from all major state agencies attended. A web page was also developed to promote the October cyber security events and highlight available resources.

   The Commonwealth Office of Technology also distributed cyber security toolkit materials from MS-ISAC to representatives of numerous state agencies for distribution throughout state government. Many of the materials were strategically placed in high traffic areas within state government office buildings in Frankfort, including the Commonwealth Office of Technology's state data center.

3. **Citizens**
   A cyber security newsletter is published each month on COT's security website. The newsletter content is obtained from MS-ISAC and is rebranded and republished by COT's CISO office. It contains cyber security tips and information on how to stay safe online. http://technology.ky.gov/security/CyberAwareness.htm

4. **IT/Security Staff**
   COT issues regular 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/security/security_alerts.htm

2008
Proclamation signed by Governor Steve Beshear. Awareness activities included two informational cyber security awareness events, sponsored by the Commonwealth Office of Technology that were held at Kentucky's Commonwealth Data Center. The events were conducted with the assistance of two strategic business partners, Microsoft and Systems Design Group, who provided nationally recognized speakers for the events. These events focused on current and emerging cyber security threats and the ever increasing need for vigilance in IT and cyber security. A web page was also developed to promote the October cyber security events and highlighted available resources. All state agency Chief Information Officers and their staff were invited to participate. Approximately 90 representatives from all major state agencies attended. Some of the agencies participating were the Kentucky Personnel Cabinet, the Public Protection Cabinet, the Energy and Environment Cabinet, the Kentucky Revenue Department, the Kentucky Secretary of State, the Council on Postsecondary Education, the Auditor of Public Accounts, the Cabinet for Health and Family Services, the Department of Corrections, the Kentucky Department of Libraries and Archives, and the Commonwealth Office of Technology. (***MS-ISAC After-Action Report, 2008***)

2007
Proclamation signed by Governor Ernie Fletcher. Awareness activities in Kentucky included promotion of the MS-ISAC Cyber Security Monthly Newsletters; created internal awareness posters that were shared among multiple agencies for use as awareness materials; adding content to the State Cyber Security web page relating to cyber security; and promoting other local events relating to cyber security. The outreach effort reached an estimated 19,000 State employees. Additionally, the MS-ISAC local government materials will be used to foster relationships with County Agencies and City Governments. (***MS-ISAC After-Action Report, 2007***)

LOUISIANA

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

Louisiana IT Security Home Page:
http://oit.louisiana.gov/metadot/index.pl?id=2189;isa=Category;op=show

2008
Proclamation signed by Governor Bobby Jindal. (***MS-ISAC After-Action Report, 2008***)

2007
Proclamation signed by Governor Kathleen Babineaux Blanco. (***MS-ISAC After-Action Report, 2007***)

MAINE

Maine Security Contact: Dick Thompson (CIO); Richard.B.Thompson@MAINE.GOV

Maine IT Security Homepage: www.maine.gov/oit/security/index.shtml

MARYLAND

Maryland CISO: Ron Witkowski; Ron.Witkowski@doit.state.md.us; (410) 260-6322
Maryland IT Security Webpage:
http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx

Maryland Dept. of Information Technology Security Awareness Webpage:
http://doit.maryland.gov/support/Pages/SecurityAwareness.aspx

2008
Proclamation signed by Governor Martin O'Malley. (***MS-ISAC After-Action Report, 2008***)

MASSACHUSETTS

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

Massachusetts Security Education and Awareness Webpage:
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:
www.mass.gov/?pageID=afsubtopic&L=3&L0=Home&L1=Research+%26+Technology&L2=Cyber+Security&sid=Eoaf

MICHIGAN

Michigan CISO: Trent Carpenter; carpentert@michigan.gov

Michigan Department of Information Technology (DIT) – Cybersecurity Homepage: www.mi.gov/cybersecurity

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

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

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)

Taking it to the Citizenry—State of Michigan: In fall 2007, the state will hold a town hall meeting on cybersecurity and protecting children online. This activity is being conducted at the request of a state legislator. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Outreach, p. 10)

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: *Protecting State of Michigan Sensitive Information* is a 4 minute data breach training video that anyone can view. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Video, 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)

2008

Proclamation signed by Governor Jennifer Granholm. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Jennifer Granholm. Awareness activities included issuing awareness bulletins and e-mails; conducting seminars for state employees; Attorney General training for state employees/parents; town hall meeting. Audience was State employees – hundreds at seminars, 50,000 via e-mails; Citizens at town hall (dozens), Local government POCs. MS-ISAC Toolkit materials were given to local governments and distributed to citizens at town hall meeting; participated in the MS-ISAC Kids SafeOnline webcast; State CISO was interviewed (in September) by Comcast Cable regarding safe computing, and the program appeared throughout Michigan on their weekly family focus program. The show was shown statewide several times in October, and it was also available via "On Demand" programming around the country. (***MS-ISAC After-Action Report, 2007***)

MINNESOTA

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

Minnesota Office of Enterprise Technology – Cyber Security Awareness Website:
www.state.mn.us/portal/mn/jsp/home.do?agency=OETweb

NASCIO 2009 SURVEY RESPONSE:

Minnesota Cyber Security Awareness Website:
www.state.mn.us/portal/mn/jsp/home.do?agency=OETweb

1. **Executives/Public Officials**
   The ESO is hosting a Governor's Cabinet/State Leadership Breakfast and the 4th Annual Cyber Security Briefing for Government Executives.

2. **State Workforce**
   The ESO is coordinating 9 Capital campus cafeteria events to underscore the importance of safety in the workplace and protecting our citizen's data. Also being launched is the Cyber Security Awareness Website which includes the "For State Employees" section offering workplace resources as well as several PSA's, podcasts, and many security related articles including "Security Policies Help Keep Our Workplace Safe."

3. **Citizens**
   The Office of Enterprise Technology's Enterprise Security Office (ESO) is launching its Cyber Security Awareness Website "For Parents and Families" and "General Information" sections which provides links to many resources, tips, and articles including cyber bullying, keeping kids safe online, and no-cost security tools. We are also making plans to appear on the Governor's Weekly Radio Program throughout the month of October scheduling nationally recognized special guests to speak on a variety of cyber security awareness topics.

4. **IT/Security Staff**
   IT/Security Staff: The ESO is coordinating extensive training for more than 100 IT professionals through the SANS Program (Application Developers plus various others).

2008

Proclamation signed by Governor Tim Pawlenty. Awareness activities included representatives of the Enterprise Security Office hosting five different cafeteria visits (one per week) to promote security awareness. The visits consisted of a booth with a variety of information security related handouts, bookmarks, a security quiz, free cookies and apple cider and a computer set up with a local program designed to check the strength of people's passwords. We also surveyed people who visited the booth as to what they would like to see in the future with regards to security awareness. On October 20th, the Enterprise Security Office hosted an IT Briefing for Government Executives. This event was attended by approximately 120 government executives (commissioners) and included several legislators. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Tim Pawlenty. In an effort to raise awareness, three separate events were held in different Capitol campus cafeterias with cyber security quizzes. Working with our legislative representative, we created a letter that went to all of our State legislators along with cyber security awareness bookmarks to hand out to grade/high school students when they visit the Capitol building throughout the year. The posters from the MSISAC Toolkit were distributed to all agency security officers to post throughout their organizations. The Enterprise Security Office compliance manager assisted one local school with the MS-ISAC Kids Online Webcast and also handed out over 100 calendars. Cyber security awareness month was marketed via the website and in several emails sent out to agency information security officers. We worked with our Department of Education to spread to the word throughout the K12 community about the Kids Online Webcast. In addition, we continue to distribute MS-ISAC Toolkit materials to agency security officers, via our small agency support initiatives, and will be making these materials available at the Enterprise Security Office booth at our annual IT Symposium in December. The symposium draws over 1,000 IT professionals from state and local government. (***MS-ISAC After-Action Report, 2007***)

MISSISSIPPI

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

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

NASCIO 2009 SURVEY RESPONSE:

The State of Mississippi officially created the CISO position and the Information Security Division (ISD) of the Department of Information Technology Services in January 2009. Since that time they have been developing the foundation for this new division including a complete re-write of Enterprise Security Policy, development of an Enterprise Security Plan, development of a security website, and establishing communications contacts with our individual state agencies.

In regard to Cybersecurity Awareness Month, Mississippi is actively pursuing a proclamation by the Governor's Office and developing the initial stages of a program primarily aimed at state agencies and their end users.

1. **Executives/Public Officials**
   Enterprise Security Policy specifies that "Agency heads are responsible for the oversight of their respective agency's IT security and will be required to confirm in writing that the agency is in compliance with this policy. The annual security verification letter must be submitted to ITS by January 31st each year. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as any updates to them since the last approval." This policy holds the Executives and Public Officials at their respective agencies accountable for security compliance which includes appropriate security training and awareness programs for their technical staff and end users.

2. **State Workforce**
   Enterprise Security Policy specifies that, "Each agency must ensure staff is appropriately trained in IT security procedures. Each agency must make staff aware of the need for IT security and train them to perform the security procedures for which they are responsible. Agencies must participate in appropriate security alert response organizations at the state and regional levels." As part of the ISD Enterprise Security Plan we are developing an education and awareness program utilizing MS-ISAC materials, the ISD website, the ISD security listserv, certified training partners, and industry experts to extend additional awareness materials, information, and education to our agency contacts to facilitate their distribution to their end users/state workforce.

3. **Citizens**
   While awareness information is not currently being distributed to the citizenry via the ISD, the Enterprise Security Plan includes plans for development of a citizen's portal for security information on the ISD website and plans for public service announcements relative to security awareness as part of an ongoing program for educating the citizen as to cybersecurity and their environment. A Governor's Proclamation for October's CyberSecurity Month will be an important step in the state's efforts to increase citizen awareness.

4. **IT/Security Staff**
   There are currently only three staff members on the ISD staff. The ISD Business Plan specified that all management, administrative, and technical security positions were preferred with security certifications and required for advancement opportunities. All ISD staff members are pursuing security certifications over the next 12 to 18 months. Staff is currently being trained via online training courses and select technical training as requested.

MISSOURI

Missouri CISO: Jim Branson; Jim.Branson@oa.mo.gov

Missouri IT Security Webpage: www.cybersecurity.mo.gov/

NASCIO 2009 SURVEY RESPONSE:

1. **Executives/Public Officials**
   The Governor will be signing a proclamation declaring October as Cyber Security Month in Missouri. Cabinet-level discussions have taken place on the newly proposed cyber security training policy. The policy will require every executive branch employee to take Cyber Security Training annually.

2. **State Workforce**
   A new policy will require every executive branch State Employee to complete Cyber Security training. The Missouri Information Security Management Office installed and will maintain the State Cyber Security Training Portal. The training will also be available for elected officials and agencies outside the executive branch.

3. **Citizens**
   Missouri's Cyber Security Page has been redeveloped and has been released in preparation for Cyber Security Month. The new site has valuable security and privacy information for the citizens of Missouri and links to other sites.

4. **IT/Security Staff**
   An internal Security Portal is in place to allow collaboration and faster dissemination of information between the various agencies Security Staff. The Missouri Security Architecture Domain is continually updated to meet new threats as they arise.

2008

Proclamation signed by Governor Matt Blunt. Awareness activities included the Information Technology Division collecting information regarding cyber security awareness activities and resources available from numerous sources. The event and resource information was kept current throughout the month and shared with agency security personnel as well as posted on the public cyber security portal. The immediate audience was the agency security officers, who in turn shared the information with their agencies. The general public is the audience for the cyber security portal. (***MS-ISAC After-Action Report, 2008***)

2007

The MS-ISAC toolkit materials were distributed to security personnel for further distribution to their agencies. Electronic media was uploaded to Missouri's public Cyber Security Portal for use by the public. (***MS-ISAC After-Action Report, 2007***)

MONTANA

Montana Security Officer: Kevin Winegardner; kwinegardner@mt.gov

Montana Information Technology Services Division Webpage:
http://itsd.mt.gov/default.mcpx

2008

Proclamation signed by Governor Brian Schweitzer. Awareness activities included the distribution of awareness materials to all state agency ISOs (about 30) and approximately 150 local government organizations. (***MS-ISAC After-Action Report, 2008***)

NEBRASKA

Nebraska CISO: Brad Weakly; brad.weakly@nebraska.gov

Nebraska Cyber Security Center Webpage: www.cio.nebraska.gov/cybersecurity/

Nebraska provides a guide for agency Information Security Officers that contains detailed guidance for setting up an information security program at the agency level. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Use Agency CSOs, p. 8)

2008

Proclamation signed by Governor Dave Heineman. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Dave Heineman. The following activities were undertaken: The Poster Art contest was a resounding success. Approximately 2,000 4th and 5th graders participated across 75 elementary schools. The State awarded a Grand Prize winner and two winners were invited to the Proclamation signing ceremony where Governor Heineman presented each winner with a signed framed copy of their poster. This was covered in several local newspapers and TV stations. The State did a mass mailing with bookmarks and calendars for the schools. Every elementary and middle school (350) received a calendar, the kids Internet safety pledge template (for teachers to use) and 200 bookmarks from the MS-ISAC Toolkit. (***MS-ISAC After-Action Report, 2007***)

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

NASCIO 2009 SURVEY RESPONSE:

For the past 5 years the Governor has issued a proclamation for Cyber Security Awareness Month.

Executives and Public Officials are members of the Executive Branch and, as such, are required to take the same security awareness as every state employee. This is mandated by Nevada's Consolidated State Security Policy.

The Office of Information Security (OIS) maintains a state security awareness portal for training. This portal is only available as an intranet (non public) site. Information within the portal maps to the Consolidated State Security Policy, which, in turn, maps to NIST and ISO 2700x standards.

All new employees are also provided security awareness training as a part of their new employee orientation.

Each year the State of Nevada participates in MS-ISAC awareness activities including monthly newsletters, posters, and awareness events. This year OIS is co-sponsoring a cyber security awareness symposium with Nevada InfraGard and GMIS. One day, this event will be targeted to state cyber security professionals and will be open to the public.

All IT Security Staff are required to complete a Nevada Information Security Program (NISP) or posses and maintain a CISSP certification.

On a regular basis security awareness training is incorporated into monthly State IT Security Committee Meetings.

OIS maintains an internal intranet web site with links to awareness and training, state security policy, and services.

2008

Proclamation signed by Governor Jim Gibbons. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Jim Gibbons. (***MS-ISAC After-Action Report, 2007***)

NEW HAMPSHIRE

New Hampshire CSO: Theresa Pare-Curtis; theresa.pare-curtis@oit.nh.gov

New Hampshire Dept. of Information Technology - Security Webpage:
www.nh.gov/doit/internet/divisions/itsg/index.php

2008

Awareness activities included limited distribution of materials. (***MS-ISAC After-Action Report, 2008***)

2007

A cyber security web page was created on the state intranet that includes the MS-ISAC Digital Dashboard, monthly newsletters and some cyber security links. (***MS-ISAC After-Action Report, 2007***)

NEW JERSEY

New Jersey CISO: Paula Arcioni; paula.arcioni@oit.state.nj.us
New Jersey Info Secure: www.state.nj.us/njinfosecure/

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.

2008

Proclamation signed by Governor John Corzine. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor John Corzine. (***MS-ISAC After-Action Report, 2007***)

NEW MEXICO

New Mexico Dept. of Information Technology - Security Webpage:
www.doit.state.nm.us/security.html

2008

Proclamation signed by Governor Bill Richardson. Awareness activities included Cyber Security Intrusion Detection Training offered by the state to all state agencies. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Bill Richardson. (***MS-ISAC After-Action Report, 2007***)

NEW YORK

New York Office of the CIO - IT Security Contact: Julie Leeper Evans; julie.evans@cio.ny.gov

New York Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) – Events and Training Webpage: www.cscic.state.ny.us/security/conferences/

New York CSCIC Contact: Will Pelgrin**;** william.pelgrin@cscic.state.ny.us

The New York Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) offers a variety of training materials on its website:

Cyber Security Videos for Home Users ((CSCIC; www.cscic.state.ny.us/security/conferences/)

Cyber Security User Awareness Videos; (CSCIC; www.cscic.state.ny.us/security/conferences/)

Cyber Security Training Videos for Business Managers; (CSCIC; www.cscic.state.ny.us/security/conferences/)

Training Material for Local Governments; (CSCIC; www.cscic.state.ny.us/security/conferences/)

Bi-Monthly Cyber Security Webcasts; (CSCIC; www.cscic.state.ny.us/security/conferences/)

2008

Proclamation signed by Governor David Paterson. NYC Mayor Bloomberg also signed a proclamation. Awareness activities included hosting the National Webcast on Phishing; conducting a NYS poster contest which was open to all New York State students in the fourth and fifth grades; branding and distributing the MS-ISAC toolkit to all state agency information security officers (ISOs) and to members of the Legislature; issuing a press release promoting Awareness Month, the webcast and the toolkit material; providing a training event for state agency ISOs; posting toolkit material on State public website; branding the cyber security PSA and posted on website; branding the MS-ISAC October Cyber Security Tips Newsletter on Phishing and distributed to state agency ISOs and local governments for distribution; newsletter was also posted on public website; participating in Cyber Security Summits in Albany and New York City; presenting on cyber security topics and distributing toolkit material to government, academia, the private sector and the general public at various conferences and meetings. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Eliot Spitzer. A number of activities took place, including the following: the Third Annual Cyber Security Awareness Conference: Kids Safe Online, on

October 17. Nearly 1,000 students, teachers, parents, law enforcement and other adults attended the day-long event. The Conference featured a variety of sessions focused on how to keep children safe while using the Internet. The Conference was launched with a VIP Reception with remarks by Michael Balboni, Deputy Secretary for Public Safety for Governor Spitzer, with a keynote presentation by Maria Sansone, Host of Yahoo's "The9." At the Reception, Deputy Secretary Balboni announced the winners of the New York State Cyber Security Poster Art Contest. The contest was open to all New York State students in the fourth and fifth grades and provided a great opportunity for students to be creative in expressing their understanding of good cyber security practices. Another highlight of the Conference was the live broadcast of the MS-ISAC's national Webcast *Cyber Citizens: Defenders of Cyber Space*, in front of an audience of more than 400 4th and 5th grade students and their teachers. Additionally, more than 10,000 students and teachers across the country viewed the webcast over the Internet. The MS-ISAC Toolkit was distributed to all State agencies and counties across the State. A press release announcing Awareness Month and the New York State activities was distributed to the media. Local television and radio stations covered the Conference. (***MS-ISAC After-Action Report, 2007***)

NORTH CAROLINA

North Carolina CISO: Ann Garrett; ann.garrett@its.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: www.esrmo.scio.nc.gov/CyberSecurity.htm

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

NASCIO 2009 SURVEY RESPONSE:

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. The Governor's IT Score Card includes IT Security metrics. 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.

3. **Citizens**
   Several departments/agencies offer targeted information for various groups. The NC Attorney General offers a comprehensive consumer protection website for state citizens.

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) 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. ITS has a full time training director to support each employees training plan goals. 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.

2008

Proclamation signed by Governor Michael F. Easley. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Michael F. Easley. (***MS-ISAC After-Action Report, 2007***)

NORTH DAKOTA

North Dakota CISO: Lisa Feldner (CIO); lfeldner@nd.gov

North Dakota Cyber Awareness Webpage: www.nd.gov/itd/security/awareness.html

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

Security Training, Awareness and Reference Tool (START) is for state employees and others who want to use it and includes common IT security terms, vulnerabilities, and ways to protect IT resources. The tool includes a wide range of topics from PC security to Internet usage to telephone issues. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Online training, p. 12)

2008

Proclamation signed by Governor John Hoeven. Awareness activities included creation of a State Cyber Security Portal; presentation during State Quarterly IT Directional Meeting in September; distribution of Cyber Security Toolkit materials to interested agencies; distribution of Monthly Cyber Security Tips Newsletters to all agency IT Security staff for redistribution to agency personnel; Cyber Security Educational Booth at State Information Technology Department Employee Recognition Week Annual Chili Cook-off and Talent Fair; attaching Cyber Security Awareness posters on every conference room calendar, providing tips and a reminder that October is Cyber Security Awareness Month; and the State Office of Attorney General utilized the branded Public Service Announcements from MS-ISAC to reach general public. The audience included various state agencies' IT staff, as well as the general public. The State Office of Attorney General utilized the branded Public Service Announcements from MS-ISAC to reach general public. (***MS-ISAC After-Action Report, 2008***)

2007

Distributed MS-ISAC Toolkit material to state agencies. (***MS-ISAC After-Action Report, 2007***)

OHIO

Ohio CISO: Kimberly Trapani; Kimberly.Trapani@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:
www.privacy.ohio.gov/education/

IT Security-Privacy Home Page: http://privacy.ohio.gov/

2008

Proclamation signed by Governor Ted Strickland. Awareness activities included hosting the Ohio Privacy & Security Summit as the second day of the Ohio Digital Government Summit (September 30 – October 1, 2008) held in Columbus, Ohio. Over 500 people registered for the Ohio Digital Government Summit, including the Ohio Privacy & Security Summit. Registrants were primarily state and local government employees or officials. The event sold out. (***MS-ISAC After-Action Report, 2008***)

OKLAHOMA

Oklahoma CISO: Ken Ontko; ken.ontko@osf.ok.gov

Oklahoma IT Security Webpage: www.ok.gov/OSF/Information_Services/Security.html

NASCIO 2009 SURVEY RESPONSE:

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

2. **State Workforce**
   Oklahoma is in the early stages of implementing the MS-ISAC's Cyber Security Awareness Training Application.

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

4. **IT/Security Staff**
   Activities include:
   a) Three Quarterly Cyber Security Focus Group half day meetings;
   b) 5th Annual Cyber Security Awareness Seminar (2 day event planned for December this year, using a "Crawl, Walk, Run Approach")
      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) 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'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.

2008

Proclamation signed by Governor Brad Henry. Awareness activities included distribution of literature (MS-ISAC posters and local government cyber security booklets, and iKeepSafe Parent Resource CD) to all participants of quarterly InfraGard meeting in October. MS-ISAC Toolkit materials were distributed at the statewide Cyber Security Conference. Audience for Awareness Month activities included hundreds of participants from State and Federal agencies, Higher Education, InfraGard and other public and private sectors. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Brad Henry. Awareness Month activities included: distribution of literature (MS-ISAC posters and local government cyber security booklets, and iKeepSafe Parent Resource CD) to all participants of quarterly InfraGard meeting in October. Presentation of MS-ISAC Toolkit materials at statewide Cyber Security Conference on December 7, 2007 to all attendees. Audience for Awareness Month activities included more than 500 individuals from state agencies, higher education, Infragard and others. (***MS-ISAC After-Action Report, 2007***)

OREGON

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

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

Oregon Information Security Resource Center: http://secureinfo.oregon.gov/

Oregon's 2009 recognition awards submission details the security risk assessment initiative the state has implemented over the past three years. It describes 2007 and 2008 reviews and analysis that established baseline risk assessments in various categories, among which was security awareness and education. Thereafter, the submission describes significant progress in awareness and education once risks were identified. See the submission for further details; *Oregon Department of Administrative Services – Enterprise Information Security Business Risk Assessment, May 11, 2009.*

2008

Proclamation signed by Governor Ted Kulongoski. Awareness activities included the distribution of toolkit materials to all State agencies. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Ted Kulongoski. In an effort to raise awareness, the MSISAC Toolkit materials were distributed to stakeholder groups and a new Information Security Resource Center Website was launched. Materials were made available to other state agencies through the Website and materials provided by MS-ISAC were distributed. Oregon conducted outreach through the information security officers and CIOs at approximately 20 state agencies. (***MS-ISAC After-Action Report, 2007***)

PENNSYLVANIA

Pennsylvania CISO: Robert Maley; rmaley@state.pa.us

Pennsylvania IT Security Homepage:
www.portal.state.pa.us/portal/server.pt?open=512&objID=337&mode=2

Pennsylvania Cybersecurity Awareness Webpage:
www.portal.state.pa.us/portal/server.pt/community/security_awareness/494

Enterprise Security Architecture—Commonwealth of Pennsylvania: Awareness and training are included as a critical part of Pennsylvania's overall Enterprise Security Architecture. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Baseline (?) p. 4)

Legislative Awareness—Commonwealth of Pennsylvania: To build awareness among legislators and citizens, Pennsylvania conducts an annual "Security Awareness Day" at the state Capitol to raise awareness. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Awareness, p. 6)

Commonwealth of Pennsylvania also holds CISO Roundtables as learning sessions with guest speakers. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Use Agency CSOs, p. 8)

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

The Commonwealth held a cross-agency cyber security training exercise in which eleven agencies participated over two days in the table-top exercise. A lessons-learned discussion followed resulting in a formal report. Pennsylvania also participated in the MS-ISAC's Cyber Tempest (a regional effort with five states participating). In addition, the Commonwealth will be participating in DHS's Cyber Storm II in 2008. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Training, p. 12)

2008

Proclamation signed by Governor Edward Rendell. Awareness activities included the distribution of a new security awareness course to all Commonwealth employees via the learning management system. It is mandatory that all commonwealth employees take the course. During the month of October over 45,000 Commonwealth employees successfully completed the course. In mid-October the Commonwealth cyber-security conference was held at the Keystone building in Harrisburg, Pa. Andy Purdy was the keynote speaker. Over 20 different security vendors participated in the event in 26 different security sessions. A vendor exposition was also held in the main atrium of the building. Over 200 security personnel from most commonwealth agencies as well as county and local security professionals attended the conference. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Edward Rendell. The following activities were undertaken: the First Annual Cyber Security Conference was held at the Commonwealth Technology Center in Harrisburg. Six subject matter experts collectively held a total of 23 educational sessions throughout the day. Audience for the Conference were Commonwealth Agencies (over 22 state agencies). Additionally, members from NSA and Homeland Security attended. All Presentations and Power Points have been made available for download on our CyberSecurity site. The MS-ISAC Toolkit materials were distributed to all attendees of the Conference as well as distributed throughout the month for agencies to use. Posters were prominently displayed in all areas of the buildings. (***MS-ISAC After-Action Report, 2007***)

PUERTO RICO

Puerto Rico Security Contact: Juan E. Rodriguez de Hostos (CIO); jerodriguez@fortaleza.gobierno.pr

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/

Rhode Island Cybersecurity User Awareness Webpage:
www.doit.ri.gov/security/identity.php

NASCIO 2009 SURVEY RESPONSE:

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.

2007

The MS-ISAC Toolkit materials were distributed to partner agencies and schools reaching approximately 6,000-7000 employees across 40 agencies. (***MS-ISAC After-Action Report, 2007***)

SOUTH CAROLINA

South Carolina CISO: James MacDougall; macdoug@cio.sc.gov
South Carolina ISAC: https://sc-isac.sc.gov/
South Carolina IT Security Homepage:
www.cio.sc.gov/productsandservices/securitymain.htm
Security Training, Awareness and Policy Services:
www.cio.sc.gov/productsandservices/securitytraining.htm

2008

Proclamation signed by Governor Mark Sanford. Governor Sanford signed the Proclamation. Awareness activities included an all day Cyber Security conference on October 16 at the SC State Museum auditorium with state, local, higher education, and K12 security representatives attending. The featured presenters included SC Chief Security Officer, SC Law Enforcement Division (SLED), FBI Cyber Squad, US Secret Service, and several security vendors. We distributed MS-ISAC Toolkit materials and South Carolina SC-ISAC materials to all attendees. Working with the Department of Education, we initiated a project to install IDS devices in 85 school districts to provide ongoing monitoring and support and to register them with the US-CERT web site to share information and raise awareness. This project is 85% complete. Cyber Security information is now included in bi-monthly newsletters sent to all agency directors, the security website was enhanced, and weekly conference calls were initiated for SC-CSIRT members. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Mark Sanford. (***MS-ISAC After-Action Report, 2007***)

SOUTH DAKOTA

South Dakota CISO: Jim Edman; jim.edman@state.sd.us; 605-773-4861

South Dakota Bureau of Information Technology Cyber Security Website:
www.state.sd.us/bit/bitservices/standards/cybersecurity.htm

NASCIO 2009 SURVEY RESPONSE:

1. **Citizen awareness** – distribute MS-ISAC toolkit material at 'Capital for a Day'. Government events that are held at various cities around the state, whose focus is on the community and its citizens.

2. **State workforce and Citizen awareness** – South Dakota now maintains a Cyber Security web page located at: www.state.sd.us/bit/bitservices/standards/cybersecurity.htm

Newsletters:
www.state.sd.us/bit/Services/CyberSecurity/newsletters/MSISAC%20Cyber%20Tip%20July%202007.pdf

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)

2008

Proclamation signed by Governor Mike Rounds. Awareness activities included the creation of a new cyber security page for the state. (***MS-ISAC After-Action Report, 2008***)

TENNESSEE

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

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

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

This state's Cyber Academy is an online tutorial that includes lessons on all types of computer security issues with quiz questions interspersed throughout. Anyone can take this online quiz, although it is geared to state employees. (Source: ***NASCIO IT Security Awareness and Training: Changing the Culture of State Government, 2007***; Online training, p. 12)

2008

Proclamation signed by Governor Phil Bredesen. Awareness activities included issuing Weekly Cyber Tips, and developing three short webcasts. The State also utilized the SANS partnership and offered Defensible .NET to 54 students. While the theme was not strictly Cyber Security Awareness, the State conducted meetings with client agency management to promote the security program. Developers and system administrators were the target audience for the class. End-users were the target for the Cyber Tips and webcasts. Information about the webcasts and the Cyber Tips were sent to approximately 42,000 employees. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Phil Bredesen. Awareness activities included participation in the MS-ISAC cyber security webcast, including the First Lady's Assistant; conducted a password poster campaign, posted in more than 200 locations during the month of October; hosted a SANS partnership class with more than 120 students. (***MS-ISAC After-Action Report, 2007***)

TEXAS

Texas CISO: Bill Perez; Bill.perez@dir.state.tx.us

Texas Dept. of Information Resources – SecureTexas Website:
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)

2008

Proclamation signed by Governor Rick Perry. Awareness activities included the launch of the TX-ISAC Secure Portal, which was aggressively publicized during this period resulting in over 100 state entities enrolling/registering for access to the site; extra editions of the Cyber Security Tips newsletter were distributed each week during the month of October; co-sponsored a three-part webcast series, hosted by Verizon Business Security Solutions, on October 8 & 21, and November 18. The series addressed the many security challenges associated with the extended enterprise – data breaches, data loss and identity management. Publicized the Cyber Security National Webcast Initiative on Phishing during October; Supported the fourth annual workshop on cyber security education and training for states and communities hosted by the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio; Sponsored additional high quality training, such as SANS Web Application Security two-day workshop, a Secure Web Programmer course and a Carnegie Mellon/SEI course on Computer Emergency Response Team development. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Rick Perry. (***MS-ISAC After-Action Report, 2007***)

UTAH

Utah CISO: Michael Casey; mcasey@utah.gov

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

Utah DTS Security Awareness Webpage:
http://dts.utah.gov/security/awareness/index.html

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 2009 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)

2008

Proclamation signed by Governor Jon Huntsman. Awareness activities included the Department of Technology Services inviting a speaker each Wednesday and conducting two sessions and streamed it out to all state employees. After the sessions were over the streaming was edited and put on our security site for all to view. This made it possible for those not attending to see the events at a later date. The target audience was state employees, city and county employees, State Board of Education, and some private citizens. (***MS-ISAC After-Action Report, 2008***)

VERMONT

Vermont Information Security Webpage: http://itsecurity.vermont.gov/

VIRGINIA

Virginia CISO: John Green; john.green@vita.virginia.gov; 804-416-6013

Virginia State IT Security Webpage: www.vita.virginia.gov/security/

Virginia – Information Security Toolkit Webpage:
www.vita.virginia.gov/security/default.aspx?id=5146

NASCIO 2009 SURVEY RESPONSE:

1. **Executives/Public Officials**
   One of the Commonwealth of Virginia (COV) Information Security Council committees, Making Information Security an Executive Management Priority (MISEMP) Committee, is dedicated to educating and raising the information security awareness of COV executives.

   Ongoing initiatives include: security presentations at the Commonwealth Management Institute, Virginia Executive Institute and cabinet briefing, as well as security articles in the weekly Leadership Communiqué for agency heads and Cabinet members. Future plans include a devoted executive section in the Information Security Awareness Toolkit, a quick reference guide for executives on certain key security responsibilities and expanded coverage of information security topics in the curricula for the Commonwealth Management Institute and Virginia Executive Institute.

   Website Link: MISEMP Committee, Information Security Awareness Toolkit

2. **State Workforce**
   The Commonwealth Information Security Standard requires that each agency develop an information security training program, including annual training and regular distribution of security information, so that each IT system user is aware of and understands specific security concepts that provide protection of Commonwealth information.

   Monthly publications including the Network News e-bulletin for state agencies and institutions and the Service Bulletin for localities and institutions of higher education include a link to the Information Security Tips publication. The internal Commonwealth payroll system is used to broadcast security one-line reminders and to publicize COV security publications.

   Website Links: COV IT Security Standard, Network News, Service Bulletin

3. **Citizens**
   Citizens are provided with information security awareness information for use at work and at home through monthly distributions and a toolkit.

Information Security Tips: This distribution, which is a collaboration with the Multi-State Information Sharing and Analysis Center (MS-ISAC), informs citizens of general security topics, concerns and what actions or practices they can take to protect their systems and/or information.

Citizen's Information Security Advisory: This distribution informs citizens of software security related vulnerabilities and the security updates and/or actions required to protect their home computers.

Information Security Awareness Toolkit: The toolkit provides information for citizens regarding internet security to protect them and their children.

Website Links: Information Security Tips, Citizen's Information Security Advisory, Information Security Awareness Toolkit

4. **IT/Security Staff**

Commonwealth Information Security professionals are provided with the opportunity to attend regularly scheduled security meetings and conferences and are provided with weekly security advisories.

Commonwealth Information Security Conference: This is an annual conference for state and local government attendees.

Information Security Officers Advisory Group (ISOAG) Meeting: This is a monthly meeting that provides an opportunity to inform and instruct Information Security Officers on COV security practices and discussion of common issues and resolutions.

Commonwealth Security Resource Center: The online resource center provides security advisories to inform IS professionals of software security related vulnerabilities and the security updates and/or actions required to protect the Commonwealth systems and COV security attack statistics.

Information Security Awareness Toolkit: The toolkit provides information for information security professionals to share with agencies, such as videos, posters, bookmarks, guides and brochures.

Website Links: COV Information Security Conference, Information Security Officers Advisory Group, Commonwealth Security Resource Center, Information Security Awareness Toolkit

2008

Proclamation signed by Governor Tim Kaine. Awareness activities included a variety of events held by multiple agencies and localities in the Commonwealth of Virginia, ranging from all day conferences to lunch time speakers with giveaways to week long events. The audience varied - employees and IT users were dominant but students, citizens and all levels of government were included. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Tim Kaine. Commonwealth Information Security Council wrote an article weekly for the Governor's Leadership Communiqué which is the electronic newsletter that goes to the Cabinet officials and agency heads in the Executive Branch; a number of state agencies conducted awareness and education activities. Activities were targeted to end users of the Commonwealth Network and citizens. The MS-ISAC Toolkit was posted on the website and distributed through a variety of channels. (***MS-ISAC After-Action Report, 2007***)

WASHINGTON

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

2008

Proclamation signed by Governor Christine Gregoire. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Christine Gregoire. (***MS-ISAC After-Action Report, 2007***)

WEST VIRGINIA

West Virginia CISO: Jim Richards; Jim.A.Richards@wv.gov

West Virginia Office of Information Security and Controls Webpage:
www.state.wv.us/ot/article2.cfm?atl=E7F0EC88-B89D-11D5-92170020781CA4C6&fs=1

In addition to other cyber-awareness activities, the West Virginia Office of Technology is holding a cyber security seminar on October 19. The day-long seminar will address the areas of cyber threats, effective practices to safeguard computer information, personal accountability, risk management, and privacy issues. The event's target audience is public sector officials and employees, but the general public and private sector representatives are also encouraged to attend. The event is also being made available as a live webcast, and a recorded version of the seminar will be online following the event.

2008

Proclamation signed by Governor Joe Manchin III. Awareness activities included participation in two events. The first one was a "Lunch and Learn session on Information Security." The event was open to all and was attended by approximately 35 people. The theme was "Meet Your Information Security Team." Discussion centered around NASCIO "AT RISK" video. MS-ISAC toolkit materials were handed out at this event. The second event was conducted on October 25th, and was a "Shred Day." This event provided immediate shredding-while-you-watch for anyone who came. The day involved a steady stream of participants, some with fairly large quantities of material. The response was very positive and appreciated. It was a successful event for a first-time event and threat of rain. Shredding company provided service at no charge. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Joe Manchin III. MS-ISAC Toolkit materials have been posted and distributed to state employees. (***MS-ISAC After-Action Report, 2007***)

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

2009

Proclamation planned to be signed by Governor Doyle.
Social Networking presentations on the pros and cons of Web 2.0 offered to state agencies and professional organizations.
Identity theft presentations offered to state agencies.
Cyber component for national preparedness month during September on http://readywisconsin.wi.gov/readywi/informed/cyber_crime.asp available to business, government and citizens.
Distributing MS-ISAC Toolkit items (posters, pamphlets, bookmarks, calendars) to state agency security officers (52 agencies, 38,000 employees), monthly newsletters to agency security officers and CIO's to distribute or post within the agencies for all employees.
Make MS-ISAC toolkit available on website available to business, government and citizens.
Broadcast availability of toolkit to local governments via listserv.
Monthly security meetings with agency CISO's discussing current cyber threats and security awareness.
Daily/Weekly updates on Cyber threats and information in publications to Wisconsin Law Enforcement.
Division of Enterprise Technology has a dedicated resource for Homeland Security and the state CIO is a member of the WI Homeland Security Council that meets monthly

2008

Proclamation signed by Governor Jim Doyle. (***MS-ISAC After-Action Report, 2008***)

2007

Proclamation signed by Governor Jim Doyle. Awareness activities included distributing the MS-ISAC Toolkit items (posters, pamphlets, bookmarks) to State Agency Security officers (52 agencies, 38,000 employees); calendars were distributed to 4th & 5th grade teachers; Brown Bag presentation was held on Identity Theft for State Staff; Cyber Security presentation to professional groups; approximately 2,575 letters were distributed to the principals/administrators of the Wisconsin Public and Private schools which included the signed Proclamation and other cyber security materials. The materials were also posted on the public website. (***MS-ISAC After-Action Report, 2007***)

WYOMING

Wyoming Security Contact: Bob von Wolffradt (CIO); rvonwo@wyo.gov
Wyoming Cyber Security Homepage: www.wyoming.gov/cybersecurity.aspx

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

2008

Proclamation signed by Governor David Freudenthal. Awareness activities included handing out toolkit materials to all state agencies, briefing all committees and subcommittees of Governance model on need for cyber security awareness, and briefed cyber awareness actions at Governor's cabinet meeting. Target audience was State government employees. (***MS-ISAC After-Action Report, 2008***)