#CompTIADCFlyIn

CompTIA®

DC FLY-IN

February 5-6, 2019 | Washington, D.C.

Table of Contents

Welcome to the 2019 CompTIA DC Fly-In

Dear CompTIA DC Fly-In Participant:

Thank you for joining the 2019 CompTIA DC Fly-In! We are excited to welcome you to Washington, D.C. for several days of networking, policy education, and outreach to Capitol Hill. The 2019 Fly-In is an important opportunity to elevate our industry's voice to policymakers and we appreciate your time and commitment to this effort.

It goes without saying, but this is certainly an interesting time in Washington, D.C. Most notably the 2018 election has brought significant change to Congress, including a new majority in the House of Representatives and several new Members of Congress in both chambers, new committee leadership on key committees, and a new policy agenda. This change will bring some risk and some opportunity for the industry and the Fly-In will help to position our policy priorities early in the new Congress.

As you know, our industry continues to face some significant policy challenges as political views around data, privacy, trade, immigration, and corporate America have evolved. At the same time, there are champions throughout our federal government that are developing and advancing innovative solutions around cybersecurity, emerging technologies, workforce, and tax reform that will help advance many priorities within our industry.

We have an exciting agenda for your time in D.C., which will include an afternoon of panel discussions around relevant policy topics, an evening to honor our technology policy champions, a breakfast discussion with policymakers and senior staff, and an afternoon on Capitol Hill to meet with your elected Members of Congress and Senators. It's a full agenda, but one that will provide plenty of time for networking, discussion, and sharing your perspective with your elected officials.

In our Hill visits this year we will focus on advancing the discussion around the role technology should play in building our nation's infrastructure. Congress and the White House have prioritized infrastructure in 2019 and we want to make sure our industry is part of that discussion. Our outreach will also be a good opportunity to introduce the industry to the 116th Congress, which has close to 100 new policymakers.

Again, your willingness to engage in our policy agenda is an important way to ensure that our policymakers understand the role the technology industry plays in our economy, our communities, our ability to remain globally competitive, and our daily lives. Thank you for joining the 2019 DC Fly-In and we look forward to seeing you in Washington, D.C.

In the meantime, if you have any questions please feel free to contact me.

Sincerely,

Elizabeth Hyman
Executive Vice President
CompTIA Public Sector & Advocacy

The Current Landscape in Washington, D.C.

The House and Representatives and the Senate have recently started the 116th Congress, which welcomed 90 new Representatives and eight new Senators. They returned to Washington, D.C. after a contentious 2018 election, which brought a Democratic majority to the House after being in the minority for eight years, while also slightly expanding the Republican majority in the Senate. The election will dynamically change the landscape in the Nation's Capital over the course of the next two years and, as a result, the policy agenda is expected to change.

The new Democratic majority will prioritize (in part) an aggressive oversight and investigations agenda, which will focus on issues near the President and his Administration ranging from alleged misuse of federal funds to alleged collaboration with the Russians during the 2016 election (and many issues in between). This oversight will take place within the committees in the House and will be directed entirely by the new Democratic chairs and the Democratic leadership.

The House Democratic legislative agenda will focus on two distinct areas. The first (which is expected early in the Congress) is "messaging" legislation, which are bills that focus on priorities of the Democratic political base but have little likelihood of advancing beyond the House (i.e. healthcare reform, climate change policy, net neutrality, etc.). Additionally, House Democrats will focus on legislation that has the potential for bipartisan compromise and could advance through the Senate and to the President's desk (i.e. drug prices, infrastructure, etc.).

While the House Democrats will have complete control over legislation moving through the House, the Senate Republican majority will need bipartisanship to move almost any piece of legislation as Senate rules require 60 votes to advance a bill.

Without question the Democratic House, Republican Senate, and Republican White House will all have their own priorities and policy agendas, but there is hope that all three can come together on several legislative priorities in the coming year.

The looming 2020 presidential election adds an additional layer of complexity to Washington, D.C. with many Democratic presidential candidates expected to announce their candidacy early this year. Technology issues continue to face a mixed level of opportunity and risk within the federal policy debate. The President continues to support tariffs on products imported from China, many of which impact our industry, despite ongoing negotiations with the Chinese government. There has also been little progress around immigration reform, including proposals that would help solidify the technology workforce pipeline.

There has recently been an increased focus on data privacy, which will likely result in privacy legislation this year. While it is unclear what form that legislation will take, there is strong leadership among policymakers in both chambers who want to pass meaningful legislation in partnership with the technology industry. The key question will be whether there can be reconciliation between the House and Senate, particularly on the matter of federal preemption.

There are also several issues that are expected to continue to receive strong, bipartisan support and could make very strong progress in the near-term. Infrastructure legislation (including broad investment in technology infrastructure) is a key priority for both parties and the White House. This could be a good opportunity to increase investment in broadband and emerging technologies and will be the focus of our "ask" when talking to policymakers on Capitol Hill.

Additionally, apprenticeships and the technology workforce continue to be a priority for many policymakers. In the last Congress we saw the introduction and strong support for the CHANCE in Tech Act, which was the focus of last year's DC Fly-In, the Administration and Congress putting a focus on apprenticeships.

The 116th Congress will be a significantly partisan atmosphere, although there will be some opportunity for bipartisan compromise. This year, with the 2020 election still far away, will be the best opportunity for this Congress to be productive. As the election nears, messaging will replace policymaking and the election will dominate all the attention and effort in Washington, D.C.

IT Industry Outlook 2019

The Next Big Thing is dead. Long live the Next Big Thing. Few phrases better capture the anticipation, intrigue, and magic of tech innovation. The phrase has been an apt descriptor for such standouts as the market-ready product that quickly revolutionizes the tech landscape (think first smartphone release). Increasingly, though, that phenomena is less relevant in a world defined not by 'one big thing,' but rather, the iterative fusion of technology building blocks coupled with a generous helping of people and process. This may entail the stacking of foundational infrastructure and enabling components with emerging general-purpose technologies, such as AI, and then rounded out with data, an 'as-a-service' user experience, and business process optimization. The implications are both exciting – the ingredients of innovation have never been more accessible, and trying, as users and technology providers work to understand an ever-growing set of building blocks and how the pieces fit to drive digital transformation. Against this backdrop, CompTIA explores the forces shaping the information technology industry, its workforce, and its business models in the year ahead.

The global information technology industry is on pace to surpass $5 trillion in 2019, according to the research consultancy IDC. The enormity of the industry is a function of many of the trends discussed in this report. Economies, jobs, and personal lives are becoming more digital, more connected, and increasingly, more automated. Waves of innovation build over time powering the technology growth engine that appears to be on the cusp of another major leap forward.

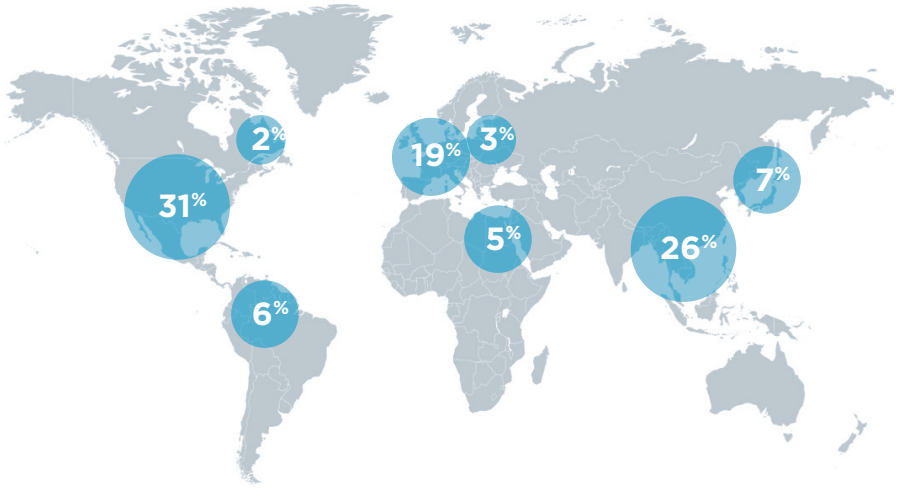
The United States is the largest tech market in the world, representing 31% of the total, or approximately $1.6 trillion for 2019. In the U.S., as well as in many other countries, the tech sector accounts for a significant portion of economic activity. CompTIA's *Cyberstates* report reveals the economic impact of the U.S. tech sector, measured as a percentage of gross domestic product, exceeding that of most other industries, including notable sectors such as retail, construction, and transportation.

Trends to Watch for 2019

Building on previous iterations of CompTIA's IT Industry Outlook, the trends to watch for 2019 revolve around technology, but that is really only one facet of the bigger picture. Complementary trends covering the business of technology, workforce dynamics, and macroeconomic conditions provide context and grounding.

The Global Information Technology Industry: $5.0 Trillion

Estimated 2019 spending at constant currency, according to IDC | Encompasses hardware, software, services, telecommunications and emtech



Cloud, Edge, and 5G Form the Modern Economic Infrastructure

There have been many labels for the most recent waves of technology that are redefining business and society, and one of these labels is the "Fourth Industrial Revolution." This suggests not only a drastic change in the way work is done, but a new foundational infrastructure that enables that work. Just as previous eras of industry were driven by the creation of railroads, telephone networks and power grids, the modern digital economy rests on a foundation built on these emerging components.

IoT and AI Open New Possibilities in Ambient Computing

For most people, the changes taking place in IT infrastructure will happen behind the scenes, but there will be changes in the front-end experience as well. With mobile devices and cellular networks, there has already been a shift in the perception of where computing takes place. It is no longer confined to an office or home, but is increasingly viewed as something that can be done from any location.

Distributed Technology Models Challenge Existing Structures

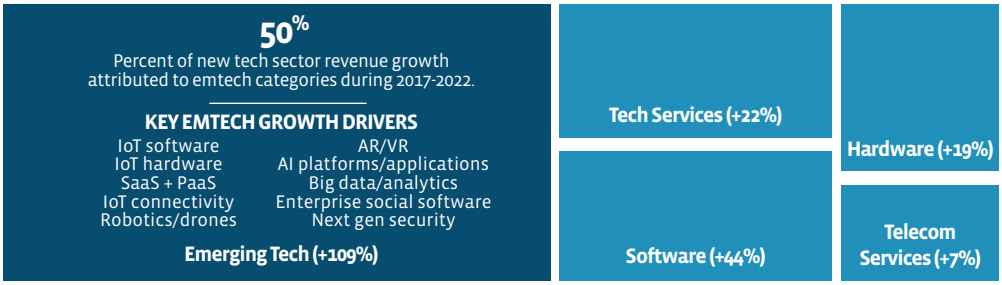
The past year has not been especially kind to blockchain and other distributed ledger technologies (DLT). Cryptocurrency values have fallen precipitously, and killer apps have not yet emerged. Other types of distributed technology, such as distributed databases or the Tor browser, leverage distributed networks to extend established architectural concepts. DLT takes things a step further, introducing an entirely new architectural approach made possible by distributed networks and cryptography.

Stackable Technologies Supercharge Digitization Efforts

The concept of "stacks" is a common convention in describing how Lego-like building blocks come together to form a whole. Software stacks, such as LAMP or MEAN, or, skillsets, such as full stack developer or CompTIA Security Infrastructure Expert (CISE), often come to mind. Taking this idea one step further yields what can be characterized as stackable technologies. As the name implies, stackable technologies allow organizations to piece together components to meet an end goal.

Emerging Tech Categories Drive Revenue Growth

Estimated contribution of new global tech spending during the 2017–2022 time period | Source: IDC



Business of Emerging Technology Prompts Sales Channels Reinvention

Blockchain, AI, VR, IoT, drones. Those are but a few of the newer technologies busting onto the scene, promising to shake up how businesses and consumers navigate their way through innumerable aspects of life and work. For the channel, how much is hype vs. reality? A little of both right now, truth be told, but in 2019 more reality and less hype will come to fore for all players in the business of emerging tech.

Partnerships Bridge Gaps in New Tech Ecosystem

Partner-to-partner (P2P) collaboration has always been a bit of holy grail in the channel. A way to fill skills gaps, a way to present a more comprehensive front to customers, a way to be bigger than you are. Looking ahead to today, there is renewed optimism about partnerships, due in large part to the expanding ecosystem of new channel players from the SaaS world eager to pair up with traditional infrastructure practitioners. These partnerships are not exclusive to SaaS and other software providers. Today, non-core technology entities such as law firms, accounting firms, digital marketers, consultants, and even consumer goods companies (think P&G, IKEA, Kohler…) are offering or influencing tech services as well.

Hyper-Personalization Takes Customer Experience to Next Level

Today's customers are more tech-savvy, more diverse, and more finicky than ever. From desiring seamless customer service to demanding myriad digital options for commerce, many buyers are no longer just looking for the right product, but also seeking a satisfying experience in attaining it. The catch word is "hyper-personalization." This model takes the time-honored concept of segmenting your customers into specific buckets (small, medium or large-sized, for example) to the extreme. It brings marketing and engagement down to the individual level.

Persistent Tech-Worker Shortages Fuel New, Creative Solutions

No surprise, the IT industry's tight labor market and tech skills gap challenges continue unabated. In fact, it's not just a problem for the technology industry, but one that is affecting most every industry in the economy. Just about any organization with job openings, especially for disciplines around emerging technologies, data analytics, application development and the like, finding and retaining workers has likely been tough-going. But while the tech-labor shortage remains a challenge, it also has sparked some creative thinking in recruiting talent, expanding the pipeline, and engaging with new generations of digitally-savvy workers.

Digital-Human Models Begin to Shape the Workplace of Tomorrow

While the dire warnings of "the robots are coming for our jobs" tend to draw the headlines, the reality of the situation is far more nuanced. Automating technologies has undoubtedly displaced segments of workers through substitution. This represents one end of the human-technology continuum; with the

other end being workers using tools where technology plays a passive role (think email or traditional spreadsheets). Between these two endpoints sits a hybrid model whereby humans leverage and act on technology; and intelligent technology proactively does the same to workers. The underlying assumption with this model is the recognition that humans and intelligent technologies will always have strengths and weaknesses, much like any team.

Technology Professionals Take the Lead in Anticipating Unintended Consequences
From the global economy to everyday activities, technology is changing the world. However, for those working in technology, this is not a chance to simply claim victory and reap rewards. Changes at the scale made possible by technology will inevitably cause ripple effects. Those effects have been coming to light over the past year, from security and privacy incidents to AI bias to technology that is not quite ready for prime time. While these big-picture issues have typically been the concern of a CIO, everyday technology professionals will now be expanding their expertise from hard-core technical skills to include cross-departmental collaboration and strategic business thinking. This broader skill set will allow tech pros to drive conversations around unintended consequences. In today's landscape, technology may sometimes be cast in a negative light, but the tech industry itself will learn from the past and set the course for a prosperous and conscientious future.

High Tech Increasingly Transforms Low Tech
More technology is finding its way into what could be characterized as "low tech" business activities or occupations. To clarify, low tech doesn't necessarily mean low skill or lacking in sophistication, but rather, up until recently, there hasn't been a need or justification for a heavy-tech presence. Sectors that fit this description may include restaurants, farming, delivery of goods, building management, and environmental management, just to name a few. More specifically, consider how sensors, data, AI, and robotics process automation (RPA) have the potential to impact the entire chain from the growing of food, to the preparation of food, to the delivery of food. This is occurring on the workforce front as well as occupations once far removed from technology are becoming increasingly digital dependent.

Global Tech Hubs Put Spotlight on the Ingredients for Innovation
The ingredients of innovation have never been more accessible. The data bear this out as tech hubs have sprouted up across the globe (think Toronto, Nairobi, Budapest, Singapore, Stockholm, Dubai, and Sao Paulo, to name just a few). While Silicon Valley and other U.S. cities remain dominant players, their share of the total "innovation pie" is shrinking due to accelerating growth in markets around the world. This means the next breakthrough in fintech, smart cities, AI, robotics, quantum computing, or 'to-be-determined' could occur in any number of global tech hubs. Countries looking to leapfrog ahead increasingly pursue efforts to enhance their appeal, which typically starts with building the most tech-savvy workforce possible.

Access the full IT Industry Trends Analysis report at:
CompTIA.org/resources/it-industry-trends-analysis

Prioritizing Smart Technologies Within an Infrastructure Package

America has a history of creating infrastructure milestones that have led to significant prosperity and national advantages. Dating back to the advent of the transcontinental railroad and moving forward through the Rural Electrification Act, the Interstate Highway System, to the deployment of the basis of the Internet from the Advanced Research Projects Agency (known as ARPANET), these milestones have created competitive advantages that continue to this day. Our future will no doubt rest on the next generation of infrastructure.

Both Congress and the White House have prioritized passing an "infrastructure package," which would help to modernize outdated infrastructure in a wide variety of sectors, including transportation, telecommunications, rural America, and energy. In all these sectors, innovative smart technologies can help to increase efficiencies and effectiveness within existing infrastructure and set the foundation for future innovation and advancement. We strongly believe that any infrastructure package should include funding for core smart technologies that will help to build, secure, and advance our communities.

Broadband Connectivity: According to the Federal Communications Commission (FCC), 24 million people in the U.S. lack access to terrestrial broadband internet, the majority of which are in rural areas. Providing funding for broadband projects within any infrastructure package, especially in rural communities, will help to close the digital divide and provide opportunities to enhance education, business, healthcare, agriculture, and open the window to innovation.

Smart Technologies to Enhance Public Utilities: Identifying problems with public utilities and providing new and safe communications channels between residents and utilities will reduce challenges. An infrastructure package should include funding for these important technologies to enhance the consumer experience, reduce costs, and increase effectiveness.

Cyber Solutions to Secure the Energy Grid: Cybersecurity threats to critical infrastructure, including the energy grid, continue to pose significant risks. Security upgrades can provide additional protections to the energy grid. An infrastructure package should include funding for these security upgrades, which will help identify and respond to threats, while further securing our critical energy infrastructure.

Smart Transportation Solutions to Maximize Efficiency and Safety of our Roads, Bridges, Railways and Airports: According to a recent report, congestion cost $305 billion last year. Some of the lost production caused by congestion could be recaptured if we deployed smart infrastructure technology such as intelligent transportation management software and roadway sensors that monitor freeway conditions and reroute public transit and networked traffic lights that communicate with each other and adapt to changing traffic patterns.

As we deploy smart infrastructure technology across the transportation, water, and energy ecosystems, we should not do so in a siloed fashion. We will truly experience the impact of smart infrastructure technology when the technology is cross pollinating across those silos. We need a comprehensive system where water, power, and transportation each affect the other components.

Request: We urge Congress to include specific funding for technologies that will complement and enhance any physical infrastructure investments.

Infrastructure

Frequently Asked Questions (FAQs)

Why is infrastructure important to advocate for now?

An infrastructure package is one priority that is shared by Republicans and Democrats in Congress as well as the President. The new Democratic majority in the House of Representatives is likely to advance an infrastructure package very early this year. The Democratic majority in the House has said they would like to pass an infrastructure package within the first six months. We want to make sure technology priorities are a part of this package and now is the best time to advocate for our infrastructure priorities.

What will be included in an "infrastructure package" passed by Congress?

Traditionally, Congress has viewed infrastructure mostly as building roads and bridges and other transportation priorities. Over the last few years, Congress has expanded their view of infrastructure to include many other sectors, including smart cities, critical infrastructure, energy, broadband, etc. This more expansive view is welcome, but limited funding will limit the scope of an infrastructure package. The technology industry wants to keep the focus on innovative solutions that will make our infrastructure more resilient and will set the foundation for future growth and innovation. Congress' goal with an infrastructure package must be not only to strengthen our nation's infrastructure, but also create new jobs and grow the economy.

What are the hurdles to passing an infrastructure package?

Ultimately, funding will be the largest hurdle for Congress passing infrastructure legislation. Republicans, Democrats, and the White House all have different funding priorities and priorities for how to "pay for" the legislation. The level of funding and where those funds will come from are often at the center of the infrastructure debate.

Democrats have been advocating for a plan that calls for $500 billion in funding by issuing 30-year bonds as well as an increase to the federal gas tax (which would be dedicated to transportation infrastructure). It is likely that Democrats will likely push for a similar plan this year, although the level of funds could be higher.

The White House has been advocating for incentives to states and public-private partnerships. In total, they would spend $200 billion to spur additional growth through these non-federal mechanisms. Given the adjustment in the Congressional landscape, the White House is likely to shift somewhat around their reliance on public-private partnerships, which have not been a priority for Democrats.

There are several other proposals that would provide innovative financing, including developing an infrastructure bank. At this point, those proposals haven't moved very far.

We continue to expect that funding will be the core issue debated between Republicans and Democrats and will ultimately guide the debate on what policy priorities (and at what funding levels) will advance.

What does the technology industry want included in the infrastructure package?

When meeting with policymakers on Capitol Hill, we will be asking that Congress prioritize smart technology solutions, including federal funding for broadband connectivity (especially in rural communities), smart technologies to enhance public utilities, cyber solutions to protect the energy grid, and smart transportation solutions that increase efficiency on our nation's roads, bridges, highways, and airports.

What are some examples of technology solutions within these broader category areas we are advocating for?

On Capitol Hill, we will be advocating for funding for technology to be included within four key areas (broadband, transportation, energy grid, public utilities). We won't prescribe the specific technological solution, but rather advocate for funding broadly. However, below are some top-line examples of where this funding could go:

- Broadband: Grants to states that will build broadband infrastructure in rural communities that could provide more broadband access to those that don't currently have enough internet connectivity
- Transportation: Grants for states and localities to embed sensors into roads for autonomous vehicles
- Energy Grid: Funding for grid and microgrid technology to help modernize the electricity grid as well as cyber security technologies to help secure the grid
- Public Utilities: Incentives for states to provide communities grants that would help fund technology that would improve the efficiency of water and sewer services

Have infrastructure packages been introduced yet?

No, there have not yet been infrastructure packages introduced. However, Democrats and the President released their own documents outlining an infrastructure package last year, although we expect the content to change when the infrastructure debate begins this year.

2019 Policy Priorities

Advance Tax & Regulatory Policies that Spur Innovation and Grow Our Economy

The U.S. technology industry is a $1.5 trillion market and employs nearly 11.5 million Americans. Fiscal discipline and targeted funding for investments in innovation are essential to continue economic growth. We support reasonable tax policies that promote innovation, entrepreneurship, and capital investment.

- *Create a permanent and competitive tax code that protects small businesses, including pass-through entities:*
  - Make permanent the lowered tax deduction for pass-through entities that is currently set to expire in 2025
  - Implement a policy allowing firms to deduct the lesser of their start-up expenses or $20,000
  - Improve access to capital and provide expanded support mechanisms for high-growth businesses
- *Ensure simplicity and fairness in interstate taxation*
  - Interstate sales tax legislation should not result in additional compliance burden to businesses, and any legislation should include a small business exemption;
  - Reduce compliance burdens on today's digital workforce by enacting the "Mobile Workforce State Income Tax Simplification Act;"
  - Support certainty in sales tax applications by enacting the "Digital Goods and Services Tax Fairness Act"; and
  - Support fairness in interstate business activities by enacting the "Business Activity Tax Simplification Act."

Lead in Secure Internet Based Platform Technologies

Economic expansion in IT rests on the creation of new and innovative business models that leverage trusted, secure and accessible Internet based platforms. We support common sense data and cybersecurity policies that secure our networks and promote responsible use of consumer data so the technology experience can continue to expand and improve.

- *Enhance national cybersecurity and critical infrastructure protection through support for an environment that fosters real time threat sharing between the government and the private sector and addresses the bad actors.*
  - Support an incentive-based voluntary approach to cybersecurity (articulated in Executive Order 13636 and its directive to the National Institute of Standards and Technologies (NIST) to develop a framework) that utilizes industry best practices and promotes voluntary adoption; and

  - o Establish greater penalties for cybercriminals to deter and combat bad actors, and punish criminals

- *Support a national standard for data breach notification that pre-empts the patchwork of state laws to allow entities to focus on notification and resolving the breach instead of compliance with a myriad of conflicting laws;*
- *Develop sensible definitions around nascent technologies such as biometrics and geolocation to ensure neutrality while still allowing for technological advancements;*
- *Support continued innovation in encryption technologies and working with Congress and law enforcement to establish frameworks for securing data while exploring collaborative approaches to helping law enforcement keep Americans safe; and*
- *Support surveillance reforms to continue to rebuild trust across the Atlantic and promote even enforcement of the GDPR and continued renewal of the EU-U.S. Privacy Shield; and*
- *Support federal privacy and data security legislation that preempts state laws and provides the U.S. with a viable alternative to the GDPR model of privacy and security regulation on a global scale.*

Support New and Emerging Technology Platforms through Thoughtful Policies

Advancements in cloud computing, mobility, machine to machine (M2M), and unified communications platforms, the growing commercial significance of unmanned aerial vehicles, and other applications such as mobile payments are rapidly creating new opportunities for economic advancement while also raising a host of new public policy considerations.

- *Work to establish the investment, regulatory and legal environment that will allow broader adoption of the Internet of Things (IoT):*
  - o Work with the stakeholder community to continue to develop and strengthen the DHS and NIST IOT Security Frameworks;
  - o Work within the NTIA IOT Security Updatability working groups, seek a common set of IOT related standards; and
  - o Monitor and address any IOT security related legislation.
- *Work with the CompTIA stakeholder community to help define and advocate for the role of smart technology in the 21st century infrastructure ecosystem;*
- *Work with the smart stakeholder community to continue to seek advancements that will lead to more widespread adoption of smart technology products and services;*
- *Help accelerate the federal government's goal of improving digital service delivery and customer experience through mindful legislation*

- *Seek policy advancements and best practices around cloud, mobility, big data, open data, data analytics, blockchain and unmanned aerial systems (UAS).*
- *While remaining mindful of legitimate privacy and safety implications, resist over-regulation of unmanned aerial vehicles that would unnecessarily curtail legitimate commercial uses;*
- *Monitor the ongoing discussions on artificial intelligence and automation as they pertain to both the 21st century technology workforce and the Internet of Things.*
- *Work with the stakeholder community to help adoption of CompTIA Blockchain Guide policy recommendations.*
- *Continued advocacy efforts for smart cities legislation; and*
- *Work to establish a nurturing regulatory and legislative environment that will allow the broader adoption of autonomous vehicles and other vehicle technology. In particular, strongly advocate for the SELF DRIVE Act, AV 3.0 and AV Start Act.*

Support Skills for the 21st Century Workforce

CompTIA uniquely sits at the intersection of innovation, education and economic growth. We support policies that expand life-long education in the computer sciences and basic IT skills, and promote a skilled workforce that spurs job growth and our ability to compete globally.

- *Support the workforce by enacting the "Championing Apprenticeships for New Careers and Employees in Technology Act;"*
- *Advocate for policies that emphasize early academic support for science, technology, engineering, and math (STEM) instruction and carry these efforts through higher education institutions, to prepare students and workers for lifelong learning opportunities;*
- *Support the reasonable use and responsible stewardship of student data by schools, districts, and service providers, such as analyzing student data to deliver personalized learning experiences and improve products for use;*
- *Support and develop initiatives that encourage minorities, veterans and under-represented communities to pursue IT career paths;*
- *Recognize that the ability to recruit and retain the strongest workforce means supporting an inclusive workplace – one that welcomes people of all faiths, race, ethnicity, sexual orientation and gender identity;*

- *Ensure the government workforce has necessary IT security skills:*
  - Support the National Initiative for Cybersecurity Education (NICE); and
  - Seek adequate awareness support and funding for government IT workforce recruitment, training, certification and retention.
- *Support high-skilled immigration reform:*
  - Increase green cards for high-skilled STEM graduates;
  - Create new visas for U.S. educated students and entrepreneurs to lessen the demand on the H-1B category;
  - Adopt market-based visa caps; and
  - Grow domestic sources of talent through support of STEM at all levels of education.

Address Availability and Delivery of Broadband Communications

The internet is the infrastructure of the global economy. To ensure innovation, economic growth and social interaction, it is imperative that we keep the Internet open, encourage deployment of new, faster broadband networks and find ways to get more Americans online.

- *Support an open internet through rules prohibiting blocking, throttling, commercially unreasonable paid prioritization, and other anticompetitive behavior by ISPs.*
- *Support policies that improve broadband competition and the growth of IoT by removing barriers to the deployment of broadband infrastructure, including wireless infrastructure such as small cells.*
- *Promote policies to get more Americans online and to increase broadband adoption.*
- *Advocate for policies to make more spectrum available for licensed, lightly licensed, and unlicensed use to support 5G, IoT, and rural broadband on an exclusive or shared basis, including for implementing incentives to encourage government spectrum users to share, sell or lease their spectrum.*

Data Breach Notification

The Issue:

There is currently no national standard for how a company must notify its customers in the wake of a data breach. Instead, companies must navigate a complex web of 50 different, often conflicting, regularly-changing state data breach notification laws in the aftermath of a breach. With the increasingly mobile and decentralized nature of our economy, data storage and dissemination technologies, it can be nearly impossible for companies to determine which state laws apply when a breach occurs. The current regulatory landscape not only places an immense financial compliance burden on businesses, but also delays the process of getting information into the hands of those who need it most: the customers whose data was compromised.

What CompTIA Supports:

A national standard for data breach notification would provide consumers and businesses with consistency and predictability on how consumer notice must be provided. Until Congress passes a national standard, CompTIA and its membership continue to advocate for the following in breach notice bills.

- **"Harm" Trigger for Acquired Data** – The notification requirement should be triggered when there is a real risk of actual harm, not a theoretical concept that could lead to over-notification about data breaches that really aren't harmful.
- **No Private Right of Action** – Individuals should not be able to sue companies who have suffered a data breach for actions covered by federal data security and data breach notification laws. The businesses who have suffered breaches are victims of criminal activity.
- **Narrow Definition of "Personal Information"** – To avoid over notification of consumers and unnecessary costs, the definition of "personal information" in the legislation should not include information accessible through public records. For example, merely the combination of a name, address and birthday should not qualify as personal information.
- **Preemption of State Laws** – Any federal data security and data breach notification law should preempt state laws and requirements. Without strong preemption language, the compliance burden for small businesses will not be alleviated and the effectiveness of any law would be significantly undermined.
- **Exemption for Use of Technology that Renders Data Unusable or Unreadable** – Federal legislation should include an exemption from notification requirements for companies who utilize technologies to render data unusable or unreadable. This exemption should be technology-neutral.

- **Limits on Financial Penalties** – Massive financial penalties are unwarranted, and could force small businesses out of existence. Penalties should be reasonable, and should take into account the size of the company that suffered the breach and the type of data that was accessed.
- **No Fixed Data Security Requirements** – Data security requirements should not be specifically enumerated within the legislation. Benchmark security standards of today may become outdated over time, requiring companies to possibly maintain outdated systems because of government mandate.
- **No Overly Burdensome Notification Requirements** – Data breach notification legislation should avoid overly prescriptive notification requirements. In the event of a breach, companies should dedicate their resources to efforts that most directly notify and protect consumers. Additional requirements, such as those mandating the creation of call centers or the provision of credit reports, would divert resources away from small businesses seeking to protect and inform their customers.
- **Reasonable Notification Timeframe** – Legislation should require a reasonable timeframe for notification, which includes allowances for risk assessment without requiring a specific time limit that must apply to every case.
- **Take Other Laws into Account** – Companies that are subject to other data security and/or breach notification laws, such as HIPAA, Gramm-Leach-Bliley or the Fair Credit Reporting Act, should be exempt from these requirements.

Work to Reform the Electronic Communications Privacy Act (ECPA)

The Issue:

The Electronic Communications Privacy Act (ECPA) was originally passed in 1986, when email and text messaging were still nascent technologies, and deemed all stored electronic communications over 180 days old to be "abandoned." Under ECPA, law enforcement and government agencies can acquire these abandoned emails and text messages from a service provider without a warrant, simply needing a subpoena to obtain access. The House unanimously passed the Email Privacy Act, an ECPA reform bill, in both April 2016 and February, 2017, but the bill has repeatedly stalled in the Senate Judiciary Committee and hasn't received a floor vote.

What CompTIA Supports:

ECPA must be reformed to require government agencies and law enforcement to obtain a warrant to compel service providers to disclose the contents of emails, text messages, and other private communications stored by a service provider.

Specifically, CompTIA supports:

- **Congress Should Pass the Email Privacy Act as Passed by the House in 2016 and 2017** – The Email Privacy Act (H.R. 387), which unanimously passed the House in February, 2017, was the product of a carefully negotiated compromise between industry, public interest groups and House Judiciary Committee staff. Despite overwhelming support for the bill, several members of the Senate Judiciary Committee have continued to hold up the bill with unrelated amendments opposed by both industry and the public interest community. Congress should pass this bill in 2019.
- **No Civil Agency Exceptions** – Some civil agencies, such as the SEC, have asked for an exception to the warrant requirement because they do not have the ability to issue warrants. Such an exception would destroy the benefits gained by ECPA reform. It would erode privacy by codifying new powers for civil agencies that they do not already have. Civil agencies can still get access to emails and texts by serving subpoenas on users, not service providers.
- **No Emergency Exception** – Under current practice, the government may request digital content from providers by declaring an emergency situation. Providers may then decide whether or not to comply based on the circumstances. However, there has been a push to require providers to comply any time the government declares an emergency. This has dangerous potential for abuse. Service providers don't want to be responsible for derailing criminal investigations, but requiring compliance with "emergencies" means that the government simply needs to declare an emergency to get the information it wants.

Free Up Spectrum for Innovation, Rural Broadband, 5G and IoT

The Issue:

Wireless broadband use has skyrocketed, and demand for wireless data is expected to continue to grow exponentially in the coming years. Wireless speeds are increasing too, and in some rural areas, wireless broadband may be a better long-term solution to broadband access than wireline. However, there simply is not enough available spectrum to meet this coming demand, even as unlicensed spectrum begins to carry more and more of the wireless traffic. The growth of the Internet of Things (IoT) market is creating even more demand for data, and the number of IoT devices in use will continue to increase. 5G networks will also require the use of a variety of different spectrum bands, combining low-, mid-, and high-band spectrum.

Auctioning more spectrum licenses alone cannot meet the ever-growing demand for data. Unlicensed spectrum is an essential complement to licensed spectrum. As Congress, the FCC and NTIA work to make new spectrum bands available for wireless use, some bands simply cannot be cleared and auctioned, and instead are only usable if shared with incumbent users in an unlicensed capacity. Unlicensed spectrum can be used for Wi-Fi, Bluetooth, offloading wireless traffic, and providing broadband in rural areas. It also allows companies who cannot afford to purchase spectrum licenses to use spectrum in new and innovative ways.

What CompTIA Supports:

Congress, the FCC, NTIA and other government agencies must do everything within their power to make more spectrum available for licensed, unlicensed, and lightly licensed use.

Specifically, CompTIA supports:

- **More Federal Spectrum Available for Both Licensed & Unlicensed Use Without Technology-Specific Restrictions on its Use** – The Federal Government is the largest holder of spectrum suitable for wireless use, and even they will admit that they are not using their spectrum efficiently. Clearing and auctioning spectrum (as we saw in the AWS auction) is one effective way to get spectrum to market, but it is too costly in many situations. We must come up with new, creative ways to get government spectrum in the hands of those who need it most, be it for licensed or unlicensed use, without placing technology-specific restrictions on how it may be used.
- **Moving Forward on 5 GHz** – The FCC has already made great strides on freeing up unlicensed spectrum in the 5 GHz band, but the Commission should continue to work towards making spectrum available for unlicensed use in the U-NII-4 band.
- **Continuing to Pave the Way for 5G** – The FCC took a major step towards making 5G a reality with their Spectrum Frontiers Order, which opened up nearly 11 GHz of licensed and unlicensed spectrum for flexible-use wireless broadband, but there is still work to be done. The Commission also has several ongoing proceedings focused on making mid-band spectrum available for both licensed and unlicensed use, and we hope they continue to progress on the 3.7-4.2 GHz band and the 6 GHz band.

Blockchain

The Issue:

Blockchain technology is perhaps the most talked about and yet the most misunderstood emerging technology in the world today. Since its inception, the secure, distributed ledger technology has widely been viewed through the lens of virtual currencies, particularly the hype surrounding the buying and trading of Bitcoin and other digital coin offerings. Indeed, surveys have shown that consumers are largely aware of what Bitcoin is, but do not know or understand about the blockchain technology that powers it.

What CompTIA Supports:

CompTIA suggests policymakers consider developing policies for blockchain environments that encourage developers and market participants to continue innovating and providing solutions that will aid the public sector in achieving its mission and goals. In order to do so, policymakers should understand the promise, the uses and the questions that blockchain currently presents.

Specifically, CompTIA supports:

The Creation of a Federal Blockchain Stakeholders Advisory Group – The group, which would consist of private industry, academia, non-profits, and trade associations, would be responsible for examining the following aspects of the blockchain technology ecosystem:

- Current and future security requirements
- Regulatory environment
- Standards and interoperability
- Defined marketplace and potential for disruption
- The current use of blockchain technology by federal agencies

Regulatory Sandboxes – To help manage risk, drive economic development and develop a strong regulatory regime, CompTIA recommends that the federal government and state governments consider creating a blockchain and emerging technology "regulatory sandbox."

Pilot Toolkit – One of the more effective tools to help incorporate blockchain technology is the pilot toolkit. CompTIA champions the use of pilot toolkits and recommends that an organization focus on the following four elements when considering the creation of a toolkit:

- The reason why your organization would need blockchain
- The workings of the blockchain protocol and technological framework options
- Your organization's information technology environment
- How to develop sophisticated applications

Global Digital Trade

The Issue:

As U.S. business operates in a global digital environment, information, goods, and services cross borders more frequently and easily than ever before. Firms selling goods or providing services digitally have taken local and national markets to a global scale. Many governments have responded to these changes by seeking to control digital trade in blunt and disruptive ways. Some of these rules responsive to legitimate public policy goals; others are explicitly protectionist.

Global digital trade is crucial to today's economy. Current laws, regulations and trade agreements often lag behind the fast-paced developments through the emergence of the internet and thereby enabled business practices. Regulators and policy makers should acknowledge the need for a comprehensive set of rules addressing issues of the digital economy, including commitments to open and free internet access that combats restrictions on cross-border data flows, data localization requirements, and other barriers to digital trade with cutting-edge obligations.

What CompTIA Supports:

As part of the offensive trade strategy, CompTIA works to ensure the free and open transfer of data around the world and opposes localization measures and other national security overreaches that pose a threat to the industry. We advocate for inclusion of these newly established principles designed to promote the digital economy in ongoing trade negotiations and in other international fora. As International fora consider e-commerce or other work streams to address digital trade, CompTIA will determine, with member input, where to engage in a meaningful way.

U.S.-China Trade

The Issue:

China is one of the world's largest markets for the information and communications technology (ICT) sector, and one that American technology companies cite as a priority for their global operations and competitiveness. As China aims to make itself a technology leader of the future, it is rolling out a high volume of programs to achieve its goals, often in an opaque manner. As part of its policies, China is also encouraging, if not requiring, the transfer of technology and IP to Chinese joint venture entities.

Under the Section 301 Investigation, in March 2018, the Office of the United States Trade Representative (USTR) issued a report into the investigation on China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation. The report identifies that the U.S. economy has suffered from Chinese policies, including its unfair forced technology transfers that require U.S. and other foreign firms to transfer sensitive technology to the Chinese government.

The President signed a proclamation directing the Administration to take a range of actions in response to the report issued, including imposing tariffs on identified imports from China.

Current Status:

Three tranches of tariffs have been levied as of July 6, August 23, and September 24, 2018. Tariffs are in place on many tech-related products and components including printer parts, integrated circuits, semiconductor devices, thermostats, computer equipment used in cloud, AI, and blockchain technology, among others. The President indicated that a list of $267 billion in imports from China that could be subject to tariffs next.

What CompTIA Supports:

While the Administration's investigation into China's intellectual property practices provides for tools to resolve this long-standing issue, tariffs and an ineffective trade war will only punish American consumers and companies while doing little to actually change China's trade practice.

The best solution to stopping China's intellectual property theft practices and forced technology transfer policies is in working with Congress to develop a comprehensive strategic policy that can effectively address those longstanding challenges in China. We urge Congress and the administration to do that, and to continue to negotiate with China while collaborating with our allies who face the same challenges.

CompTIA Recommendations for Chinese Reforms to Address Trade and Investment Barriers:

- China must provide U.S. cloud service providers with full and non-discriminatory market access.
- China must allow cross-border data transfers for business purposes.
- China must halt all draft measures and standards that require or encourage the disclosure of IP, source code, or enterprise standards.
- China must immediately notify all Chinese government subsidies related to ICT industries, including those specified within the Made in China 2025 initiative to both the United States and the WTO. China will further terminate prohibited and trade-distorting subsidies.
- China must require Chinese enterprises to halt infringement and or misappropriation of intellectual property.

United-States-Mexico-Canada Agreement (USMCA)

The Issue:

In August 2017, the Trump Administration commenced negotiations with Canada and Mexico with respect to modernizing the North American Free Trade Agreement (NAFTA). CompTIA developed recommendations for a new NAFTA, filed comments through the Federal Register Notice and testified at the public hearing.

Current Status:

On October 1, 2018, the U.S. Trade Representative officially released the language for the trilateral trade deal between the U.S., Mexico, and Canada called the United States-Mexico-Canada Agreement (USMCA). President Trump and counterparts from Canada and Mexico are projected to officially sign the deal by the end of November. Once the agreement is signed, President Trump has a 60-day window to deliver a report to Congress on the changes to U.S. law that would be required to implement the agreement. The USMCA must be ratified by each country's legislature. Entry into force will occur on the first day of the third month following notification by the last party to implement the agreement under its domestic law. U.S. midterm elections, as well as remaining issues to be resolved with regard to the Section 232 steel and aluminum tariffs that President Trump has levied against Canada, Mexico, and the European Union may complicate ratification.

Priority objectives for CompTIA members in the USMCA include: market access, customs and trade facilitation, rules of origin, digital trade, government procurement and intellectual property.

What CompTIA Supports:

CompTIA supports the renegotiation of NAFTA with the following objectives:

- Retain existing provisions that have worked well for the technology industry, as outlined in CompTIA's NAFTA recommendations.
- Increased opportunities for market access.
- Digital trade commitments that ensure free flow of data and prevent localization.

Smart Cities & Communities

The Issue:

While cities and communities are making progress toward improving living standards and social and environmental sustainability, the impact can be limited by narrow project scopes and obsolete systems. Cities and communities can accelerate and enhance the results of their efforts by adopting a smart cities and communities approach with supporting technologies.

What CompTIA Supports:

Federal investment in smart cities and communities will help drive economic growth, drive innovation, help create jobs, promote citizen services, while increasing the adoption of smart technology products and services. We support the Smart Cities and Communities Act. The primary focus of the Act is to help coordinate the various federal agency smart city initiatives, as well as create a technology demonstration grant program. We also support the Smart Technology for Resilient, Efficient, Economic and Reliable Transportation in Cities and Communities Act (STREET Act). This Act will provide grants to small and medium sized cities on a competitive basis. Finally, we support the creation and focus of the Congressional Smart Cities Caucus.

Additional Background:

A smart city and community uses information and communications technology (ICT) to enhance its livability, workability and sustainability. It collects information about itself using sensors, devices or other systems, and sends the data to an analytics system to understand what's happening now and what's likely to happen next.

Most cities greater than 750,000 in population have at least one — and usually multiple — smart city projects underway in one sector or another. But few cities and communities have a comprehensive, long-term, integrated plan. In fact, there are only a handful of cities worldwide that are well on their way to a full adoption of smart cities technology in an integrated way across all sectors. And many of the real-world smart city examples are typically much larger or smaller than how we traditionally define cities. They're either occurring on a more regional basis or as small neighborhood-by-neighborhood projects.

There is vast potential to provide smart city and community benefits to a larger number of citizens and those benefits are immense.

First, is the potential to empower citizens, allowing access to unparalleled services provided by local government. These services — spanning several different sectors including transportation, energy, water management and public safety — have the potential to be transformational to the citizen while creating significant efficiencies for the city and community.

Another is the creation of new jobs. As cities grow their smart technology and services capabilities, there are several emerging employment opportunity sectors:

- **Infrastructure** – Cities will need to have large teams to help deploy the vast array of sensors that will constitute the Internet of Things (IoT) smart city and community ecosystem.
- **Cybersecurity** – With internet-connected sensors, best-in-class cybersecurity solutions and applications are an absolute necessity. A well-trained workforce will need to implement the cyber solutions across the infrastructure ecosystem.
- **Analytics** – An immense amount of data coming off the IoT sensors will need to be analyzed. City governments will need to beef up their analytical capabilities in order to ensure that citizens gain the most benefits from the analyzed data.

Workforce Development: Cybersecurity

The Issue:

Our cybersecurity infrastructure is under constant attack from nation states, organized crime groups, and rogue individuals who wish to do our nation harm. The Federal government is struggling to recruit and retain the talent they need to protect against and respond to these attacks. In July 2016, the Office of Management and Budget released a memo outlining a Federal Workforce Strategy as it relates to the cybersecurity. According to the memo, "these cyber threats demonstrate the need for critical security tools, and equally as important, the need to employ the Federal civilian cybersecurity workforce with the necessary knowledge, skills, and abilities to use those tools to enhance the security of the Federal digital infrastructure and improve the ability to detect and respond to cyber incidents when they occur."

What CompTIA Supports:

CompTIA supports expanding and enhancing our Federal cyber workforce by all means necessary. This includes:

- Updating our existing laws to ensure that government is able to use authorized and appropriated funds to build out its cyber workforce;
- Eliminating unnecessary roadblocks to recruitment of cyber professionals;
- Expanding the government's use of industry-recognized credentials as a way of professionalizing the cyber workforce, and;
- Ensuring that all future cyber workforce legislation includes avenues for both training and certification.

Immigration Reform

The Issue:

Our current immigration system is broken and causing the United States to lag behind in a competitive global marketplace for talent. By not addressing the failings of our immigration system we are threatening our future productivity, ingenuity and the competitiveness of key sectors of our economy, including and especially technology.

What CompTIA Supports:

- **Increase Green Cards for High-Skilled STEM Graduates** – CompTIA supports increased access to Green Cards for high-skilled STEM graduates by expanding the exemptions and eliminating the annual per country limits for employment based Green Cards.
- **Create New Visas for U.S. Educated Students and Entrepreneurs** – These new visas will help fill the thousands of IT-related jobs currently open, furthering opportunities for starting and growing new businesses in the United States.
- **Market-based Visa Caps** – Using market-based caps on H1B visas are the best way to adjust to the supply and demand in the U.S. economy.
- **Growing Domestic Sources of Talent** – CompTIA, our member companies and our affiliated Creating IT Futures Foundation are strongly committed to improving U.S. science, technology, engineering and mathematics (STEM) education and encouraging more young Americans to choose careers in those fields. Key to that effort is encouraging federal, state and local investment in STEM curriculum for students from kindergarten through high school with a structured pipeline to higher education. CompTIA uniquely sits at the intersection of innovation, education, and economic growth. We support policies that expand life-long education and promote a skilled workforce that spurs job growth and our ability to compete globally. Quality education, worker training – and retraining – will help ensure the availability of a skilled and competitive workforce.

Internet of Things (IoT)

The Issue:

The Internet of Things (IoT) is a series of smart devices connected to one another and to analytics and hosting platforms via the Internet. As the IoT continues to grow, both challenges and opportunities will arise. Central to the continued growth of IoT are policy principles that are transparent on privacy issues, highlight security in the IoT lifecycle, and stress open standards. CompTIA urges policymakers and regulators to tread lightly in this space, which is still in an early stage of development, so that innovation and the attendant societal benefits will continue to flourish.

What CompTIA Supports:

- **Regulatory and Legislative Moderation** – CompTIA supports a federal strategy for IoT that harmonizes guidelines for IoT devices across all agencies and industries. To accomplish this, Congress must pass legislation that will direct one agency to lead the discussion. The Developing Innovation and Growing the Internet of Things (DIGIT) Act, for example, would place the Department of Commerce in this role). Congress should, however, avoid broad legislation regulating IoT, particularly regarding privacy and data security practices. We already have federal and state privacy and data security laws on the books and passing IoT-specific legislation will only serve to stifle innovation in a nascent industry. Instead, multi-stakeholder groups involving actors from government and industry should work together to develop guidelines and industry best practices in this space based on existing privacy and data security laws and frameworks. CompTIA supports both the NTIA IOT security multi-stakeholder process as well as the NIST IoT Cybersecurity Framework.

- **Broadband** – CompTIA supports the deployment of a robust broadband infrastructure to support the IoT. To accomplish this, we need support from federal, state and local governments to assist in facilitating broadband deployment (see our Broadband Deployment one-pager for more detail).

- **Spectrum** – To support the growth in IoT devices, CompTIA believes that the federal government needs to make more spectrum available for both licensed and unlicensed use without placing technology-specific restrictions on how it can be used (see our Spectrum one-pager for more detail).

- **Regulatory Sandboxes** – To incentivize more IoT innovation and experimentation, companies need to be assured that the risk/reward balance is favorable. To help manage risk, drive economic development and develop a strong regulatory regime, CompTIA recommends that federal and state governments consider creating IoT regulatory sandboxes. These sandboxes provide a set of pre-approved, published rules that allow companies to test their products and business models. The rules help limit exposure and provide best practices and steps for testing innovative practices.

- **Privacy & Data Security** – Congress should avoid broad IoT-specific legislation regarding companies' privacy and data security practices. A number of federal and state privacy and data security laws and guidelines are already on the books and provide a sufficient framework to regulate IoT at this time. That said, industry can and should lead with respect to "design by security" and risk mitigation to provide businesses, government and citizens with maximum trust in IoT.
- **Standards** – We support a multi-stakeholder approach for setting voluntary IoT standards for interoperability. We are concerned that without agreed-upon standards, we could encounter a problematic piecemeal regulatory approach that stifles innovation in the industry.
- **Research and Development** – We support a federal government position that emphasizes research and development in the form of federal grants to help facilitate public-private partnerships. Of particular interest are grants focusing on cyber related IoT R&D.
- **Governance** – A key component of the federal IoT ecosystem is a well-structured governance model. Following the Senate's DIGIT Act, we support a governance structure which is led by the Department of Commerce, that incorporates all of the federal agency stakeholders.

Office of Technology Assessment (OTA)

The Issue:

The impact of, and reliance on technology on America's economic prosperity and national security over the last decade has grown tremendously. As this reliance has grown, so has the cybersecurity threat. Cybersecurity breaches are becoming more devastating in their scale and cost. Several global players are now challenging U.S. dominance in science, technology, and innovation. In traditional areas of national security and economic dominance, our technological advantage, is eroding. New technologies present new challenges in security and privacy, and an increasingly complex regulatory environment requires more expertise than Congress currently has. These questions are only increasing in frequency and the stakes are getting higher. Congress needs a nonpartisan body within its ranks that can provide detailed advice on tech and innovation.

What CompTIA Supports:

CompTIA recommends that Congress reestablish the Office of Technology Assessment (OTA) and restore funding for the Office. In particular, CompTIA would like to see the Office reestablished with a renewed focus on areas where expertise in Congress is most needed: understanding emerging technologies and cybersecurity.

- CompTIA supports the initial legislative steps that were taken this Congress to examine the idea of reestablishing the Office.
- The current legislation requires the Congressional Research Service to examine the need for an additional entity to bestow technological guidance.
- The legislation also requires the Government Accountability Office to evaluate how to give its tech assessment program increased visibility and relevance.

The Office of Technology Assessment (OTA) was an office of the United States Congress from 1972 to 1995. OTA's purpose was to provide Congressional members and committees with objective and authoritative analysis of the complex scientific and technical issues of the late 20th century, (i.e.) technology assessment. It was a leader in practicing and encouraging delivery of public services in innovative and inexpensive ways, including early involvement in the distribution of government documents through electronic publishing. Its model was widely copied around the world.

Federal Government Investment in Research & Development

The Issue:

We are living in an era where innovation, agility and imagination are all essential in order to keep pace with exponential technological transformation taking place in our society. In government, federal agencies are playing catch-up from years of underfunded research and development (R&D) impacted by economic constraints and sequestration, while other nations have increased their public and private R&D investments at a faster rate. There is a longstanding notion that R&D is the backbone of a globally competitive, knowledge-driven economy. In 2010, economist Gary Becker stated that "modern economies are based on the command of knowledge and information." It is essential that the U.S. sustains its investment in R&D.

Michael D. Griffin, the new Under Secretary of Defense for Research and Engineering, has placed an emphasis on emerging technology with supporting R&D budget. Griffin has stated publicly that "The reality is that we live in a time of global access to technology and global access to scientific talent. It is no longer preeminently concentrated here in America. Innovation will remain important, always, but given this global dispersion of technology and talent, greater speed in translating technology into fielded capability is where we can achieve and maintain our technological edge."

This is good news as the government invests and partners in programs and solutions for some of our greatest challenges, including cybersecurity, Smart Cities, big data, quantum computing, space exploration, health and medicine, blockchain, artificial intelligence, and the Internet of Things. Continued R&D investment will help drive innovation and spur competitiveness.

What CompTIA Supports:

CompTIA supports increases in R&D funding that support advancements in big data, cloud computing, high performance computing, automation, artificial intelligence, biometrics, blockchain technology, and cybersecurity (as it relates to emerging technologies and services). In particular, we support increases to the following federal R&D budgets.

- **The Networking and Information technology Research and Development (NITRD) Program** – A federally funded program designed to increase coordination, productivity and effectiveness among federal agency R&D efforts in networking and IT. This program can be successful in helping to drive innovation as long as it has an adequate budget.
- **The Defense Advanced Research Projects Agency (DARPA) R&D Budget** – DARPA has helped drive innovation on a number of issues, including connected vehicles, spectrum, cybersecurity, the Internet of Things, and blockchain technology.

- **The National Labs and Federally Funded Research and Development Centers (FFRDCs)** – These are the nation's R&D incubators and have compiled a treasure trove of technologies and applications for defense and the civilian interests. The benefits of the labs' role include experienced capability in rapid prototyping of new technologies ready for transitioning; showcasing; and commercialization.
- **Funding of the Small Business Innovation Research (SBIR) Program** – SBIR enables small businesses to explore their technological potential and provides the incentive to profit from its commercialization.

Use of Consumer and Enterprise Unmanned Aerial Vehicles

The Issue:

Unmanned Aerial Vehicles ("UAVs," also known as drones) offer immense opportunities for innovation, from cargo delivery to emergency response to simply photographing places that humans cannot get to. UAV innovation is occurring at a breakneck pace. However, regulations are not currently in place to allow for UAVs to be used in many innovative ways. The FAA released their Small UAS Rule in June 2016, which limits UAV use to visual line-of-sight, during the day, and away from people. These rules, while a great first step, still prevent UAVs from being used for a number of enterprise purposes.

What CompTIA Supports:

CompTIA supports a much broader use of UAVs than the FAA permits in its new rules. Congress and the FAA have both demonstrated interest in crafting rules for enterprise uses of drones, but there is much to be done before they are put in place. We believe that Congress and the FAA should strive to establish flexible rules that allow for enterprise UAVs to go beyond line-of-sight and above populated areas. Further, Congress and the FAA should work to continue to develop standards for airspace management to allow for safer, broader operation of UAVs.

CompTIA supports and advocates for policy changes that will not only embrace, but encourage, the growth of the UAV industry. These include measures to:

- Permit the operation of small UAVs beyond visual line-of-sight.
- Support the development of infrastructure to safely manage the widespread use of low-altitude airspace.
- Enable broader UAS access to commercial mobile services and unlicensed spectrum vital to the safe and widespread integration of UAS.
- Embrace the carriage and delivery potential of UAV technology in a wide array of capacities, ranging from humanitarian aid to commercial operations.

CompTIA believes government must implement thoughtful regulations that reflect and anticipate the rapid growth of the industry. Ultimately, CompTIA supports policies that enable, rather than hinder, the use of UAVs and advocates for risk-based regulations which will allow for the safe and expedited integration of small UAVs into the national air space (NAS).

Affiliate Nexus

The Issue:

With the explosive growth in the e-commerce marketplace there has never been a greater need for reasoned and competitive tax policies that promote research and development, innovation, and entrepreneurship. It is estimated that nearly two-thirds of Americans shop online, generating e-commerce sales of more than $127 billion in Q2 2018. And, there are no signs that this economic engine is slowing down. It is expected that nearly 20 percent of all retail sales will be conducted online by 2022. In June 2018, the Supreme Court handed down its decision in the *South Dakota v. Wayfair, Inc.* case. Its decision effectively overturns *Quill's* physical presence standard. The court ruled in the case that the state of South Dakota can require out-of-state retailers to collect and remit online sales taxes. This ruling is a win for states and localities across the country who have been seeking creative avenues to force online sellers to collect and remit sales taxes.

While the high court did hand down a ruling, Congress hasn't completely given up on the idea of taxing internet sales across state lines. In September 2018, Rep. Jim Sensenbrenner (R-WI) introduced the Online Sales Simplicity and Small Business Relief Act. The bill would ban states from retroactively imposing sales tax collection duties on remote online sellers; require all states to push back economic nexus implementation dates to January 1, 2019; and establish a small seller exemption, meaning a remote seller with gross annual receipts below $10 million in the U.S. is not required to collect and remit sales tax. Other original cosponsors on the bill include Rep. Anna Eshoo (D-CA), Rep. Jeff Duncan (R-SC), and Zoe Lofgren (D-CA).

Both Congress and state legislatures will face decisions in coming months over how –and in some cases, if –to respond now that the longstanding wait on the *South Dakota v. Wayfair* case has ended. While the 5-4 ruling opens the door for states to require out-of-state online retailers and other remote sellers to collect sales tax from their customers, questions have started swirling about what might come next as states start to take advantage of the decision. Lawmakers from both parties have acknowledged that they are interested in following up on the court's ruling with state legislation.

What CompTIA Supports:

CompTIA supports solutions that (1) do not increase the compliance burdens on small- and medium-sized businesses, (2) ensure sellers can continue to sell their goods and services across state lines, (3) foster online commerce, (4) create a seller exemption for small business, and (5) protect businesses from new and costly regulations or taxes.

The debate surrounding the collection and remittance of online sales taxes should be refocused to balance the needs of states to collect these taxes with the ability of businesses to cover these new compliance costs. States need to collect sales and use taxes owed, but the costs associated with moving this compliance burden from individual taxpayers onto businesses must also be considered.

Digital Goods and Services

The Issue:

According to recent data, 88 percent of Americans are using the internet and over 200 million internet users will make an online purchase this year alone.[1] The digital economy continues to play a strong role in both the growth of the internet and the ability for businesses to better deliver digital goods and services.

Given the importance of the digital economy to our member companies and the need to ensure we can continue to foster innovation and economic growth within this sector, we strongly support the Digital Goods and Services Tax Fairness Act. This legislation will prevent hurdles to growth and create a much-needed tax framework that will provide certainty to consumers, providers, and state/local governments, while preventing duplicative and discriminatory taxes.

CompTIA opposes taxes on digital products. However, for those jurisdictions that have opted to impose these taxes, we recognize the need to provide consistency and simplicity across state borders. There should never be a situation when multiple jurisdictions can tax the same digital good or service and a framework must be established to ensure that a single purchase is sourced in one state and not multiple states.

What CompTIA Supports:

CompTIA supports legislation such as the Digital Goods and Services Tax Fairness Act. This legislation would (i) provide consistency in determining which jurisdiction can tax a transaction (at the appropriate sales tax rate), and (ii) prohibit unfair and unrelated discriminatory taxes. While CompTIA opposes taxes on digital products, we do support legislation that would provide consistent treatment across state lines when digital products are taxed by state or local jurisdictions. The Digital Goods and Services Tax Fairness Act addresses our concerns by accomplishing two key objectives:

First, the legislation sources the purchase of a digital good or service to the consumer's home address (not the location of the consumer at the time of downloading a product or the location of the server). Therefore, only one state would have the ability to tax the transaction – if that state chose to do so. Congress took a similar approach in 2000 when it passed the Mobile Telecom Sourcing Act, which essentially sourced wireless and mobile telecommunications services to the consumer's home address to eliminate confusion around which taxing jurisdiction had the right to tax wireless services.

Secondly, the legislation would prohibit discriminatory taxes. If a state decides to tax a downloadable song, for example, the rate should be the same as if that same song was purchased in a "brick and mortar" store. Prohibiting discriminatory taxes simply brings parity between digital products and their tangible counterparts.

Consistent with our support for the Digital Goods and Services Tax Fairness Act, CompTIA calls on states to reject new taxes on electronically transferred digital products and electronically delivered services such as data processing, hosting and related services. Such a broad expansion of the sales tax base to include electronically transferred goods and services, particularly those that are actually business inputs, is bad public policy and will result in multiple and discriminatory taxation.

1 Pew Research Center "Internet/Broadband Fact Sheet." January 12, 2017. http://www.pewinternet.org/fact-sheet/internet-broadband/

Mobile Workforce

The Issue:

Some states are imposing income taxes on non-residents after very brief work-related stays. This makes tax compliance more complicated for individuals and their employers; it also deters business-related travel.

What CompTIA Supports:

CompTIA supports H.R. 1393/S. 540, the Mobile Workforce State Income Tax Simplification Act of 2017, which would establish national standards for state income taxation of non-residents. The House passed this legislation on June 20, 2017. This legislation would allow employee wages or compensation to be taxed by only the (i) state of the employee's residence, and (ii) the state within which the employee is present and performing employment duties for more than 30 days during the calendar year.

Employees who are required to move from state to state should not be required to file and pay state income taxes for brief periods of work, (i.e.), 30 days or less. This legislation does not exempt the employee from state taxes; it just provides that only the employee's state of residence or any state in which the employee worked for more than 30 days are permitted to require the employee to file and remit state taxes.

CompTIA supports legislation at the state level that simplifies nonresident employee and employer requirements to report and withhold state income taxes. CompTIA supports the balance between the business needs of today's mobile workforce and each state's authority to determine its own tax law.

Message Points:

1. The Mobile Workforce State Income Tax Simplification Act of 2017 would establish a fair and uniform 30-day threshold to help ensure the appropriate amount of tax is paid to state and local jurisdictions without placing undue burdens on employees and their employers.
2. Most individuals are unaware of the current patchwork of non-resident state income tax filing rules, and many employers must incur extraordinary expenses to comply with withholding requirements.
3. Each state has its own set of requirements for filing non-resident individual income tax returns and commensurate rules for employer withholding on those employees.
4. The legislation would enhance compliance with state personal income tax laws while significantly reducing the onerous burdens placed both on employees who travel outside their resident states for temporary periods and on employers who have corresponding withholding and reporting requirements.

Principles of Federal Privacy Legislation

- **Preventing Harm** – First and foremost, the goal of any federal privacy law should be to prevent personal information from being misused in ways that could harm individuals.
  - Data Security – Companies in possession of personal information should adapt appropriate safeguards to secure that information.
  - Risk-based Approach – Not all information collected should be treated equally under the law. The greater the risk that the information could be used in a harmful manner, the stronger the protections should be regarding that type of data. Similarly, some uses of information provide greater risk of harm to consumers than others and should be regulated as such.
  - Privacy and Security By-Design – Companies that collect and use of personal information should be build privacy and security protections into their products and services at the development stage.
- **Transparency** – Companies that collect and use personal information should provide easily accessible and understandable information to their customers about what data they are collecting, how that information is being used, and what choices individuals have about information collection and use.
  - The manner and format of how this information is communicated to consumers and how they can effectuate choices will depend on a variety of factors, including whether a product is consumer-facing.
- **Data Collection/Usage** – Collection and usage of personal information should be limited to the uses conveyed to customers as described above and, when necessary to provide a service requested by a customer. Any further collection or uses should require explicit user consent.
  - When practicable, users should be provided with the ability to choose how their data is collected and used, but should also be made aware that the consequences of said choices could result in diminished functionality of the product or service or the inability to use the product or service.
- **Platform/Technological Neutrality** – A federal privacy law should apply equally to all companies collecting data and should not impose different rules on different business models. Further, the law should not require the use of any specific technologies. Companies should have flexibility in how they choose to comply with the regulations.
- **Preemption** – A federal law must preempt state privacy and data protection laws to avoid compliance issues with, ultimately, 51 different state privacy and data protection laws. However, state attorneys general should have the ability to enforce the federal law.

Hill Meeting Best Practices

During your visit to Washington, D.C. you will attend numerous meetings on the Hill. Whether these meetings are with staff or Members of Congress, it is important to remember a few important tips:

The dress code is business professional.
• When Congress is in session, the office dress code is business professional.
• Most people attending meetings follow that same dress code.

You will be provided a schedule of all your meetings – make sure to arrive to the offices a few minutes early.
- The detailed schedule will contain locations of all your meetings.
- There are three House office buildings – Cannon, Longworth and Rayburn.
- There are three Senate office buildings – Dirksen, Hart and Russell.
- Remember, there are security screenings at each building entrance. Plan for extra time to get through security.

Be prepared.
- Read over the biography of the Member, where they are from, and their key issues and positions.
- Detailed information on the Members will be provided by CompTIA.

If the Member of Congress is in attendance, address them as "Congressman," "Congresswoman," or "Senator."
- In many cases you will be meeting with a member of the staff; however, these staff members are responsible for representing their boss and providing them will all necessary information on important topics.
- Remember to stay on message throughout the meeting; focus on the issues you came to discuss.
- You will be provided with all the necessary messaging information prior to your meeting by CompTIA staff.

Leave contact information and any materials you have brought with you as leave-behinds.
- You will be provided any necessary leave-behind materials prior to your meetings.

Remember to thank them for the meeting as you are leaving!
- Also, thank them again via email or a handwritten note later.
- A second thank you allows you to not only show your appreciation for their time, but to remain in contact.

Provide CompTIA staff with any outstanding questions or follow-up materials requested by the staff.

Frequently Asked Questions

Q. How do I identify the buildings where my meetings are located?

A. We will be providing you with a comprehensive schedule of all your meetings. Meetings in House offices will be in the Rayburn Building, Longworth Building and Cannon Building. Meetings in the Senate will take place in the Hart Building, Dirksen Building and Russell Building. All of these buildings have security procedures that include metal detectors. Therefore, plan for some additional time to enter buildings. All Senate buildings are connected internally and all House buildings are connected internally. Therefore, if you have multiple meetings in House offices, for example, you will not have to reenter security. One thing to note: House offices have a numeric system that identifies not only the room number but the building as well. Room numbers in the Cannon Building are three digits (e.g. 234, located on the second floor). Room numbers in the Longworth Building are four digits and begin with the number 1 (e.g. 1234, located on the second floor, as the "1" only signifies the building, not the floor). Room numbers in the Rayburn Building are four digits and begin with the number 2 (e.g. 2434, located on the fourth floor, as the "2" only signifies the building, not the floor).

Q. Am I able to watch the House and Senate floor proceedings live?

A. Yes. All visitors to the Capitol complex can visit the House and Senate chambers to watch debates and votes whenever the House and Senate are in session. In order to gain access to the viewing galleries, you must obtain a "gallery pass" from your Member of Congress or Senator. Simply visit their office and ask a member of their staff for a House or Senate gallery pass. They also should be able to guide you toward the appropriate entrance to the Capitol.

Q. I need some additional information on an issue. With whom should I speak?

A. The CompTIA Public Advocacy team is happy to provide you with a further briefing or briefing materials on policy issues prior to your D.C. visit or after you arrive. Please contact Mary Artes at martes@comptia.org if you need additional information or data on any issue. Additionally, CompTIA staff will be providing in-person briefings prior to the meetings as part of the DC Fly-In program.

Q. How long do meetings traditionally last on Capitol Hill?

A. Meetings are generally scheduled in 15-30 minute blocks with staff. However, meetings are sometimes shorter based on votes and Committee hearings, which can be very unpredictable.

Q. Will I be attending meetings alone?

A. No. We have set up meetings in a manner that sends small groups of CompTIA members to multiple meetings together in an effort to increase our voice and allow our issues to be elevated on Capitol Hill.

Q. Who should lead the meeting?

A. Members of Congress, Senators, and their Staff are primarily focused on the opinions and priorities of their constituents. Therefore, if there is a constituent in the meeting, they should lead the meeting and identify himself or herself as a constituent at the start of the meetings. It will then be important for all of the other attendees to introduce themselves and provide a very short background on their company and where they are located prior to a discussion on the issues.

Q. Are there issues we should not mention in a Congressional office?

A. Yes. Congressional offices are legally separated from campaign offices and, therefore, Members of Congress and their staff are prohibited from discussing or coordinating any campaign activity from their offices. Therefore, it is important that you not mention their campaigns and/or discuss any interaction you may have had with their campaign offices.

Q. Why am I scheduled to meet with a staff member instead of a Member of Congress or Senator?

A. When Congress is in session, Members of Congress and Senators have a variety of responsibilities, including: votes, committee hearings, and numerous policy and constituent meetings. Therefore, obtaining a meeting with the Member of Congress or Senator is often not possible due to scheduling conflicts. However, staff members are responsible for representing their boss and providing Members of Congress and Senators with senior-level guidance on policy issues. They play a significant role in the Congressional office, working on the issues that are important to our industry. Therefore, meetings with staff are important and your message will be appropriately communicated to the Member of Congress.

Q. How do I address a Member of Congress or Senator in a meeting?

A. Traditionally, you address a Member of Congress a "Congressman" or "Congresswoman." You address a Senator as "Senator." However, if the Member of Congress or Senator is the Chair of a Committee (which will be noted on your schedule), you address them as "Chairman" or "Chairwoman."

Q. What if I get asked a questions that I don't know the answer to?

A. This is not a problem. You can simply tell the Member of Congress or their staff that you will go back, discuss the matter with CompTIA staff, and provide additional follow up on the question. This also provides you with an excellent opportunity to continue the dialogue with that office.

Q. Would it be possible to attend other meetings if there are gaps in my schedule?

A. Yes, all participants will be provided with a master schedule will all meetings throughout the day. You are welcome to join a meeting that you are interested in as long as it doesn't interfere with your own schedule. Make sure to connect with the group early and make sure they are aware you will be attending the meeting with them.

Q. What should I do if a policymaker either commits to supporting an issue or highlights his or her opposition to the issue?

A. All information from a meeting is helpful to CompTIA staff as they continue to work on these issues throughout 2018. Intelligence from a meeting – including support or opposition to a meeting – is critical information that will ensure we follow-up with the office and know where they stand on our issues.

Q. How should I dress for my meetings on Capitol Hill?

A. As you will be visiting Congress while the House and Senate are in session, offices will be dressed in business attire. Most people attending meetings in these offices generally follow those same guidelines.

Q. If I have a medical issue on Capitol Hill, who should I call?

A. All House and Senate buildings have a nurse that attends to medical issues of staff and visitors. Should you need to visit the nurse while on Capitol Hill, call (202) 224-3121 and ask to be connected to the nurse's station in the building you are currently located.

Q. Are there areas to purchase food and drinks in the House and Senate office buildings?

A. Yes. In the House, there are cafeterias located in the Longworth and Rayburn Buildings on the basement levels. The cafeteria on the Senate side is located in the basement of the Dirksen Building. All buildings in the House and Senate have additional food options, which are usually located in the basement.

Q. Where is the closest Metro to my meetings?

A. On the House side, the Capitol South metro station (Orange/Blue Lines) is located just outside of the Cannon Building. On the Senate side, the closest metro station is located within Union Station (Red Line).

Q. If I need to do some work between meetings, where should I go?

A. The House of Representatives has Wi-Fi in their cafeterias and eating locations in each building.

Q. If my plans change and I am unable to attend the Fly-In, who do I contact?

A. If you are not able to attend all or part of the Fly-In and have previously RSVP'd, please contact Mary Artes (martes@comptia.org) immediately and let her know how your schedule has changed. We will be arranging meetings on Capitol Hill based on your attendance and will want to cancel or adjust those as soon as possible if you will not be in attendance.

Important Contacts

CompTIA Policy Staff

Elizabeth Hyman
Executive Vice President,
Public Sector & Advocacy
EHyman@comptia.org
Phone: 202.577.9570

Liz Navlen
Vice President, Membership
& Communications,
Public Sector & Advocacy
LNavlen@comptia.org
Phone: 917.855.1367

David Logsdon
Senior Director, Public Advocacy
New and Emerging Technologies
Dlogsdon@comptia.org
Phone: 202.682.4440

Randi Parker
Senior Director, Public Advocacy
Cybersecurity / Workforce Development
RParker@comptia.org
Phone: 202.445.7188

Matthew Starr
Director, Public Advocacy
Broadband and Telecom / Privacy
MStarr@comptia.org
Phone: 703.328.4369

Geoffrey Lane
Director, Public Advocacy
Tax
GLane@comptia.org
Phone: 937.243.0992

Stefanie Holland
Director, International Government
and Regulatory Affairs
SHolland@comptia.org
Phone: 262-339-7764

Mary Artes
Senior Administration Specialist
Martes@comptia.org
Phone: 301.643.6651

Kevin Callahan
Director, State Government Affairs
Kcallahan@comptia.org
Phone: 202.682.4448

Membership

Ann Corcoran
Director, Member Relations,
Public Advocacy
ACorcoran@comptia.org
Phone: 202.503.3632

Michele Weatherly
Director, Member Acquisition,
Public Advocacy
Mweatherly@comptia.org
Phone: 202.503.3642

Ioana Lewis
Member Relations Specialist, Public Sector
Ilewis@comptia.org
Phone: 703.887.8138

Communications

Roger Hughlett
Senior Manager, Communications
RHughlett@comptia.org
Phone: 571.289.5282

Events

Lisa McKellar
Vice President, Events and Creative
LMckellar@comptia.org
Phone: 202.251.3242

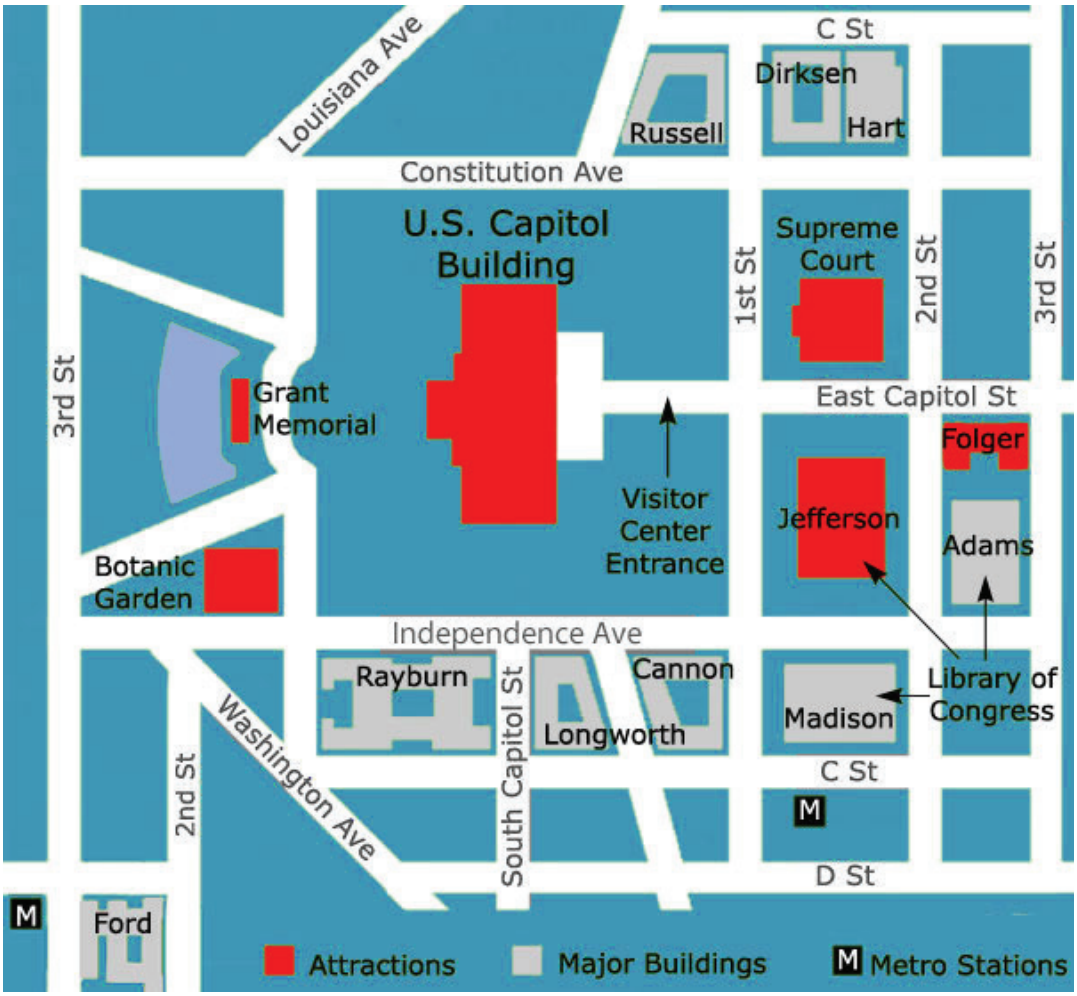
Brooke Shevtsov
Specialist, Events
BShevtsov@comptia.org
Phone: 312.507.9023

Transportation to Washington, D.C.

There are a number of transportation options for sightseeing and traveling throughout the city or heading to the airport.

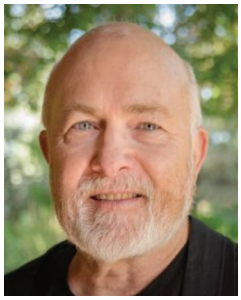
Capitol Hill

The map below is an outline of Capitol Hill. Please note the Senate buildings in the top right hand corner and the House Offices in the bottom center of the map.



Meet the DC Fly-In Speakers

Chloe Autio
Policy Analyst
Corporate and Government Affairs
Intel Corporation



Philip Bane
Managing Director
Smart Cities Council

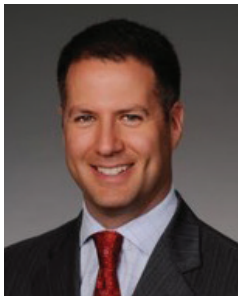
Nicole Bivens Collinson
President
International Trade, Government Relations and Federal Affairs Specialist
Sandler, Travis & Rosenberg, P.A

Chris Calabrese
Vice President for Policy
Center for Democracy & Technology

Brendan Carr
FCC Commissioner

Austin Carson
Government Relations
NVIDIA

Charles Cooper
Executive Vice President
Signal Group



Eric Einhorn
Senior Counsel for Technology and Communications Policy
Office of United States Senator Brian Schatz

Alexandra Givens
Executive Director
Institute for Technology Policy
Georgetown University Law Center

Travis Hall
Telecommunications Policy Specialist
Office of Policy Analysis and Development (OPAD), National Telecommunications and Information Administration (NTIA)
U.S. Department of Commerce

Tim Herbert
Senior Vice President
Research and Market Intelligence
CompTIA

Elizabeth Hyman
Executive Vice President
Public Advocacy
CompTIA

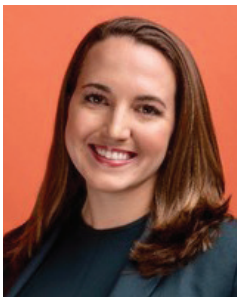
Robert Latta
Congressman
United States House of Representatives (R-OH)

Steve LeVine
Future Editor
Axios

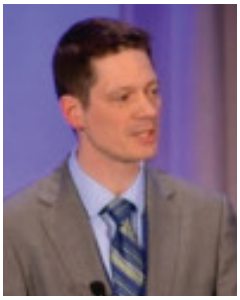
Michael V. Mansour
Legislative Director
Office of U.S. Representative Adam Kinzinger

Rebecca Rainey
Employment and Immigration Reporter
Politico

Carolyn Renick
Program Analyst
Department of Labor, Office of Apprenticeship



Kelly Riddle
Legislative Assistant
Office of United States Senator Jacky Rosen



John Sipple
Senior Software Engineer
Machine Learning
Google and DIU

Lamar Smith
Senior Consultant
Akin Gump & Former
U.S. Representative

Deb Socia
Executive Director
Next Century Cities

Matthew Starr
Director
Public Advocacy
CompTIA

Richard Ward
Senior Director of National
Security Policy
Edison Electric Institute (EEI)

Yael Weinman
Associate General Counsel
Privacy
Verizon

Download the myCompTIA Fly-In App!

See who's speaking, access the agenda and connect with attendees during and after the conference when you download the myCompTIA Fly-In app.

Download the app in the App Store or Google Play by searching ***CompTIA Events***. You will receive a separate invitation by email to access your profile on the site.

CompTIA Public Advocacy Office
515 2nd Street, NE
Washington, DC 20002
www.comptia.org/advocacy
Twitter: @CompTIAAdvocacy

CompTIA Worldwide Headquarters
CompTIA Member Services, LLC
3500 Lacey Road, Suite 100,
Downers Grove, IL 60515
CompTIA.org