ALTERNATIVE FUTURES: DATA PRIVACY, STORAGE, AND TRANSMISSION PLAYER GUIDE

Secure Tomorrow Series

BACKGROUND

How prepared are critical infrastructure sectors in light of potential data privacy, storage, and transmission trends? *Alternative Futures: Data Privacy, Storage, and Transmission*[1] presents you with scenarios that could plausibly occur within the next 5 to 10 years. During each round, you and your opponents will take turns proposing initiatives and debating strategies that will shape critical infrastructure resilience and security in light of potential data privacy, storage, and transmission trends. How successfully you manage to present your arguments for (or against) these initiatives determine their chances of success. Depending on your role for the round, you can score points for either successfully implementing or countering initiatives.

The National Risk Management Center has developed this game as part of a broader effort by the Cybersecurity and Infrastructure Security Agency (CISA) to plan strategically for its future operating environment. The long-term goal of this project is to develop a repeatable and defensible process that (1) identifies emerging and evolving risks to critical infrastructure systems, and (2) identifies and analyzes the key indicators, trends, accelerators, and derailers associated with those risks to help critical infrastructure stakeholders direct their risk management activities.

A key part of informing this effort is to obtain knowledge and perspectives from a diverse group of stakeholders and subject matter experts. For players, the game hopefully represents a fun and interactive way for you to think broadly about future threats and opportunities, learn from your peers, and identify strategies to inform preparedness activities.

The game takes approximately three hours to complete. This includes an introduction and description of the current state, three rounds of gameplay (each about 40–50 minutes long), and a final 20-minute open discussion period to collect any final feedback from players and wrap up the game.

PLAYER ROLES AND ASSIGNMENTS

At the start of the game, each player will be assigned one of three roles. Players will rotate roles in subsequent rounds, so that they fill different roles through the course of the game. The three roles are as follows:

- The Innovator(s): Responsible for developing initiatives and arguments in support of those initiatives.
- The Devil's Advocate: Responsible for developing counterarguments to the initiatives proposed by the Innovator.
- The Judge: Responsible for adjudicating the validity of the Innovator's arguments versus the counterarguments made by the Devil's Advocate for a particular initiative and determining the initiative's likelihood of success.

Players will bring their personal knowledge, experience, and perspectives to debate strategies that will shape critical infrastructure resilience and security in light of potential data privacy, storage, and transmission trends. Players should consider policies, programs, investments, public-private partnerships, research and development, or other actions that, if successfully put into motion today, they believe will better position and prepare one or more critical infrastructure sectors for the future. In preparing for the game, players may want to think about the following questions:

[1] *Alternative Futures: Data Privacy, Storage, and Transmission* combines two Secure Tomorrow Series topics: Anonymity and Privacy and Data Storage and Transmission.

- What risks and opportunities are associated with the current trends in data storage and transmission?
- What risks and opportunities are associated with the current trends in privacy and anonymity?
- What are the implications for future critical infrastructure resilience and security?
- Are there specific ramifications for one or more critical infrastructure sectors?
- Is there a role for CISA to address threats and uncertainties associated with data privacy, storage, and transmission?
- Are there other trends that may influence data privacy, storage, and transmission?

CURRENT STATE

For years, companies have increasingly monetized data, with data promising to unlock the potential for artificial intelligence (AI) to predict and even shape human behavior. Users are required to share personal data with organizations to receive useful services and personalized products. Several emerging trends are contributing to a loss of privacy and anonymity and an increasingly insecure landscape for data storage and transmission:

1. The monetization of data has created an unregulated market for user data—a Wild West where so-called third-party data brokers have amassed significant amounts of data at the individual level. For example, Oracle claims to have data on 80 percent of the U.S.'s internet-using population, with more than 30,000 data attributes per user.[2]
2. Anonymity has largely been lost. Although organizations have been de-identifying datasets to avoid personal data concerns,[3] numerous cases have shown that advances in machine learning, AI, and supercomputers are enabling re-identification of users through the "mosaic effect."[4]
3. With a growing consumer digital footprint, data from third-party cookies,[5] location services,[6] "fingerprinting,"[7] and pre-built user profiles[8] allow interested parties to follow users across platforms, micro-target users, and tailor disinformation campaigns.[9]
4. The global data sphere is projected to triple over the next 5 years from 59 Zettabytes in 2020 to 175 Zettabytes by 2025.[10] Meanwhile, larger data volumes are contributing a greater reliance on public cloud-storage providers.[11]

---

[2] Aliya Ram and Madhumita Murgia, "Data Brokers: Regulators Try to Rein in the 'Privacy Deathstars,'" *Financial Times*, January 8, 2019, https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.
[3] Subject matter expert interview with Secure Tomorrow Series (STS) team, September 11, 2020.
[4] Natasha Lomas, "Researchers spotlight the lie of 'anonymous' data," *Tech Crunch*, July 24, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?renderMode=ie11; and Alex Hern, "'Anonymised' data can never be totally anonymous, says study," *The Guardian*, July 23, 2019, https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.
[5] Federal Trade Commission, "Online Tracking," last accessed September 4, 2020, https://www.consumer.ftc.gov/articles/0042-online-tracking.
[6] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *The New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[7] Fingerprinting is the improved online tracking version of the cookie, collects specific information about the user's devices such as screen resolution, model, operating system, etc. that cannot easily concealed or changed to track users online; Brian X. Chen, "'Fingerprinting' to Track Us Online Is on the Rise. Here's What to Do," *The New York Times*, July 3, 2019, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[8] Craig Timberg, "Critics say Facebook's powerful ad tools may imperil democracy. But politicians love them," *The Washington Post*, December 9, 2019, https://www.washingtonpost.com/technology/2019/12/09/critics-say-facebooks-powerful-ad-tools-may-imperil-democracy-politicians-love-them/.
[9] Subject matter expert interview with Secure Tomorrow Series (STS) team, September 15, 2020.

5. Many countries are taking action to ensure control over national data by prohibiting transfers of data out of the country or by seeking to limit foreign access to certain kinds of data; they sometimes go as far as controlling and limiting content dissemination online. Data localization will greatly slow or prevent the flow of data worldwide, increasing private sector costs, enabling foreign adversaries to hoard data, and limiting the ability of U.S. firms to innovate.
6. Within the U.S., companies are struggling to comply with a patchwork of state data-privacy regulations.[12] Further complicating compliance efforts, companies within specific sectors, such as finance and healthcare, must adhere to federal data-privacy regulations. The evolving landscape increases uncertainty for companies, which can result in additional costs or lost investments.

PLAYING THE GAME

Alternative Futures: Data Privacy, Storage, and Transmission has three rounds, each of which will present the players with a scenario that could plausibly occur within the next 5 to 10 years. In Round 1, the Innovator(s) will have 15 minutes to identify up to three initiatives that will support critical infrastructure resilience and security in response to the specified scenario disruptor. For each initiative, the Innovator(s) will then describe up to three supporting arguments for why the initiative will succeed. The Devil's Advocate will then have 10 minutes to describe up to three counterarguments for each initiative. Each counterargument can be directed at one or more of the arguments presented in favor of the initiative's success, or underscore a new concern that may cause the initiative to fail. The Innovator(s) will then have 5 minutes to rebut any or all of the counterarguments. The Judge will listen to both sides of the debate and ultimately determine if each initiative has a high, medium, or low likelihood of success. The Judge will have 5 minutes to present the rationale for his or her determinations and roll a 20-sided die to see if each initiative succeeds or fails.

The die simulates the unpredictability of the supporting environment for initiatives, and the game's inability to account for all positive and negative factors that might influence success.

- An initiative with a **high** likelihood of success will be implemented with a roll of 6 or higher (75 percent chance).
- An initiative with a **medium** likelihood of success will be implemented with a roll of 11 or higher (50 percent chance).
- An initiative with a **low** likelihood of success will be implemented with a roll of 16 or higher (25 percent chance).

An open-discussion period may occur after resolving the success or failure of the initiatives to continue any discussions cut short by previous time constraints.

In Rounds 2 and 3, the participants will rotate roles.

---

[10] David Reinsel, John Gantz, and John Rydning, Data Age 2025: The Digitization of the World from Edge to Core (November 2018), IDC, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
[11] Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction (New York: Rosetta Books, 2019).
[12] Michael Beckerman, "Americans Will Pay a Price for State Privacy Laws," *The New York Times*, October, 14, 2019, https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html.

DISRUPTORS

Social, technological, environmental, economic, and political (STEEP) influences have the potential to alter the trajectory of future trends or disrupt them altogether. For example, urbanization is a social disruptor that has the potential to significantly affect the resilience of lifeline sectors; an unexpected election result is a political disruptor that could significantly affect funding for critical infrastructure projects; and cyberattacks are a technological disruptor with a wide range of cascading implications for all critical infrastructure sectors.

To account for a changing future environment, each round features a STEEP disruptor scenario that may limit player actions; alter the trajectory of current data privacy, storage, or transmission trends; or require players to consider the implications of an event. The possible scenarios to choose from during the game are described in Appendices I–V. As an added incentive for players to craft compelling arguments and counterarguments, the winning player of each round is awarded the ability to select the STEEP disruptor category for the next round.

WINNING THE GAME

If the Innovator (or Innovator team) successfully implements a majority of their initiatives, the Innovator(s) wins the round. Alternatively, if the Devil's Advocate counters a majority of the initiatives, he or she wins the round. While the game is designed to encourage competition between the players, its main purpose is to generate discussions that develop well-conceived and thought-provoking initiatives. Your collective subject matter expertise is what matters, regardless of the outcomes of each round.

GAME SCHEDULE

TABLE 1—SCHEDULE FOR CONDUCTING THE MATRIX GAME

MATRIX GAME STAGES (~3 HOURS)				
Introduction	-	Welcome participants and discuss game purpose (Controller)	3 Min	18 Min Total
	-	Explain game rules (Controller)	5 Min	
	-	Practice round	7 Min	
	-	Introduce current state and potential implications (Controller)	3 Min	
Round 1	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	41–51 Min Total
	-	Craft initiatives and present arguments (Innovator)	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator)	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open discussion period	< 10 Min	
	-	Select STEEP disruptor	1 Min	
Round 2	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	41–51 Min Total
	-	Craft initiatives and present arguments (Innovator)	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator)	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open discussion period	< 10 Min	
	-	Select STEEP disruptor	1 Min	
Round 3	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	40–50 Min Total
	-	Craft initiatives and present arguments (Innovator)	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator)	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open discussion period	< 10 Min	
Wrap Up	-	Determine final game status of critical infrastructure security and resilience (Controller)	5 Min	20 Min Total
	-	Open discussion period (Players)	15 Min	

Participants are reminded that any information shared during this game is provided on a voluntary basis. Sensitive information, to include confidential or proprietary information, should not be shared. Information shared during this game may be recorded for the purposes of facilitating the program and discussions; however, discussion or disclosure of information in these sessions is not a substitute for submission under the Protected Critical Infrastructure Information (PCII) Program. Information may therefore be subject to Freedom of Information Act (FOIA) requests or other mechanisms that would publicize any information shared and/or recorded.

APPENDIX I: SOCIAL DISRUPTOR

1. INCREASED NUMBER OF EMPLOYEES TELEWORKING

At one point during the 2020-21 COVID-19 pandemic, more than one-third of employed U.S. adults were teleworking, including more than 56 percent of government workers. Over the next five years, the percentage of the U.S. workforce with remote-work arrangements has continued to grow significantly. By 2025, more than 50 percent of U.S. organizations have shifted at least some portion of their employees to remote work permanently, particularly within local, state, and federal government agencies and tech-related industries. For example, almost half of Facebook employees continue to work remotely and two-thirds of government employees spend a minimum of 20 hours a week working remotely.

Increased telework has prompted organizations to reevaluate required data structures to support the needs of remote workers and increase their resilience. With increased demand for remote access comes increased risk, and examples abound of employees accessing sensitive data inappropriately or connecting to networks without following appropriate security protocols. Malicious actors have seized on security vulnerabilities associated with remote work, leading to several high-profile examples of data breaches and cybersecurity incidents:

- *In 2023, malware operators launched sophisticated spear-phishing attacks targeting teleworkers to steal their usernames and passwords and gain access to sensitive data within their organizations' networks. One breach at a popular social media company exposed the personal information of more than 100 million people, which were sold to spammers and used to develop targeted financial scams and other spear-phishing attempts. An internal investigation revealed that the company did not use multi-factor authentication (MFA) for remote access. A Justice Department investigation indicates that a Chinese government-linked hacking group was behind the attack.*
- *In 2024, hackers gained access to numerous public and private organizations through a compromised virtual private network (VPN) software update that opened users up to a common hack, known as a "man in the middle" attack, which allows an unauthorized third party to see everything the user is doing and/or redirect them to a malicious server. The FBI traced the VPN software hack to a cybercrime organization.*

Considerations

What initiatives are necessary to account for security risks and vulnerabilities to data security as remote work continues to increase?

- *What additional actions should be taken to support efforts by owners and operators to secure critical infrastructure from cyberattacks targeting remote operations?*
- *What plausible steps can the federal government take to address weak security practices by the public and private sectors? How might CISA specifically contribute?*

2. SOCIAL CREDIT SYSTEM

U.S. data brokers have consolidated from a few hundred into the "Big Five" and it's become standard practice to engage their services. Reminiscent of China's social credit system,[13] these agencies run background checks on people's financial fitness, employment history, political affiliations, webpages frequently visited, and closest social connections for all manner of applications, including supporting investigations by law enforcement agencies. U.S. government agencies have also begun to contract with these agencies to revamp security clearance programs.

The vast amount of data stored with data brokers makes them prime targets of cyberattacks from state or non-state actors. The Big Five have repeatedly assured customers and the U.S. government that systems are in place to mitigate risks. However, two recent examples highlight their continued vulnerabilities:

- *In 2023, malware operators launched sophisticated spear-phishing attacks on Big Five employees. One breach exposed the personal information of more than 100 million people, which was sold to spammers and used to develop targeted financial scams and other spear-phishing attempts. A Justice Department investigation indicates that a Chinese government–linked hacking group was behind the attack.*
- *In 2024, the FBI uncovered a plot in which a disgruntled employee was offering to sell classified security clearance data to foreign governments. Investigations revealed multiple security vulnerabilities and weak access control practices within the company.*

Considerations

What initiatives are necessary to protect the integrity and privacy of personal data under a system in which data broker services are highly sought after by individuals, corporates, and government agencies?

- *How should you support efforts to achieve the right balance between preserving privacy and benefiting from this data?*
- *What plausible steps can the federal government take to enhance privacy protections from data brokers offering social credit system services? How might CISA specifically contribute?*

[13] See https://www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/

APPENDIX II: TECHNOLOGICAL DISRUPTOR

CYBERATTACKS THROUGH EDGE DEVICES

A growth area of the Internet of Things (IoT) are edge devices, which store and process data locally to minimize the delays inherent in sending data back and forth from the cloud. By 2025, the U.S. market for edge hardware has reached $200 billion.

Unfortunately, these devices come with their own cybersecurity concerns. Edge devices are often poorly protected and positioned at the boundaries of interconnected networks, and they dramatically increase the attack surface. Cybersecurity attacks on edge devices can be difficult to detect; IT administrators rarely engage in the detailed level of network traffic monitoring necessary to do so. Bad actors can string together many edge devices and take advantage of their processing power to conduct cyberattacks.

Three recent cyberattacks illustrate some of the security weaknesses:

- *A major pharmaceutical manufacturing company was using edge devices to track its equipment levels and perform predictive maintenance. Its fleet of 30,000 edge devices—split between several factories and transport vehicles—were infected by a virus that uses the network for cryptocurrency mining. As a result, the processing speed of all these devices slowed to a crawl. Because of how the devices communicate with each other, the virus proves technically infeasible to remove and the company is forced to replace its entire fleet of devices.*
- *In 2024, a major virus, using Mirai source code, strung together hundreds of thousands of unsecured, internet-connected edge devices to launch a distributed denial-of-service (DDoS) attack on a major internet service provider lasting for a shocking seven days. More broadly, the growing number of edge and IoT devices has doubled the number of DDoS attacks globally from 7.9 million in 2018 to 15.4 million in 2023.*
- *An auto manufacturer's "smart" assembly plant was shut down for several hours when a ransomware attack locked all of the robotic devices on the factory floor. The manufacturer paid the ransom—approximately $100,000 in bitcoin—to have its devices unlocked.*

Considerations

What initiatives can you think of to address cybersecurity threats faced by critical infrastructure owners and operators as use of edge devices increases?

- *Are you aware of any industries or critical infrastructure sectors that have or are likely to invest in edge computing? How does the risk differ from edge devices versus IoT sensors? What possible consequences might occur from a cyberattack?*
- *As edge computing takes off, what initiatives can be put in place to mitigate current concerns about cyber vulnerabilities associated with edge devices?*
- *What knowledge gaps might CISA address to assist critical infrastructure owners on the security implications of implementing an edge-device architecture for data collection and processing? How can the federal government best assist critical infrastructure owners on this issue?*

APPENDIX III: ECONOMIC DISRUPTOR

BALANCING PROTECTIONS FOR CORPORATE INSIDER INFORMATION AND EMPLOYEE PRIVACY

In the years following the COVID-19 pandemic, U.S. and European economies are mired in a prolonged recession, with several major multinational corporations having filed for bankruptcy. In 2023, security experts recognized a disturbing trend where competitors, foreign governments, and other nefarious actors use micro-targeting tactics to identify vulnerable employees of failing companies who may be willing to sell insider information, including data, prediction models, and trade secrets. In light of this, companies started implementing employee sentiment and activity monitoring programs. These programs track employee online behavior—both inside and outside the office—for potentially suspicious behavior to identify insider threats.[14] Companies using these programs tout that they are mitigating threats by tracking employee spending habits, web searches, and social medial connections. One notable example in 2024 involved a defense contractor who offered to sell schematics for the Navy's next-generation attack submarine to an undercover FBI agent. However, employees, unions, and advocacy groups like the ACLU are raising privacy concerns.

Considerations

How should you support critical infrastructure partners' efforts to achieve the right balance between preserving the security of their intellectual property and their employees' expectations for privacy?

- *How could CISA and federal agencies better support critical infrastructure owners in their efforts to balance employee data privacy and potential security risks?*
- *How could critical infrastructure owners mitigate concerns and possible backlash—both internal and external to their organizations—from implementing sentiment analysis?*
- *What ethical considerations need to be taken into account when implementing an employee sentiment and activity monitoring program? What bodies and actors are best suited to address these considerations?*
- *Are there systemic risks introduced by allowing individual companies to decide whether or not to conduct a sentiment and activity monitoring program? How might federal agencies mitigate some of these risks while retaining the advantages of these programs?*

[14] See https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring/ and https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy

APPENDIX IV: ENVIRONMENTAL DISRUPTOR

DATA CENTER OPERATIONS

Extreme weather is increasing across the U.S.: "arctic bombs" in the North and Northeast, hurricanes and storm surge along the East Coast and the Gulf, flooding in the Midwest and Great Plains, wildfires on the West Coast, and heatwaves in the South and Southwest. The ongoing barrage of natural hazards has become a significant threat to data storage centers, which have to deal with both damage to their facilities and interruption of their power supplies.

- *Flooding, fire, and other hazards have damaged facilities and permanently destroyed data, most notably in California when the wildfires of 2023 led to the shutdown of 13 data centers near Sacramento. Hurricane Mindy in 2021 caused flooding of two data centers in Charleston, South Carolina, and Hurricane Helene in 2024 swamped five data centers in the Jacksonville, Florida, area.*
- *Power and water interruptions not only prevent access to data, but also can lead to overheating in facilities. In 2022, a heatwave in eastern Texas caused a two-day blackout and 33 data centers experienced at least a partial shutdown.*

Further, as observed in the aforementioned Texas example, data centers tend to cluster in hubs and any hazard that can impact one of them often impacts several. Lastly, given the range of data that can be housed in a data center and the way data is often split between facilities, it's proven difficult to predict what or who will be impacted by a data center going off-line.

Considerations

What initiatives can you think of to safeguard access to data housed at data centers at risk from water and electrical interruptions and other damages from wildfire, high wind, high temperatures, and rising sea-levels?

- *How can you support critical infrastructure partners in becoming more informed about vulnerabilities to data centers and potential risks to the data housed there?*
- *What plausible steps can the federal government take to safeguard data housed in data centers? How might CISA specifically contribute?*

APPENDIX V: POLITICAL DISRUPTOR

1. LACK OF NATIONAL PRIVACY LEGISLATION

In 2024, the European Court of Justice rules that the U.S. cannot be trusted as a safe destination for transferring, storing, or processing EU citizen data. In light of this ruling, U.S. organizations are now scrambling to figure out how to identify and separate the data of EU citizens and make alternative storage arrangements. Additionally, since diversifying datasets is key to developing better algorithms and training them, having EU data is absolutely crucial for U.S. AI research and development efforts. Without this data, the U.S. risks falling behind to competitors like China.

Considerations

What initiatives can you think of to mitigate the effects of differing legislation and requirements between the U.S. and the EU for data transferring, storage, or processing?

- *Would this scenario lead to further implications for data storage, processing, and transfer with other countries?*
- *What plausible steps can the federal government take to support critical infrastructure partners' efforts to comply with EU requirements without sacrificing AI research and development? How might CISA specifically contribute?*
- *What provisions might need to be added to a U.S. version of data privacy legislation?*

2. FRACTURING GLOBAL INTERNET

Following trends in digital sovereignty and as a reflection of India's own nationalist movement, Indian Prime Minister Narendra Modi, after claiming a third term in 2024, declares that India will segment its internet from the global internet as a matter of "Indian national security." India will follow China's "Great Firewall" model, which famously employs filters to selectively block certain internet sites, words, IP addresses, and so on. Further, all data on Indian citizens must be stored in India.

The growing fragmentation of the internet is problematic for the Border Gateway Protocol, which is the global navigation system that manages the flow of data around the world. Incompatibility between web services, communication standards, and hardware devices are causing a growing number of problems with information routing, with potentially severe effects on international businesses. For instance:

- *A routing error caused all traffic to a popular music streaming site to be temporarily routed to a small Pennsylvania construction company's website for almost an hour.*
- *Large chunks of network traffic belonging to MasterCard, Visa, and more than two dozen other financial-services companies were routed briefly through a Russian telecom, exposing millions of customers' personal and financial data.*
- *An international shipping company found that a problematic latency in its data traffic, which was impacting its operations, was caused by malicious rerouting of internet traffic.*

Considerations

How should critical infrastructure owners and operators prepare for a future in which international data and transmission protocols are less readily available or not available at all?

- *What actions could CISA and the federal government take to address the failure of international protocols for managing data transmission? What mitigation actions could be taken now to prepare for that future?*
- *The global trend towards cyber sovereignty is driven by a combination of concerns about U.S. surveillance, digital colonialism, being trapped between China and the U.S.'s great-power politics, protectionism for domestic industries, and genuine concerns about security risks inherent in the global internet model. What can CISA and the federal government do to increase faith in the global internet and reduce the temptation to opt-out?*