Keynote Speaker: Carole House – English Transcript

00:15

"Hi, I'm Carol House. I work as a special advisor for cybersecurity and critical infrastructure at the White House National Security Council. I just came back to the NSC after spending a few years outside of government, but I've held various roles before, really focusing on where technology meets national security. I've worked at the Treasury, done three tours at the White House, and I was also a captain in the Army. So, first off, I just want to say thank you."

00:43

I'm really glad to be here today to chat with you about an important topic that's been a focus for a lot of work happening in the US government. Before I get into some of the great things we've been working on, I want to explain why this issue matters to me from my role at the National Security Council. We have a lot of goals for our financial system, including making sure it stays stable and supporting consumers.

01:13

We're working on fighting financial criminals and money launderers while boosting our leadership in tech innovation. It's all about reinforcing our role in the global financial system. Financial inclusion plays a big part in these goals, and it's also affected by them. So, when we tackle issues like money laundering and terrorism financing, it's not something we do in isolation. Financial inclusion isn't just a goal on its own; it ties into a lot of other important factors. Everything's connected here.

01:46

We're all on the same page about making sure everyone has access to safe, affordable, and secure financial products and services. This is key for our nation's economic security. Now, I want to shift gears a bit and discuss the role of technology. Our efforts to boost security and trust online are really important for financial inclusion, especially since we've been talking about how important it is to include everyone in a system that actually works.

02:16

"We need to have proper safeguards to stop consumers from being exploited for their data or falling victim to cybercriminals and other bad actors. That's not what we want for

financial inclusion in our systems. As we rely more and more on technology, and as everything becomes more digital, we really need to find ways to ensure that these technologies can provide better access without putting people at risk."

02:47

"We're working on making services more accessible to everyone, including citizens and other key players. It's important to use technology in a positive way to stop bad actors from taking advantage of the good ones. We want to keep pushing for economic opportunities and making sure everyone, including Americans and people around the world, can access what they need. First, I want to discuss digital identity, which I've been involved with for years since my time at the Treasury, where I led our identity initiatives."

03:19

Identity is a big deal. The fast pace of innovation in the internet, smartphones, and other digital tech has made life so much easier for everyday Americans. But when these folks try to navigate the physical world online, they often run into a lot of bumps and chances for being taken advantage of. Without a solid digital identity, those bumps just get worse. As online payments, shopping, and interactions keep rising, the need for a better solution is only growing.

03:50

We're working on creating robust identity solutions that make it easy, secure, affordable, and reliable for people to identify themselves and others in digital systems. Identity is a complex issue, just like everything related to financial inclusion, which is also complicated and constantly changing. It has a lot of implications for cybersecurity, economic growth, privacy, and more. That's why conversations like the ones happening this week between the government and industry are so important to explore.

04:22

Identity is a big deal when it comes to cybersecurity, and for good reason. A lot of cyber incidents happen because of weak identity and access management. We could've prevented many of these issues by using stronger solutions, like multi-factor authentication. We've also seen that issues with identity solutions are behind a lot of cybercrime, especially when it comes to financial fraud.

04:54

"Like, synthetic identity fraud messes with identity verification, and then there are account takeovers that exploit weaknesses in how we authenticate identities. Plus, business email

compromise targets flaws in the authorization and verification processes between trusted partners. We've heard from industry folks that a huge number of ransomware attacks could have been avoided just by using MFA, or multi-factor authentication solutions. Identity is also really central to the whole zero trust approach."

05:25

Implementations, you know, are basically strategies in cybersecurity that assume your networks might be compromised. This means you need to give the least amount of access to critical and sensitive information. All of this ties back to financial inclusion in digital ecosystems, which requires us to think about how to maintain strong identity practices to avoid exploitation while still promoting that inclusion. We just need to make sure everything is safe.

05:55

"I've been working on making sure everyone has access to financial services. In my previous job, before I returned to government, I was the chair of the Commodity Futures Trading Commission in the US and also led the Technology Advisory Committee. During that time, I helped put together two reports on artificial intelligence and digital assets. Now, at the White House, I've been supporting initiatives related to these areas."

06:25

"Making sure artificial intelligence is secure and that we develop digital assets like cryptocurrency and central bank digital currencies responsibly is super important. Both AI and digital assets show how we're shifting towards decentralization and making tech more accessible to everyone. It's exciting to see how technologies like ChatGPT and LLaMA are becoming available to more people, pushing the boundaries of what's possible."

06:56

There's an amazing opportunity here, but from an economic and national security angle, it's also a bit scary because it could give cybercriminals a chance to access things they shouldn't. These cybercrime groups can use this advanced technology to run widespread fraud schemes, which is a big worry for us. For instance, we advised financial institutions on some of the main tactics we saw when I was working there.

07:29

"We're working to fight fraud schemes like business email compromise. We suggested they implement a multi-step authorization process for high-value transactions. But now, with the rise of advanced deep fake technology, it's getting easier for even less skilled

cybercriminals to bypass these protections. AI is making it simpler for them to pull off these scams."

08:03

The U.S. government is making AI technology easier to access. They're doing this through initiatives like setting up an AI Safety Institute at NIST and other efforts across the government. The goal is to encourage the safe and responsible development of AI, while also making sure we can use it quickly and effectively. This will help us create better risk management frameworks and assessments.

08:32

"We don't just make random decisions about broad groups of people. We also use technology to fight widespread fraud. These are some of the steps we're taking across the US government to ensure safe and secure access to financial services. This is where national security and financial inclusion goals come together. I'm really honored to have the chance to talk to all of you and be part of these conversations."

09:01

"Things are going great this week! I really appreciate the chance to talk to all of you—it's such an honor!"