Blockchain? Trump Admin Seeking Alternatives To Social Security Numbers

Calls for a universal ID system has skyrocketed since the Equifax breach and Technocrats are chomping at the bit to uniquely identify everyone, everywhere. This leapfrogs the concept of RealID by a country mile, and would be twice as dangerous to privacy. TN Editor

On October 4, 2017, following the extensive security failure of Equifax Inc., reports indicate that the Trump administration is exploring alternatives to the standard means of identity provenance: Social Security numbers.

Special assistant to the president and White House cybersecurity coordinator Rob Joyce spoke Tuesday at a Washington cyber conference on what he described as an outdated identity system. "I feel very strongly that the Social Security number has outlived its usefulness. Every time we use the Social Security number, you put it at risk."

In light of the fact that 143 million US customers' private

information was accessed by hackers, the 45th presidential administration is leaning on other federal departments to help find an adequate replacement for the existing system, while exposing its weaknesses.

Appearing before the House Energy and Commerce Committee in an effort to offer an explanation for the hack was Equifax CEO Richard Smith, who was the recipient of admonition from both sides of the political aisle. Smith faced questions regarding the scale of the data breach and why Equifax executives failed to act swiftly to disclose the information. Mere days after the hack, three CEOs of Equifax sold shares worth $2 million (according to the SEC) but claim to have had no knowledge of the attack.

Smith pointed to a growing number of hackers who are targeting Social Security numbers as evidence of their vulnerability. He said:

> *"The concept of a Social Security number in this environment being private and secure – I think it's time as a country to think beyond that. What is a better way to identify consumers in our country in a very secure way? I think that way is something different than an SSN, a date of birth and a name."*

Joyce indicated that a better system would include the implementation of a "modern cryptographic identifier," going on to say, "It's a flawed system that we can't roll back that risk after we know we've had a compromise. I personally know my Social Security number has been compromised at least four times in my lifetime. That's just untenable."

Examples that harken back to Estonia's digital identity program were made by Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology in Washington, as he described a system wherein a "physical token," embedded with a private key, could be issued to individuals in conjunction with a PIN. This would allow citizens to establish that they were who they claim to be, the same way one would with a debit card.

"Your pin unlocks your ability to use that big number [or private key]," said Hall, who acknowledged that while "it's very promising" as well as

technically feasible, it is still a “pretty big endeavor,” with a substantial cost for deployment to every US citizen.

Bob Stasio, fellow at the Truman National Security Project and former chief of operations at the National Security Agency’s Cyber Operations Center, pointed to blockchain technology as a means of creating numbers that are mathematically impossible to maliciously replicate. Rather than relying on a numeric system that was implemented in 1936, blockchain technology can provide “a much more efficient and mathematically sound method of transaction, identification and validation.”

Read full story here…