

Carroll, Ryan

From: Jose Arteaga <j.arteaga@netzero.net>
Sent: Thursday, July 19, 2018 4:22 PM
To: iipp2018
Subject: FW: Establishing a minimum acceptable standard of qualification in the cyber-security industry

From: Jose Arteaga [mailto:j.arteaga@netzero.net]
Sent: Thursday, July 19, 2018 1:09 PM
To: David J. Redl (dredl@ntia.doc.gov); David J. Redl (dkinkoph@ntia.doc.gov); David J. Redl (jwasilewski@ntia.doc.gov)
Subject: FW: Establishing a minimum acceptable standard of qualification in the cyber-security industry

From: Jose Arteaga [mailto:j.arteaga@netzero.net]
Sent: Tuesday, September 12, 2017 11:25 AM
To: 'David W. Burns (david.burns@usmayors.org)'; 'David W. Burns (mayor@nola.gov)'; 'David W. Burns (tom.cochran@usmayors.org)'; Ben Carson (ben.carson@hud.gov); David De Vries (david.devries@opm.gov); Jason Gray (ocio@ed.gov); Jeff Sessions (jeff.sessions@usdoj.gov); John Zangardi (john.zangardi@dodcio.defense.gov); Kristen Baldwin (kristen.baldwin@dot.gov); Louis Giannotti (giannott@usna.edu); 'Margaret "Margie" H. Graves'; Mike Pence (info@mike.pence.com); Rex Tillerson (rex.tillerson@state.gov); Richard Staropoli (richard.staropoli@hq.dhs.gov); Rick Perry (rick.perry@energy.gov); Secretary TBA (engagement@ostp.eop.gov); Steve Mnuchin (steve.mnuchin@treasury.gov); Sylvia Burns (sylvia.burns@ios.doi.gov); Tom Price (tom.price@hhs.gov); Bob Thomas (bob.thomas@nga.org); Brian Sandoval (governor@govmail.state.nv.us); Mark Dayton (mark.dayton@state.mn.us); Nelson P. Moe (cio@vita.virginia.gov); Scott Pattison
Cc: 'Mark Raymond (mark.raymond@ct.gov)'; 'Mark Raymond (drobinson@NASCIO.org)'; 'Mark Raymond (lthompson@nascio.org)'; Blend Qatipi (bqatipi@politico.com); Brian L. Roberts (brian.roberts@corporate.com); Eric Chabrow (echabrow@ismgcorp.com); Gerard Goroski (gerard.goroski@voicemediagroup.com); Jamshid Khazenie (jkhazenie@gannett.com); Jeff Zucker (jeff.zucker@cnn.com); Keith Koffler (keith.koffler@whitehousedossier.com); Keith Murdoch (keith.murdoch@foxinc.com); Les Moonves (les.moonves@cbcorporation.com); Marc Frons (marc.frons@newscorp.com); Paula Kerger; Randy Falco (randy.falco@corporate.univision.com); Rich Mitchell (rich.mitchell@conservativedailynews.com); Steve Burke (steve.burke@nbcuniversal.com)
Subject: Establishing a minimum acceptable standard of qualification in the cyber-security industry

01010111 01000101 01000010 00100000 01001110 01000101 01010100 01010111 01001111 01010010
01001011 00100000 01010011 01001000 01001001 01000101 01001100 01000100

WNS

Secure by design

“WNS can’t stop hackers from trying to breach your devices but WNS can stop hackers from succeeding.”

THE BIGGEST INTERNET ISSUES IN THE WORLD

(July 19, 2018) <https://www.politico.com/newsletters/morning-cybersecurity>

Cybersecurity should be among the chief international internet priorities of the National Telecommunications and Information Administration, several groups told the agency this week in comments the NTIA solicited.

The General Contractor license exam, the Bar exam, the Board Certification exam, etc. are all designed to develop minimum acceptable standards of qualification for their respective professions. This helps to ensure an acceptable level of quality of the products and/or services is offered to the public.

NAFCU urges Congress for national data security standard following Equifax data breach

(September 8, 2017) <https://www.cuinsight.com/press-release/nafcu-urges-congress-national-data-security-standard-following-equifax-data-breach>

National Association of Federally-Insured Credit Unions (NAFCU) President and CEO Dan Berger today in a letter urged congressional leaders to support national data security standards for retailers and others who collect and store consumers' personal and financial information following news of the Equifax data breach.

Equifax's Seismic Breach Tests Trump's Pledge to Dismantle Rules

(September 12, 2017) <https://www.bloomberg.com/news/articles/2017-09-12/equifax-s-seismic-breach-tests-trump-pledge-to-dismantle-rules>

The massive Equifax Inc. data breach has triggered demands on Capitol Hill for stiffer rules and new requirements for what financial companies must do to fend off cyberattacks.

A few weeks ago, Web Network Shield contacted the FTC regarding establishing a penetration test as a mandatory effective tool to establish a minimum acceptable standard of qualification to market and sell cyber security products to consumers in the US.

Equifax is getting crushed – and traders are betting it's going to get so much worse

(September 11, 2017)

<http://www.businessinsider.com/equifax-stock-price-options-traders-on-further-decline-after-security-breach-2017-9>

Equifax has already plunged 18% since it announced last week that hackers may have the personal details of nearly half the US population.

Equifax Faces Mounting Anger, \$70 Billion Lawsuit

Congress Calls for Hearings; Security Watchers Call for CEO's Resignation

(September 11, 2017) <https://www.databreachtoday.com/equifax-faces-mounting-anger-70-billion-lawsuit-a-10282>

Utahns sue Equifax for \$5B over data breach

(September 11, 2017) <https://www.ksl.com/?sid=45767608&nid=148&title=utahns-sue-equifax-for-5b-over-data-breach>

Equifax failed to implement adequate security measures to safeguard consumers' personal information and willfully ignored weaknesses in the computer system, including prior hacks...

Since 2014, Web Network Shield has tried to work with governments at the municipal, county, state, and federal levels to control the escalating cost of recovering from a cyber-attack utilizing URA (unauthorized remote access) by offering an effective security program that immediately detects and prevents URA.

Web Network Shield strongly encourages Congress to act with a sense urgency to establish a minimum acceptable standard of qualification.

Web Network Shield mission statement:

Web Network Shield (WNS) seeks to become customer-focused, focusing our strategies and budgets on the technologies, systems and processes that win, serve and retain customers by immediately detecting and preventing URA from unregistered URLs and mimicked IP addresses.

This electronic message, including any attachments, is for the use of the intended recipient(s) only. If you have received this message in error, please notify the sender immediately and then delete it. Precautions have been taken to minimize the risk of transmitting software viruses but please be advised to conduct your own virus checks on any attachment to this message. If you are the intended recipient and you do not wish to receive similar electronic messages from us in the future then please respond to the sender to this effect.

01001000 01100001 01110110 01100101 00100000 01100001 00100000 01100111 01101111 01101111
01100100 00100000 01100100 01100001 01111001 00100001