# MEDIA RELEASE

## The US Federal Government has secured its email borders, as best they can, leading into the upcoming US Federal Election, but questions still remain!

Zulu Labs Inc, the leading cyber email trust network has released its latest research into the US Federal Government's cyber email security implementation and whether the upcoming federal election is secured from email interference.

Rock Springs, Wyoming, – October 28, 2020

Zulu Labs Inc, the developer of the World's only email trust metric, Trusted Sender Score, has finalized the latest research into the US Federal Government's implementation of required cyber email security authentication protocols designed to protect email borders from spoof phishing email attacks and business email compromise attacks.

**The Department of Homeland Security's binding directive 18-01**, required all US Federal Departments to have implemented the most secure email authentication protocol possible by of October 16 2018. This directive was aimed to shield United States Federal Government email domains from being used in spoof phishing email attacks against US citizens, US organizations and general email users across the World. This directive made the US the Federal Government absolute leaders in the implementation of the specific protocol.

Research conducted by Zulu Labs Inc through the Trusted Sender Score community-based initiative, can confirm that **84% of surveyed US Federal Government Department** domains have implemented the protocol to the level mandated by the 18-01 binding directive.

US Federal implementation of the required email security authentication when compared to other Federal Governments **(Australia 17%, Brazil 7.1%, Costa Rica 7.8%, New Zealand 2.9%, Singapore 2.8% and The United Kingdom* 16%)** is a significant achievement. **Concerns remain over the 4.4% implementation by US State Governments and just 15% of S&P 500 companies.**

Several unknown factors remain vital to the security of the upcoming election from email interference. Questions include:

How much US Federal Agencies and Departments rely on email from external third parties? And;

What inbound authentication scrutiny has been enforced federally?

These questions are vital as there are numerous examples of organizations contracted to the federal government that have not secured their domains however their services and products are being replied upon.

There are other factors which also include Zulu Labs Inc President, David Barnes, being the first to make public his research into how a protected and compliant domain can still in fact be compromised under certain conditions. In addition to breaking the authentication protocol, research conducted throughout 2020 shows that the parliaments and/or congresses of countries such as Australia, Brazil, Canada, China, Mexico, New Zealand, Russia, Singapore and The United Kingdom are all still able to be used in a spoof email attack against the United States. **This means that under certain conditions the US Federal Government email borders are vulnerable.**

"Whilst the US Federal Government has taken a global lead in the implementation of, what we have now described as, 'DMARC Compliance' or otherwise referred to as the required and mandated email authentication protocol, **interference in this upcoming Federal Election cannot be ruled-out.** Interference via email will be subject to the trustworthiness of third-party emails and if any government officials have subsequently performed any action based on illegitimate emails received" said Zulu Labs Inc President, David Barnes.

"To have complete peace of mind would mean that all emails being received by US Federal Government agencies and departments would have to meet the required authentication protocol and other Trusted Sender Score metrics, and this is just commercially not achievable as of yet for the entire Government. **We do however encourage the Department of Homeland Security to increase requirements for all emails being received to at bare minimum a Trusted Sender Score of 7 or more**, this way and only this way, will the US protect critical email borders" continued David.

Zulu Labs Inc via Trusted Sender Score provides all research and metrics quoted in this media release free of charge and we welcome enquiries with respects to statements made within this release. Further information is available on our websites https://trustedsenderscore.com and https://zuluedm.com/trusted-sender. Organizations wishing to secure their email domain from being used in spoof attacks and to secure their organization from third party spoof and phishing attacks are encouraged to register for Trusted Sender Network or make contract with our consultants.

ENDS

Media Enquiries

Zulu Labs Inc. 1993 Dewar Drive, Rock Springs WY 82901
http://zululabs.com/media-releases.php

David Barnes
support@zululabs.com

* United Kingdom research is not limited to Federal Government departments only and includes county and other departments and agencies. That is 3126 UK Government domains in comparison to 143 US Federal domains.