Questions for the Record from Representative Darrell Issa for Mr. Nicholas Andersen
Protecting Our Edge: Trade Secrets and the Global AI Arms Race
May 7, 2025

---

1. **AI infrastructure is not currently treated or identified as "critical infrastructure" for cybersecurity purposes. What would identifying AI infrastructure as "critical infrastructure" mean from a cybersecurity standpoint? If AI infrastructure is added to an already long list of critical infrastructure, what resources will be needed to avoid overstretching? What other actions do you recommend?**

Designating Artificial Intelligence (AI) infrastructure as critical infrastructure would signal that the U.S. government recognizes its foundational role in economic competitiveness, national security, and information dominance. From a cybersecurity standpoint, this designation would:

- Prioritize AI providers for threat intelligence sharing through partnerships with agencies such as the Cybersecurity and Infrastructure Security Agency (CISA);
- Encourage or require actions such as those outlined in Executive Order (EO) 13636 or follow-on policy; and
- Open the door to voluntary CISA assessments and support mechanisms currently reserved for traditional critical infrastructure sectors.

That said, adding AI to the already broad list of critical infrastructure sectors risks diluting focus unless it's strategically scoped. I recommend we treat AI model training infrastructure, model weights, and underlying compute resources (especially significant Graphics Processing Unit (GPU) clusters and Large Language Model (LLM) data repositories) as assets that are treating as having higher consequence levels—equivalent to financial exchanges or bulk power systems.

To prevent overstretching CISA and Sector Risk Management Agencies (SRMAs), we should:

- Establish a distinct sub-sector under the Information Technology or Communications sectors;
- Use public-private partnerships to leverage the private sector's own visibility; and
- Focus federal support on crown jewel systems, not broad compliance burdens.

2. **Have U.S. AI companies done enough to protect their infrastructure from cyber breaches, and if not, what do they need to do differently?**

Most leading AI firms have taken cybersecurity seriously—but the stakes have changed, and their posture has not kept pace with the geopolitical threat environment. We're talking about infrastructure that, if exfiltrated or corrupted, could enable economic sabotage, disinformation at scale, or the advancement of adversarial military AI systems.

Key gaps include:

- Lack of consistent segmentation between dev, test, and deployment environments;
- Overreliance on internal trust models instead of zero trust principles;

- Insufficient red-teaming and adversarial testing of model integrity; and
- Weak tracking and protection of model weights, which are increasingly a national security asset.

Companies need to treat AI model weights and training infrastructure with the same rigor that defense contractors treat classified information.

3. **Has the U.S. government done enough to protect AI companies from cyber breaches? Is the threat of retaliatory cyber-activities a useful tool for dissuading malign activities? Should the U.S. government more aggressively use such tools?**

The government has not done enough to contextualize the threat environment for these companies —primarily because AI companies don't yet fall within prioritized protection frameworks like the Defense Industrial Base or designated critical infrastructure. However, I don't see a future where the U.S. government shifts to active defense of these companies.

We need:

- Better integration of AI firms into CISA-led ecosystems for pre-disruption intelligence sharing;
- Explicit Federal Bureau of Investigation (FBI) and Intelligence Community (IC) focus on counterintelligence risks facing AI labs and chip manufacturers; and
- Potential export control enforcement tied not just to physical chips, but intangible model access and technical talent.

As for retaliation: yes, cyber deterrence must be part of our arsenal. But retaliation must be proportionate, deniable when necessary, and tied to clear red lines. The U.S. must make it costly for state-sponsored Advanced Persistent Threats (APTs) to go after our crown jewel tech sectors—especially when those same adversaries are leveraging our innovation for military gain that seeks to hold our citizens and critical infrastructure at risk.

4. **Would addressing cyber threats alone be sufficient to protect the technological leadership of U.S.-based AI companies, or do other types of threats exist as well? Do large numbers of illegal immigrants entering the country put pressure on the resources available to identify and investigate individuals who pose risks of economic espionage and other insider threat activities?**

Cyber threats are only one vector. Insider threats, talent exfiltration, Intellectual Property (IP) theft via research collaborations, and influence operations are all being used by adversaries, particularly the Chinese Communist Party, to undermine our AI advantage.

The overwhelmed immigration and vetting system absolutely create vulnerability. DHS and FBI counterintelligence units are already stretched thin, and the resources needed to continue managing the fallout of mass illegal immigration diverts resources away from vetting visa holders, monitoring insider threats, and investigating foreign talent programs used to access U.S. labs and companies.

Questions for the Record from Representative Darrell Issa for Mr. Nicholas Andersen
Protecting Our Edge: Trade Secrets and the Global AI Arms Race
May 7, 2025

We need to:

- Reassert control of our borders;
- Prioritize counterintelligence resourcing; and
- Limit access to sensitive AI projects by individuals tied to foreign adversaries, especially where espionage risk is elevated.

Cybersecurity is critical—but if we ignore the human vector, we will lose the AI race not through malware, but through misjudged openness and unchecked infiltration.