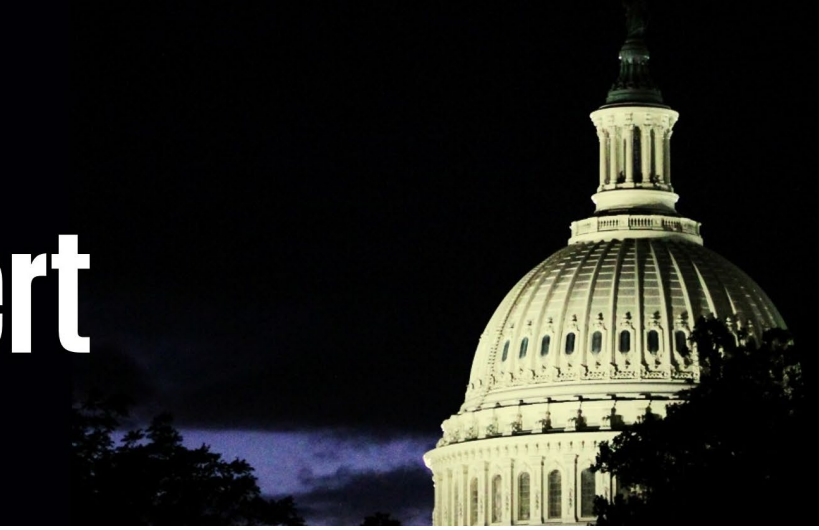
KPMG

Regulatory Alert

Regulatory Insights



March 2023

White House Announces National Cybersecurity Strategy

KPMG Regulatory Insight:

- *The Administration's strategy, which builds on a previous Executive Order and other efforts, stresses the importance of public-private collaboration to achieve its cybersecurity goals.*
- *Key objectives include:*
  - *Shifting liability for software products and services to promote security development practices*
  - *Ensuring that Federal grant programs promote investments in new infrastructure that are secure and resilient*
- *Areas of regulatory focus will include:*
  - *Strength of cybersecurity risk management and governance*
  - *Threat and vulnerability management*
  - *Identity and access management*
  - *Compliance with incident response and reporting requirements*
  - *Consumer data collection and use*
  - *Consumer data privacy*

(See KPMG Regulatory Insights' 2023 Regulatory Challenges: Data and Cybersecurity; Technology and Resiliency.)

The White House announced a new National Cybersecurity Strategy (Strategy) that builds on the May 2021 Executive Order "Improving the Nation's Cybersecurity." The Strategy outlines the Administration's approach to cybersecurity, which entails building and enhancing collaboration between the public and private sectors along five pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

To achieve the envisioned collaboration, the Administration suggests there is a need to make two fundamental shifts in cybersecurity roles, responsibilities, and resources:

- *Rebalance the Responsibility to Defend Cyberspace*, including protecting data and assuring reliability of critical systems, to the owners and operators of critical systems that hold data and enable society to function, as well as technology providers that build and service these systems.
- *Realign Incentives to Favor Long-Term Investments* that lay a strong, resilient foundation to build the future of a digital ecosystem.

To that end, the Strategy calls for:

- New legislation, including bills to address
  - Liability for software products and services, a safe harbor framework, and vulnerability disclosures
  - Limits on collection, use, transfer, and maintenance of personal data along with national requirements to secure personal data.
- New and updated cybersecurity regulations, utilizing frameworks "tailored for each sector's risk profile,

harmonized to reduce duplication," and "calibrated to meet the needs of national security and public safety."

Highlights of the Strategy follow.

National Cybersecurity Strategy

The five pillars and underlying strategic objectives (outlined below) are intended to address what the Administration characterizes as software and systems that are becoming increasingly complex, providing value to companies and consumers, but also increasing collective insecurity by "layering new functionality and technology onto already intricate and brittle systems at the expense of security and resilience."

Pillar One – Defend Critical Infrastructure:

The Administration notes that cybersecurity requirements have been proposed or finalized for several industries, including owners and operators of critical infrastructure, banking organizations, public companies, and others. (For more details, see KPMG Regulatory Insights' Point of View: *Enhancing the cybersecurity risk framework*). The Strategy calls for collaboration between industry, owners and operators of critical infrastructure, federal agencies, product vendors and service providers, and other stakeholders to achieve the following strategic objectives:

- Establishing cybersecurity requirements to support national security and public safety
- Scaling public-private collaboration
- Integrating federal cybersecurity centers
- Updating federal incident response plans and processes
- Modernizing federal defenses

Pillar Two – Disrupt and Dismantle Threat Actors

The Strategy calls for the integration of diplomatic, information, military (both kinetic and cyber), financial, intelligence, and law enforcement capabilities with the goal of making "malicious actors incapable of mounting sustained cyber-enabled campaigns that threaten the national security or public safety of the United States." Strategic objectives include:

- Integrating federal disruption activities
- Enhancing public-private operational collaboration to disrupt adversaries
- Increasing the speed and scale of intelligence sharing and victim notification
- Preventing abuse of U.S.-based infrastructure
- Countering cybercrime, defeating ransomware

Pillar Three – Shape Market Forces to Drive Security and Resilience

Citing continued disruptions of critical infrastructure and thefts of personal data, the Strategy calls for shaping markets forces "to place responsibility on those within the digital ecosystem that are best positioned to reduce risk." This includes using federal purchasing power and grant-making to incentivize broad adoption of best practices in cybersecurity and resilience to achieve the following strategic objectives:

- Holding the stewards of consumer data accountable
- Driving the development of secure "Internet of Things" (IoT) devices
- Shifting liability for insecure software products and services to entities that fail to take reasonable precautions to secure their software
- Using federal grants and other incentives to build in security
- Leveraging federal procurement to improve accountability
- Exploring a federal cyber insurance backstop

Pillar Four – Invest in a Resilient Future

The Strategy calls for leveraging strategic public investment in innovation, R&D, and education through multiple programs, including some new grant programs and funding opportunities established in the 2021 Infrastructure law and 2022 Inflation Reduction Act (See KPMG's Regulatory Alerts, here, here, and here). Strategic objectives include:

- Securing the technical foundation of the internet
- Reinvigorating federal research and development for cybersecurity
- Preparing for our post-quantum future
- Securing our clean energy future
- Supporting development of a digital identity ecosystem
- Developing a national strategy to strengthen our cyber workforce

Pillar Five – Forge International Partnerships to Pursue Shared Goals

To "counter common threats, preserve and reinforce global internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible," the Strategy calls for working to scale the model of collaboration by national cybersecurity stakeholders (described above) to cooperate with the international community. Strategic objectives include:

- Building coalitions to counter threats to our digital ecosystem

- Strengthening international partner capacity
- Expanding U.S. ability to assist allies and partners
- Building coalitions to reinforce global norms of responsible state behavior
- Securing global supply chains for information, communications, and operational technology products and services

Implementation

Under the oversight of staff from the National Security Council, the Office of National Cyber Director (ONCD) will coordinate implementation of the Strategy, including working with interagency partners to develop and publish implementation plans.

For more information, please contact Amy Matsuo or Charlie Jacco.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia