FOR IMMEDIATE RELEASE
April 12, 2016

Contact: Lindsey Held (202) 224-4515

Wyden Statement at Finance Committee Hearing on Cybersecurity and Protecting Taxpayer Information

As Prepared for Delivery

Hackers and crooks, including many working for foreign crime syndicates, are jumping at every opportunity they have to steal hard-earned money and sensitive personal data from U.S. taxpayers. It happens online and in the real world. And in my view, taxpayers have been failed by the agencies, the companies, and the policymakers here in Congress they rely on to protect them.

It was unacceptable for the IRS to leave the front door open to hackers by using a weak authentication process for its "get transcript" system. It meant thieves could walk through the door and steal the tax information of three quarters of a million taxpayers.

And to make matters worse, after the IRS mailed special Identity Protection PIN numbers to the hacking victims, it repeated its mistake and used lax security online. For the tax scammers, once again it was as easy as going online, plugging in the personal data you've already stolen, and pretending to be somebody who's lost their IP PIN. So after leaving the front door open, the IRS left the back door open, too. There is no excuse for this.

But poor protection of tax payer information is not just a problem at the IRS – there's a lot of blame to go around. Already this tax season, hackers have gotten into the inadequately guarded systems of private software firms and stolen personal information from thousands of people. And it's my judgement that you can't have an honest discussion about protecting taxpayer information without including the vulnerabilities from e-file providers, as well as crooked return preparers who operate in the shadows and steal from customers.

For years Republicans and Democrats agreed on the need for minimum standards for return preparers, but Congress has sat back and watched while criminals have come in and preyed on taxpayers. When it comes to blocking hackers, Congress has done next to nothing while the IRS loses its ability to hire the experts who can keep taxpayer information safe.

If you're a top-notch tech expert, you're already taking a pay cut to work in public service compared to what you'd earn at firms in Oregon or California. Now, without what's called "streamlined critical pay authority," it can take four to six months to bring a new hire on board at the IRS. So let's be clear: Taxpayer information is under assault every day, but the IRS does not have the legal authority it needs from Congress to build a cybersecurity team that can beat back the crooks.

Already there's been an exodus of high-ranking IRS tech staff. The Director of Cybersecurity Operations left a month ago. The terms for the remaining employees working under this authority continue to expire, including for one of our witnesses, Chief Technology Officer Terence Milholland. Come 2017, there will not be any left.

So today, instead of rehashing the past and beating up on one agency or one firm, this committee ought to focus on how to step up the fight against hackers and crooks across the board. It's my view that streamlined critical pay authority is a key part of the solution. There was a bipartisan bill ready to go last fall, and this committee ought to move forward on it as soon as possible. Furthermore, Congress needs to make more than token investments in IT at the IRS. Congress has held the IRS' tech budget below where it was six years ago, but you can bet that the hackers haven't backed down since then.

Next, the IRS and private firms need to do much more to keep taxpayer information safe in their systems. The "get transcript" hack I mentioned earlier has been well-documented. And a recent audit by the Online Trust Alliance found that the security maintained by private free-file services did not meet expectations. It is unacceptable for troves of taxpayer data to be more vulnerable to hacking than many social media or email accounts. And the Committee ought to consider whether the IRS has the authority it needs to guarantee that the security used by private software firms is up to snuff.

While many tax preparers are honest practitioners, there are always some bad apples in the barrel. Last year Senator Cardin and I introduced a bill giving IRS the authority to regulate tax return preparers. Senator Hatch and I have worked to create a bipartisan identity theft bill for markup in the Finance Committee, which I had hoped would include the regulation of return preparers. It is still my view that people handling sensitive taxpayer information should meet minimum standards and that the Committee should vote to require that.

It's already open season for hackers to steal money and data from hard-working Americans, so congressional inaction should not make the situation worse. With tax day approaching, millions of Americans are filing their returns online, through the mail, or with a private return preparer. This committee has a responsibility to protect taxpayers no matter what filing method they choose. So I see this hearing as an opportunity to find bipartisan solutions on all fronts.

###