ADV 2020-34
SECURITY SUMMIT

ADVISORY FOR TAX PROFESSIONALS
AUGUST 4, 2020

Security Summit: Use VPN to protect data from thieves

Tax professionals urged to safeguard client information and their businesses

PROVIDENCE — As more tax professionals consider teleworking during the coronavirus (COVID-19) pandemic, the Security Summit today urged tax practitioners to secure remote locations by using a virtual private network (VPN) to protect against cyber intruders.

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the internet and the company network. As teleworking or working from home continues during the pandemic, VPNs are critical to protecting and securing internet connections, according to the Internal Revenue Service, the Rhode Island Division of Taxation, and other partners in the Security Summit

"For firms expanding telework options during this time, a virtual private network is a must have," said IRS Commissioner Chuck Rettig. "We continue to see tax pros fall victim to attacks every week. These networks are something you can't afford to go without. The risk is real. Taking steps now can protect your clients and protect your businesses."

Failure to use VPNs risks remote takeovers by cyberthieves; criminals can access the tax professional's entire office network simply by accessing an employee's remote internet connection, said Rhode Island Tax Administrator Neena Savage. Tax professionals should seek out cybersecurity experts if they can afford it. If not, practitioners can search for "Best VPNs" to find a legitimate vendor. Also, major technology sites often provide lists of top services. Remember, never click on "pop-up" ads marketing a security product because such ads generally are scams.

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) offers the following advice regarding the use of VPNs:

- Update VPNs, network infrastructure devices, and devices being used to remote into work environments, by using the latest software patches and security configurations.
- Alert employees to an expected increase in phishing attempts.
- Ensure information technology security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Implement multi-factor authentication on all VPN connections to increase security. If multi-factor is not implemented, require teleworkers to use strong passwords.
- Ensure IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.

The Security Summit consists of the IRS, the Rhode Island Division of Taxation, other states' tax agencies, and the tax community -- including tax preparation firms, software developers, tax professional organizations, and financial institutions. Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers.