OPENING STATEMENT

Ranking Member Daniel Lipinski (D-IL)
of the Subcommittee on Research and Technology

House Committee on Science, Space, and Technology
Subcommittee on Research and Technology
"Can the IRS Protect Taxpayers' Personal Information?"
April 14, 2016

Thank you Chairwoman Comstock for holding this hearing, and welcome to the witnesses. I know this is a busy season for you, and I appreciate you taking the time to appear before us this morning.

Today, we will be discussing cybersecurity breaches at two IRS online service portals. This hearing follows the reports of unauthorized access to the personal information of more than 700,000 American taxpayers, and the theft of money from taxpayers that likely came about as a result. Just about every American can expect to interact with the IRS during his or her life, and the agency's responsibilities make it privy to significant amounts of personal information about all of these individuals. Consequently, data breaches at the IRS are particularly troubling and we should closely examine what IRS has done wrong when it comes to protecting the personal information of Americans, how it can do better in regard to cybersecurity, and what Congress can do to better support IRS cybersecurity efforts. In meeting their obligation to pay taxes, Americans should have confidence that the IRS is taking all possible steps to protect them from cyber thieves.

Cybersecurity remains an evolving challenge across federal agencies as well as the private sector. Standards that were leading edge a year ago may be outdated today. Security is not a one-time goal to be achieved and placed on autopilot; it is a process that requires vigilance, continual learning, and fast dissemination of critical information to prevent and respond to new threats. While no entity, public or private, can protect data with 100% certainty, we must be nimble in learning from failures or missteps in cybersecurity policies and procedures. To this end, we should heed the careful and detailed recommendations of the GAO and the Inspectors General. We must also ensure that decisions on cybersecurity policies are backed by a process that supports accountability, robust and forward-looking decision-making, and a clear sense of

the consequences that can stem from data security failures. Unfortunately, it is not at all apparent from the recent breaches at the IRS that the agency's policies were governed by such a comprehensive process. The two breaches that we are discussing today – the Get Transcript application and the Identity Protection PIN application – should not be viewed in isolation. Both of these breaches were facilitated in part by the same security weakness, namely the overreliance on out of the wallet questions derived from credit report data. While in principle the answers to such questions should only be known by taxpayers, in practice they can often be guessed or uncovered from sources such as social media or websites compiling public record data. As a result, a breach in one application should have tipped off the IRS that the other was vulnerable as well. Yet the agency continued to make online IP PIN retrieval available long after shutting down the Get Transcript application because of security concerns. Further, the agency continued to do so even after the Treasury Inspector General for Tax Administration, or TIGTA, warned the IRS to shut down the IP PIN tool as well. We must get clarity on what steps the IRS is taking to ensure internal information sharing so that any breaches and their implications are quickly assessed across the entire organization and not just separate units or staff dealing directly with a problem at hand. Further, we must examine why the IRS ignored or deprioritized the TIGTA recommendation to shut down the IP PIN tool. Simply put, given how one breach built on the other, this should not have occurred.

In the context of this hearing it is important to talk about NIST, an agency that this subcommittee has jurisdiction over. NIST plays an important role in developing technical standards and providing expert advice to agencies across the government as they carry out their responsibilities under the Federal Information Security Modernization Act, of FISMA. It is clear that the IRS did not follow the risk analysis or cybersecurity and authentication standards set by NIST when it set up these portals. The most important question is "why?" Was it a lack of understanding of the standards? In this case, we need to have NIST here to talk about the standards and how to make them clearer. Or are there technical barriers to implementing the NIST standards at all? In this case, we need to have information on why these applications were allowed to go live in the first place. Or was this a strategic decision driven by tradeoffs between consumer convenience and security? In that case, we must be clear: the IRS has a unique role among federal agencies

and holds information on taxpayers that few others have. Protection of taxpayer data must be a top-level priority and we must work to ensure that a breach of this nature never happens again.

Finally, I would like to note that successful data security efforts depend on agencies being able to hire experienced cybersecurity professionals as well as having budgetary resources specifically directed toward security infrastructure. While some security failures at the IRS raise oversight questions about decision-making protocols at the management level, we also cannot ignore that successful implementation of good security practices costs money. Although this is beyond the scope of our Committee's jurisdiction, I am concerned that Congress has yet to reauthorize IRS' streamlined critical pay authority which helps the agency compete with the private sector for top cybersecurity talent. And as Congress makes funding decisions for the coming fiscal year, we must ensure that we provide resources to match current IT-specific needs.

I look forward to this morning's discussion, and I yield back the balance of my time.