Testimony of Jeanette Manfra
Senior Director, Global Risk and Compliance
U.S. House Committee on Homeland Security
May 28, 2025

Chairmen Green and Garbarino, Ranking Members Thompson and Swalwell, and distinguished Members of the Committee; thank you for the opportunity to appear before you today. My name is Jeanette Manfra, and I am the Senior Director for Global Risk and Compliance for Google Cloud. We appreciate the House Committee on Homeland Security holding this important hearing, and we look forward to sharing Google's perspective on opportunities for regulatory harmonization and compliance modernization to enable the entire ecosystem to better protect itself against rising threats.

Technology advances, threats evolve, the cybersecurity landscape changes, and cybersecurity defenders must adapt to it all if they want their approaches to stay current. In an interconnected world facing growing cyber attacks, it is critical to ensure that technology systems are resilient to keep people safe. For more than 20 years, Google has pioneered a Secure by Design approach, meaning we embed security into every phase of the software development lifecycle — not just at the beginning or the end.

Google Cloud offers a suite of world class security solutions, including identity and access management, data security, network security, incident response services, threat intelligence, and much more. We are proud to have been a pioneer of zero trust architectures, and we are committed to partnering with customers to ensure they can deploy securely in the cloud while meeting their compliance obligations through every step of their cloud migration journey. At Google Cloud, we believe in a Shared Fate model that goes beyond traditional shared responsibility. We work closely with our customers to achieve optimal security and risk outcomes, and we continuously invest in robust security capabilities and transparency protocols to maintain the most trusted platform.

As we continue to pursue excellence in security for ourselves and our customers, we also believe there is an opportunity to modernize our approach to compliance.

Importance of Regulatory Harmonization and Recommendations

Regulating cybersecurity at the national scale is complex, poses unique challenges, and carries high stakes. Regulatory and compliance regimes impact the resilience of critical infrastructure, economic development, the pace of technological innovation, military deployments and capabilities, and the daily lives of American citizens. As a result, cybersecurity regulation should be carefully balanced: promoting strong cybersecurity baseline standards while allowing flexibility to account for evolving technology and the ever-changing threat landscape.

Google recommends a regulatory approach that is agile and focuses on aligning baseline requirements across sectors. The approach must also allow for additional sector-specific requirements that are complementary to and not duplicative of or in conflict with those standard baselines. This approach would increase adoption of security principles across the federal government, critical infrastructure, and the private sector. Regulatory agility will help reduce compliance burdens, enhance coordination, build public trust, and allow for a more resilient approach as threats change, new economic sectors emerge, and agency responsibilities change and shift over time.

Regulations must prioritize tangible outcomes over mere checklist compliance. Google's commitment to openness, interoperability, transparency, responsibility, a secure-by-design approach, intelligent security systems, and collaborative efforts can only be fully realized within such an adaptable regulatory environment. We urge Congress to modernize cybersecurity regulations and create a stable baseline that existing sectors can adhere to and future sectors can adopt as a reliable guide for improving security and resilience.

To achieve regulatory harmonization, Google offers a few central recommendations. First, leverage well-established standards and processes for any contemplated security baseline approach. In our view, initiatives like the Federal Risk and Authorization Management Program (FedRAMP) are already established with support from the public and private sector. We welcome GSA's work to modernize the FedRAMP program, including through increased automation, and we further encourage leveraging Open Security Controls Assessment Language (OSCAL) for more streamlined authorizations. Second, any harmonized standards should implement a risk-based approach - ensuring compliance options are aligned to specific risk levels or categories to maximize flexibility and efficiency commensurate with the level of risk associated with a particular technology, application, or use case. And finally, complement harmonization through a clear approach to reciprocity for different certification regimes (such as FedRAMP levels, DoD SRG Impact Levels, and other existing or future programs).

As the Committee considers mechanisms to achieve regulatory harmonization, we also urge Members to continue to foster public-private dialogue on the topic. We encourage the Committee to consider a global harmonized approach to ensure enterprises and service providers can focus on security outcomes as a top priority. Google remains committed to the security of the digital ecosystem and would be pleased to consult on future cybersecurity regulations.

* * *

Thank you for convening this important hearing. We look forward to continuing to further raise awareness about cybersecurity threats and defenses, and the work we are doing at Google Cloud to keep networks protected.