COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrastructure Protection Subcommittee Ranking Member Eric Swalwell (D-CA)

Design vs. Default: Analyzing Shifts in Cybersecurity

December 5, 2024

In recent decades, we have witnessed remarkable technological progress that has changed every aspect of our lives, and with rapid advances in AI, we can expect this transformation to continue in the coming years.

Much of this innovation has taken place here in America, including in my district in the Bay Area, and the competition between technology companies globally to develop new products and services has benefited people around the world.

A challenge with this digital revolution is that the innovation that has transformed how we communicate, store our data, and access vital services has not always been matched with a level of security necessary to protect us from foreign adversaries and criminal gangs.

Every day we read about cyber incidents that demonstrate the security built into our digital ecosystem is insufficient to protect our privacy or critical infrastructure.

To combat this problem, we must rely on the same innovative spirit that has fueled our recent technological progress to also transform how we secure our networks.

This idea underpinned President Biden's National Cybersecurity Strategy when it committed to "building toward a future digital ecosystem that is more inherently defensible and resilient."

And under Director Easterly's leadership, CISA has led the way with its Secure by Design Initiative, partnering with allied countries and private sector partners to develop principles on how we can better embed security into technology going forward.

Critical to this effort is an understanding that security must primarily be the responsibility of those with the most expertise and resources.

For too long, the response to many cyber incidents is a reminder to turn on multifactor authentication or training on how to spot a phishing attack.

Don't get me wrong—there's a role for cybersecurity training and best practices for end users.

But, humans are fallible, and asking consumers to defend themselves against well-resourced criminal gangs and nation-state actors is a doomed strategy.

Instead, we must reduce the burden on end users by embedding security into technology and turning on security features by default.

This fundamental shift in how we think about security will not be easy, and it will take time, resources, and cooperation between government and the private sector.

The efforts we have seen under the Biden Administration have made significant progress, but we must continue this initiative in the coming years.

Today's hearing will be an opportunity to hear directly from private sector experts on the promise of secure by design, the challenges we will face in shifting to this new paradigm, and how the Federal government can better support and incentivize improved security.

It is critical that terms like secure by design and secure by default not become buzzwords in marketing schemes but instead result in meaningfully improved security outcomes.

I hope our witnesses will help this subcommittee better understand how we can support private sector innovations in security and move toward a more secure digital ecosystem.

Before I close, this is likely our last subcommittee hearing before a new administration takes office.

CISA's Secure by Design Initiative is just one example of the many vital projects CISA carries out.

Efforts in the next administration to weaken or abolish CISA could have devastating impacts on our national security, and I hope we can work in a bipartisan way to support this vital agency.

# # #

Media contact: 202-225-9978