Lili Colon

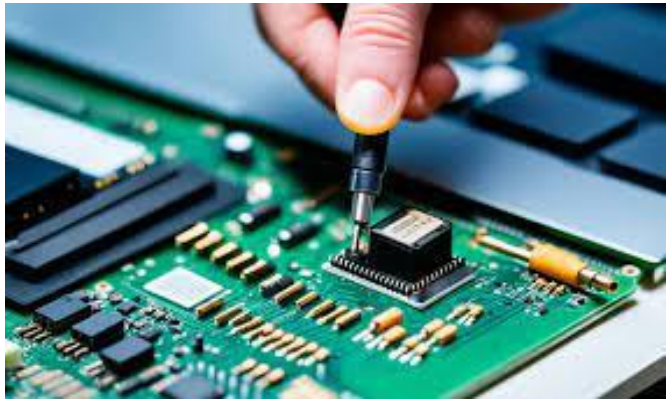
Principal Deputy Director

Office of Cybersecurity, Energy Security, and Emergency Response

U.S. Department of Energy

Threat and Hazard Types

Physical Security Attacks

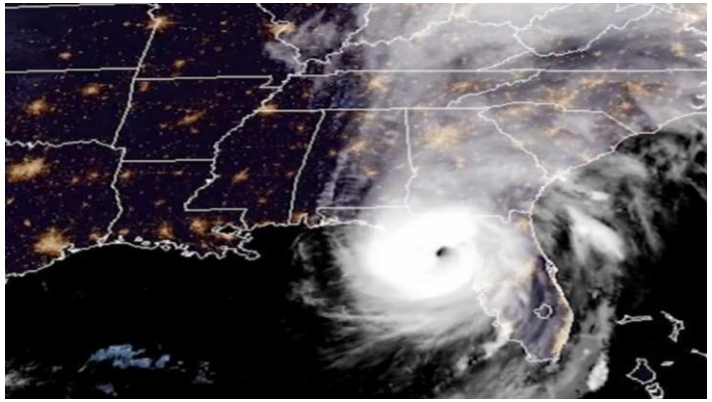


- Sabotage
- Vandalism
- Ballistic damage
- Electromagnetic Pulses (EMP)

Cybersecurity Attacks

- Transnational cyber criminals
- Critical infrastructure
- Industrial Control Systems
- Satellite communications
- Energy suppliers

Natural Hazards



- Extreme weather (hurricanes, tornados, floods, heat, wind, hail, snowstorms, etc.)
- Wildfire ignition
- Seismic activity
- Geomagnetic Disturbances (GMDs)

Cyber Threats Require Proactive Defense

- U.S. energy infrastructure faces threats from nation-state actors, cyber attacks, physical attacks, and natural hazard disruptions.
- Nation-state adversaries have been prepositioning inside U.S. critical energy infrastructure for years.
- These threats can have cascading effects on U.S. energy and interdependent sectors, including water, finance, telecommunications, and transportation.

Nation-State Cyber Threats

Methods applied by ransomware groups, hacktivists, and cyber criminals are faster, more prevalent and sophisticated than ever before, making detection and mitigation difficult for cyber specialists

CHINA – The most active and persistent cyber threat to U.S. critical infrastructure networks.

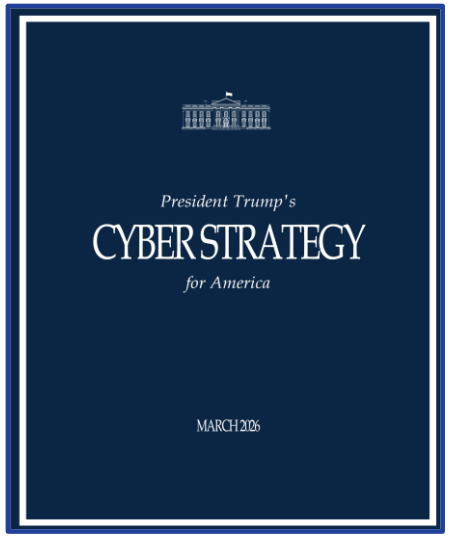
RUSSIA – Uses an array of tools that fall into the “gray zone” of geopolitical competition below the level of direct conflict

IRAN – Cyber operators have used cyberattacks against poorly defended targets and weaker opponents.

NORTH KOREA – Conduct cyber crimes and attacks to support the military and cyber espionage to fill gaps in weapons programs.

President Trump's Cyber Strategy for America

Builds upon earlier cyber-related actions and describes the Administration's policies and postures on cybersecurity to ensure that the U.S. is unrivaled in cyberspace



Six cross-cutting pillars for U.S. government and private sector coordination:

1. Shape Adversary Behavior — Layered cyber deterrence
2. Promote Common Sense Regulation — Streamline regulations
3. Modernize & Secure Federal Government Networks — Accelerate post-quantum cryptography, AI-enabled cyber security tools, and threat hunt-operations
4. Secure Critical Infrastructure — Prioritize identifying and protecting assets and supply chains
5. Sustain Superiority in Critical and Emerging Technologies — Quantum computing, cryptocurrencies, AI, and blockchain technologies
6. Build Talent and Capacity — Address cyber education & workforce needs

U.S. Department of Energy Strategic Goals

Roadmap to secure America's energy future, foster unparalleled scientific and technological innovation, and strengthen national security

1. Assert American Energy Dominance
2. Win the AI Race – Mission Genisis
3. Secure Critical Material Supply Chains
4. Catalyze America's Nuclear Energy Renaissance
5. Ensure Unrivaled American Leadership in Critical and Emerging Technologies
6. Accelerate National Security Programs

U.S. Department of Energy

Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

Mission

Strengthen the security and resilience of the U.S. energy sector

Vision

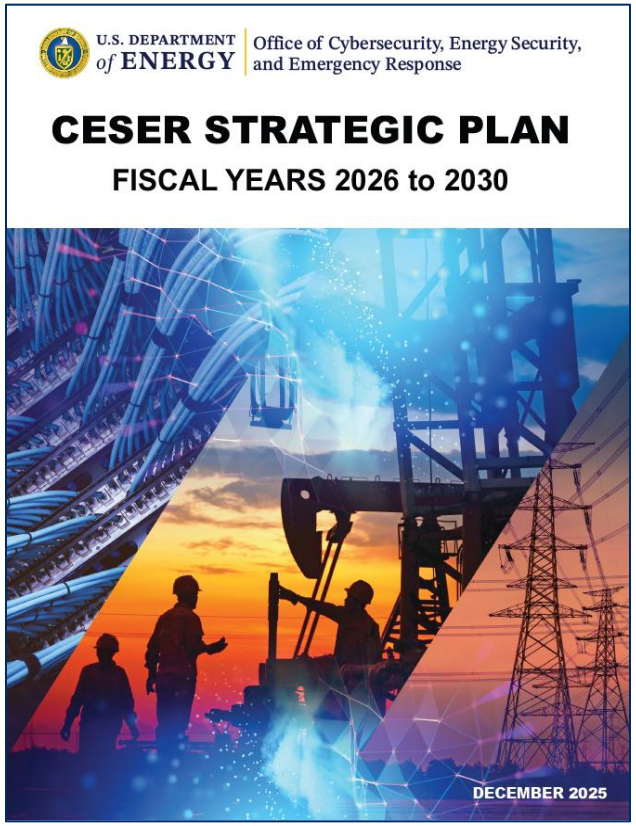
A secure, resilient, and adaptive energy sector capable of withstanding emerging threats and providing reliable energy for the national defense and all Americans

Sector Risk Management Agency (SRMA)

CESER is the designated SRMA for the Energy Sector

- Safeguards energy sector critical infrastructure
- Applies a risk-based approach that prioritizes national economic security, public health, and federal government essential functions
- Protects against all threats and hazards
- Invests in infrastructure modernization to advance physical and virtual assets and systems
- Engages in cross-sector partnerships to promote energy infrastructure security and resilience
- Coordinates U.S. government engagements with private sector partners

CESER Strategic Plan



The Strategic Plan lays the foundation for CESER and stakeholders working together to secure the U.S. energy sector over the next five years

The plan aligns the CESER mission with distinct goals, capabilities, and objectives

Guiding Principle

"Providing Timely and Actionable Information to the Energy Sector"

This principle is a catalyst for enduring alliances between CESER and the energy industry

Mutual focus is on reducing risk exposure and safeguarding infrastructure and supply chains from harm

CESER-sponsored programs engage energy owners and operators in addressing current and future threats effectively

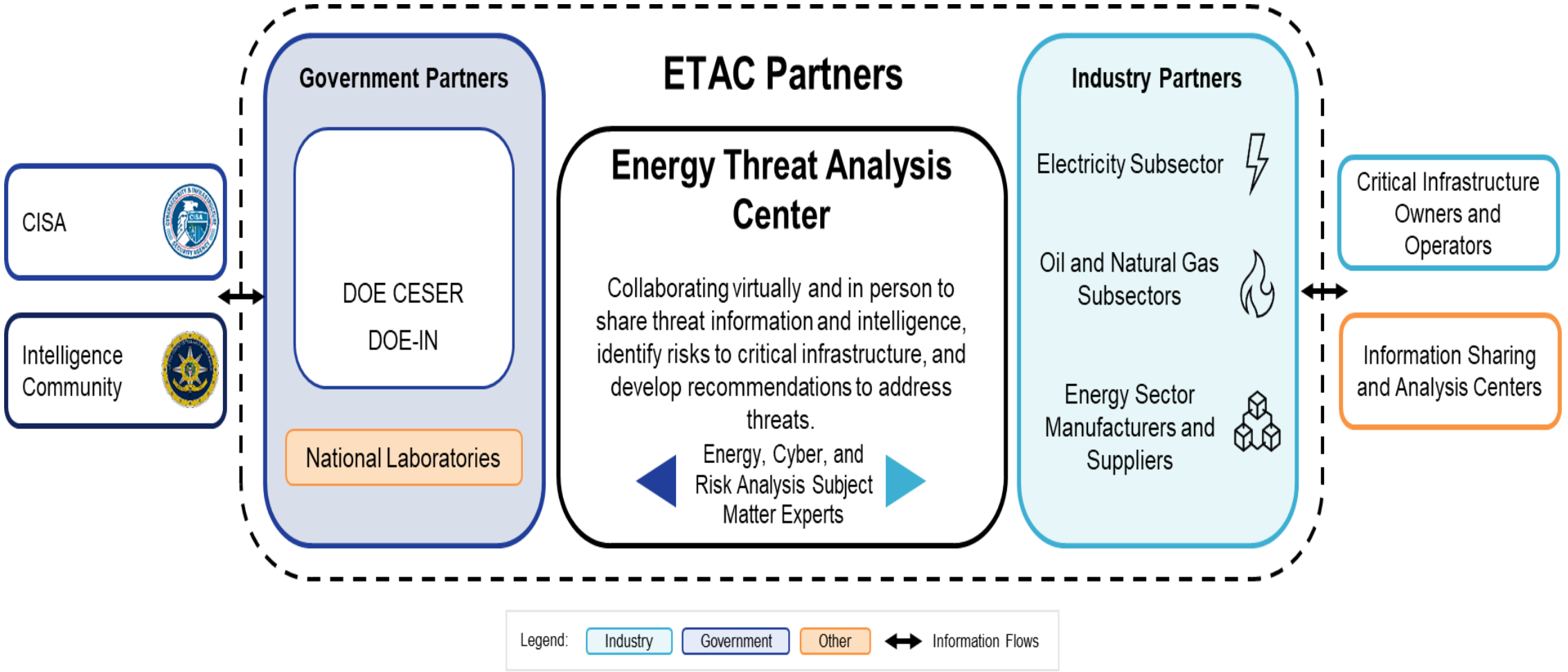
CESER is augmenting traditional threat analysis and reporting capabilities to improve critical infrastructure, prioritizing security, reliability, and efficiency of operations

"The Department of Energy is focused on the need to meet growing energy demand while strengthening the resilience and security of the U.S. energy infrastructure against all threats and hazards."

U.S. Secretary of Energy
Christopher Wright

◆ ETAC ◆ CyTRICS ◆ CRISP ◆ ESCC ◆ ONG SCC ◆ SLTT Program ◆

Guiding Principle – Energy Threat Analysis Center (ETAC)



Strategic Goal 1

Develop World-Class Security Technologies

A primary goal of CESER is to develop cutting-edge technologies useful to energy partners

CESER subject matter experts work with utility and oil and gas company cohorts on practical, scalable technologies

Their aim is to protect infrastructure, systems, and supply chains in real-time threat situations

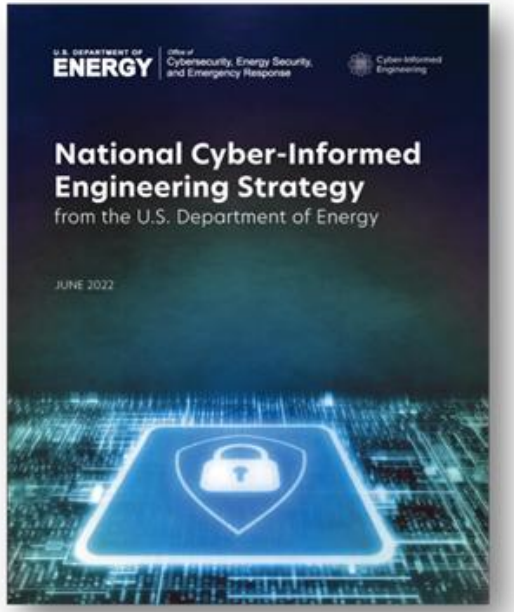
CESER technology projects anticipate the evolution of interconnected energy systems to improve resilience, security, and affordability

◆ AI FORTS ◆ CYBER-INFORMED ENGINEERING ◆ GENESIS MISSION ◆

Strategic Goal 1 – Cyber Informed Engineering

Cyber-Informed Engineering (CIE) prevents cyber attacks from affecting the safety, reliability and performance of critical energy systems

- CIE tools are adopted through training and application.
- By “engineering out” cyber risks at the earliest stages in design, energy systems can mitigate and eliminate cyber attacks.
- CIE Community of Practice has 350 members from 175 energy companies, vendors, engineering firms, universities, and standards organizations.



CESER Products

- CIE Adoption Pathway
- CIE controls database
- Model-based systems engineering
- Integrating into process automation
- Cyber conservative operations
- Curriculum Guide 2.0
- Hazards process analysis

Strategic Goal 2

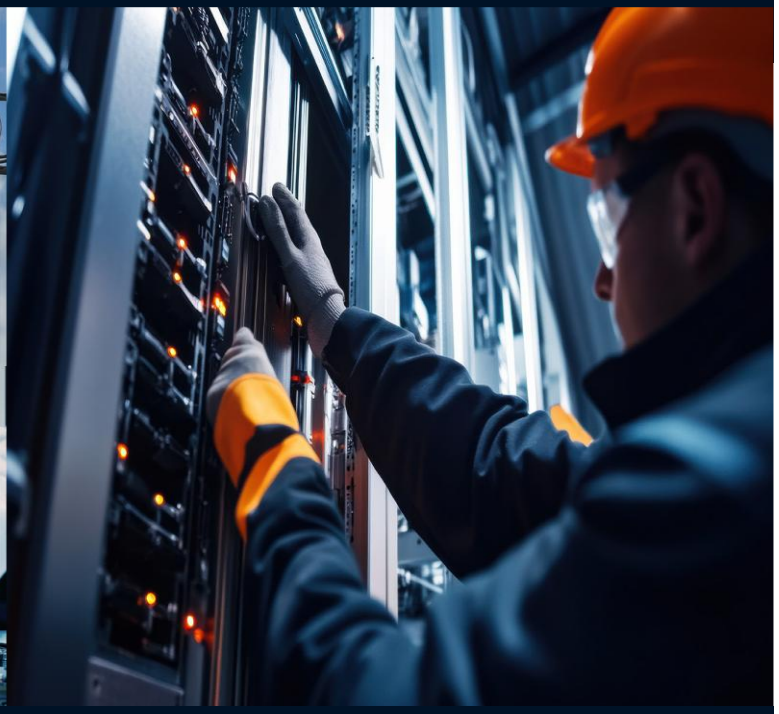
Harden U.S. Energy Infrastructure

CESER strives to improve energy system resilience for American communities and national security

CESER provides technical assistance to speed innovation on hardware, software, and equipment solutions

Hardening critical infrastructure encompasses:

- Cybersecurity measures
- Physical security
- Prototypes for effective recovery from disruptions Petroleum Reserve (SPR)
- to



◆ PROJECT ARMOR ◆ RMUC ◆ WORKFORCE DEVELOPMENT ◆

Strategic Goal 2 – Project ARMOR

Project ARMOR is a CESER multi-faceted cyber and physical security program to protect the U.S. Defense Critical Energy Infrastructure (DCEI)

CESER and energy sector partners are working together to:

- Identify the highest priority critical defense facilities (CDFs) at national security sites
- Perform assessments of security and resilience of the energy infrastructure providing power to the CDFs
- Harden CDFs through cyber and physical security enhancements
- Provide on-going monitoring, maintenance, and technical support

Generation Units

Transmission Circuit

Transmission Substation

Distribution Circuit

Distribution Substation

NG Compressor Station

Oil Refinery and Terminal Storage

Refined Product Pipelines

Refined Product Distribution Logistics

Strategic Goal 3

Respond and Recover from Incidents

CESER is the lead U.S. government coordinating agency for the energy sector during emergencies

When natural disasters, physical attacks, or cyber incidents occur, CESER intervenes to minimize disruptions and support reliable energy

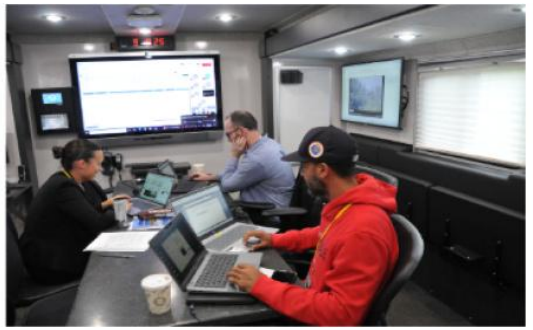
CESER has authority to issue emergency orders and concur with fuel standard waivers to deliver power and fuel

◆ ESF #12 ◆ EAGLE-I ◆ FPA § 202(c) ◆ INCIDENT RESPONSE ◆ EXERCISES ◆

Strategic Goal 3 – *Liberty Eclipse*

Liberty Eclipse is an annual full-scale cybersecurity preparedness exercise

- Federal and energy sector operational technology (OT) and cybersecurity experts come together to validate the security of cyber defense systems and incident response plans.
- Collaboration and testing results are used to make improvements in detection strategies and tools and Continuity of Service playbooks.
- Participants assess and defend OT equipment in a real-time, live testbed environment while attacked by national laboratory personnel leveraging real world adversarial tactics, techniques, and procedures.



Collaboration & Coordination

State, Local, Tribal, and Territorial (SLTT) Governments

NASEO
National Association of State Energy Officials

National Association of Regulatory Utility Commissioners

American Public Power Association

NCSL

NEMA™

National Governors Association

Energy Government Coordinating Council (EGCC)

Industry-Led Councils

ESCC
Electricity Subsector Coordinating Council

Oil and Natural Gas Subsector Coordinating Council

Central to the CESER mission is proactive collaboration with industry, federal agencies, international allies, and SLTT stakeholders

Sector Interdependencies

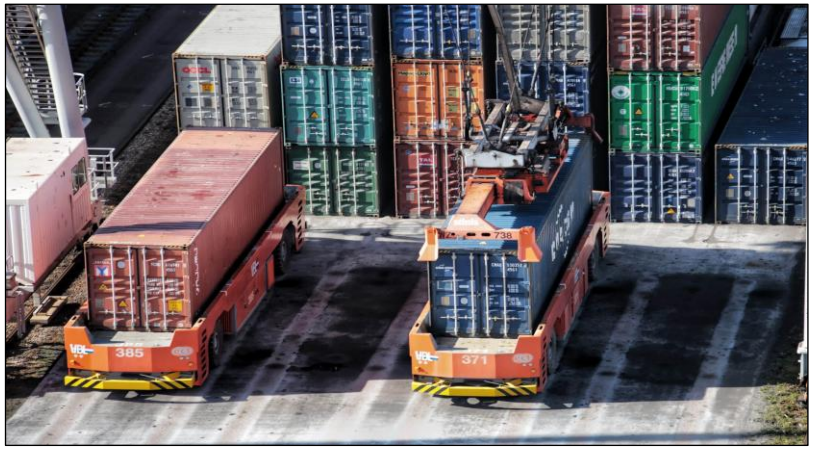
"Energy is the infrastructure of life… crucial to national security and the quality of life for all Americans."

U.S. Secretary of Energy Christopher Wright

- The energy sector has vital interconnected infrastructure components, a multi-faceted operational environment, and varied ownership and regulatory structures.
- CESER develops integrated cyber and physical security solutions to meet energy sector-specific needs and cross-sector dependencies.
- Through continuing proactive collaboration, CESER maintains real time situational awareness essential for rapid response to disruptions and crises.

CESER Successes

- **Supply Chain Cybersecurity Principles** – Strengthened manufacturer to end-user supply networks for cybersecurity and resilience
- **Research Projects** – Developed mitigation tools and technologies to secure energy systems from cybersecurity, physical threats, and hazards
- **AI-FORTS** – Investing in President Trump's Mission Genesis to secure networks from AI-enabled attacks and to use AI to protect energy critical infrastructure
- **Emergency Recovery and Response** – Apply emergency authorities (e.g. Federal Power Act § 202(c)) to support operations for multiple hurricanes, severe weather, extreme flooding, and other incidents.



Energy Resilience – A Shared Global Imperative

U.S. Government Commitments, Investments, and Collaboration

- President Trump's Cyber Strategy for America
- U.S. Department of Energy Strategic Goals
- CESER Strategic Plan

How can we be bold in meeting sector challenges together?

U.S. DEPARTMENT *of* ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response

THE DEAL IS PART OF THE DEFENSE

How security continues to evolve through the product, procurement, and the systems around them.

Lisa Carrington
Director Procurement
Arizona Public Service


RELIABILITY IS A SYSTEMS OUTCOME
Shaped not only by the technology itself, but by the systems around it.


THE DEVICE WAS NEVER THE WHOLE STORY
The people using it
The expectations around it
The vigilance required to defend

SUPPLY CHAIN IS BECOMING THE NEXT CHAPTER

Earlier product scrutiny
Smarter tool selection
Stronger supplier expectations

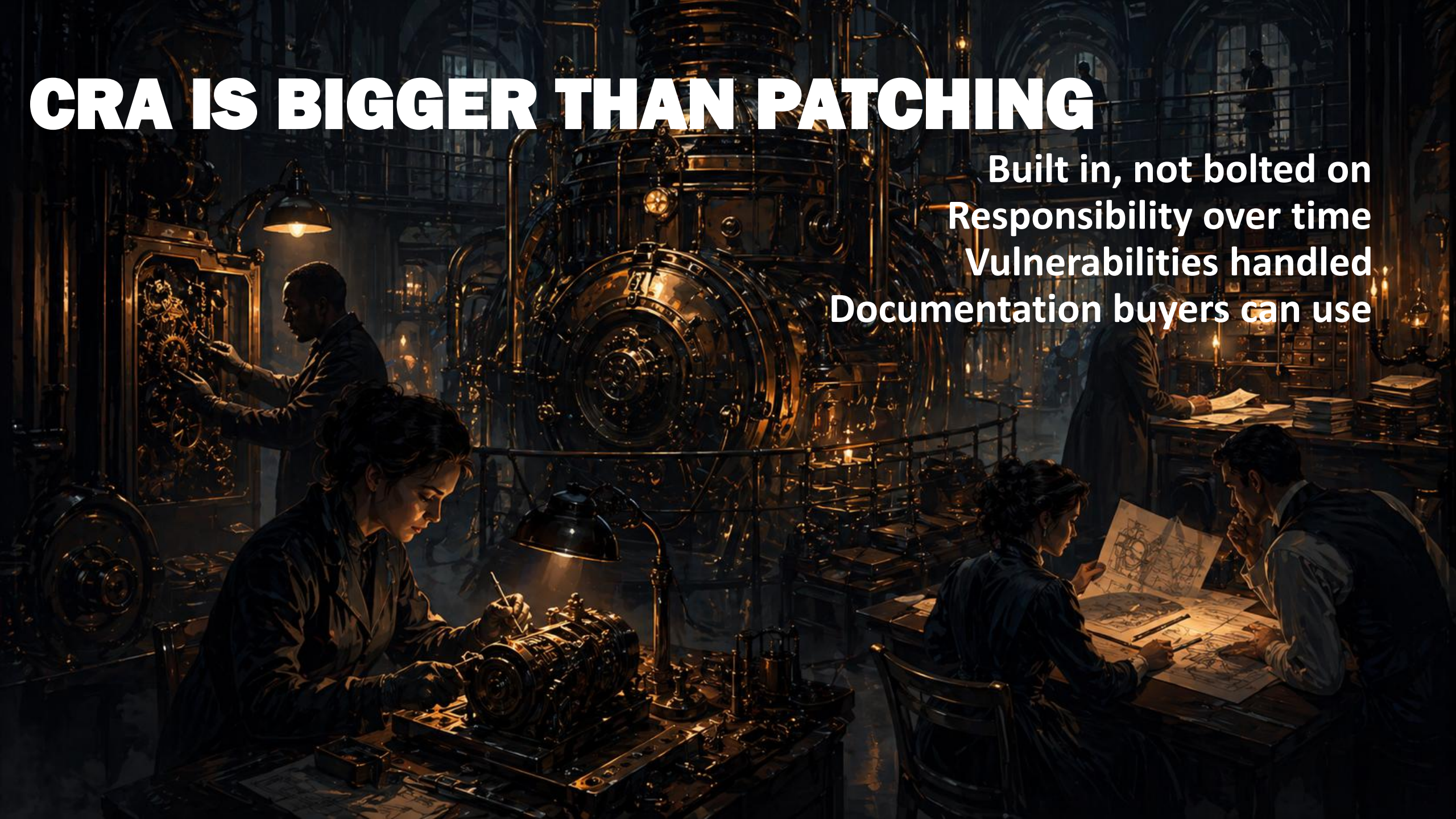

SUPPLY CHAIN SECURITY
IS EVOLVING

THREE SHIFTS WORTH WATCHING

Product security requirements are expanding
Sector specific expectations are being operationalized
Documentation and transparency is growing

CRA IS MOVING SECURITY UPSTREAM

Requirements start in the product
Manufacturers own more
Responsibility lasts longer


CRA IS BIGGER THAN PATCHING
Built in, not bolted on
Responsibility over time
Vulnerabilities handled
Documentation buyers can use


WHY SHOULD WE CARE ABOUT A EUROPEAN REGULATION?
Global suppliers
Changing artifacts
Changing expectations
Changing conversations

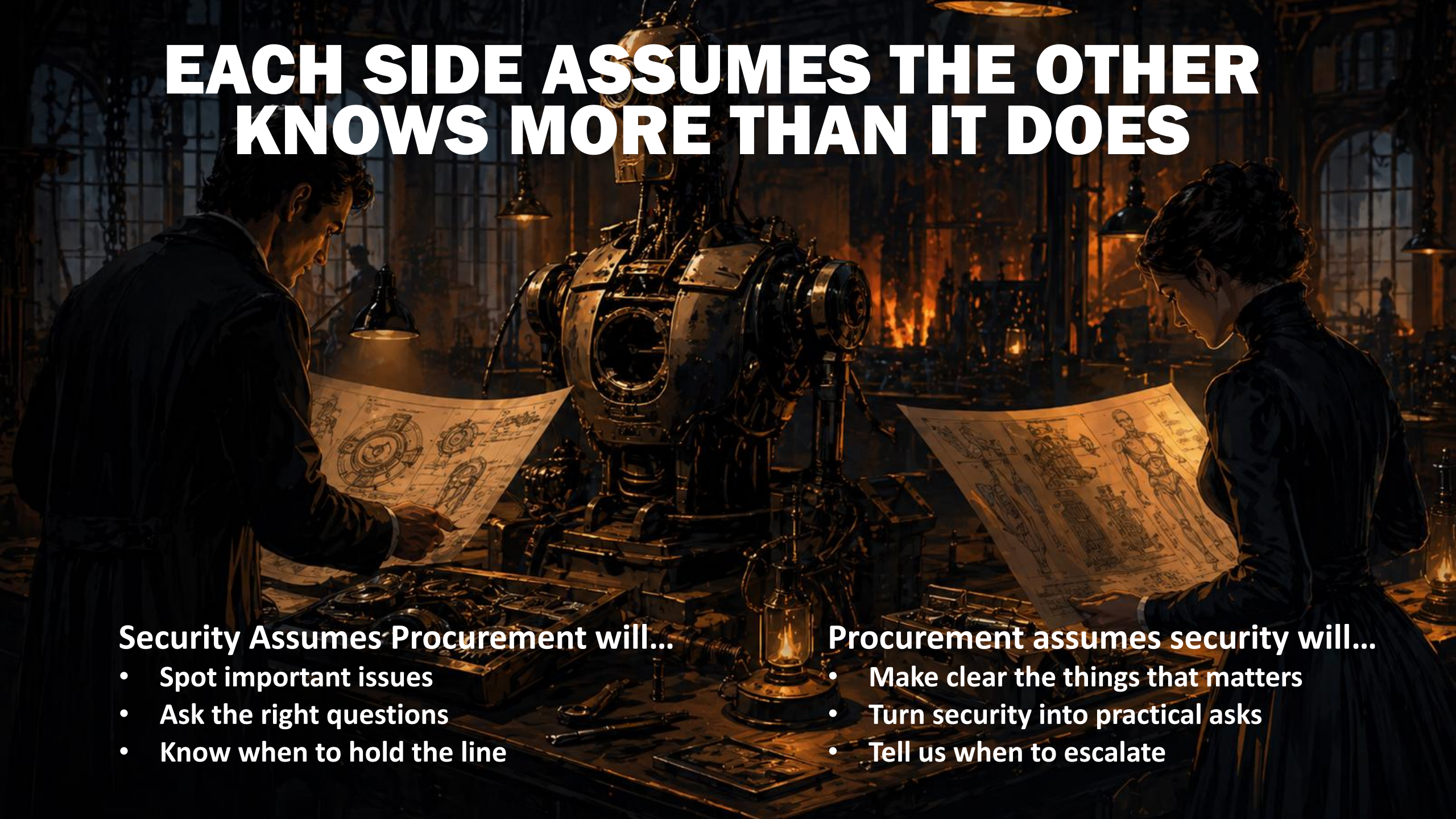

THE US UTILITY SECTOR IS GETTING MORE EXPLICIT TOO
Clearer trigger points
More practical procurement guidance
A wider supplier-risk lens

PROGRESS IS REAL. BUT IT STILL HAS TO BECOME ACTION

Better requirements
Better structure
Better visibility


THE GAP IS NOT AWARENESS
IT'S TRANSLATION

EACH SIDE ASSUMES THE OTHER KNOWS MORE THAN IT DOES



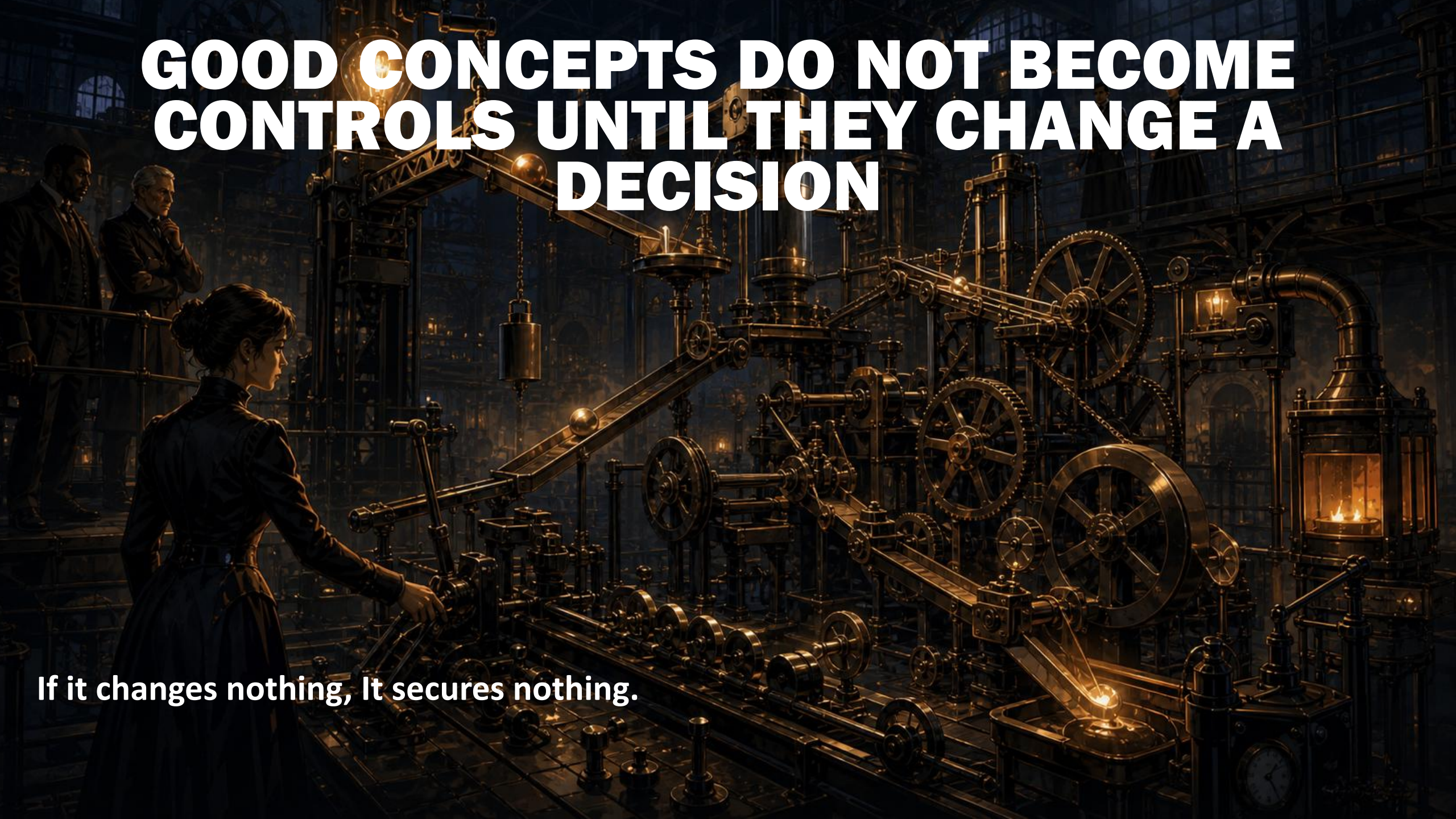
Security Assumes Procurement will…

- Spot important issues
- Ask the right questions
- Know when to hold the line

Procurement assumes security will…

- Make clear the things that matters
- Turn security into practical asks
- Tell us when to escalate

GOOD CONCEPTS DO NOT BECOME CONTROLS UNTIL THEY CHANGE A DECISION



If it changes nothing, It secures nothing.

WE LET SECURITY SLIP AWAY BEFORE WE EVEN BUY THE PRODUCT

In supplier questions
In evaluation criteria
In contract expectations

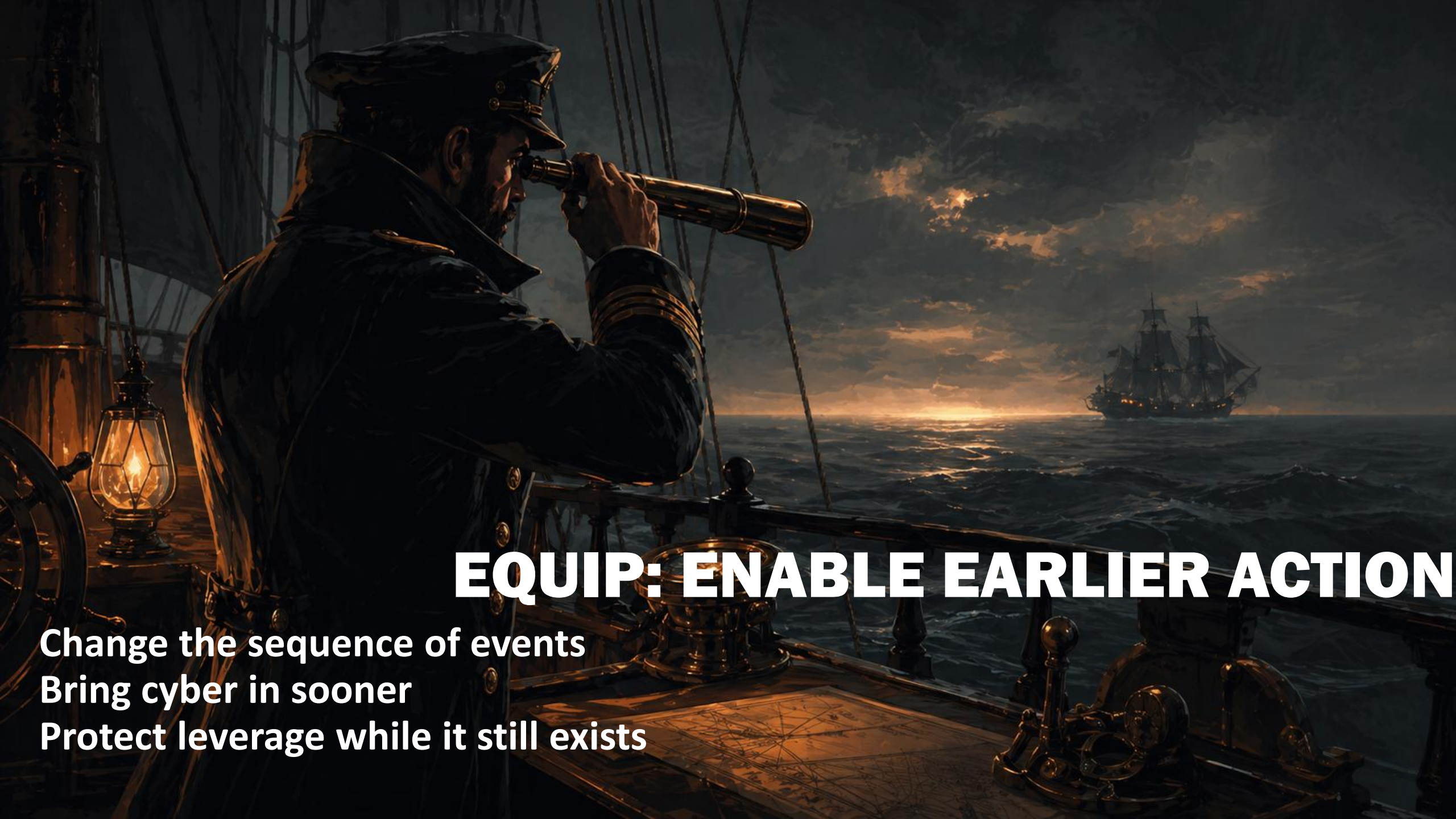

THE LAST OF THE LEVERS
Where choices still shape outcomes
Where expectations can still be set
Where signals can still be sent


Price
Speed
Commercial Risk
Supply Assurance
SECURITY ENTERS AN EXISTING DECISION MODEL


TRANSLATE - EQUIP - SIGNAL
Translate security into risk
Equip procurement to act
Signal to suppliers that security matters

TRANSLATE: HELP PROCUREMENT RECOGNIZE SECURITY RISK

What makes an offering riskier?
When does it deserve more scrutiny?
How does it change the buying approach?



EQUIP: ENABLE EARLIER ACTION

Change the sequence of events
Bring cyber in sooner
Protect leverage while it still exists


SIGNAL: MAKE SECURITY MATTER BEFORE THE AWARD
In what gets required
In what gets negotiated
In what gets preferred

SIGNAL: MAKE SECURITY MATTER IN THE CONTRACT

In commitments
In incentives
In consequences

SIGNAL: IT TAKES CARROTS TO CHANGE BEHAVIOR

Reward better security outcomes
Reduce friction for stronger suppliers
Make security visible in the economics

WHAT INCENTIVES ACTUALLY LOOK LIKE

Relationship Objectives:

Product Feature Reviews
Mutual Marketing
Security Roadmap Access
Discolsure Coordination

Financial Instruments:

Performance Bonds
Retainage Structures
Escrow Arrangements
Roadmap Agreements
Volume Incentives

Security becomes a way to create value while reducing risk


SIGNAL: KEEP REINFORCING IT AFTER AWARD
In reviews
In renewals
In repeated follow-up

SECURITY HAS TO BUILD THE RIGHT BRIDGE

Before there is a problem
Traveled In both directions
Strong enough to last

PRACTICAL THINGS YOU CAN DO

Pick one project or RFP

Learn the purchasing workflow, then improve it

Bring procurement into the mission

Teach basic security in procurement language

Build a carrot or two

Stay involved after award


THIS IS HOW SECURITY CONTINUES TO EVOLVE
In the devices themselves, and in the operational, regulatory, and human systems that surround them.

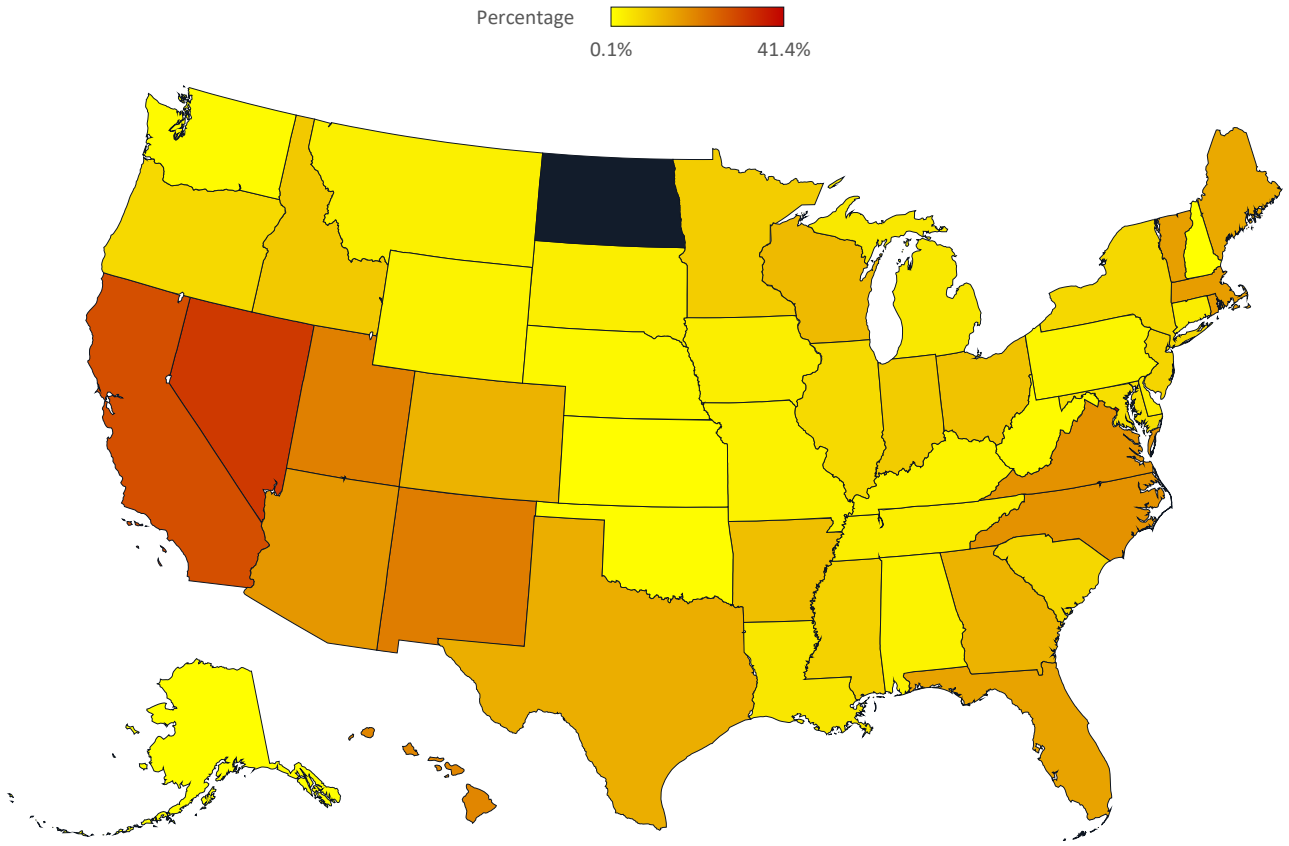

Questions
Pre-Purchase Risk Reduction Working Group
https://cabreza.com/initiatives/pre-purchase

IN BROAD DAYLIGHT

U.S. Grid Exposed to Risks from PRC-Made Inverter Equipment

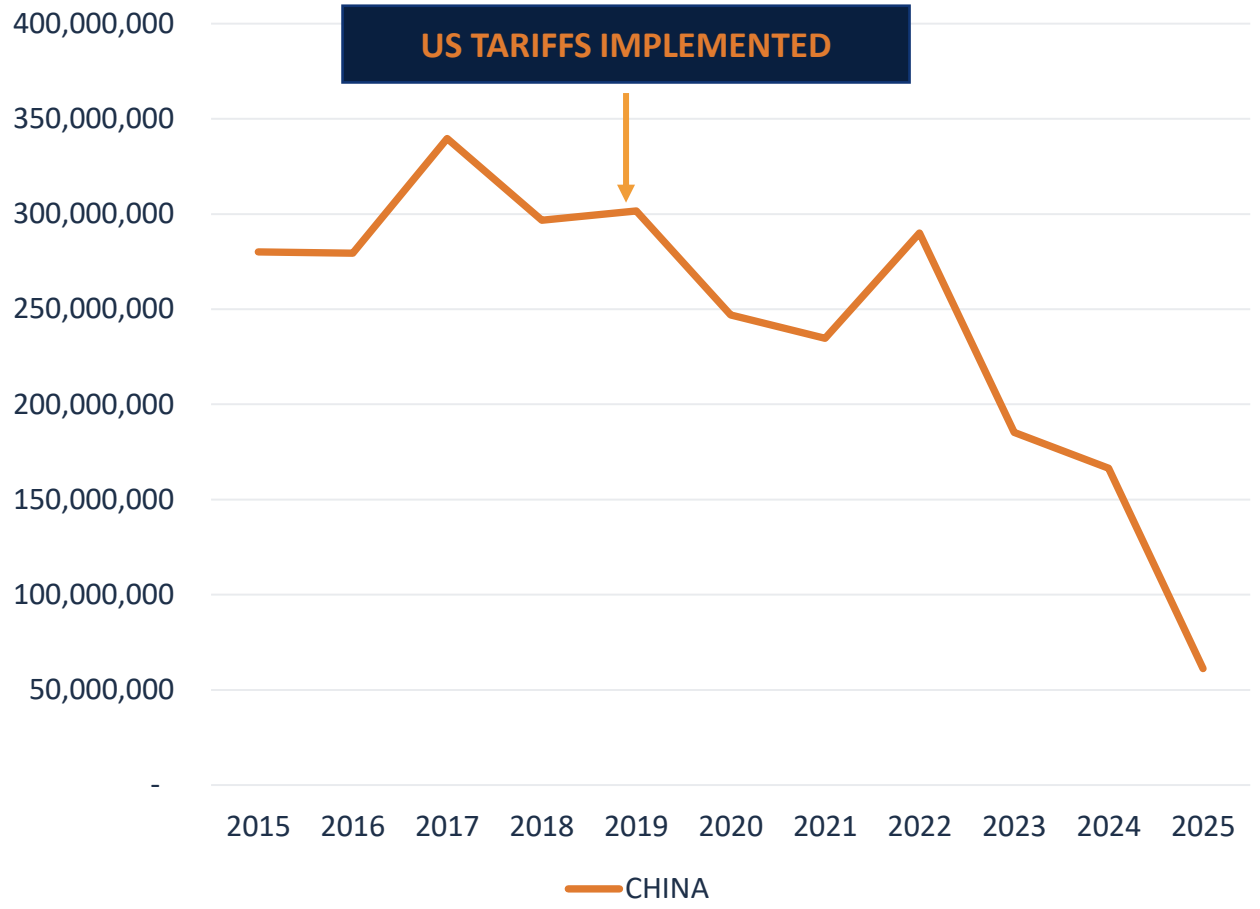
ENERGY IS INCREASINGLY DEPENDENT ON IBRs

- As of 2025, solar power accounts for roughly **10.3%** of US capacity.
- Roughly **80%** of new added grid capacity in 2025 were solar (~50%) and BESS (~30%).



PRC COMPANIES PLAY AN OUTSIZED ROLE

- The PRC exported **2.68 billion kg** of material classified under HTS code 8504.40.9570—which includes all sizes of inverters and BESS
- Despite U.S. tariffs in 2019, **the PRC has remained the largest exporter of IBR.**



SURVEY OF U.S. UTILITIES ON USE OF RISKY PRC SUPPLIERS

An analysis of energy and utility companies representing 12% of the U.S. grid identified at least **23 PRC inverter and Battery Energy Storage System (BESS)** suppliers integrated into U.S. infrastructure.

13 / 23

PRC companies have at least one Strider-designated statecraft risk.

86%

of the companies use inverters/BESS manufactured by risky suppliers.

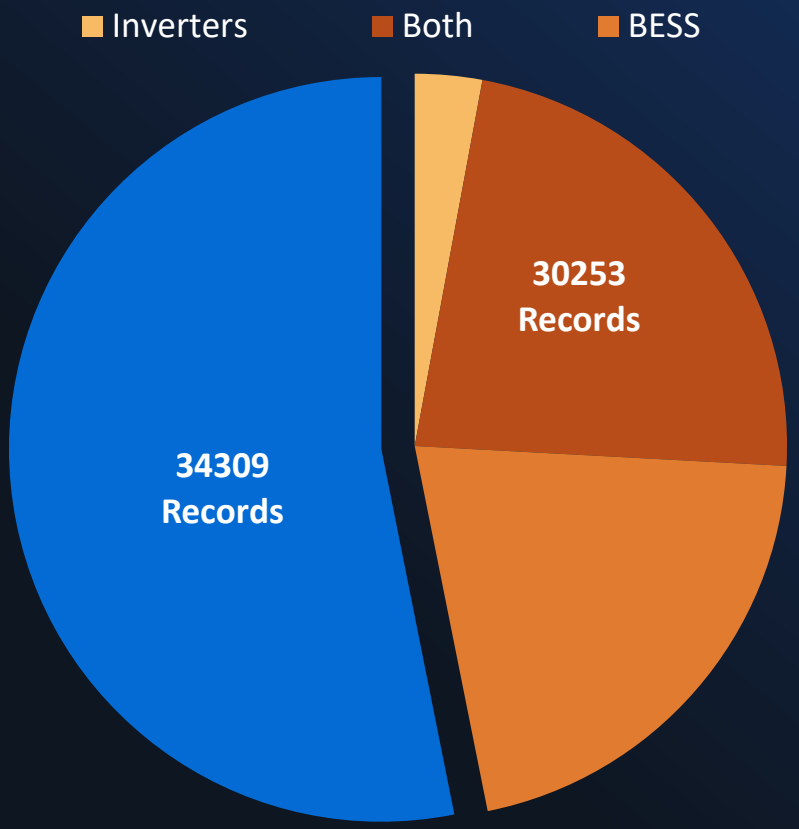
71%

of the companies use Sungrow inverters.

43%

of the companies use Huawei inverters.

INVERTER & BESS SHIPPING RECORDS (2015 to 2024)

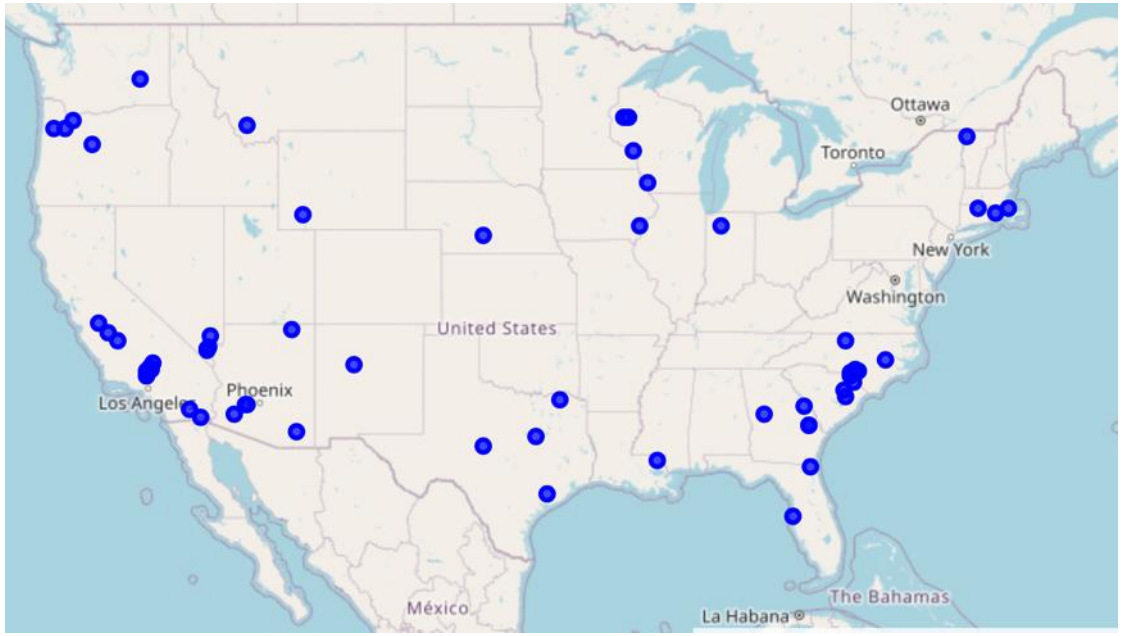


COMPANY	NUMBER OF RECORDS	PRODUCTS
Ecoflow	3829	BESS and Inverters
CATL	2572	BESS
Jinko Solar	2296	BESS and Inverters
JA Solar	1590	BESS and Inverters
CHINT/NOARK Electric	1186	Inverters
Huawei	498	BESS and Inverters
Sungrow	358	BESS and Inverters
GoodWe	120	BESS and Inverters
Gotion/Gotion High Tech	110	BESS
Other Risky Companies	17694	

THE U.S. RELIES ON PRC IBR EQUIPMENT

An analysis of 6,272 PV sites across 22 states identified 66 sites (with a combined installed capacity of 5,400 megawatts) operating inverters and BESS manufactured by **high-risk PRC companies.**

- 50 PV sites with **Sungrow** manufactured inverters
- 10 sites with **BYD** manufactured BESS
- 4 sites with **CHINT** manufactured inverters
- 1 site with **CATL** manufactured BESS
- 1 site with **Sungrow** manufactured BESS



HOW THE PRC IS TARGETING THE U.S. GRID

PRE-POSITIONING

In 2024, US intelligence services confirmed that PRC state-sponsored groups compromised energy networks.

REMOTE ACCESS + DESIGN KNOWLEDGE

Modern inverters are networked and remotely managed, increasing security risks.

In 2025, undocumented components were found in PRC-made inverters.

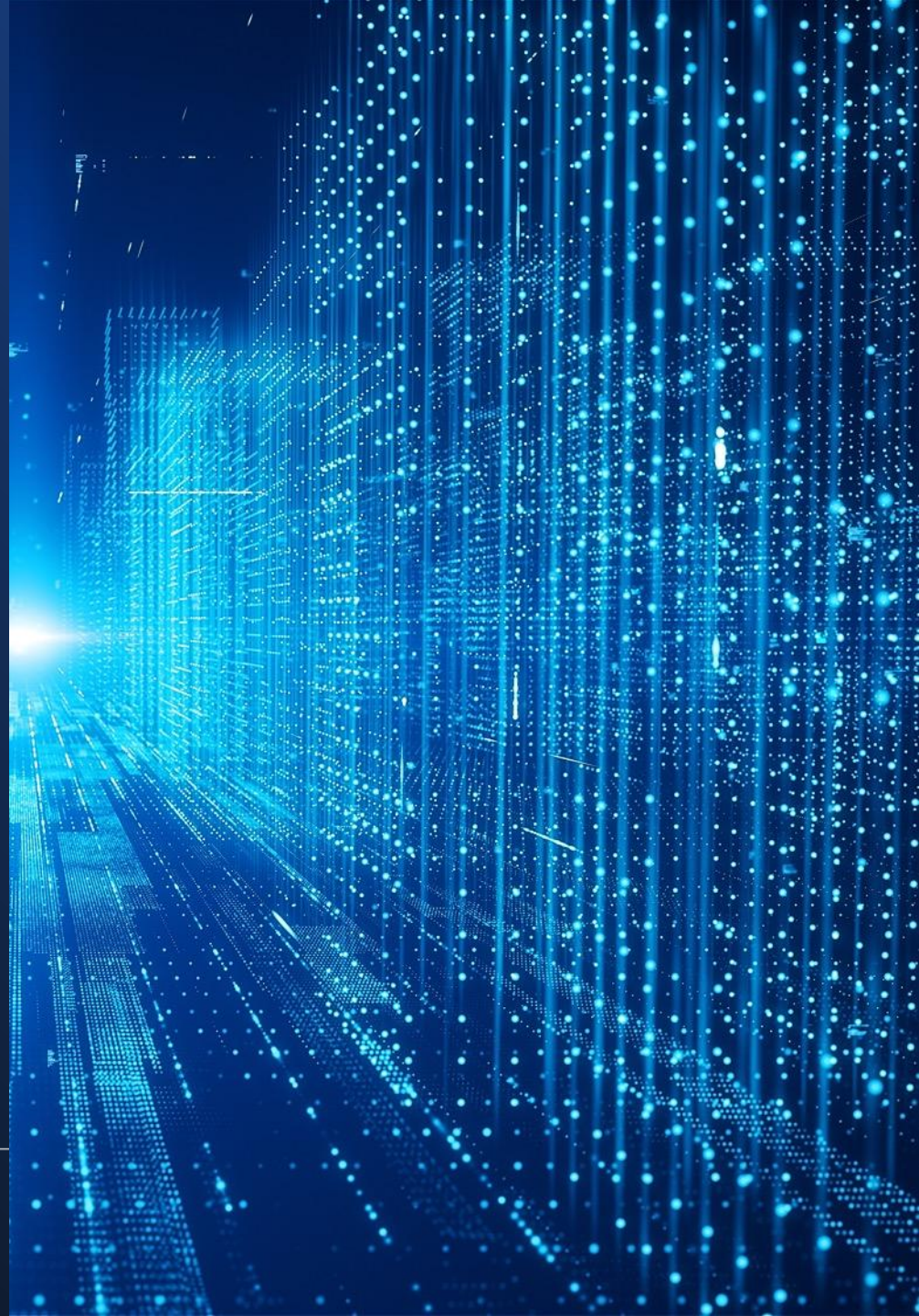
RESEARCH ON US GRID ATTACKS

367 PRC-authored research publications on attacks to U.S. power grids.

Strider identified a body of almost 500 additional research publications never translated into English

RECENT PRC RESEARCH ON SMART GRID ATTACKS

- **“Exploring Smart Grid Vulnerability Against Smart Inverter Parameter Tampering Attack”**
  by National Key Laboratory of Industrial Control Technology, 2025
- **“False Data Injection Attacks on Data-Driven Algorithms in Smart Grids Utilizing Distributed Power Supplies”**
  by Nanjing University & Southeast University, 2025
- **“Dynamical Failures Driven by False Load Injection Attacks Against Smart Grid”**
  by PLA National University of Defense Technology, 2022



Strider’s products and services are meant to safeguard your trade secrets, intellectual property, and other highly confidential information. They should not be used for any purpose covered by the Fair Credit Reporting Act. Strider’s data can only be used for specific non-FCRA (Fair Credit Reporting Act) purposes.
Processing of Personal Data. If you use any of Strider’s products and services to process personal data, you must provide legally adequate privacy notices and obtain necessary consents for the processing of such data, and you represent to us that you are processing such data in accordance with applicable law.