U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Washington, DC 20528

National Association of Corporate Directors members,

You may have seen that CISA recently launched a Secure by Design Pledge at the RSA Conference, which, as of mid-June, over 150 companies have signed. By catalyzing action with some of the largest software manufacturers, the pledge marks a major milestone in CISA's Secure by Design initiative, and we are deeply grateful for these commitments.

Informed by the ever more complex technology threat landscape we face, the pledge asks companies to commit to seven concrete actions. Collectively, these commitments aim to better secure the technology that our critical infrastructure and broader US economy rely on through investments in preventable defects that are all too easily exploited by bad actors.

As board members of companies that both produce and depend on software to deliver goods and services, you have the collective power to generate a strong demand signal that products must be built to be secure by design.

We need your help to drive the supply and demand for secure products.
I invite you to show your commitment to working over the next year to show your support for measurable progress toward the following seven goals:

1. Increase multi-factor authentication use;
2. Reduce default passwords;
3. Reduce entire classes of vulnerability;
4. Increase the installation of security patches by customers;
5. Publish a vulnerability disclosure policy;
6. Demonstrate transparency in vulnerability reporting; and
7. Increase the ability for customers to gather evidence of cybersecurity intrusions affecting their products.

The Risks and Solutions Are Clear
The software defects we see today belong to known classes of vulnerability for which effective mitigations have been known for years, or even decades. Despite awareness of these chronic defects, many companies continue to build and sell technology with such built-in dangers, putting our nation and our economy at risk, particularly from Chinese cyber actors who are intent on launching disruptive attacks against our critical infrastructure here at home. As I stated in recent Congressional testimony before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party:

> "*The threat is not theoretical: CISA teams have found and eradicated Chinese intrusions into critical infrastructure across multiple sectors, including aviation, energy, water, and telecommunications. And what we've found to date is likely the tip of the iceberg. The reality is, however, eradicating malicious Chinese activity, bolstering the resilience of critical infrastructure, or even going on the offense to disrupt and impose costs, are all necessary, but insufficient. While the PRC is a sophisticated cyber adversary, many of its methods to break into our critical infrastructure are not. They don't have to be. Why? Because we've made it easy for them. The truth is that, in many cases, the PRC is taking advantage of known product defects.*"

Indeed, for far too long, software manufacturers have prioritized speed to market and new features over security, citing market demand for such features and noting that there is little incentive for security. Cost is a big factor too—we recognize this as an economics issue as much as a technical one—and we encourage a more expansive view of the costs of security and insecurity—by considering the costs that customers bear every day in compensating for insecure technology as well as the costs of fixing "recalls" rather than making upfront investments in preventing defects in the first place.

We need to catalyze a shift in the market for software products. That's where I'm hoping to enlist your support.

Everyone Can Act Today

To drive business decisions around security, we know that there must be a strong demand signal from customers. CISA will continue to drive awareness and education with enterprise software customers while also providing the tools and language needed to demand security during procurement. Your company can also take significant action to protect our nation.

If you serve at a company that is an enterprise software manufacturer, we encourage you to take the Secure by Design Pledge. In doing so, you are helping not just protect your own company's customers, but our entire critical infrastructure by helping lay the foundation for more secure by design software. Our Secure by Design team can be contacted at SecureByDesign@cisa.dhs.gov.

If you serve at a company that is not an enterprise software manufacturer, we encourage you to create a "Secure by Demand" movement by asking more of your company's software suppliers. As a first step, we encourage you to publicly demonstrate your support for the Secure by Design Pledge—and look for progress from your vendors in line with the items in the pledge. As a next step, we hope that you can help make secure by design products the norm by integrating secure by design approaches—as articulated in our pledge—in your contractual language or during acquisition processes.

We are deeply grateful for your continued collaboration to measurably reduce the most pressing cybersecurity threats to our nation. As the nation's cyber defense agency, we are privileged to serve as your close partner in protecting the critical infrastructure Americans rely on every hour of every day.

Please do not hesitate to reach out to SecureByDesign@cisa.dhs.gov if we can support you in any way.

Sincerely,

Jen Easterly
Director