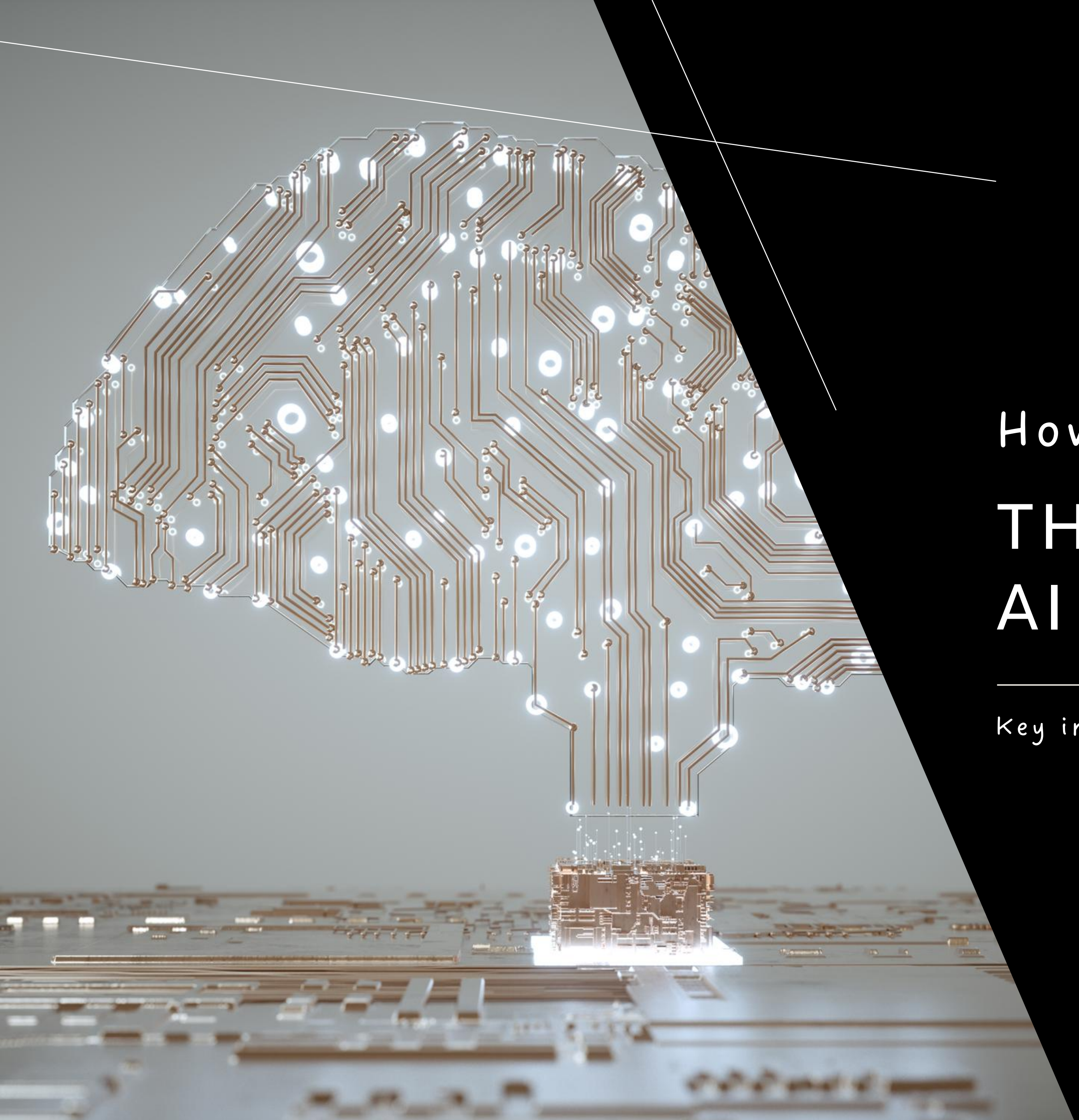
ResilientTech Advisors | July 2025



How business leaders can leverage

THE WHITE HOUSE'S AI ACTION PLAN

Key insights & actions for navigating the 2025 AI landscape

THE WHITE HOUSE’S AI ACTION PLAN OUTLINES A COMPREHENSIVE FEDERAL STRATEGY TO STRENGTHEN U.S. AI LEADERSHIP ON THE GLOBAL STAGE.

Released in July 2025, the plan focuses on rapidly accelerating AI development, building national infrastructure to support it, & aligning international alliances to protect U.S. technological leadership.

The plan is organized into three pillars.

1. **Accelerate** AI Innovation
2. **Build** American AI Infrastructure
3. **Lead** in International AI Diplomacy & Security

Cross-Cutting Themes

- **Speed & deregulation** are prioritized across every pillar.
- **National security, economic competitiveness, & freedom of expression** are cited as guiding principles.
- **Government coordination will be led by new interagency councils** focused on AI adoption, risk, & infrastructure buildout.

Winning the Race, AMERICA’S AI ACTION PLAN

PILLAR I: ACCELERATE AI INNOVATION

Deregulation First: Rescinds prior executive orders & FTC actions seen as barriers to innovation. Directs funding away from states with restrictive AI laws.[1]

Open-Source Support: Encourages development & global adoption of open-weight AI models aligned with U.S. values.[2]

Free Speech Protections: Orders revisions to NIST's AI Risk Management Framework to eliminate language on misinformation, DEI, & climate change.[3]

Sector-Based AI Adoption: Launches regulatory sandboxes & standards for AI use in healthcare, defense, & energy.

Workforce Transition: Calls for rapid retraining programs, apprenticeships, & AI literacy across the U.S. labor force.

Scientific AI Investment: Supports AI-enabled labs, open scientific datasets, & research into AI interpretability, safety, & evaluation.

Federal & Defense AI Use: Accelerates government AI adoption through procurement reform, workforce exchanges, & DoD-specific AI initiatives.

[1] **Federal Trade Commission (FTC)** is the U.S. agency responsible for enforcing antitrust law and protecting consumers from deceptive or unfair business practices, including AI-related claims & market behaviors.

[2] **Open-weight AI models** are shared publicly so others can use or build on them, unlike private models that keep their inner workings secret.

[3] The **NIST AI Risk Management Framework** is a voluntary guidance document for managing risks across the AI lifecycle.

PILLAR II: BUILD AMERICAN AI INFRASTRUCTURE

Data Center Expansion: Streamlines environmental permitting for AI infrastructure on public lands.

Grid Modernization: Aims to stabilize & expand the national energy grid to meet rising AI demand.

Semiconductor Strategy: Focuses on reshoring chip production through deregulated CHIPS Act execution.[4]

Secure Federal Compute: Builds high-security data centers for classified AI work & national security use.

Skilled Trades Focus: Invests in trades like HVAC, electrical, & cloud systems engineering as critical AI enablers.

Cybersecurity & AI Resilience: Creates an AI-ISAC, enhances AI incident response, & promotes secure-by-design development practices.[5]

[4] The CHIPS and Science Act of 2022 provides over $50B in federal investment to boost U.S. semiconductor manufacturing, research, and workforce development. The AI Action Plan builds on this foundation by streamlining CHIPS funding and permitting for AI-aligned infrastructure and innovation. (CHIPS: Creating Helpful Incentives to Produce Semiconductors)

[5] ISACs (Information Sharing and Analysis Centers) are public-private partnerships that facilitate cyber threat sharing and coordination within specific sectors.

PILLAR III: LEAD IN INTERNATIONAL AI DIPLOMACY & SECURITY

Export U.S. AI Stack: Offers allies full-stack AI packages (chips, models, tools) with security-aligned standards.

Confront Chinese Influence: Pushes back on CCP-aligned AI norms in global forums.[6]

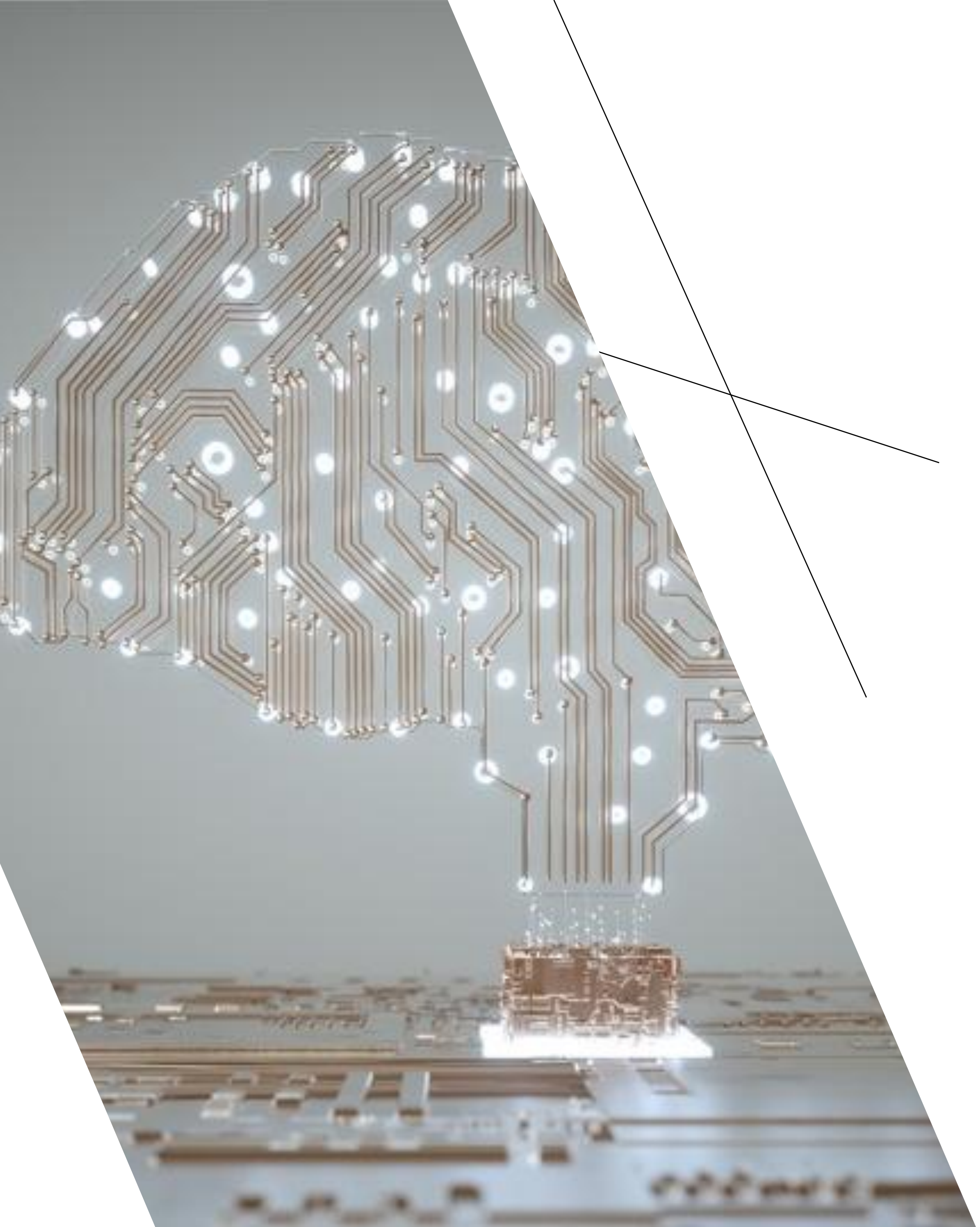
Enforce Chip Export Controls: Expands tracking of compute chips & closes export loopholes for subcomponents.

Align Allied Policies: Uses diplomatic pressure & trade tools to drive harmonized export & security controls.

Frontier Risk Evaluation: Evaluates both U.S. & foreign AI models for cyber, biological, & national security risks.[7]

6: **CCP refers to the Chinese Communist Party**, the ruling political party of the People's Republic of China.

7: **Frontier AI** refers to the most advanced general-purpose models. The U.S. aims to assess their potential misuse in areas like cyber attacks, biothreats, & national security, whether developed domestically or abroad.



AI IS NO LONGER A TOMORROW TOPIC. LEADERS NEED TO MAKE DECISIONS ABOUT AI TODAY.

Both public & private sector leaders face critical questions:

- Where can we use AI to **evolve our operations**?
- How do we align AI ambition with **operational & fiscal reality**?
- Are we securing **AI innovation & infrastructure**?
- How do we make sure **our IP** is protected?
- Are our **operations, data, security & legal** teams aligned?
- **Is our workforce ready** for what's next?
- Where are the ***real* risks** to data, operations, or trust?

HOW BUSINESS & TECNOLOGY LEADERS CAN LEVERAGE THE AI ACTION PLAN

Accelerate AI projects while the policy window is open - The plan emphasizes deregulation & speed. Now is the time to move bold ideas forward.

Secure your technical foundation - Infrastructure, compute, & talent are essential because they shape what's possible.

Build cross-border resilience - U.S. innovation may clash with stricter AI rules abroad. Expect compliance friction & adjust your global strategies.[8]

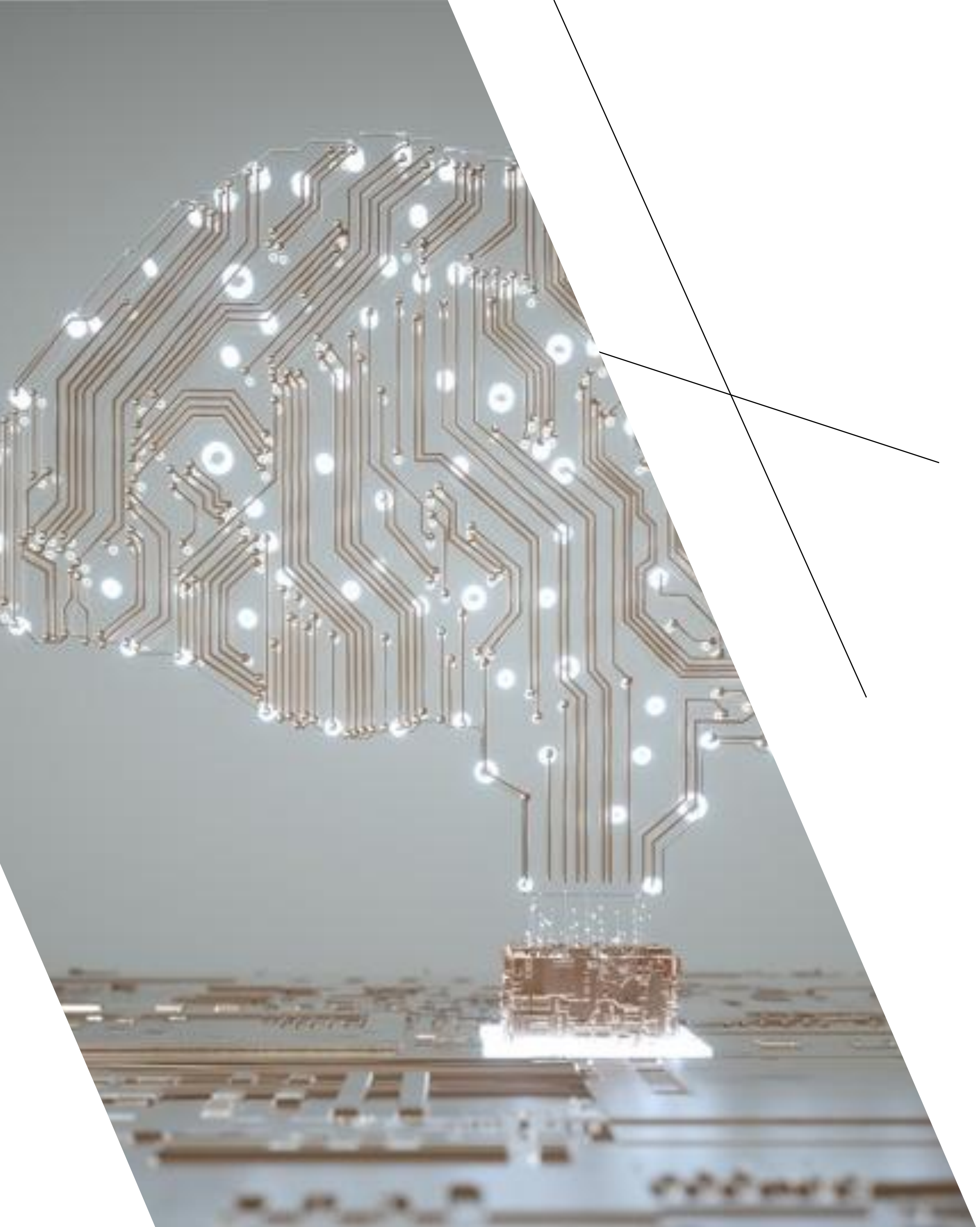
Avoid AI risk theater - Don't waste cycles on hypothetical threats. Focus on clear, high-value use cases & real-world security, privacy, & equity risks.

Get ahead of AI talent pressure - Skilled talent remains scarce. Build internal capabilities, re-skill teams, & prepare your organization for AI integration at scale.

Assess your AI alignment with national priorities - If you touch energy, health, manufacturing, or defense, your AI efforts may open doors to national partnerships (& heightened scrutiny). Operate accordingly.

Engage with interagency initiatives - Government AI councils are gaining momentum. Participation offers early access to threat intel, emerging policy, & public-private pilots.

8: While the U.S. emphasizes speed, allies like the EU (AI Act), Canada (AIDA), and Brazil (PL 2338/2023) are advancing stricter AI governance focused on transparency, accountability, & risk controls.



WE TURN STRATEGY INTO EXECUTION & FRICTION INTO CLARITY.

ResilientTech Advisors helps organizations:

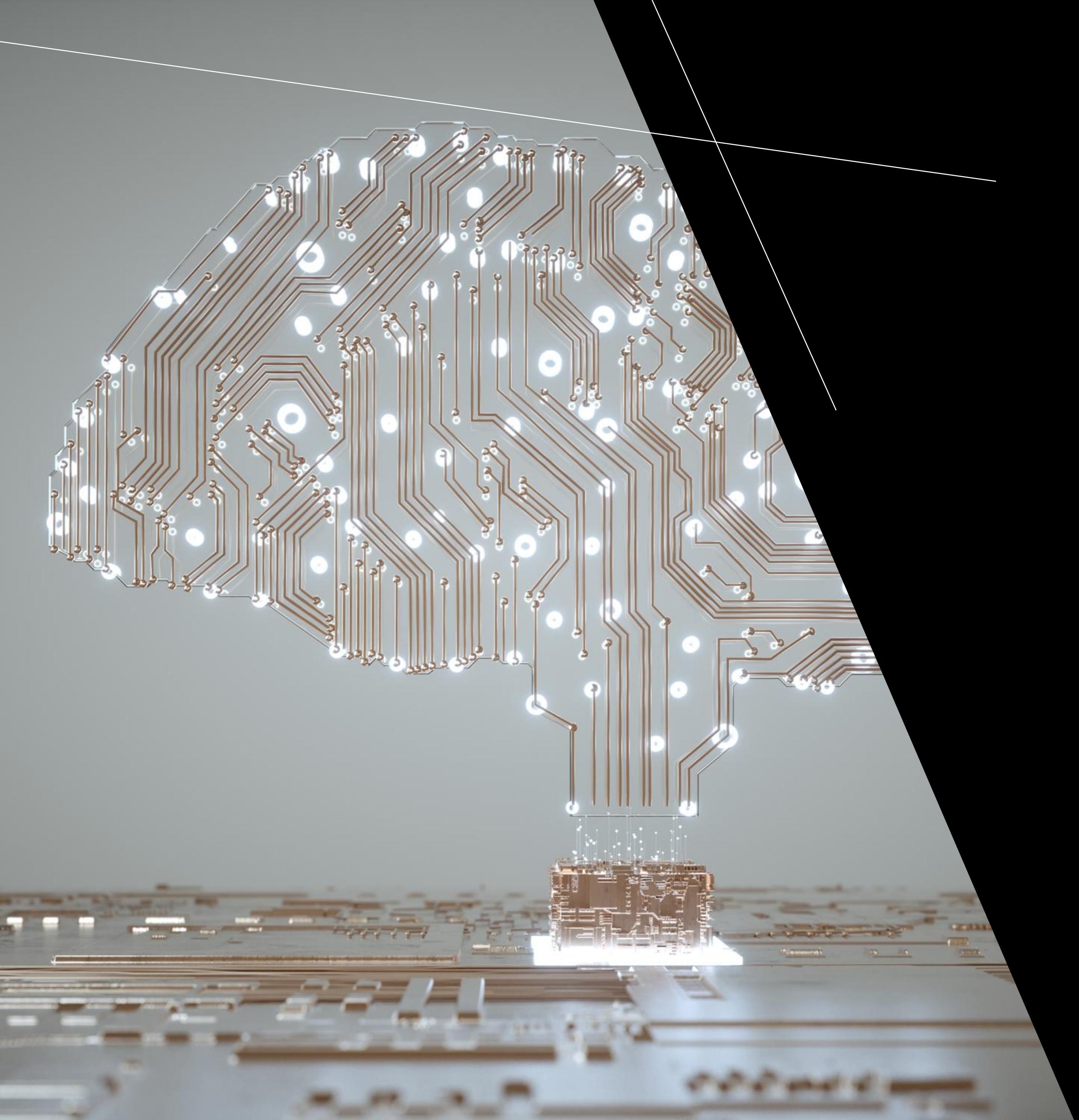
Evaluate readiness across identity, data protection, compliance, & third-party risk.

Translate AI strategy into action while protecting mission-critical systems & reputations.

Design security governance that supports innovation instead of blocking it.

Build cross-functional playbooks for AI risk, adoption, & workforce adaptation.

Engage CISOs & legal leaders early, so AI is resilient & responsible.



RESILIENTTECH ADVISORS HAS SUPPORTED AGENCIES MANAGING **$87B+** IN PUBLIC FUNDS, RESTORED TRUST AFTER MAJOR SECURITY INCIDENTS, & EMBEDDED AI INTO SECURE OPERATIONS WITH MEASURABLE RESULTS.

Whether you're scaling AI innovation, ensuring secure adoption, or preparing your workforce, we bring clarity & outcomes.

Contact us for a confidential conversation

ResilientTech Advisors
jchatman@resilienttechadvisors.com