TECHNET
THE VOICE OF AMERICAN INNOVATION

2026 FEDERAL POLICY PRINCIPLES

TechNet champions a comprehensive, pro-innovation agenda that enables companies and entrepreneurs to create jobs and economic opportunities for people across the country; empowers American workers and students with the skills and knowledge needed to seize those opportunities and prosper; enhances our national security, global competitiveness, and technological superiority; and promotes freedom, unity, and equity.

TechNet's diverse membership includes many of the most dynamic businesses operating in the United States today, ranging from startups to the most iconic companies on the planet and represents over 5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

1. Privacy
2. Artificial Intelligence
3. Cybersecurity
4. Data Security and Data Breach Notification
5. Intellectual Property and Patent Reform
6. Tax
7. Trade
8. High Growth Startups and Venture Capital
9. Immigration
10. Education and Workforce Development
11. The Future of Work
12. Non-Discrimination
13. Expanding Internet Connectivity and Promoting a Healthy Internet Ecosystem
14. Intermediary Liability and Safety Online
15. Energy Infrastructure
16. Future of Transportation and Mobility
17. Secure and Safe Repair
18. Modernizing Government Technology and Federal Procurement Policy
19. Financial Technology and Financial Services
20. Digital Identity
21. Health Care and Telehealth

PRIVACY

Our members provide services and enhanced experiences for their customers and fuel economic growth and opportunity across our nation. In doing so, our member companies consistently place a high priority on consumer privacy. When it comes to the future of the federal privacy landscape, we support the following:

- Reasonable frameworks that set out organizational accountability as well as clear privacy rights for consumers, including rights to access, correct, delete, and port their data with reasonable limitations that take into account technical and privacy limitations.
    - Policymakers should ensure any frameworks adopted do not: undermine privacy or data security interests; stymie the ability to prevent, detect, or defend against fraud or other unlawful activity, or protect the security and integrity of systems; interfere

- with law enforcement or judicial proceedings; or impose unduly burdensome or excessive requirements (particularly for small and medium-sized businesses, non-profit organizations, and new market entrants), including requirements that would exceed a consumer's reasonable expectation of privacy.

Congress Should Act

- Congress should enact comprehensive federal privacy legislation that protects all Americans regardless of where they live and preempts state laws related to the federal standard, thereby ending the growing state-by-state privacy patchwork and preventing another patchwork from developing in the future. Absent a uniform federal standard, companies will continue to face regulatory fragmentation that hinders innovation and competitiveness in a fast-moving digital marketplace.
- Federal privacy legislation should be tech- and sector-neutral and apply across sectors to both online and offline entities that collect and process personal information, and avoid imposing any outright bans, prohibitions, or moratoriums on specific technologies.

Uniform Laws and Regulations Will Enhance Compliance, Promote Even-Handed Enforcement, and Enable Innovation

- Federal policies should incentivize effective risk-based management.
- Any law should recognize the value of reasonable data collection, processing, use, and retention activities, including using data to provide customer service, authenticate a consumer's identity, process or fulfill orders and transactions, improve services, and the ability to personalize to consumers and make them aware of offered products and services.
- Federal law should establish a flexible framework that provides consumers with appropriate disclosures and control mechanisms with respect to how their information will be processed.
- Collection, processing, and retention of personal and sensitive data should be adequate, relevant, and reasonably necessary in relation to the purposes requested by, or as disclosed to, the consumer.
- Consumer consent, where applicable, should generally be required only for processing sensitive personal information or when there are material adverse changes to the processing of personal information previously collected. Any consent regime should be designed with the limitations of software, hardware, and data management in mind and should not be overly burdensome to the consumer or technology provider. It should also be flexible and convenient for all users regardless of socioeconomic or disability status.
- New federal laws should mirror state approaches by acknowledging commonsense exceptions and exemptions in definitions of personal data, including exemptions for publicly available information and appropriate entities.
- Clear definitions in a federal law for "personal information," "sensitive personal information," and "de-identified information" are essential.
- Any law should avoid restricting consumer access to free, ad-supported services, harming small and medium-sized businesses and non-profit organizations, and undermining a healthy Internet ecosystem, such as unduly burdensome restrictions on first-party, contextual, and personalized advertising. Similarly, any law should not impede the ability to detect and stop sophisticated fraud schemes.
- Consumers, rather than regulators, should be the arbiters of beneficial and valuable private sector technological innovation. We oppose proposals that would unduly restrict consumers' ability to access new, beneficial, and innovative technologies, products, and services.
- Because technology and security threats to consumer privacy evolve constantly, legislation should recognize that security requirements should be risk-based, technology-neutral, and flexible. In addition, federal privacy legislation should not force data controllers to share consumer data with third parties.
- Federal privacy legislation should not treat data transfers across commonly owned affiliates as third-party transfers.
- Private rights of action and other tools that encourage litigation have the potential to undermine innovation and must be avoided.

- A right to cure should be provided, and monetary judgments should be tied to actual harms caused by violations.
- In addition, consumers and businesses should be free to enter into pre-dispute arbitration agreements to resolve disputes.
- Stringent age verification to access online platforms requires the collection, processing, and storage of users' sensitive personally identifiable information, like birth dates and government identification, and should be avoided. This conflicts with data privacy best practices like privacy by design and data minimization, creates new vectors for fraud, and eliminates anonymity online.
- Privacy laws should not broadly prohibit government use of third-party data, which is often an integral component of providing effective and efficient government services as well as protecting against fraud.
- Federal privacy legislation should incentivize private and public sectors to take protective privacy measures, such as de-identification and pseudonymization when implemented with appropriate administrative, physical, and technical controls.
- Privacy laws should include an affirmative defense for controllers or processors maintaining a written privacy policy that reasonably conforms to the National Institutes of Standards and Technology (NIST) Privacy Framework.

Companies Must Proactively Promote Transparency and Security

- We caution against state and local government mandating "real-time" and seamless data portability, or other data sharing requirements that are not clearly necessary and proportionate to a specific defined public purpose, or that do not take into account the privacy implications and technical challenges of adhering to such a mandate.
- We caution against overly restrictive regulations on the uses of biometric technology or automated decision-making systems.

Clarify the Role of the Federal Trade Commission and Preserve the Role of State Attorneys General in Enforcement

- In comprehensive federal privacy legislation, clear requirements should be set forth in the law, and guardrails should be in place to avoid issuance of regulations that would create uncertainty and undermine America's leadership in innovation. The FTC should be the exclusive federal regulator enforcing the law.
- Congress should clarify the scope of the FTC's authority to regulate privacy and data security matters that impact significant portions of the American economy. Until such time that Congress provides the agency with clear authorization, the FTC should refrain from expansive rulemaking.
- Congress should ensure the FTC has the resources it needs to effectively enforce privacy and data security requirements that protect consumers from tangible privacy harms, while also preserving the ability of state attorneys general to protect their constituents and enforce the law based on the federal standard.
- The FTC should maintain its existing efforts of case-by-case enforcement actions rather than pursuing expansive regulatory rulemaking.

Congress Should Pass a Strong Federal Data Breach Notification Law

- Congress should pass a strong federal data breach notification law, which preempts existing state-level notification laws and establishes one robust set of uniform protections for all Americans. More details about TechNet's federal data security principles can be found here.

Ensure New Entrants, Small- and Medium-Sized Businesses, Non-Profits, and Underserved-, and Under-resourced Innovators Are Not Adversely Affected by Burdensome Regulations

- Small, medium-sized, minority-owned, rural, non-profit, and other under-resourced businesses face disproportionate burdens and unique challenges in complying with complex privacy laws and regulations at home and abroad that in some cases overlap or conflict.

Policymakers should evaluate the global privacy landscape with the goal of promoting interoperability that allows American businesses to innovate and compete globally.
- For some innovative young companies that have limited personnel and resources to devote to overly stringent compliance efforts, regulations that are too prescriptive could stifle growth. Congress should set baseline requirements and provide flexibility in how to comply, avoiding prescriptive programmatic requirements and considering the unique needs and resource constraints of small and medium-sized businesses and new market entrants.
- Congress should consider regulatory relief for startups and small businesses if the information they process is limited in nature or does not include sensitive information.
- Congress should establish robust training resources within the Department of Commerce, Small Business Administration, Federal Trade Commission, and/or other appropriate agencies that can provide guidance to startups and small businesses, particularly minority-owned and rural businesses, to ensure compliance with basic privacy requirements.
- Furthermore, we must ensure the complexity of privacy requirements does not effectively become a barrier to entry for new potential innovators. Congress and the administration must therefore ensure that fundamental core privacy protections for consumers are in place without stifling free market forces.

The United States Must Lead Globally

- As the home of the world's preeminent tech sector, the United States must proactively demonstrate global leadership by participating in multi-lateral, multi-stakeholder forums to promote interoperability among privacy frameworks within trade discussions.
- TechNet supports the 2022 European Union-U.S. Data Privacy Framework, and preserving Executive Order 14086 on Enhancing Safeguards for United States Signals Intelligence Activities.
- TechNet believes efforts to promote digital trade and negotiate new trade agreements must promote predictable seamless data flows across international borders.
- TechNet supports the efforts of the United States and its partners to expand the Global Cross Border Privacy Rules system and talks in the Organization for Economic Co-operation and Development on Trusted Government Access. In addition, TechNet urges the United States to support the free flow of data. Specifically, the United States must reassert its leadership on digital trade, including formally reversing its October 2023 announcement that abandoned longstanding, bipartisan digital trade positions at the World Trade Organization. The United States must stand firm against forced data localization and support the cross-border flow of data. It must also continue to challenge mandatory tech transfers and source code disclosures, while ensuring non-discriminatory treatment of digital products.

Facial Recognition Technology

Facial recognition technology can be utilized in a variety of use cases, many of which can improve security and access for individuals using services online. Facial recognition technology can enable remote access to essential services, removing location- and mobility-based barriers to access. In addition, different types of facial recognition technology can be used to facilitate entry to locations and stop fraud and protect consumers.

TechNet believes the following:

- Legislation should not prohibit or effectively prohibit the use of facial recognition technology.
- Legislation should not reduce access to non-identifiable diverse datasets necessary to train models to reduce bias.
- Policymakers should recognize the wide variety of use cases for technologies that detect and/or recognize faces or other parts of the human form and avoid over-regulating visual technologies that do not affect individual privacy.

Protecting Children and Teens

Protecting children and teens is a top priority for the technology industry. When examining protections for children and teens, Congress should:

- Align any updates with the *Children's Online Privacy Protection Act* (COPPA), including continued adherence to an actual knowledge standard and focus on services directed to minors.
- Avoid imposing vague standards and obligations on the design and presentation of content that would run afoul of the First Amendment and fail to provide clear notice to companies about their obligations.
- Avoid imposing overly broad age restrictions on platform access and consider the unintended consequences of such approaches.
- Ensure any proposals are technology and sector neutral.
- Provide as much flexibility as possible, particularly for small- and medium-sized enterprises (SMEs), on implementation, and protect the overall wellbeing of children and teens.
- Ensure that student data is protected, while also providing parents, teachers, and students the ability to access educational tools to promote innovation and technology in the classroom.
- Include clear language to expressly preempt state children's privacy laws that relate to any federal law, to end the current patchwork and prevent another patchwork from developing in the future.
- Grant exclusive federal enforcement authority to the FTC, without expanding the scope of the types of organizations over which the FTC has authority, while preserving the ability of state attorneys general to protect their constituents and enforce the law based on the federal standard.
- Provide law enforcement agencies with the resources and tools to hold perpetrators of child sexual exploitation material accountable.

ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is a transformational technology that has the potential to revolutionize how we live and work and help us solve the most significant challenges of our time. AI can enhance productivity, democratize and expand access to important services, and improve product innovation. TechNet members represent many of the leading AI and automated systems developers, researchers, deployers, and users.

Leverage Existing Laws and Adopt a Risk-Based Approach for Effective AI Regulation

- States are enacting a growing array of AI regulations that vary in scope and substance, creating a fragmented legal landscape that could go beyond the complexities present with the current patchwork of state privacy laws. A consistent risk-based approach, accompanied by federal preemption of state laws and regulations, is needed to provide clear national guidance and to prevent a patchwork of differing state laws that could impede innovation and progress. A consistent and level playing field for all entities developing, deploying, and using AI is essential.
- As policymakers consider new regulations for AI, it is important to note there are already existing rules under sectoral regulation and laws that prohibit unlawful behavior, including such behavior perpetuated through the use of AI. For example, many existing civil rights laws apply to AI models used in education, healthcare, employment, housing, financial services, and accessing goods and services. Such laws and regulations, which benefit from existing well-developed regulatory and enforcement frameworks, focus on preventing and providing recourse against the prohibited conduct rather than the means by which the conduct was accomplished.

- A federal AI framework should build upon and align with these existing statutes, making clear that where federal law already addresses a given harm or risk, it preempts additional or inconsistent state regulation.
- Any new laws or regulations, as well as guidance documents and enforcement statements, should focus on known or rationally anticipated harms that could be prevented or addressed by filling gaps in existing legal regimes. Notably, any new laws or regulations should be narrowly scoped to target identifiable gaps. Further, when considering new AI laws or regulations, policymakers should take into account the following:
    - Prioritize clear definitions of "artificial intelligence" (focusing on autonomous systems that make inferences and that are distinct from static or rules-based algorithms), "deployer," "developer," "high-risk AI," and other terms related to scope.
    - It is crucial for policymakers to recognize the diverse array of stakeholders involved in AI systems and across the AI value chain. A tiered, risk-based approach to AI governance should align obligations with each entity's role and responsibility in the AI supply chain.
    - Careful consideration must be given to defining and designating regulatory responsibility that aligns with the roles and interactions of these entities.
    - The AI startup ecosystem is vital to maintaining America's competitive edge in the global economy. Potential implications for small and mid-size businesses must be considered, especially in terms of ensuring their access to a diverse AI ecosystem.
    - Avoid any "shutdown" requirements as these will disincentivize downstream innovation and create disparities in the global competition to develop AI capabilities.
    - Any new regulations should be subject to existing Regulatory Impact Assessment analyses.
- Policymakers should adopt an incremental and collaborative approach to AI governance. To promote innovation and adapt to technological changes, we encourage the use of evidence-based regulatory tools like safe harbors, which allow the industry to test and share best practices.
- Federal agencies should reaffirm that existing copyright principles — particularly the fair use doctrine — remain technology-neutral and continue to apply when AI systems use data for transformative purposes such as model training, research, or model evaluation.
- Laws should not impose broad opt-outs that conflict with practical realities of functionality that serve consumers' interests, such as the ability of a website to provide search results.
- Ensure that the considerations and relevant requirements regarding the use of commercial AI systems by a federal/state/local government agency should be calibrated to the level of risk the intended use case poses, consistent with any new AI frameworks applicable to the private sector.
- TechNet believes there should be a central coordinator of the federal government's development, deployment, and use of AI systems that ensures that AI policy and regulations are consistent across agencies and industries. This coordinator should ensure that AI policies are risk-based and that all rules and regulations that entities are subject to are based on the level of risk the AI use case entails and not on what regulatory body may claim authority over an entity. This coordinator should partner with existing subject matter agencies on particularly complex or technical use cases that may benefit from specialized expertise.
- The NIST AI Risk Management Framework (AI RMF 1.0) should be promoted as a voluntary model for AI lifecycle management, including design, development, deployment, and post-deployment.
- Private rights of action must be avoided because they can undermine innovation, subject small and large businesses to abusive and frivolous litigation tactics and strain the judicial system.
- Leverage existing enforcement mechanisms and protections from intermediary liability to address AI enforcement challenges.
- Policymakers should prioritize global cooperation and coordination in AI regulations, and they should seek to avoid regulatory divergence when it could harm innovation, trade, and investment critical to U.S. AI leadership.
- Establish a national privacy standard to promote consistent regulation of Americans' data. A comprehensive and preemptive federal privacy law that protects consumers and provides businesses certainty about their responsibility is an essential component of a coherent national

AI-focused policy. A clear national framework will also help build trust in AI systems. TechNet's principles on privacy can be found here.

Responsible AI Evaluations

- Any transparency, explainability, or audit requirements imposed on AI systems must account for protecting personal information and carefully balance the proprietary and trade secret protections regarding the AI system and the technical feasibility of implementing such requirements. It must also not jeopardize the safety, cybersecurity, and anti-fraud systems of AI-driven services.
    - For example, disclosure of actual training data without appropriate safeguards risks disclosing customer and company confidential and proprietary information. Similarly, consideration should be given to the fact that privacy and other concerns are minimized with respect to training data which is ephemeral and becomes sufficiently abstracted within a model such that the original training data cannot be recovered.
    - Regulators do not need unfettered access to proprietary AI models to assess their safety. Any proposed AI audit requirements need to be reasonable, outcome-based, and focused on AI-based systems that are deployed in the market.
- Leading AI developers and academics are continuing to research and improve how to best explain the output of generative AI systems. We encourage the federal government to support continued research and development into best practices for explainability, transparency, and auditing and discourage "one-size-fits-all" regulations as this technology continues to evolve.
    - Ensure any requirements on content provenance allow for flexibility of provenance techniques across various modalities (image, audio, video).
- Regulations requiring enhanced disclosures for users or regulators should apply only to high-risk applications that lack existing regulatory structure — policy, law, or otherwise — to govern situations where the AI system's compromise, misuse, or destruction would be reasonably likely to result in loss of life, liberty, or significant legal effects.
- TechNet supports efforts to solidify a well-resourced non-regulatory entity that is based on measurement science and focused on national security to lead international efforts to establish AI operation, security, and audit standards, such as the U.S. Center for AI Standards and Innovation (CAISI). We believe it is important for NIST to continue its longtime work of advancing measurement science and collaborating with private industry to develop responsible safety practices.

  Transparency
    - We urge policymakers to avoid one-size-fits-all transparency requirements on AI systems, as there will likely be differences between the transparency required between different actors across the AI value chain. When it comes to the transparency requirements between developers and deployers, it is essential that any such requirements establish a commitment that developers will share all relevant information that deployers would need to support their applicable regulatory compliance. Since users of AI will not have the same regulatory compliance responsibilities as deployers, any transparency requirements or audit reporting may reasonably differ and be limited only for high-risk uses of AI.
    - Support public education efforts on how AI systems operate in order to help demystify AI.
    - TechNet supports the disclosure of generative AI content to users in line with industry best practices. Industry leaders are still researching how to best indicate content has been AI-generated and when such indications are appropriate. We are supportive of this ongoing discussion and research to best inform the American public about the content they are viewing.

  External Reviews
    - TechNet believes it is premature to mandate independent third-party auditing of AI systems. Mandating an independent audit before appropriate technical standards and conformity assessment requirements are established could open AI systems to national security threats, trade secrets theft, and inaccurate audit reports.

  - We believe AI auditing standards, ethics, or oversight rules must consider the use-case-specific auditing needs, calibrated to the risk of the specific use case, set to measurable benchmarks, and ensure safe and ethical practices to promote continued innovation while also protecting intellectual property, trade secrets, and security.
  - Reciprocity of AI audit findings across local, state, and federal jurisdictions should also be accepted to limit resource burden and sustain market access for the AI startup ecosystem.

Mitigate Potential Bias

- Throughout its lifecycle, AI development and performance must be appropriately monitored and evaluated. Reasonable measures to identify, track, and mitigate unintended bias and discrimination should be implemented.
- Different actors such as developers, deployers, and users of AI systems should implement oversight and accountability processes appropriate to their role in the AI value chain to ensure safety, fairness, and trustworthiness; protect against malicious activity; and address flawed data sets or assumptions.
- Existing anti-discrimination laws already apply to AI models in many important contexts, including housing, health, employment, and consumer financial services (i.e., the *Fair Housing Act*, Section 1557 of the *Affordable Care Act*, Title VII of the *Civil Rights Act of 1964*, and the *Equal Credit Opportunity Act*). Therefore, additional legislative and/or regulatory obligations in these areas at this time would be unnecessarily duplicative, create inconsistent or conflicting standards, and chill innovation in the United States. Instead, policymakers should leverage existing tools to address concerns of bias.
- TechNet members follow legal guidelines at all stages when developing, testing, and monitoring AI assessments, and in many cases, they test for group differences beyond those required by law.
  - In cases where bias may result despite a party's best efforts to mitigate, the party should be given a rebuttable presumption of reasonable care if they have complied with the relevant law.
- To support innovation and the development of new bias-detection techniques, legislation should exclude from scope: (1) AI systems and models specifically developed and put into service for the sole purpose of scientific research and development; and (2) scientific research and development activity on AI systems or models prior to being placed on the market or put into service.

Secure Advanced Systems

- Leverage security by design principles to enhance cybersecurity within AI systems at the start of their lifecycle.
- Empower America's cyber defenders by funding the use of AI-enhanced cybersecurity services and tools within the federal government.
- Strengthen the adoption of AI cybersecurity awareness training to help minimize risk and prevent loss of intellectual property, data, and money.
- Support bidirectional information sharing and cyber threat programs accounting for threat actors leveraging AI.
- Avoid mandating backdoors, licensing keys, or a "right of first refusal" for advanced AI chips.
- Given rapidly continuing advancements in chip technology, avoid setting technical parameters in statute to control the sales of advanced AI chips.

Build the Infrastructure to Catalyze the Innovation Economy

- To secure America's position as the global leader in AI, we recommend prioritizing and streamlining investments in AI infrastructure and supply chains, including through modernized energy grids, high-speed broadband, and advanced semiconductor manufacturing.
- Support public-private partnerships in establishing and maintaining upskilling and reskilling programs to help Americans best utilize and improve their productivity with automated tools.

    - Some of these programs will be government-funded and designed, but many companies are already providing useful resources to help Americans advance their careers. Governments at all levels should seek to understand and build on what is already working.
    - Promoting upskilling, investing in workforce programs, and encouraging registered apprenticeships offers a proactive approach to fostering diversity among AI developers, deployers, monitors, and users. This is a valuable strategy to address bias and workforce concerns throughout the AI lifecycle.
    - Develop a skills taxonomy for AI, similar to cybersecurity, in order to encourage skills portability and creation of recognized industry certifications.
- Support government funding for AI security and standards research and infrastructure.
    - Congress should authorize and fund the National AI Research Resource (NAIRR). The NAIRR is important to foster the development of the U.S. domestic AI research ecosystem and maintain U.S. leadership in AI on the global stage.
    - Most of the world's leading AI developers are outside of government institutions.; Governments need to engage these experts by utilizing public-private partnerships to inform the development of regulation and guidance, build modern government AI systems, and incorporate AI efficiencies into government services.
    - Government agencies need dedicated funding sources for AI deployment and governance.
- Support the creation of a dual-intent science, technology, engineering, and math (STEM) visa for foreign students who have earned master's level or higher degree from U.S. colleges and universities. This would promote economic growth and innovation in AI by ensuring that talented innovators educated and trained in the United States can become citizens and create jobs here.
- Support the federal government's strategic hiring of AI experts and the filling of vacant technology roles. Bolstering our federal workforce with needed talent will allow key government agencies to enhance their capacity to monitor, utilize, and ensure responsible and impactful AI development and deployment.
- Support the creation of federal AI regulatory sandboxes, particularly in the highly regulated areas of financial services and healthcare, to encourage deployment of responsible and impactful AI technologies.
- TechNet supports expanded government utilization of AI to improve access to important services, enhanced efficiency, cost savings, data-driven decision-making, and more equitable and inclusive service provision, ultimately benefiting citizens and society as a whole.
    - TechNet supports the government in developing "AI Ready Data." The United States federal government is one of the biggest producers of data in the world, and these important datasets are already fueling innovation in the public and private sectors. As we move to greater deployment of AI systems, ensuring this data is well-organized will allow these modern tools to deliver faster, cost-effective, and more accurate insights.

CYBERSECURITY

In order to meet the cybersecurity needs of today's increasingly interconnected digital world, policymakers and industry leaders must focus efforts on educating and training a highly skilled workforce, modernizing government Information Technology (IT), and building long-lasting public/private partnerships. TechNet supports the adoption and use of voluntary, adaptable, risk management-based approaches to meet this changing environment and effectively manage cybersecurity risk. TechNet supports the following principles and objectives:

- Alignment of policies, legislation, regulations, and guidance with flexible, stakeholder-driven, risk management-based approaches to cybersecurity.

  - Promotion of voluntary private sector adoption of the NIST Cybersecurity Framework (Framework).
  - Further guidance for and oversight of Framework adoption by federal agencies, per Executive Order 13800; and promotion of Framework-like approaches (adaptable, stakeholder-driven, risk management-based) with international partners.
  - Appropriate implementation of the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* with final regulations that reflect industry feedback and the statutory intent of Congress, especially the promotion and implementation of incident reporting harmonization.
  - A comprehensive risk-based cybersecurity strategy that increases the security and resilience of all networks and prepares for and mitigates cyberattacks through the voluntary coordination of industry and government.
  - Policy and market-based incentives, including federal regulatory safe harbors, to encourage companies to appropriately manage risks in accordance with industry standards and best practices, and to encourage companies to share threat intelligence, particularly where it pertains to AI-driven deepfake attacks.
  - Avoidance of regulations that increase compliance costs but do not provide commensurate benefits for cybersecurity interests.
  - Improved accountability, reporting requirements, and uniform standards for federal agencies as they comply with cybersecurity laws, regulations, and executive actions.
  - Public/private initiatives that support improving the cyber defense capabilities of small businesses.
  - Harmonization of conflicting requirements in the private sector with attention paid to reducing duplicative and conflicting reporting requirements to minimize time, expense, and complexity of compliance and enhance security.
  - Address cyber threats to the supply chain of the National Industrial Base.
  - Preserve the ability of technology companies to deploy end-to-end encryption and refrain from mandates that weaken its protections.
- Continued focus on the Office of the National Cyber Director's efforts to promote cybersecurity regulatory harmonization.
- Support for the development of the U.S. Cyber Trust Mark Initiative, a voluntary cybersecurity labeling program for Internet of Things (IoT) devices and products, to leverage market forces to drive cybersecurity in IoT.
- Continued funding for and implementation of the *Modernizing Government Technology Act* that focuses on driving down cybersecurity risk and enabling modernization of IT systems. Agencies must report on existing networks that cannot be fixed and must be replaced.
- Reauthorization of the *Cybersecurity Information Sharing Act of 2015*, which facilitates a risk-based strategy by promoting the sharing of actionable cyberthreat information from government to industry, from industry to government, and among private companies.
- The U.S. government should promote greater sharing of cyberthreat information with the private sector in a timely, straightforward, and actionable manner, and ensure government agencies are funded and staffed with the necessary resources to efficiently manage the collection of data. The federal government should track and publish its own performance metrics, including the amount of time that occurs from (1) breach-to-detection, (2) detection-to-response, and (3) detection-to-sharing of the cyberthreat indicators.
- Appropriate liability protections when participating in government cybersecurity information sharing programs.
- Regulators should be cognizant of sector-specific risks and build off of existing successful sector-specific regulations. Any new cybersecurity requirements should build off of and grant reciprocity to existing cybersecurity compliance frameworks.
- Government efforts to develop norms that support an open, interoperable, secure, and reliable cyberspace. Cyberattacks by state and non-state actors threaten international and national security, democratic processes, the global economy, the free flow of ideas and information, and the safety, security, and privacy of individuals.
- An increase in attention for cybersecurity in international forums, including the G20, and increased U.S. government engagement in international bodies, such as the UNECE World Forum for the Harmonization of Vehicle Regulations (WP.29).

- No federal government mandates on the design of products and services. The federal government should be particularly careful to avoid requirements that could weaken the security of technology used to protect sensitive personal information and critical systems.
- Cybersecurity efforts at the federal and state levels to protect the integrity of election systems and related information technology infrastructure.
- A renewed focus on enhancing attribution and bringing cyber criminals to justice.
- Education, workforce, and immigration policies that help the United States develop and retain the world's best cyber workforce.
- Continued and additional funding for states to procure consolidated cybersecurity services on behalf of local entities to thwart the increasing ransomware attacks against our local government systems and school districts, including through reauthorizing the DHS State and Local Cybersecurity Grant Program, which lapsed on September 30, 2025.
- The continuation and further development of Information Sharing and Analysis Centers (ISACs) that provide critical infrastructure owners and operators a forum to detect, share, and analyze cyber threat information.
- Congress should act:
    - Federal legislation is needed to provide harmonized and consistent standards throughout the United States to set cybersecurity guidelines and security expectations. Federal legislation should be tech- and sector-neutral and apply to online and offline entities alike that collect and process personal information.
    - Congress and other federal and state government entities must be collaborative partners in advancing the protection of consumers and the furtherance of innovation in the 21st-century data-driven economy.
    - Congress and the administration should consider and incorporate certain national and international frameworks, with a particular focus on interoperability and secure data flows, as they develop a framework for baseline legislation.
- Additional funding for federal and state agencies to invest in educational programs, tools, and other resources that help American small businesses and critical infrastructure owners and operators better protect themselves from the increasing amount of cyberattacks. Funding should also help federal and state agencies adopt AI-enhanced fraud detection tools, including liveness detection.

DATA SECURITY AND DATA BREACH NOTIFICATION

- TechNet supports a strong federal data breach notification law establishing a robust set of uniform protections for all Americans that is risk-based and focused on the likelihood of actual substantial harm to consumers.
- A single national breach notification standard will provide companies and consumers with consistent, actionable notice of a data breach that could result in substantial harm–and should include the following:
    - Notice if there is a risk of substantial harm;
    - Sufficient time for the private sector to report confirmed intrusions; and
    - Notification requirements should consider any needed delays to determine the nature of any breach, including law enforcement requests for delay; the need to protect the intellectual property of reporting parties; and the need to protect information that could undermine the security of other individuals, companies, or systems, and sensitive information, including consumer data.
- A federal data breach notification law should preempt the patchwork of state laws in this area and consider other federal breach notification obligations.
- Data breach notification policy should only impact an entity if their network or system has been breached and acquisition of personally identifiable information has occurred. Reporting requirements that relate to unsuccessful attempts are not risk-based, will waste limited resources, and result in cumbersome contractual terms that create friction without providing

any substantive benefits to data subjects. Entities should not be held responsible for, or be required to rectify, breaches outside of their control or responsibility.

- Statutory requirements and obligations should be aligned with generally accepted cybersecurity frameworks like NIST's Cybersecurity Framework 2.0, rather than impose specific security standards, which change over time.
- Data rendered unusable by encryption, redaction, or any other security method or technology should not be considered having been breached.
- The standard giving rise to notification should be data acquired and not simply accessed. Notification requirements should be triggered by the determination that a breach has occurred, not merely by the initial discovery of a potential incident.
- The distinction between an account takeover of a customer's online account and a data breach should be explicitly recognized in statutes, with differentiated provisions and reporting methodologies.
- Any statutory definition of personally identifiable information that triggers notification should exclude publicly available data and be limited to information that, if compromised, could identify a specific individual and lead to substantial harm.
- The statutory notification obligation to consumers should rest with the first party that has the relationship with the end user, but parties should have the ability to determine by contract their respective roles.
- Public safety entities should be provided the appropriate level of resources to help deter, identify, track, and hold accountable perpetrators of identity theft-and provide assistance to consumers. Support for deepfake and liveness detection may be warranted as well.
- Enforcement of a new federal data breach notification statute should be limited to only the FTC and state attorneys general. Notification obligations should take into consideration notification obligations under other federal laws.
- Legislation should not include private rights of action, civil penalties, or other tools that encourage litigation. These mechanisms would significantly undermine the effectiveness of a federal data breach notification law by discouraging reporting, without providing corresponding protections for consumers.

INTELLECTUAL PROPERTY AND PATENT REFORM

TechNet advocates for a healthy patent system that yields high-quality patents, promotes all forms of innovation, deters frivolous patent litigation, and compensates patent owners based on the value of their contributions.

The U.S. Patent and Trademark Office (PTO) must continue to develop and implement patent examination rules, procedures, and guidance to promote the issuance of high-quality patents that provide clear public notice of claim scope to downstream innovators and implementers. Congress should ensure that the PTO retains flexibility to set appropriate user fees and that all user fees stay with the agency to fund its operations. As a key part of this policy goal, Congress and the PTO should uphold the Inter Partes Review (IPR) process established under the bipartisan America Invents Act. IPRs allow for patents to be reviewed by a panel of highly skilled patent judges with technical degrees, who are best suited to review complex technology. A critical element for a strong patent system is ensuring high quality patents and that mechanisms exist to efficiently correct any errors made during the patent application process. The IPR process plays this crucial role in the patent ecosystem by allowing for efficient review and elimination of erroneously issued patents and preserving the strong, balanced patent system at the heart of American innovation. TechNet opposes reforms that hinder or block access to the IPR process, particularly ones based on discretionary reasons divorced from the merits of patentability or that are not explicitly provided by Congress.

Also, Congress should increase funding for intellectual property-specific law enforcement training through the Intellectual Property Enforcement Grant Program within the Department of Justice's Bureau of Justice Assistance.

TechNet supports reforms that deter litigation abuse in the courts and the International Trade Commission, including policies that promote domestic public interest and discourage vague and unsupported infringement allegations, asymmetric discovery burdens, presumptions of irreparable harm or compensable damages where no such harm or damages exist, forum shopping, and manipulation by litigation funders who take advantage of patent owners and the judicial system for their own financial gain.

TechNet encourages the USPTO to promote guidance and regulations that provide clarity around the patentability of AI technologies. Additionally, protecting the right and ability to perform computational analysis on data is necessary to create effective AI models and ensure the U.S. remains the leader in AI development. Any changes to existing copyright law that would restrict access to AI training data will hamstring America's ability to innovate and compete globally. Rather than implementing new statutory requirements or restrictions the U.S. Copyright Office should ensure that any further guidance focuses on protecting the core provisions of copyright law and fair use doctrine that offer technology-neutral protections to legitimate rightsholders and innovators. This will encourage a balance where creators' rights remain honored while ensuring continued progress in developing groundbreaking AI technologies. Federal agencies should advocate for copyright policies, both in the U.S. and abroad, that support and reinforce our national leadership in innovative AI technologies.

TAX

The U.S. corporate tax system provides a globally competitive tax rate that encourages companies to invest in America and benefits U.S. workers, families, and communities. Policymakers at all levels should maintain and build upon this successful tax system to encourage investment in American businesses.

Specifically, federal policymakers should preserve a competitive corporate tax rate along with policies that allow businesses to deduct all expenses in the year they occur. Federal tax and budget policy should also renew investments in private sector research and development (R&D) to ignite innovation, create jobs, and increase our global competitiveness. Federal policymakers should also support tax policies that encourage U.S. manufacturing of key technologies such as semiconductors. Policymakers should also seek opportunities to support startups and entrepreneurs through tax policy that promotes stock ownership.

To maintain a competitive international tax system that promotes innovation and growth, federal policymakers should preserve U.S. tax laws that encourages multinational companies to continue to invest and innovate in the United States. The U.S. should challenge discriminatory taxes proposed or placed upon U.S. technology companies by foreign tax authorities.

TRADE

The United States is the global leader in developing and deploying innovative technologies. The high-tech economy is a vital component of U.S. economic competitiveness and future growth. It is imperative that the administration and Congress recognize and promote our economy's innovative strengths and pursue a pro-growth trade agenda that produces economic growth, creates jobs, benefits consumers, strengthens U.S. competitiveness, and stands up for U.S. economic interests abroad. Maintaining and strengthening the rules-based global trading system, including through strong digital trade provisions, will ensure that American businesses and workers are able to compete

fairly in the global marketplace, pursue global market opportunities, and is a critical component of strengthening supply chain resiliency.

The United States must also stand against discriminatory and unfair trade practices that target U.S. firms. The United States can improve market access for the technology sector by developing and cultivating strong relationships with our international trading partners, leading efforts to shape global trade rules, upholding digital trade, and avoiding unilateral tariffs and trade wars that hurt American consumers, workers, and businesses of all sizes, and are ineffective at changing unfair and discriminatory trade practices that distort the global economy.

TechNet puts forward the following policy recommendations:

- Congress and the administration should work to advance comprehensive trade negotiations and agreements with willing partners in bilateral frameworks and plurilateral frameworks while ensuring that U.S. free trade agreement partners continue to comply with commitments made under existing trade agreements. Congressional support for these endeavors is crucial.
- International trade agreements should create regulatory certainty, reduce barriers to markets for digitally delivered and other information-technology oriented goods and services, promote the free flow of data across borders, contain "safe harbors" against intermediary liability, and include strong protections for intellectual property.
- Recognizing the administration's national security objectives, TechNet supports a stable, consistent tariff policy that ensures market access and free flow of goods and services. Reliance on tariffs (reciprocal tariffs and Section 232 tariffs, among others) as a measure to seek short term, non-binding trade agreements contributes to a permanent state of uncertainty and should be limited and fact-dependent. In addition, finding an effective conclusion to the trade war with China should lead to the removal of the harmful Section 301 tariffs that raise prices for American consumers. At the same time, the United States must reassert global leadership on trade policy to curb China's discriminatory practices by leveraging the combined market power of our international partners and allies, especially with respect to critical and emerging technologies and market access, which means the United States should limit the use of broad, unilateral tariffs on information technology products from those same partners and allies. Finally, all of this should be done with a view toward minimizing and managing potential supply chain disruptions that harm American innovation and leadership.
- It is imperative that the Indo-Pacific Economic Framework includes quality digital trade standards, supply chain diversification and resiliency improvements, and strong investor protections, especially as China's influence grows in the region and throughout the world.
- Develop a balanced approach to export and import controls that effectively protects critical national security interests while enabling export of U.S. technology to ensure continued U.S. global competitiveness.
- The United States should push back against discriminatory measures that target U.S. tech firms. The United States should also work to prevent and reverse the adoption of discriminatory regulatory and tax policies, such as Digital Service Taxes which target or otherwise disproportionately impact certain companies or business models. At the same time, the administration should work closely with Congress to enact measures such as a federal privacy law that will influence global policy and trade decisions affecting U.S. companies in relation to the cross-border flow of data and use of data for existing and future critical and emerging technologies.
- Given the impact of government-restricted lists on the supply chain, the technology sector would benefit from greater transparency into the process of how and what agencies consider in producing such lists, including the criteria used to determine what constitutes a threat and which specific companies have been identified. It is critical to strike the right balance of combating legitimate threats without making overly broad changes that could have unintended consequences of putting American companies at a disadvantage and emboldening our foreign competitors. Any restrictions impacting the supply chains for critical and emerging technologies must have a sufficient phase-in period to allow for American businesses to make needed transitions in ways that minimize disruptions and negative consequences.

- Congress and the administration should pursue customs modernization and open payment systems that support-e-commerce and digital trade flows, particularly by small- and medium-sized enterprises (SMEs).
- To further facilitate trade and bring customs relief to small businesses and consumer sellers, the administration should restore the $800 de minimis threshold and work with Congress to avoid undue burdens on global commerce. Moreover, Congress and the administration should identify use cases that have faced particular challenges following the elimination of the de minimis threshold, including the importation of used goods and the importation of goods that were made in the U.S. Finally, Congress should ensure that U.S. Customs & Border Protection has the resources and technology it needs to protect consumers and enforce U.S. laws.
- The United States must exercise strong leadership at the World Trade Organization (WTO). U.S. representatives should seek to further trade liberalization via the WTO, including reductions in tariff and non-tariff barriers to information, communications, and advanced energy technology products, services, and investments. The United States should work to create market access opportunities by expanding the geographic scope and updating the product coverage of the WTO's Information Technology Agreement (ITA) and should continue to push for the permanence of the WTO Moratorium on Customs Duties on electronic transmissions.
- Additionally, the United States must formally reverse its October 2023 announcement abandoning longstanding, bipartisan digital trade positions at the WTO, and resume its position as a global leader in advocating for prohibitions on forced data localization, tech transfer, and source code disclosure, while ensuring non-discriminatory treatment of digital products.
- The U.S. Trade Representative should strongly assert its mandate to consult and coordinate with other Executive Branch agencies, while driving market-opening, and job-creating outcomes that drive economic growth.

HIGH GROWTH STARTUPS AND VENTURE CAPITAL

Startups, including venture-backed startups, are disproportionately responsible for the innovations that drive economic growth and job creation in the United States. In fact, startups are responsible for most of the net new U.S. jobs created since 1997. The venture capital business model is based on investors taking risks and making investments in early to later-stage startups, in order to accelerate innovation and the startups' growth. These long-term capital investments provide young companies with the time and resources they need to build products, develop new ideas, hire personnel, and expand, and have fueled extraordinary innovation in the United States for decades.

TechNet advances a policy agenda that supports the American innovation ecosystem, which includes venture capital firms and startups, whose success will determine the country's future competitiveness.

While promoting a competitive and innovation-driven marketplace, policies should also recognize the role of effective enforcement of competition laws in protecting consumers and sustaining market dynamism, particularly where startup entry and innovation may be at risk.

To thrive, startups need access to capital and markets, innovation, and talent.

Access to Capital and Markets

Startups thrive when they have access to capital and markets and operate within a balanced regulatory regime that promotes innovation and does not restrict access to exit opportunities. Startups typically operate in a loss position for several years, deliberately choosing instead to invest heavily in growth activities such as research and hiring and necessarily generating tax assets. Federal policymakers can improve the capital allocation process for existing and new startups through targeted reforms to regulations and tax laws.

The following policies are essential to promoting the startup ecosystem:

- Federal policies that reduce unnecessary barriers for private companies opting to go public and stay public and reject efforts to unnecessarily restrict these companies' access to public equity markets.
- Federal policies that promote competition and startup access to capital.
- A regulatory regime that recognizes mergers and acquisitions are essential to the thriving startup ecosystem.
- A regulatory regime that allows consumers to determine the success of companies, rather than the government.
- Efforts by federal agencies to appropriately enforce long-standing consumer protection laws.
- Federal policies that protect the competitive process, innovation incentives, and consumers, while avoiding privacy, cybersecurity, or national security risks.
- Reducing bias against acquisitions by large companies to avoid unintended, long-term consequences on investment and innovation.

Access to Innovation

Public policy should help startups and small businesses move projects efficiently from the idea phase to the new business phase. Additionally, the federal government should adopt public policies that encourage small businesses to adopt technologies to grow and scale.

TechNet supports the following policies:

- Federal efforts to create regional technology hubs where federal resources could catalyze regional innovation and opportunity and bolster competitive advantages in emerging technologies.
- Federal tax and budget policy that renews investments in private sector research and development (R&D) to ignite innovation, create jobs, and increase our global competitiveness.
- The exploration of new ownership models, including co-ownership between inventors and universities.
- Patent policies that level the playing field to promote innovation in all sectors of the economy and minimize frivolous litigation. TechNet's principles on intellectual property and patent reform can be found here.
- Procurement reform at the local, state, and federal levels that acknowledges the evolving technology landscape and enables governments to purchase and utilize innovative and secure products on a technology-neutral basis.

Access to Talent

TechNet supports efforts to grow and strengthen America's talent pipeline by ensuring equitable access to digital skills training across occupations; encouraging and supporting American students to pursue STEM fields, particularly computer science education; and reforming our immigration policies to attract and retain the best global talent.

- The modern American workforce requires a flexible employment environment that allows workers to find opportunities that best match their skills, interests, and availability. TechNet's principles on the future of work can be found here.
- An educated, diverse American workforce is the lifeblood of the innovation economy. More significant federal investments in education and the workforce will help all American students and workers succeed in a global, interconnected, and technology-driven economy. TechNet's principles on education can be found here.
- The world's most talented innovators and entrepreneurs should be able to stay in the United States and contribute to our economy, rather than be forced out to start businesses in competitor nations. To that end, TechNet supports comprehensive immigration reform, and our principles on immigration can be found here.

IMMIGRATION

Federal action limiting legal employment-based immigration undermines America's economic and national security interests by stifling innovation, stunting job growth, and exacerbating ongoing skills gaps in our nation's critical industries. Additional funding for critical industries and emerging technologies is not enough. For the United States to successfully compete in the 21st Century global economy and maintain our leadership in emerging technologies such as artificial intelligence, Congress and the administration must work together to pass immigration reform, including the following proposals that will help America win the next era of innovation:

Attracting Critically Needed Talent in Emerging and Foundational Technologies to Our Shores

- Exemptions from annual green card caps for advanced STEM degree holders in emerging and foundational technology fields.
- Raising the H-1B visa cap to meet the growing demand for high-skilled talent.
- Avoiding exorbitant fees associated with the H-1B visa and other programs that could discourage or make it impossible for companies, including startups and small companies, to access the talent they need to grow and compete.
- Creation of a startup visa to encourage entrepreneurs from around the world to grow companies and jobs in the United States.
- Increased flexibility for the movement of high-skilled workers and entrepreneurs starting a new company or expanding a company's footprint in the United States.
- Updates to the methodology for prevailing wage determinations to reflect employers' compensation structures, including, but not limited to, stock-based compensation.
- Protection of the OPT and STEM OPT programs to allow foreign students to continue their training in the United States.
- Allowance for dual intent visa applications by foreign students seeking to study in the United States.
- Efforts by federal, state, and local governments to ensure the United States continues its proud tradition of welcoming refugees in our communities, including, sharing data with employers on where refugees are settling, and the type of skills individuals possess.
- Enhanced vetting and information gathering on particular individuals spending time in certain countries to address Intellectual Property (IP) theft to critical domestic industries.
- Increased transparency around the retrogression of visa numbers, particularly for individuals with current priority dates.
- Updating the H-1B lottery system to ensure the process is not used to game the system through misuse and fraud and prioritizes roles critical to U.S. economic competitiveness. Lottery selections should be based on high-value, innovation-driven sectors and job types, not indiscriminately across all occupations by wage level, salary, or career stage. Any reforms to the lottery system should not disproportionately impact SMEs or the diversity of types of positions that would be prioritized under any reforms.

Providing Much-Needed Certainty for Young Immigrants

- A pathway to citizenship for all Dreamers, including the nearly 700,000 individuals covered by the Deferred Action for Childhood Arrivals (DACA) policy, as well as the 400,000 DACA-eligible Dreamers denied protections due to ongoing litigation.
- Protections from aging out for "documented Dreamers," the children of parents who are long-term visa holders in the United States.

Optimizing Existing Immigration Programs

- Streamlining of high-skilled immigration processes to ensure the utilization of all available green cards each fiscal year.
- Modernization of employment-based immigration programs to eliminate fraud, punish bad actors, and be responsive to America's economic and national security needs.
- Ensuring that family visa determinations are considered in conjunction with employment-based visa determinations to allow families to stay together while ensuring that spouses and children are not counted against the cap on high-skilled immigration.
- Elimination of outdated per-country caps that do not track to America's strategic needs.
- Recapture of unused visas that have been unallocated due to flaws in our immigration system.
- Provisions to ensure that program fees for H-1B visa applicants are used effectively, match the supply of H-1B visas to demand, and reduce the backlog of employment-based green cards.

EDUCATION AND WORKFORCE DEVELOPMENT

The United States is losing its competitive edge compared to countries like China due to its lack of focus on science, technology, engineering, and math (STEM) education. American companies throughout the entire tech ecosystem consistently face talent shortages. TechNet supports efforts to grow and strengthen America's talent pipeline by ensuring equitable access to digital and AI skills training across occupations; encouraging and supporting American students and workers to pursue careers in in-demand STEM fields, particularly computer science education; and retooling our immigration policies to attract global talent. TechNet advocates for greater federal investments in education, apprenticeships, and workforce training to help all American students and workers succeed in a global, interconnected, and technology-driven economy.

TechNet supports:

- Education and workforce development policies focusing on greater access to digital skills and digital and financial training across industries and empowering workers to keep their skills updated and in line with the changing demands and nature of work in the 21st century.
- Apprenticeships and career and technical education programs (degree and non-degree) that advance the knowledge and/or skills necessary for high-demand technical career pathways.
- The adoption of financial and digital literacy standards as requirements for high school graduation for all students.
- Efforts to streamline processes for accessing job training funds, including efforts to incentivize reciprocity for eligible training providers.
- The expansion of online skills and workforce training programs for underserved and underrepresented communities.
- Expanding computer science and AI offerings in high schools and allowing qualified computer science courses to fulfill a core high school graduation requirement.
- Robust and sustained efforts to train and recruit more high-quality STEM and computer science teachers through effective professional development and teacher training programs.
- Promotion of the K-12 Computer Science Framework.
- Policies that encourage the use of digital content and technology, including access to high-speed broadband and connectivity in the classroom, as well as increased internet adoption at home.
- Fully funding STEM education programs enacted in the *CHIPS and Science Act of 2022.*
- Ensuring that student data is protected, while also providing parents, teachers, and students the ability to access educational tools to promote innovation and technology in the classroom.
- Increased public/private partnerships with HBCUs, PBIs, HSIs, and Tribal Colleges and Universities to develop broader and deeper curriculum to promote STEM education and careers to create a more diverse workforce.
- The National Science Foundation to more equitably allocate funding for research with a focus on early childhood and to support research on the factors that encourage or discourage girls to

engage in STEM activities, including computer science. TechNet also supports increased funding for programs that help girls learn computer science.
- Tax incentives to encourage employers to invest in the skills of the current workforce.
- Greater use of innovation and data to help workers understand available training and career paths and policies which would make it easier for individuals to differentiate between credentials and search for quality programs that are likely to lead to in-demand and higher-wage jobs.
- Greater transparency of student career and salary outcomes in America's postsecondary education system to provide America's students with accurate information to help attain post-graduate employment opportunities.
- Lifelong learning, retraining, and reskilling policies and programs that allow workers to attain the education and skills they need to stay current as jobs evolve and advance their careers.
- Broader work-based training programs, including support for transitional employment which would provide subsidies for time-limited, wage-paid work experiences and skills development.
- Employers and employees should be free to enter into mutually agreeable arrangements, such as predispute arbitration, to resolve employment-related disputes and obtain a faster and more cost-effective resolution of such disputes.
- In general, federal preemption regarding employment-related issues.
- Policies to attract and retain advanced STEM degree students from around the world who study at U.S. institutions of higher education to continue their career development in the United States.

THE FUTURE OF WORK

As AI technology becomes increasingly integrated into the U.S. economy and the daily lives of people across the globe, TechNet urges policymakers to consider the many opportunities that AI presents for job creation, career advancement, worker empowerment and wellbeing, and workplace safety and accessibility. Federal policies should ensure that all workers are able to benefit from and take advantage of AI-driven opportunities. Congress and the administration should prioritize investments in programs to support and prepare U.S. workers for the digital and AI-driven economy, including:

- Strong and readily available STEM education;
- Greater government investments in upskilling, reskilling, and training programs, and pathways;
- Increase equitable access to digital skills training across occupations and expand online skills; and
- Workforce training programs for underserved and underrepresented communities.

The continued growth of the gig and sharing (or "on demand") economy has created income opportunities in virtually every corner of the country, allowing people to work independently and on preferred discretionary schedules, expand their businesses, and provide for themselves and their families with greater flexibility. At the same time, remote and hybrid work have brought economic, social, and environmental benefits and will remain a pillar of work across all industries moving forward.

Policymakers should ensure that efforts to oversee or regulate new technologies further innovation and individual empowerment instead of stifling it. To that end, TechNet supports the following principles:

Gig and Sharing Economy

- The modern workforce requires a flexible environment that allows workers to find opportunities that best match their skills, interests, and availability on their own terms. TechNet opposes efforts to eliminate or restrict this essential flexibility, including restrictions

on the use of independent contractor and consultant classifications, inflexible overtime rules, and indiscriminate expansion of collective bargaining rules.
- Tax and labor policies should promote economic opportunities, provide clarity, and avoid significant administrative burdens for business creators or independent contractors.
- Federal policies should promote innovative efforts to establish portable benefits programs that provide benefits for workers who have traditionally lacked those opportunities. These efforts should enable companies to provide benefits to independent workers while protecting those workers' independence.

Maximizing the Benefits of Remote and Hybrid Work

- TechNet supports government policies that broaden the inclusive economic opportunities afforded by remote and hybrid work, including for caretakers, the disabled, and those without access to major economic centers. To that end, we support the establishment of a predictable legal framework that reflects the permanent nature of fully remote and hybrid work across industries.
- As part of such a framework, tax and labor policies should promote the adoption of flexible work opportunities and recognize the unique designs of these innovative business models.
- TechNet appreciates that minimum hourly rates and minimum required salaries (for determining exempt status under the FLSA and related state laws) will increase over time, and supports predictable, gradual increases.
- Similarly, we support public investment in broadband infrastructure in unserved and underserved locations and efforts to incentivize the development of co-working spaces, which would provide for broader fully remote and hybrid work opportunities in both rural and urban environments. TechNet's priorities on broadband policy can be found here.

NON-DISCRIMINATION

The technology industry is committed to promoting an inclusive workforce and nation that reflects the diversity of our customers and people. Policymakers should pursue education, workforce development, and immigration policies that will empower the best and brightest people to continue making important contributions to our nation and communities. TechNet opposes all forms of discrimination on the basis of nationality, ethnicity, race, religion, age, disability, sexual orientation, age, gender, or gender identity. The private and public sectors should help close opportunity gaps through increased access to education, employment, health, finance, and housing.

EXPANDING HIGH SPEED INTERNET CONNECTIVITY AND PROMOTING A HEALTHY INTERNET ECOSYSTEM

The internet is a vital tool for people's access to information and empowerment. Broadband includes several high-speed transmission technologies that can deliver broadband service, including hybrid fiber coax, fiber optic, fixed wireless, low earth orbit satellite, and mobile wireless, and is used below to refer to all of them in a technology-neutral manner. Policymakers should also support investment in broadband build-out to unserved areas and continued private investment in broadband networks and cloud services.

TechNet supports:

- Policies that facilitate continued private investment in broadband services and streamlined network infrastructure deployment, including at the local level.

- Policies that promote public/private partnerships in deploying broadband connectivity to unserved and underserved areas, as defined by the *Infrastructure Investment and Jobs Act*.
- Robust funding and swift implementation of policies that expand connectivity and internet access in unserved and underserved areas, as defined by the *Infrastructure Investment and Jobs Act* in a technology-neutral manner, including unserved and underserved anchor institutions, to facilitate online learning and the delivery of telehealth services.
- Policies that encourage and support the continuation of successful affordability programs for low-income subscribers that help ensure the seamless delivery of benefits and greater economic opportunity for those recipients, including the ability for all broadband service providers to be part of the solution, without unnecessary regulatory burdens or rate setting.
- Continued refinement of, and reliance on, the FCC's Broadband Data Collection map.
- Policies that foster a light-touch regulatory environment and that encourage a competitive marketplace that spurs innovation and private-sector investment to ensure the United States remains a leader in high-speed connectivity.
- Policies to increase the availability of licensed, unlicensed, and shared spectrum, and mid-band spectrum in particular, for a variety of connectivity technologies.
- Policies that promote the use of secure and trusted network equipment vendors, both domestically and globally, while recognizing the complexity of modern supply chains.
- Federal policy initiatives that can expedite broadband deployment, such as "Dig Once" or "One Federal Decision" and access to federal lands and buildings, and consistent interpretation of environmental and cultural resource rules across agencies.
- Technology-neutral policies that reduce burdens on communications service providers, including easing restrictions on rights of way, speed cell tower siting and permitting, and prohibiting excessive pole attachment charges by some municipalities and co-ops, so that broadband buildout can expand rapidly.
- Tax policies that impact deployment of broadband infrastructure at both the federal and state level which are competitively neutral among all providers of broadband infrastructure and the services they provide so as to not competitively disadvantage one provider over another.
- Policies that promote broadband adoption and digital literacy, including digital navigator programs.
- Policies to encourage the development and commercialization of next generation communications technologies, such as Open RAN, AI-Native networks, and 6G.
- Policies to promote the development and adoption of AI-enabled networking to improve resilience, bolster security, and optimize network management.
- Federal legislation that reflects the principles of net neutrality and a fair and open internet without heavy-handed regulation, and on a consistent, national basis, preferably passed by Congress.
- Safeguards against intermediary liability.
- Policies that provide a safe and secure user experience and promote free speech, while responsibly addressing the use of internet platforms to spread disinformation and malicious threats.

INTERMEDIARY LIABILITY AND SAFETY ONLINE

The internet ecosystem provides immense economic, social, and cultural benefits by enabling people everywhere to connect and share ideas. But the internet as we know it cannot exist without strong legal protections for the interactive computer services, including platforms, that make the internet an accessible, diverse, and functional place. Policymakers must recognize that intermediary liability protections, such as Section 230 of the Communications Decency Act of 1996, do not provide "total immunity" from wrongdoing by bad actors. Instead, intermediary liability protections merely enable organizations of all sizes, from the smallest startups to the world's largest companies, to provide interactive computer services for users to connect and share ideas. Innovators rely on intermediary liability protections to innovate and develop new and better methods of communication.

Intermediary liability protections are based on two bedrock principles: Free speech is an important and fundamental right, and wrongdoers should be held accountable for their own actions. Without strong intermediary liability protections, interactive computer services would have no choice but to censor controversial opinions on social media, turn off user reviews on product pages, require bloggers to get approval before publishing their articles, force users to have their emails read and fact-checked by corporations before sending, and eliminate search engines that connect people with useful content and websites. One thing is certain: Making interactive computer services liable for the content generated by users online will force those providers to protect themselves by taking control of content on the internet, which is bad for users and stifles innovation.

As policymakers consider reforms to the way that the internet functions, they should reflect on the following principles:

Intermediary Liability Generally

- The First Amendment cannot exist in the 21st century without protections for the intermediaries that provide opportunities for user-generated speech.
- Policymakers should support an internet ecosystem that holds bad actors who misuse digital services responsible for their own actions.
- Intermediary liability protections make the internet a better, safer, and more useful place. Liability protections for interactive computer services allow market forces to incentivize new and innovative ways of connecting users while limiting the impact of harmful content. Liability protections allow interactive computer services to set their own rules for moderating content that best fit their own platform and users.
- Policymakers should not disadvantage interactive computer services compared with their offline counterparts.
- Algorithms are not publishing decisions and do not endorse content or speech. Rather, algorithms are automated ways of organizing data and trying to make systems more useful by connecting users with the content they need, whether that content is a product on an online marketplace, an instructional cooking video, or a better route home in heavy traffic. Additionally, internet service providers carry third-party content over their networks that they can neither see nor control.
- Policymakers should support efforts to require platforms to have reasonable processes and systems in place, based on industry best practices, to manage the prevalence and risk of illegal content.
- Non-Consensual Intimate Image (NCII) abuse causes serious harm to victims' safety, privacy, and wellbeing. TechNet supports strong, effective measures to combat NCII, and our member companies have implemented tools and policies to do so. We support implementation of the *TAKE IT DOWN Act* in ways that preserve the ability of companies of all sizes to implement the statute with the maximal flexibility needed in line with the mandates in the law.

Child Safety Online

- Intermediary liability protections empower users to select the interactive computer services that best fit their circumstances and empower platforms to develop standards for age-appropriate user experiences.
- Intermediary liability protections were created to protect interactive computer services that choose to remove problematic or harmful content, and have resulted in proactive, voluntary innovations that make the internet safer for people of all ages. Thanks to intermediary liability protections, social media platforms, email providers, and search engines are now the largest removers and reporters of suspected child sexual abuse material online.
- Policymakers should empower platforms to remove and disable harmful content, such as child sexual abuse material or non-consensual intimate imagery. Policymakers should avoid top-down, government micromanagement of interactive computer services that stifles innovation and instead promote industry collaboration to enable the development of better methods of protecting users.
- Policymakers should support robust funding and other resourcing to reduce friction for law enforcement to investigate and prosecute predators and abusers who victimize children online. Policymakers should also support public-private partnerships and community-based efforts to prevent child victimization.

ENERGY INFRASTRUCTURE

Large-scale energy demand growth is occurring at a pace and scale that presents significant challenges to the current U.S. energy grid in ways that could undermine American innovation and technological advancement. Solving the energy crisis will require enacting the right policies by lawmakers combined with innovation from the private sector. TechNet's members remain committed to collaborating with the U.S. government to build secure and resilient energy infrastructure that supports the digital ecosystem, empowers communities, drives job creation, and solidifies America's competitive advantage in the global economy.

TechNet supports sound energy policies that address this crisis based on global geopolitical engagement, cooperation, and accountability. TechNet further supports advanced energy policies that foster and promote a business climate that enables innovation while mitigating the impact of new regulations on the economic prosperity of our nation and the world. TechNet member companies are committed to addressing the energy crisis and leading by example through innovation and sustainability efforts while driving the public policy discussion toward more reliable and efficient energy infrastructure to power the future.

A whole-of-government approach should be developed to map, optimize, and manage the approval process for large-scale energy infrastructure paired with dedicated energy generation. The private sector has the financial resources to build the required data and energy infrastructure, but governments at all levels must prioritize, coordinate, and streamline the pathway to bringing online the required data and energy infrastructure. Currently, the complex regulatory and approval stack across local, state, and federal governments is a significant barrier to building the necessary infrastructure at the appropriate pace and scale.

TechNet supports technology-neutral, market-based policies that address the energy crisis and that: accelerate the deployment of emerging energy technologies; promote innovation; bring competition to the renewable energy market; and base policy development off of science-based guidelines and benchmarks.

TechNet calls for the following actions:

- Congress should pass comprehensive permitting reform legislation to resolve the inefficiencies of the U.S. permitting process.
- A federal electricity policy that will drive investments in new renewable energy generation, and investments to improve grid reliability, modernization, and resilience. Such investments will support providing businesses with the energy capacity to make needed investments at the scale and speed necessary.
- State and federal governments should prioritize removal of regulatory and process barriers to energy deployment, including by implementing generation and transmission permitting reform.
- The federal government should prioritize preservation of technology-neutral energy tax credits to ensure appropriate long-term incentive structures enable accelerated deployment of new energy resources.
- The federal government should support the export of American energy technologies through a coordinated approach across government, including increased financing, loans to allies, and tax incentives.
- The federal government should prioritize modernizing federally-owned data center infrastructure and build new data centers with next-generation hardware and software to consolidate activities in older, inefficient data centers that would lower costs, cut energy consumption, and promote sustainability.

- We support research that would help industry increase data center energy efficiency and sustainability operations.
- We support efforts by the administration to increase the domestic supply of rare earth minerals through a whole-of-government approach.
- Policymakers should focus on ensuring that all communities are able to also benefit from energy grid modernization and optimization efforts for low-cost, reliable energy.
- Specific policies should promote the adoption of hydrogen and other sources of clean energy for hard-to-decarbonize sectors like heavy-duty transport, steelmaking, and other chemical and industrial processes.
- On the roads, there should be renewed investments made in climate infrastructure and clean transportation, including the national buildout of public charging infrastructure, and incentive programs to encourage their development. In the skies, policymakers should prioritize the establishment of regulatory frameworks that will allow for the adoption and scaling of clean transportation alternatives, such as adoption of a Beyond Visual Line of Sight rule to enable advanced drone operations that represent clean, all-electric alternatives to traditional modes of infrastructure inspection, last-mile delivery, and to support public safety.
- The federal government should continue to work with public utilities and the private sector to source sustainable, reliable energy for its buildings and operations.
- State and federal resources should be invested in energy science, technology research, and development efforts to build a pathway forward through innovation.
- The federal government should provide tax incentives to promote the adoption of new energy technologies.
- Support policies that enable deployment of advanced technologies on the grid at scale, such as new nuclear, hydrogen, geothermal, and utility-scale storage solutions.
- Policies that promote market competition by enabling the faster interconnection of distributed energy resources.
- Adoption by the federal government of advanced energy technologies and clean transportation that can improve the mission of federal agencies.
- Seek global harmonization and adoption of commonsense carbon accounting rules.
- Fair, public, and equal access to energy data to enable industry and empower consumers to deploy and utilize emerging energy solutions effectively and have insight into real-time grid conditions.
- Encourage public-private partnerships to provide skills and job training that support the digital transition.
- Ensure ICT/IT (including networks) is properly defined as a sustainable activity to support sustainable finance investments in this critical sector.
- Encourage government policies that incentivize water stewardship and encourage the use of AI and IoT for monitoring water systems and enhancing infrastructure resilience.
- Encourage policies and financial incentives for business models that extend the lifespan of products.
- Encourage policymakers to pass legislation that would bring the United States into compliance with the Basel Convention governing transboundary shipments of e-waste.
- Develop and align internationally-recognized standards for sustainable public procurement.

FUTURE OF TRANSPORTATION AND MOBILITY

Autonomous vehicles (AVs), connected vehicles, electric vehicles (EVs) and advanced aviation platforms are the defining mobility innovations of today and the future. These technologies will revolutionize how Americans travel and receive goods, and will make our roadways cleaner, safer, and more accessible. TechNet supports a regulatory climate that fosters this innovation in the United States. The automotive and aviation sectors are critical to our economic growth, and the importance of U.S. leadership in these technologies can’t be overstated. New rules are required to ensure advanced automotive and aviation platforms can be safely operated here at scale so that American innovators are not forced to look overseas for new opportunities.

Drones are being used across industries and the public sector in myriad use cases, including public safety, real estate, agriculture, disaster response, infrastructure inspection, medical and goods delivery, the entertainment industry, and humanitarian relief. Drones enhance safety and reduce environmental impact of delivery in numerous commercial use cases.

Across all modes of transport, TechNet supports the principle that federal laws and regulations should be performance-based and technology-neutral, applying equally to all companies and business models. Government regulators should take into account safety best practices that manufacturers and operators already have voluntarily adopted when establishing safety frameworks, in addition to the regulatory framework that already exists and encompasses AV activity. TechNet also supports proactive efforts and investments to educate the public, government stakeholders, and interested parties on AV and advanced aviation technologies and capabilities. Incentive structures should be put in place to boost domestic manufacturing capabilities while any import restrictions should be contemplated with a view toward minimizing supply chain disruptions that could harm American innovation and leadership.

Autonomous Vehicles

- Congress should pass surface transportation reauthorization legislation that includes a comprehensive federal framework for autonomous light duty and heavy-duty vehicles and for the deployment of digital infrastructure.
- TechNet supports the establishment of a uniform national regulatory framework that promotes the safe testing, deployment, and operation of AVs. The federal government can maintain U.S. leadership in the AV sector by issuing reasonable and practical federal motor vehicles safety standards (FMVSS) that ensure safety, expediting rulemakings, granting exemptions where applicable, and clarifying federal and state roles.
- TechNet opposes laws and regulations that require human control and intervention, implement unreasonable testing procedures and operating restrictions, or arbitrarily specify or prohibit the use of different AV technologies.
- TechNet supports action by Congress to clarify that manually operated controls and equipment intended only to support a human driver are not required for SAE level 4 and level 5 vehicles. TechNet further supports the National Highway Traffic Transportation Safety Administration (NHTSA) updating the FMVSS to allow for deployment of safe AVs without currently required manual driving controls and allowing for other novel vehicle designs. TechNet further supports congressional efforts to increase the existing cap on temporary exemptions to allow for innovative AV designs to be deployed. Under current law, NHTSA can exempt up to 2,500 vehicles per manufacturer per year from existing FMVSS.
- TechNet supports modernizing FMVSS to remove deployment obstacles for AVs and/or providing guidance in those instances in which the FMVSS may be interpreted broadly to accommodate new technologies. Current regulations were written for conventional human-operated vehicles, and new considerations need to be addressed for autonomous technology. Updates should reflect the innovative designs, diverse use-cases, and enhanced safety benefits that AVs can provide. TechNet supports congressional and NHTSA action to modernize FMVSS to encourage AV innovation and deployment.
- TechNet encourages AV developers to publish voluntary safety self-assessments outlined in the NHTSA framework "*Automated Driving Systems 2.0: A Vision for Safety*" (September 2017).
- TechNet urges the Federal Motor Carrier Safety Administration (FMCSA) to complete its ADS-equipped commercial motor vehicle rulemaking in a timely fashion. The final rule should not impose arbitrary operating requirements or restrictions on autonomous CMVs, such as the presence of a human driver for certain use cases.
- TechNet supports modernizing FMCSA regulations to permit commercial motor vehicles, including those operated by a Level 4 Automated Driving System, to utilize a set of cab-mounted warning beacons instead of placing traditional warning devices around the vehicle as is currently required.
- TechNet supports the establishment of a National AV Safety Data Repository by NHTSA. The repository must be subject to strict Confidential Business Information protections.

- TechNet supports the passage of the *AV Accessibility Act*, which ensures that people with disabilities are not required to obtain a driver's license in order to ride in a ride-hail AV.
- TechNet encourages federal investment into manufacturing of advanced AV components in the United States.

Connected Vehicles

- TechNet supports the Department of Commerce's final rule on Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles. It appropriately balances national security considerations and protection of the American public, while leveling the playing field with China's restrictions on U.S.-made technology.
- TechNet supports DOT initiatives for the integration and deployment of vehicle-to-everything (V2X) technologies, such as V2X using existing commercial wireless networks. V2X technologies have the potential to significantly improve roadway safety, and support for V2X technologies from the testing stage to the widespread deployment will be important for safety and mobility needs.
- The federal government should partner with states and private stakeholders to increase support for the Department of Transportation's V2X Deployment Plan, including the near-, mid-, and long-term goals directed at infrastructure owners and operators.
- The Department of Transportation should include V2X technologies in transportation funding beyond pilot projects and demonstrations.
- Public and private sector stakeholders, including federal, state, local, and tribal governments, as well as industry and research organizations, should collaborate and coordinate on connected vehicle policy, development, and deployment.
- TechNet urges caution and proportionality as regulators define the scope of what is classified as a connected vehicle and opposes mandates for specific V2X requirements. TechNet also recommends leveraging existing laws and standards that address potential cybersecurity risks.

Electric Vehicles

- TechNet recognizes that the electrification of transportation includes all-electric vehicles (EVs) including medium and heavy-duty, electric vehicle supply equipment (EVSE), charging stations, and related smart and networked software solutions. EVs include all technology types, including battery EVs, plug-in hybrid EVs, and hydrogen fuel cell EVs.
- TechNet encourages the federal government to continue partnering with the automotive and tech sectors to enhance their significant investments and commitments to make the transition to more fuel-efficient vehicles.
- We also encourage the federal government to work with state and local governments to coordinate efforts and reduce regulatory burdens in the nationwide deployment of EVs and EV charging infrastructure, especially during the implementation of the *Infrastructure Investment and Jobs Act.*
- TechNet supports sustainable tax policy that provides industry and consumers with long-term clarity to support the investment and deployment of clean energy and transportation technologies, including EV charging infrastructure. These programs should offer opportunities for funding for different types of EV technology and prioritize supporting private market solutions and transportation modes with the greatest potential impact to electrify both a high quantity of vehicles and high-mileage applications, including personal, fleet, ridesharing, ride-hailing, autonomous vehicles, transit, micromobility, peer-to-peer car sharing, and more.
- Policies regarding payment systems for EV use and EV charging should be technology neutral and allow for a variety of technologies that offer secure and global interoperable solutions to ensure EV drivers can pay using their existing cards or mobile devices. Global implementation of EMV technology, contactless (i.e. Tap to Pay), mobile payments and tokenization establishes a foundation to deploy easy-to-use, secure open payments technology for EVs.
- TechNet supports the ISO 15118 standard for Plug & Charge as a good foundation to facilitate EV charging Open Payment capabilities for in-vehicle payments.
- TechNet supports a robust energy agenda that will spur the development and deployment of clean energy resources, including widespread access to a Clean Fuel Standard (CFS), which would create a technology-neutral market-based program that requires the incremental

reduction in the carbon intensity of transportation fuels over time. TechNet's principles on climate change can be found here.

Drones

- TechNet supports the continued development and implementation of a regulatory framework to enable safe, scalable beyond visual line of sight (BVLOS) and more advanced drone operations. TechNet welcomes the FAA's BVLOS NPRM in August 2025 and encourages FAA to include its recommended changes to the proposal in its final rule.
- FAA regulations and processes must be developed or updated to reflect drones' novel designs and operational capabilities. To fully develop a regulatory framework for commercial drone operations, the FAA should not only enable BVLOS operations, but also develop drone-specific requirements for carrying dangerous goods and for environmental review processes. TechNet supports the deliberative processes that further develop policies for safe drone operations.
- TechNet supports the continued partnership between industry and law enforcement to encourage a better understanding of the capabilities of this technology and proper mitigation of errant drone usage. Caution must be used before employing any mitigation technologies, including robust testing and coordination among the FAA and other federal agencies, to ensure they are safe and do not result in unintended consequences or interference with other lawful aircraft operations in the National Airspace System. TechNet supports the creation of a detection and tracking pilot program that is limited and tailored in scope.
- To promote increased adoption of Remote ID by expanding the means of compliance without sacrificing safety, TechNet also supports allowing mobile internet-based network identification as an acceptable means of compliance with Remote ID rules.
- Any legislative and regulatory proposals should be technology- and sector-neutral, reflect the FAA's authority to regulate the airspace, and protect critical infrastructure and fixed site facilities. Targeted legislation will lead to inefficiencies and inconsistencies in how laws are applied and could slow technological solutions and growth.

SECURE AND SAFE REPAIR

Consumers, small and large businesses, public schools, hospitals, banks, and manufacturers all need reasonable assurance that those they trust to repair their connected products will do so safely, securely, and correctly. Proposals that require original equipment manufacturers (OEMs) to provide unaffiliated repair firms with access to proprietary schematics and repair, diagnostic, and security tools create major risks to consumer safety and privacy and the security of connected infrastructure.

TechNet supports the following principles:

- OEMs and authorized repair firms are uniquely qualified to ensure the secure and safe repair of electronic products. These firms use OEM-trained technicians and original parts that are backed by the OEMs and their partners with warranties, legally enforceable contracts, quality assurance requirements, and other mechanisms that provide strong protections for consumers.
- Requiring manufacturers to disclose diagnostic tools, source code, and software developed by the manufacturer at significant cost and to provide access to tightly controlled supply chains to unaffiliated, unvetted third parties would place proprietary corporate information and sensitive customer data in the hands of unknown actors, creating a new set of intellectual property rights concerns and cybersecurity vulnerabilities.
- Private rights of action and other tools to encourage litigation must be avoided.
- Legislation should avoid a patchwork of inconsistent policies that will stifle innovation and/or are technically or operationally infeasible.

MODERNIZING GOVERNMENT TECHNOLOGY AND FEDERAL PROCUREMENT POLICY

Much of the federal government's IT infrastructure is woefully outdated. Federal entities spend nearly 80 percent of their total IT budgets on maintaining aging, insecure, and expensive systems. Obsolete technology systems are inefficient and especially susceptible to cyberattacks and put citizens' personal information at risk.

TechNet supports reauthorization of the *Modernizing Government Technology Act* (MGT Act) to modernize outdated legacy systems operating on mainframe technology and allow for continued improvement of federal information systems. Congress should appropriate the full funding required for the Technology Modernization Fund, which facilitates the development of inter-agency or federal government-wide strategies to better manage cybersecurity risk and manage the hardware and software technical debt of federal agencies. Congress should require agencies to inventory the technology they use, identify a plan to either replace or mitigate the risk posed by equipment at the end of its lifecycle, and then prioritize use of the flexibility afforded by the MGT Act to eliminate products and services that are beyond their supported lifecycle. Congress should also equip federal agencies with the resources needed to implement the Cloud Smart strategy in addition to remaining committed to procuring commercial services, products, and best practices to realize government technology modernization more efficiently. Congress should focus efforts on further consolidating human resources (HR) shared services and systems across federal civilian agencies to improve service delivery, achieve economies of scale, and drive cost savings through the adoption of a modern HR system and the elimination of redundant legacy systems across HR organizations that use similar data and outputs.

TechNet supports improvements to the Federal Risk and Authorization Management Program (FedRAMP) to ensure the federal government can acquire advanced secure cloud solutions products efficiently. We support increasing funding for FedRAMP, ensuring its authorization pipelines authorize AI solutions, and driving harmonization between civilian and Department of Defense cloud authorization regimes. We support FedRAMP providing greater transparency for applicants to know the status of their review, increased investment in Program Management Office (PMO) staff and a machine-readable process, where appropriate, to ensure timely reviews and the removal of duplicative review processes between FedRAMP and authorizing agencies. FedRAMP should also provide greater clarity to Cloud Service Providers on how to best meet the requirements to avoid conflicting guidance between the PMO, agency sponsors, or a third-party assessment organization (3PAO).

Modernizing the federal procurement process is also critical to acquiring, testing, and implementing cutting-edge technologies. The federal government should be building upon programs like the MGT Act and FedRAMP by creating technology-focused acquisition trainings and incentivizing startups to compete in the federal marketplace. In addition, clarifying requirements and exempting non-threatening products, especially related to proposals to secure the federal supply chain, will streamline procurement and reduce unnecessary delays for federal contractors.

FINANCIAL TECHNOLOGY AND FINANCIAL SERVICES

TechNet supports private sector efforts to empower consumers and small businesses to better manage their financial lives and enjoy new, safe, secure, inclusive, and reliable financial tools. Congress and federal agencies should update outdated laws and rules in order to utilize modern financial technologies and meet consumer and business demand for innovative financial products. Overall, the federal regulatory environment must be more amenable to emerging fintech innovations. As the

fintech sector grows, regulated industries are making greater use of technology service providers, which has led to some agencies attempting to expand their regulatory oversight and creates the potential for onerous and redundant compliance burdens that stifle innovation by technology companies.

TechNet supports the following:

Globally Harmonized, Principles-Based, Risk Based, Standards-Based Approach to Third-Party Risk Management and Oversight of Technology Service Providers

When agencies pursue third-party risk management rules that would apply to technology service providers, the approach should be principles-based, risk-based, and based on global standards with the goal of global alignment.

- Where critical sector regulatory agencies pursue oversight of third-party service providers, the approach should be principles-based, risk-based, and mapped to the global standards, such as ISO and NIST.
- Efforts to extend third-party risk management expectations to technology service providers should endeavor to balance effective risk management with encouraging innovation.
- Any third-party risk management regime should be developed with the intent to globally harmonize rules and align compliance expectations.
- Prudential banking regulators should continue to modernize outdated regulations that restrict third parties' ability to connect consumers' deposits and financial institutions.
- Where possible, sector-specific agencies should integrate existing third-party validations and certifications into oversight, assessment, and audit of third parties. Where possible, this should include leveraging existing cost-effective, standardized approaches like the Federal Risk and Authorization Management Program (FedRAMP).

Consumer-Authorized Data Access

- Promote financial data use regulations that allow for innovation and consumer choice, including:
    - Promoting reasonable regulation of data brokers without overly restrictive rules on innovative uses of consumer financial data.
    - Ensuring data use regulation is tech-neutral and business-model agnostic.
- Support the implementation of an open finance regulatory regime through a Section 1033 rulemaking that:
    - Establishes a robust consumer data right that promotes the free flow of consumer-authorized data across the financial ecosystem allowing consumers broader access to financial services and control over their financial data.
    - Looks to industry-developed interoperability, portability, and security standards for ensuring a seamless, standardized, and secure experience for responsibly sharing consumer data.
    - Provides a flexible, consent-based framework for notifying consumers of how their information will be shared, transmitted, stored, and utilized; and
    - Clarifies ambiguities around liability for unauthorized access, privacy, credit reporting, and data accuracy that provides clear rules of the road for consumers and ecosystem participants.

Chartering Alternatives for Fintechs

- Promote regulatory and legislative efforts to encourage Fintechs to be able to expand their service offerings through risk-based regulatory regimes that embrace competition and innovation together with systemic and consumer protections.

Financing Reforms

- Streamline rules for the online lending marketplace.

- Policymakers should promote industry best practices that protect consumers and small businesses while maximizing diversity and innovation in lending services.

Financial Empowerment

- Unlock the power of financial apps. Policymakers should empower consumers and businesses to take advantage of financial applications that help them improve security, convenience, and reliability.
- Leverage technology to reduce barriers to financial services, particularly for the unbanked and under-banked. The internet, cloud computing, blockchain, and mobile innovations should be empowered to thrive in an open environment with reasonable regulatory burdens, which requires a reassessment of existing barriers to adoption along with incentives to pursue the use of innovations that promote access to financing for individuals and small businesses.
- Promote policies for usage of open, multi-cloud solutions that allow easy portability and movement of workloads across any cloud provider.

Payment Systems Principles

- Promote enhanced security and convenience through continuous innovation. No one technology should be mandated for security and authentication, nor should one technology become a de facto mandate through "floor-setting." New rules should not deter technological innovations in payment systems.
- Promote new entrants and empower consumers to utilize a broad array of financial technology products and solutions.
- Reduce fraud in the financial industry through the empowerment of innovators and innovation, stop regulatory and legislative efforts that would force tech transfers of payments technology, and advance strong customer authentication principles that allow multi-factor authentication to reduce online fraud.
- Legislative and regulatory policies impacting electronic payments should promote continued innovation and support free markets, not regulatory mandates or price controls that fail to set a level-playing field for the entire payment and FinTech ecosystem.
- Promote the development of faster and more efficient financial services, including stablecoins that provide secure, deposit-like protections for consumers, as well as automation to improve efficiencies, including using AI and machine learning, and automated data workloads and data sharing to facilitate faster analysis.
- Provide regulatory clarity for Earned Wage Access (EWA), a key area of innovation that offers consumers greater flexibility. The Consumer Financial Protection Bureau should engage with industry to ensure ongoing responsible development and availability of a range of EWA products that can serve different consumer needs and uses.

Blockchain and Fintech Modernization

- The U.S. government should adopt a coordinated approach to blockchain technology and position the United States as a global leader in blockchain innovation.
- The U.S. government should adopt policies that safely facilitate and encourage the adoption of emerging technologies, such as blockchain, and create beneficial partnerships between financial institutions and fintech companies that improve consumer access, choice, and opportunity.
- Policymakers should promote digital asset literacy, ensuring that consumers understand the risks and benefits of digital asset technologies, including blockchain.
- Policymakers should provide clarity and regulatory certainty for business platforms build around digital assets and blockchain technologies, promoting a predictable legal environment while also ensuring that businesses are able to comply with Anti-Money Laundering (AML), Countering the Finance of Terrorism (CFT), and Know Your Customer (KYC) regulations. Compliance burdens should balance law enforcement objectives and support more advanced fraud and financial crime detection, surveillance, and mitigation methods, while utilizing and exploiting the benefits of blockchain technology analytics.

- Policymakers and regulators should advance clear tax treatment, auditing, and accounting standards for digital assets to enable appropriate compliance with regulatory requirements and provide clear guardrails for innovators.
- Policymakers ensure that developing blockchain regulations remain technology neutral, allowing for innovation in both proof of work and proof of stake models.

Federal Financial Regulator Office of Innovation

- TechNet supports efforts that will enable each of the innovation offices of financial regulators to foster innovation among the entities they regulate. TechNet encourages these offices to promote regulatory clarity for digital assets and ensure that agency rules and guidance keep pace with marketplace innovation.
- TechNet supports the creation of regulatory sandboxes to encourage innovation and operate as an educational channel for agency staff to become acquainted with emerging technologies, operations, and industry subject matter experts.

DIGITAL IDENTITY

As people and businesses increasingly rely on online services for a broader array of transactions and interactions, there is an expanding range of situations where authenticity and verification are important. In certain, high-risk contexts, verifying digital identities can reduce fraud and enhance confidence in online experiences. At the same time, an expansion of data collection requirements for purposes of verification can create a variety of new safety and privacy harms, including by creating new risks for identity fraud due to data breaches exposing individuals' personal data.

- The United States should look for ways to collaborate and harmonize frameworks, standards, and requirements as they evolve globally.
- The United States should cease the practice of collecting Social Security numbers (SSN) as an authenticator, and instead permit the Social Security Administration (SSA) to offer individuals the ability to validate the name, SSN, and date of birth they are providing match agency records. While the SSA currently offers the ability to validate financial transactions through the electronic Consent Based SSN Verification (eCBSV) system, TechNet supports expanding this capability beyond the financial services sector.
- Federal agencies should look to the private sector as a resource and partner for developing innovative solutions to digital identity verification services those agencies provide. Federal agencies should explore additional attribute validation services they can provide. TechNet encourages relevant federal agencies to create similar programs to the SSA's eCBSV system to provide additional authoritative data sources the public sector can leverage for greater assurance.
- TechNet recognizes the variety and evolving nature of approaches to verifying an individual online and does not support efforts to block any approach.
- TechNet encourages exploration of, and further research on, a variety of non-ID based approaches to determine identity and authenticity online.

HEALTH CARE AND TELEHEALTH

TechNet supports health care and life science policies that enable accessible, high-quality care for patients, while harnessing the power of innovation to improve patient outcomes, enhance the clinician experience, and reduce costs. Congress should prioritize policies that provide Americans greater

control over their health needs, accelerate the development and delivery of life-saving innovations, and that make it easier to receive care, especially in rural areas and communities with a shortage of providers. To enable continued innovation in healthcare, TechNet encourages Congress to prioritize policies that facilitate the adoption of cloud and advanced tools such as AI by pharmaceutical and medical device companies, including enabling the use of this technology in research, manufacturing, regulatory compliance, and other portions of the value chain, as well as support interoperability of health data and enable decentralized clinical trials. Federal laws, regulations, and guidance documents should avoid any statement, express or implied, that telehealth and medical care received in digital settings are less sufficient than traditional in-person care.

- Modern technologies, including the facilitation and increased use of telehealth, cloud-based tools, and remote monitoring technologies, can help improve health care delivery and outcomes. Federal regulators should encourage the expansion of virtual care and ensure access to safe and secure telehealth and digital health technologies, especially in areas with limited access to healthcare providers, including in underserved and at-risk populations. State and federal health programs should address and reflect health disparities in state and federal health programs, and policy makers should support robust investment in telehealth infrastructure, including broadband, Wi-Fi, and technology modernization among providers that treat underserved communities to ensure universal access for the benefit of all communities.

- Nutrition is health care. Lawmakers should make permanent the U.S. Department of Agriculture's Online Purchasing Pilot to improve access to healthy food for participants in the Supplemental Nutrition Assistance Program (SNAP).