Opening Statement of Chairman Ron Johnson

"*The IRS Data Breach: Steps to Protect Americans' Personal Information*"

June 2, 2015

As prepared for delivery:

Good afternoon and welcome.

Last week, the IRS announced that, from February through mid-May this year, criminals accessed the past tax returns of 100,000 Americans using IRS' own website, and attempted to access the tax information of many more.

Using stolen information on taxpayers and public data sources, criminals created fraudulent accounts on IRS.gov in the names of real taxpayers. This allowed the criminals to obtain those taxpayers' previous tax returns directly from the IRS, including data such as adjusted gross income (AGI) that criminals can use to submit fraudulent returns to the IRS. In short, IRS.gov provided criminals with the information they needed to successfully defraud taxpayers.

These criminals' ability to defraud the American taxpayer was made possible, in part, by the IRS' decision to ignore the advice of a cybersecurity expert earlier this year. In late March, prominent cybersecurity journalist Brian Krebs published an article highlighting weaknesses in the way the IRS verified users' identities on its website. The article noted that IRS.gov relied on knowledge-based questions to authenticate users that can be answered using information easily obtained online — questions like, "When did you purchase your home?" or "When did you purchase your car?"

Although the IRS was made aware of the weaknesses in its authentication practices as early as March, according to Commissioner Koskinen the IRS made a conscious decision to not make any changes to its authentication practices. It was not until after IRS employees discovered the breach in late May that the IRS disabled the "Get Transcript" functionality of its website — nearly two months after these concerns were first brought to light. Professor Kevin Fu from the University of Michigan and Mr. Jeffrey Greene from cybersecurity firm Symantec, who have joined us here today, will speak to the weaknesses of knowledge-based authentication and will discuss alternatives that would provide more security.

The case of one victim of this data breach at the IRS, Michael Kasper, was highlighted in the article brought to the IRS' attention in March. Mr. Kasper is here with us today as well. Mr. Kasper attempted to file his tax return online in February, only to discover that criminals had already filed it for him. He soon learned that the thieves had also created an account in his name at IRS.gov, apparently to obtain his past tax information in order to make their fraudulent return look legitimate. In his testimony, Mr. Kasper will expand on the details of this difficult experience, and how he was forced to track down the criminals who impersonated him without the help of the IRS.

According to the IRS, about 13,000 questionable tax returns have already been filed in the names of victims of this breach. Through these likely fraudulent returns, the IRS has transferred up to $39 million to criminals. Further, the cost to taxpayers may rise as criminals file fraudulent returns in the names of other victims.

Unfortunately, the damage to taxpayers doesn't stop there. Although the IRS will provide taxpayer-financed credit monitoring to the 100,000 victims, many forms of identity theft — such as fraudulent applications for government benefits — do not appear on credit reports. As a result, credit monitoring will not detect that form of fraud and the ultimate cost of this breach is likely much higher.

The privacy implications of this breach are profound. In this time of vigorous debate about the privacy implications of the NSA's collection of telephone metadata — phone numbers and times and dates of calls — the IRS is conducting data-mining on Americans and has allowed foreign organized crime syndicates to access the financial histories of more than 100,000 Americans.

Just as concerning is the fact that other government websites, such as Healthcare.gov, suffer from the very same authentication weaknesses. This is an issue I intend to look at deeply in the coming weeks. Federal agencies must do a better job safeguarding the massive amount of data they collect from the American people.

IRS Commissioner John Koskinen and IRS Chief Technology Officer Terence V. Milholland will also testify today, and we appreciate their appearance. We look forward to their explanations of the timeline and decision-making process they followed in setting up and securing IRS data on millions of Americans.

###