United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

October 5, 2017

Nancy A. Berryhill
Acting Commissioner of Social Security
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Dear Acting Commissioner Berryhill:

I write today to urge the Social Security Administration (SSA) to consider adding additional cybersecurity safeguards to protect online Social Security accounts from phishing and other sophisticated cyber-attacks.

SSA has been a pioneer in consumer protection and cybersecurity. In 2016, SSA began to offer multi-factor authentication (MFA) to its "*my* Social Security" online accounts as an optional security upgrade. The upgrade allowed *my* Social Security users to add an additional layer of security, by requiring a user to enter a one-time code received via text message to access the account. In June of this year, SSA made MFA mandatory for all my Social Security accounts and added an email option for receiving the code. SSA has also adopted Domain Message Authentication Reporting & Conformance (DMARC) which prevents "official-looking" phishing email messages that purport to come from ssa.gov. While these security upgrades have made it significantly harder for fraudsters to illegally access *my* Social Security accounts, the MFA methods offered by SSA— text message / email—are not resistant to other types of phishing. Just as individuals can be tricked into entering their password into a phishing website, they can also be tricked into entering a multi-factor authentication code into a fraudulent site.

In recent years, several major technology companies have embraced Universal Second Factor (U2F), a form of MFA resistant to all phishing. The FIDO (Fast IDentity Online) Alliance is promoting U2F, which provides heightened security by utilizing a small, low-cost physical USB token. Users authenticate themselves by inserting the token in their computer when prompted for authentication. Google, Facebook, and Dropbox all offer opt-in support for U2F. Likewise, Vets.gov recently announced opt-in support for U2F, proving that this technology is ready for use by government agencies. Soon more devices, such as smartphones, tablets, and computers, will be U2F ready and the purchase of the token will be unnecessary.

Given the low cost of implementation and strong additional protection that U2F provides, I urge SSA to consider supporting U2F on an opt-in basis for workers and beneficiaries who seek additional security for their *my* Social Security accounts.

If you have any questions about this request, please contact Tom Klouda on the Finance Committee staff.

Sincerely,

Ron Wyden

Ron Wyden
Ranking Member
Committee on Finance