April 7, 2025

The Honorable Brett Guthrie
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable John Joyce, MD
Vice Chairman
Committee on Energy and Commerce
U.S. House of Representatives
Washington, DC 20515

RE: Response to Data Privacy Working Group RFI

Dear Chairman Guthrie and Vice Chairman Joyce,

On behalf of Worldwide ERC (WERC), thank you for the opportunity to provide input on the development of a national data privacy and security framework. We look forward to continuing to engage with the Data Privacy Working Group and the Committee as the proposal moves through the legislative process.

WERC is the professional association representing the global talent mobility industry with over 2,750 enterprises and more than 10,000 individuals as members. Our membership is comprised of the many human resource and operations professionals representing the world's largest corporations as well as mid-sized U.S. businesses, who employ and routinely relocate employees throughout the U.S. and around the world. We also represent the essential service providers who enable the movement of talent including relocation management companies, movers, real estate brokerages, tax and immigration experts, temporary housing providers, destination service providers, and more.

Over 3 million people in the United States move each year due to a new job or job transfer, with many of them formally moved by the employer in order to facilitate the smooth operations of their businesses and accommodate economic growth and development. This movement impacts workers at all levels and virtually every community across the country. The ability to efficiently and seamlessly move workers has a critical impact on a business' ability to succeed in a competitive global business environment, for its workers to develop and thrive, and for ensuring continued American leadership on the global economic landscape. Consistent privacy laws and data protection regulations allow for better data management by employers and greater comfort for data subjects, knowing that no matter where they work and reside in the United States, they can expect a consistent level of data protection.

As part of relocating employees around the U.S., our members handle the combined data of hundreds of thousands of individuals who are transferring for work, usually across state lines. As such, essential service providers must be in compliance with the data privacy and security requirements of 50 state privacy laws and regulations. It is from this perspective we provide our comments to assist in the development of a national approach to regulating data privacy and security. The General Data Protection Regulation ("GDPR"), promulgated within the European Union and adopted by many

other countries, is an example of how a national data privacy standard can be applied. The GDPR provides general consistency of privacy regulations for companies to operate and develop their privacy and data protection framework, while maintaining independence for each regulator to enforce and protect their citizens. Implementing a U.S. national standard will bring its own complexities and considerations, and as the working group moves forward in this effort, we urge it to develop a balanced approach that maximizes protections, benefits, and operational feasibility while accounting for differences in application based on factors such as size, scope, and geography.

Data Breaches

As it stands, every state has a law regarding the requirements surrounding the identification of reportable data elements if they are exposed. A national standard should follow the common elements of those laws to ensure easier adoption by businesses and, if applicable, government agencies. The framework should provide for a consistent identification of reportable data elements, the data which must be included in a regulatory notification report and that require notification to the impacted individuals.

The national standard should also establish constancy as to the threshold number of affected data subjects within a state that would trigger notification to that state's regulator. In doing so, we also urge the working group to balance thresholds in a way that accounts for the circumstantial differences between minor, infrequent instances, such as a misrouted email, and major instances such as a ransomware threat or significant system in- and exfiltration.

With regulator reporting timeframes and data subject notifications, one challenge faced by companies is that there is disparity in the range of state-by-state requirements. These windows often don't align for situational circumstances, such as ransomware attacks, that may require more time to properly identify the impacted data subjects and the involved data elements. We recommend that the Committee account for these considerations by considering a threshold, similar to ones already used in various states, of "notification in an expedient timeframe and without unreasonable delay."

Applicability of Standards

It is vital that entities handling personal data have a clear understanding of the standards being applied to them. In developing a national standard, it is imperative that the requirements outline exactly which standards apply to their particular type of entity, as defined by the volume of data processed per year, and to the types of data that are covered. Along those same lines, requirements need to include at what point and where the standards come into place. We recommend establishing clearly defined definitions in order to best facilitate implementation and compliance.

Sensitive Data Considerations

Organizations operating within the talent mobility industry routinely handle sensitive personal information in the course of supporting transferees and their families. This includes, but is not limited to, Social Security numbers, passport information, financial and tax records, and immigration and travel documents. A national privacy standard should acknowledge the heightened sensitivity of this data and apply clear, risk-based requirements to its protection without imposing unnecessary burdens for data categories that are not routinely collected. We also encourage narrowly defined and clearly scoped provisions for specialized data types, such as children's data, to support consistent and practical implementation to avoid creating undue ambiguity in implementation.

Legal Shield

Despite the best cybersecurity measures, safeguards and procedures, the unauthorized access of data is still a threat. A federal law covering data privacy should provide those entities that demonstrate compliance with current industry best practice security standards with a safe harbor against lawsuits resulting from the unauthorized access of data and other areas of exposure in which the entities demonstrated that they were adhering to the law. Such practices are not new, and various states already have provisions in place. For example, Connecticut, Iowa, Ohio, Oklahoma, Tennessee (as of July 1, 2025), and Utah provide a safe harbor if a company subscribes to identified cybersecurity frameworks such as those established by NIST and the ISO. We recommend that the Committee set comparable provisions within any sort of national framework.

Contractual Arrangements

Regardless of the absence of a national privacy framework or state privacy requirements, relocation essential service providers recognize the need to protect the personal data of transferees. As a result, many providers establish requirements within their supplier network to safeguard personal information. Including privacy provisions within contracts is often the best way to govern data security as the requirements are tailored to the situations and arrangements between the contracted parties. A national framework needs to recognize the design of contractual arrangements to address data privacy for the individuals being provided services.

Private Rights of Action

A private right of action in data privacy legislation allows individuals to sue companies directly for alleged violations, such as data breaches. Extending this right to data subjects would create inconsistent liability, chill innovation, and encourage excessive litigation that benefits plaintiffs' attorneys more than consumers. Federal regulators are better positioned to ensure fair, consistent enforcement of data security standards. A

centralized regulatory framework—rather than fragmented lawsuits—is the most effective way to protect consumers while providing legal certainty for businesses.

Again, we look forward to working with you to help protect the data of individuals and allow the efficient movement of talent throughout our country. Should you have any follow up questions for us, please do not hesitate to contact me via the information below.

Sincerely,

Michael T. Jackson
Vice President, Public Policy and Research
Email: mjackson@talenteverywhere.org
Phone: 1-703-842-3411