KPMG

Regulatory Alert

Regulatory Insights



November 2026

Cybersecurity: CISA 2030 Strategy

KPMG Regulatory Insights:

Strategic Direction: *Establishes CISA's roadmap for cybersecurity and critical infrastructure priorities through 2030, advancing the White House's recent cyber and national resilience strategies.*

Prioritizing Risk: *Promotes risk-informed analysis to direct attention, investment, and operational effort on hardening infrastructure whose disruption would have the most severe consequences.*

The Road Ahead: *Implementation relies on broad public-private collaboration and coordination to address the increasing complexity and interconnectedness of the cyber threat landscape; consistent with the National Resilience Strategy, focus on national security, economy, public health and safety, and national infrastructure.*

The Cybersecurity and Infrastructure Security Agency (CISA) published its new strategy, "CISA 2030: Defend, Harden, Prevail," which orients the agency's planning and activities through 2030 around three pillars representing CISA's priorities. The strategy builds on the "Cyber Strategy for America," the White House's overarching policy architecture for cybersecurity and resilience (see KPMG Regulatory Alert here), and the National Resilience Strategy.

The three pillars of CISA's strategy include:

- Pillar 1 - "Defend": Detecting, disrupting, and mitigating cyber threats.
- Pillar 2 - "Harden": Prioritizing threats to national infrastructure based on risk and consequences.
- Pillar 3 - "Prevail": Mobilizing resilience through capabilities, planning, and partnerships.

CISA outlines a phased process for implementing the strategy:

- Within 60 days (approximately December 25, 2026), begin a programmatic review of its core services and capabilities.
- Within 180 days (approximately April 24, 2027), deliver an implementation and measurement approach for outcomes aligned to the pillars and objectives.
- Within 365 days (October 26, 2027), deliver a progress report on implementation.

For each pillar, the strategy sets the following key objectives:

Pillar 1: Defend

The cyber threat landscape is more complex and interconnected

Detecting, disrupting, and mitigating cyber threats and building confidence in information security systems, data, networks, and infrastructure, including:

- Integrating capabilities across federal government, State, Local, Tribal, and Territorial (SLTT) partners, industry and international organizations.
- Strengthening security and resilience of operational technology (OT), including asset visibility, anomaly detection, and supply chain integrity.

KPMG

© 2026 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

- Developing software security guidance and best practices.
- Assessing, deploying, and securing innovative technologies across industry and government.

Pillar 2: Harden

Protection of critical infrastructure is a national security and economic imperative

Prioritizing threats to national infrastructure that pose the highest risks and highest consequences, through risk-informed, consequence-based analysis to focus attention and investment, including:

- Integrating intelligence from industry and agency partners, including the intelligence community, to accelerate operational response.
- Analyzing infrastructure data to develop the National Risk Register and to prioritize and quantify risk.
- Building partnerships and collaboration frameworks for Sector Risk Management Agencies (SRMAs), SLTT partners, regions, states, communities, and owners and operators.
- Working with CISA's partners to strengthen the most essential U.S. critical infrastructure.

Pillar 3: Prevail

Defense requires a more agile, collaborative, and distributed approach

Mobilizing national resilience by transformation of capabilities, continuity of operations, coordinated planning efforts, and public-private partnerships, including:

- Advancing regional capabilities through CISA's ten regional offices, including rapid mobilization of cyber and physical security tools.
- Strengthening interoperability and continuity of National Security and Emergency Preparedness (NS/EP) communications (e.g., voice, video, data).
- Modernizing planning and exercise capabilities, including cross-sector collaboration.
- Building next-generation, interoperable infrastructure for resiliency in emergency communications, and continuity of essential functions.

For more information, please contact Michael Isensee or Matt Miller.

Contact



Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com



Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.