From: "St Pierre, James A. (Fed)" <james.st.pierre@nist.gov>

Date: Wednesday, October 26, 2016 at 1:38 PM

To: "Dodson, Donna F (Fed)" <donna.dodson@nist.gov>, "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>, "Stine, Kevin (Fed)" <kevin.stine@nist.gov>, "Barrett, Matthew P. (Fed)" <matthew.barrett@nist.gov>, Adam Sedgewick <adam.sedgewick@nist.gov>, "Romine, Charles H (Fed)" <charles.romine@nist.gov>

Subject: FW: News Clips from Wednesday, October 26, 2016

FYI – from the newsclips today thought you'd be interested in the following article:

Insurance Regulators Fine Tuning Cybersecurity Guidance

The National Law Review

... cybersecurity principles" rather than on the National Institute of Standards andTechnology's Framework for Improving Critical Infrastructure Cybersecurity.

Which includes the following:

"Information security program requirements.

Insurers will be required to develop and maintain on an ongoing basis an information security program that is appropriate given the size of the Insurer and the nature and complexity of its business and that is based on "generally accepted cybersecurity principles" rather than on the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity.*"

James St. Pierre, Deputy Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8900
Gaithersburg, MD 20899-8900
email: jimstp@nist.gov
phone: (301)-975-4124

From: deputies-bounces@nist.gov [mailto:deputies-bounces@nist.gov] **On Behalf Of** Chambers, Alicia M. (Fed)

Sent: Wednesday, October 26, 2016 1:21 PM

Subject: [Deputies] News Clips from Wednesday, October 26, 2016

Good Afternoon. Here are today's clips.

Tangled Up in Spacetime

Scientific American

This animation of quantum entanglement shows two ions entangled in an experiment performed at the National Institute of Standards and Technology. Credit: ...

US govt issues cybersecurity guidance for car makers

iT News

NHTSA developed the guidance [pdf] based on public feedback, and the US National Institute of Standards and Technology's (NIST) Framework for Improving ...

(ISC)2 wants US CISO to empower staff and widen training

FedScoop

... say something" slogan, but built around the five core principles of the NationalInstitute of Standards and Technology's Cybersecurity Framework — "Identify, ...

Serco Inc. CIO Chris Sullivan to Provide Cybersecurity Insight at ...

GovConWire

Sullivan will tackle methods to evaluate and establish data system security with Celia Paulsen from the

National Institute of Standards and Technology's ...

[Insurance Regulators Fine Tuning Cybersecurity Guidance](#)

The National Law Review

... cybersecurity principles" rather than on the National Institute of Standards andTechnology's Framework for Improving Critical Infrastructure Cybersecurity.

[Ad Industry: FCC Shouldn't Break A Privacy Model That Works](#)

MediaPost Communications

As McGeorge Bundy said in a quote now enshrined in data protection guidelines from the National Institute of Standards and Technology: "If we guard our ...

[Sen. Warner: FCC Should Clarify ISP Power to Combat Hacks](#)

Broadcasting & Cable

Has your agency discussed the possibility of establishing meaningful security standards with the National Institute of Standards and Technology?" 9. "What is the ...

[Facial recognition may be unreliable, and nearly half of US adults ...](#)

ABA Journal

Patrick Grother, a computer scientist with the Commerce Department's NationalInstitute of Standards and Technology, told NPR that if law enforcement is going ...

[CNAG-CRG-Led Study Benchmarks Computational Pipelines for ...](#)

GenomeWeb

... of three aligners and four variant callers, including several used in the current study, on 12 datasets from the National Institute of Standards and Technology.

[LI center to hire specialist to connect factories, colleges](#)

Newsday

Empire State Development announced it is taking applications for three specialists to work with the federal Manufacturing Extension Partnership program, ...

[Military Press Releases](#)

Military Technologies

... Ashoka, Blue Shield of California Foundation, INTO University Partnerships, South CarolinaManufacturing Extension Partnership, Christian Children's Fund of ...

[Eye on US biz ties, Mitra attends midnight meet](#)

Times of India

Banga, who was appointed by US President Barack Obama in the Commission on Enhancing National Cybersecurity, a key administration post tasked with ...

[Warner: Procurement and personnel key for cyber](#)

FedScoop

Later he told CyberScoop that the President's Commission on Enhancing National Cybersecurity — of which he's a member — was looking at "some things that ...

[Beaverton High grad Gigi Stoll ties for 4th in Pac-12 Preview for best ...](#)

OregonLive.com

Oregon State got a tie for 15th from junior Susie Cavanagh and a tie for 17th from junior Haley Nist and finished eighth. Madison Odiorne, a Summit High ...

[Microsoft's Cognitive Toolkit on GitHub in all its speech-recognising ...](#)

The Register

Microsoft's AI researchers have already used the toolkit to build an automated system capable of recognising recorded speech on the NIST 2000 Switchboard at ...

[Penn State, Big Data Hub selected for NTIS Joint Venture Partnership](#)

Penn State News

I am confident the partnerships between NTIS and each selected organization will unlock new federal data that will leverage advances in data science, promote ...

[US Federal Government Response Too Slow to Friday's Internet ...](#)

CircleID

... cybersecurity initiatives for the Department of Commerce's National Telecommunications and Information Administration (NTIA), in conference call on Monday.

[HHS cyber task force to look at federal approaches, info-sharing](#)

The Department of Health and Human Services' cybersecurity task force today will meet to discuss

federal approaches to healthcare industry cybersecurity and commercial sector information sharing, according to a recently released meeting agenda.

Nuclear regulators schedule meeting to review proposed cyber rules

The Nuclear Regulatory Commission's Advisory Committee on Reactor Safeguards will hold a meeting to review proposed rulemaking on cybersecurity for fuel cycle facilities on Nov. 2, according to a *Federal Register*notice.

House Science panel leaders criticize FDIC over cybersecurity

House Science Chairman Lamar Smith (R-TX) and Science oversight subcommittee Chairman Barry Loudermilk (R-GA) chastised the Federal Deposit Insurance Corporation for a lack of cybersecurity protections and response plans, in a letter sent to FDIC Chairman Martin Gruenberg last week requesting explanation of actions the agency will take to improve security.

Consumer advocates lobby for strict data rules in advance of FCC vote

Privacy and consumer advocates are urging the Federal Communications Commission to resist industry pressures and adopt on Thursday strict security and privacy regulations as laid out in the commission's proposal for broadband internet service providers.

Auto industry: NHTSA cyber guide supports industry practices, sets stage for next president

New cybersecurity guidance from the National Highway Traffic Safety Administration codifies work already done by the Obama administration to address automotive cybersecurity while complementing industry efforts and recently released best practices, according to industry sources.

ISAO standards group plans to catalog varying state info-sharing requirements

SAN ANTONIO, TX – The group tasked with writing standards for sharing cyber-threat intelligence is looking at cataloging the multitude of state reporting rules for data breaches and other data-security requirements in a next round of guidance documents to be announced later this year.

ISAC official: New ISAO guides chart future for info-sharing groups

Recently issued guidelines for establishing and operating information sharing and analysis organizations, or ISAOs, offer an important reference for longstanding info-sharing and analysis centers, or ISACs, on the future direction of efforts to share cyber-threat indicators in a way that can transcend specific industry sectors or regions, according to an official involved in drafting the new guidelines.