

From: Priester, Nicole <NicolePriester@gov.sc.gov>
Required: Symmes, Brian <BrianSymmes@gov.sc.gov>
Adams, Chaney <ChaneyAdams@gov.sc.gov>
Godfrey, Rob <RobGodfrey@gov.sc.gov>
Glaccum, David <DavidGlaccum@gov.sc.gov>
Subject: SC Cyber Announcement
Location: USC Alumni Center, 900 Senate Street, Columbia, S.C.
When: 2/24/2016 10:00:00 AM - 11:00:00 AM

Advance: Charlotte McKee
(803)209-1057

APPROVED BY: NH and MH

EVENT: SC Cyber Announcement

DATE: Wednesday, February 24, 2016

TIME: 10:00-11:00 AM

LOCATION: USC Alumni Center, 900 Senate Street, Columbia, S.C.

LOCATION SET-UP: There will be a stage with a podium and a microphone, seating will be rows of chairs.

SCHEDULING CONTACT:

Les Eisner
EISNERL@mailbox.sc.edu

ONSITE CONTACT:

Roxanne Price
(803) 777-4111
rprice@mycarolina.org

PRIMARY STAFF: Ashton Lee

ADVANCE STAFF:

PURPOSE: SC Cyber is a statewide initiative linking academia, industry, and government. Although it is based at USC, it reaches beyond any single organization to produce statewide impact in cybersecurity education, workforce development, technology development, and critical infrastructure protection.

PRESS: Yes. Press is being handles by Jeff Stensland at USC. He can be reached at STENSLAN@mailbox.sc.edu.

PUBLIC: Yes.

INVITED BY:

Les Eisner
Deputy Executive Director Office of Economic Engagement
University of South Carolina

INTRODUCED BY:

Les Eisner

ATTENDEES: Around 150 people. A mix of industry academic and government partners.

LENGTH OF SPEAKING: 10-12 minutes. No Q&A.

SPEAKING ORDER/LINE-BY-LINE:

10:10-10:05 AM	Welcome	Les Eisner
10:05-10:07 AM	Introduce Gov. Haley	Les Eisner
10:07-10:20 AM	Remarks	Gov. Haley
10:20-10:30 AM	Remarks	Dr. Harris Pastides

Remarks by three industry representatives:

10:30 AM-10:37 AM	Glenn Starkman of Soteria
10:37-10:45 AM	Tommy Suggs of KeenanSuggs Insurance
10:45-10:53 AM	James Ward of Scientific Research Corporation
10:53-11:00 AM	Closing Remarks

BACKGROUND:

SC Cyber is a statewide initiative, based at the University of South Carolina and with partners across all levels of academia, industry, and government, with a mission to develop the talent, techniques, and tools to defend critical, connected infrastructure within South Carolina and the United States. In support of this mission, SC Cyber will create and offer programs for training and workforce development, education, advanced technology development and commercialization, and critical infrastructure protection. Some examples of specific projects include:

- Delivery of certification courses to help build the base of credentialed cybersecurity professionals in programs such as the Certified Information Systems Security Professional (CISSP) as well as other in-demand cybersecurity skills
- Executive education programs covering pressing cybersecurity threats, issues, and best practices. Crafted from the talents at the University and SC Cyber's partners, these courses will be targeted at addressing the leadership issues associated with securely managing an enterprise and will provide key business and government leaders with the skills necessary to prevent attacks and respond appropriately
- Outreach to groups outside of the traditional cybersecurity community. Two of the most promising areas for this outreach are K-12, to introduce students to basic cybersecurity concepts and to instill a security mindset, and the community, to provide basic knowledge of threats and mitigation tactics to help prevent some of the most common and easily-defended attacks
- Internship and experiential learning programs for current students to gain knowledge and credentials while using real-world tools of the trade and to provide a pipeline a high-quality talent for the growing number of cybersecurity opportunities throughout the state

TALKING POINTS:

Note: The mission of this statewide initiative is to partner government, private-sector, and academia to develop the talent, techniques, and tools necessary to defend critical, connected infrastructure within South Carolina and the United States.

Introductory Remarks:

- I am honored to be here today and to be a part of this important initiative that will lead to increased cooperation across multiple industries and between numerous stakeholders.
- Reducing the risk to our networks will take a partnership between the public and private sector, and I am confident that the SC Cyber Initiative will be a leading example to the rest of the nation in achieving this goal.

General Talking Points:

1. General Points on Cybersecurity:

- a. South Carolina operates in a global economy, ranking in the top tiers of the country in foreign investment and exports.
- b. A large part of what makes our economy go is sufficient cyber infrastructure able to communicate in a secure and expedient fashion with places around the nation and the world.
- c. As such, cybersecurity and our ability to defend our infrastructure is central to the security and economic prosperity of our state and the nation.
- d. Cyber-attacks are sophisticated, difficult to detect, and difficult to prevent. In the future they will only become more sophisticated and more difficult to stop.
- e. This is why we must enhance cybersecurity tools and develop cybersecurity professionals—working in both the public and private sector—to fortify our cyber infrastructure and enhance our ability to protect our networks from intrusion.

2. What is Cybersecurity?

- a. This is a broad and fuzzy concept, and very often the definition will depend on who you ask.
- b. Generally speaking, it often refers to activities and/or measures intended to protect computers, computer networks, data, and cyberspace from attack, disruption, or damage.

3. Broad Policy Areas to Consider

- a. Education and Training:
 - i. Training must be available to bring our workforce into the cybersecurity field, and maintain our technical leadership in this crucial area.
- b. Information Sharing:
 - i. Government agencies and private industries—particularly the communications companies that run the Internet's infrastructure—need to share more information with each other about the threats they see on their networks.
- c. Detection and Protection:
 - i. Software and technology solutions must be developed and available to industry and government entities to detect system threats and protect against unauthorized intrusion.
- d. Enforcement:
 - i. Law enforcement must have the resources necessary to pursue and take-down international cyber-criminals.

4. South Carolina Agency Involvement

- a. SC Emergency Management Division has been working with numerous state and federal agencies, including DOA and SLED, to determine key agency responsibilities and capabilities.

- b. The SC Cyber Initiative represents an opportunity for our agencies to work with private industry partners, and create a willing coalition of stakeholders to address the emergency threat.