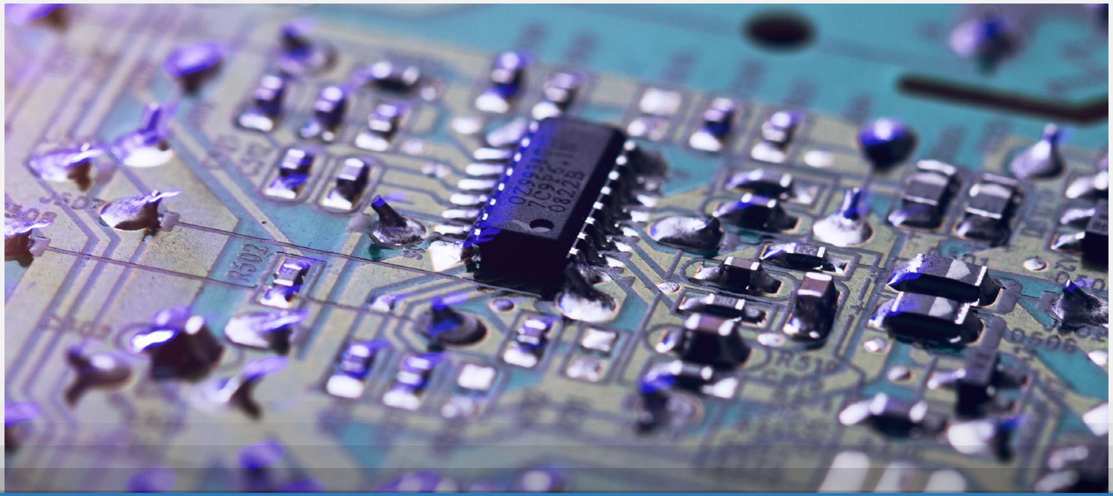


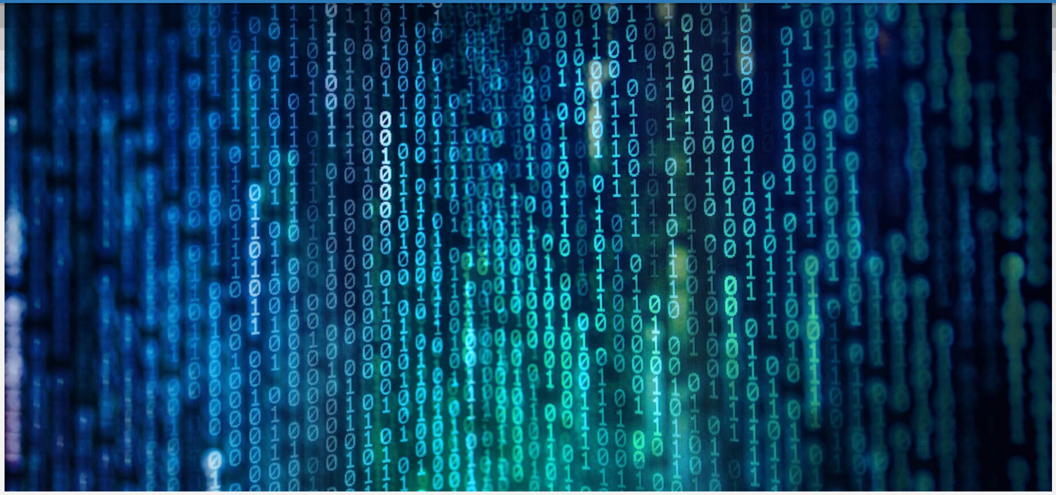
U.S. DEPARTMENT OF ENERGY

OFFICE OF Cybersecurity, Energy Security, and Emergency Response

CyTRICS™ Cyber Testing for Resilient Industrial Control Systems

E.O. 14017 - Cyber Supply Chain

August 2021



E.O. 14017 - America’s Supply Chains

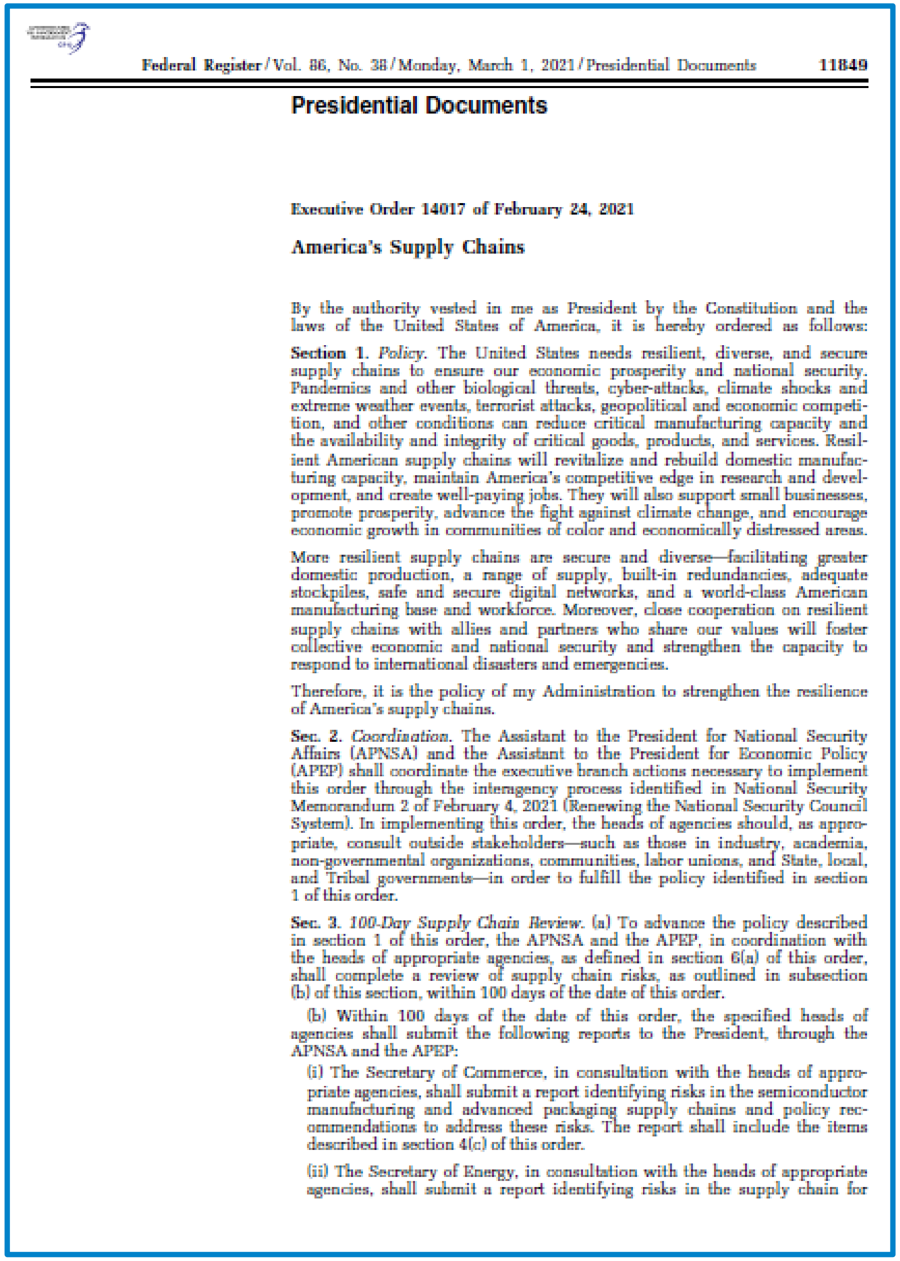
Charge: Assess supply chain vulnerabilities and recommend measures to strengthen supply chain resilience

100 Day Reports

https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

12 Month Reports – DOE Cyber Portions

- Define the **Energy Sector Industrial Base**, using best practices from the DIB
- Cyber supply chain for **high-integrity Data**; recommend policy to promote resilience
- Assess the cyber supply chain vulnerabilities for key digital components in energy sector systems – firmware, software, digital services and virtual platforms



Federal Register / Vol. 86, No. 38 / Monday, March 1, 2021 / Presidential Documents 11849

Presidential Documents

Executive Order 14017 of February 24, 2021

America’s Supply Chains

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical goods, products, and services. Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America’s competitive edge in research and development, and create well-paying jobs. They will also support small businesses, promote prosperity, advance the fight against climate change, and encourage economic growth in communities of color and economically distressed areas.

More resilient supply chains are secure and diverse—facilitating greater domestic production, a range of supply, built-in redundancies, adequate stockpiles, safe and secure digital networks, and a world-class American manufacturing base and workforce. Moreover, close cooperation on resilient supply chains with allies and partners who share our values will foster collective economic and national security and strengthen the capacity to respond to international disasters and emergencies.

Therefore, it is the policy of my Administration to strengthen the resilience of America’s supply chains.

Sec. 2. *Coordination*. The Assistant to the President for National Security Affairs (APNSA) and the Assistant to the President for Economic Policy (APEP) shall coordinate the executive branch actions necessary to implement this order through the interagency process identified in National Security Memorandum 2 of February 4, 2021 (Renewing the National Security Council System). In implementing this order, the heads of agencies should, as appropriate, consult outside stakeholders—such as those in industry, academia, non-governmental organizations, communities, labor unions, and State, local, and Tribal governments—in order to fulfill the policy identified in section 1 of this order.

Sec. 3. *100-Day Supply Chain Review*. (a) To advance the policy described in section 1 of this order, the APNSA and the APEP, in coordination with the heads of appropriate agencies, as defined in section 6(a) of this order, shall complete a review of supply chain risks, as outlined in subsection (b) of this section, within 100 days of the date of this order.

(b) Within 100 days of the date of this order, the specified heads of agencies shall submit the following reports to the President, through the APNSA and the APEP:

(i) The Secretary of Commerce, in consultation with the heads of appropriate agencies, shall submit a report identifying risks in the semiconductor manufacturing and advanced packaging supply chains and policy recommendations to address these risks. The report shall include the items described in section 4(c) of this order.

(ii) The Secretary of Energy, in consultation with the heads of appropriate agencies, shall submit a report identifying risks in the supply chain for

Energy Sector Industrial Base

- Secretary of Energy to “submit a report on supply chains for the energy sector industrial base (as determined by the Secretary of Energy).”
  - No established definition – Strategic opportunity to define
- DOE missions and stakeholders are **broad** and **diverse**
- DOE **lacks comprehensive view** of the energy sector industrial base
- Current engagements **fragmented** by individual missions within DOE.
- Key DOE missions require comprehensive ESIB engagement, e.g.,
  - Cybersecurity and counterintelligence
  - Tracking key policy impacts like job creation
  - Economic and statistical analyses
- **Frames future policy development**
  - Procurement policy, security requirements, etc.
- **Strategic foundation to build** - renewable tech brings new and different stakeholders into DOE’s industrial base
- Defining ESIB strategically positions DOE, stakeholders for this growth

Defense Industrial Base

Energy Sector Industrial Base

- Oxford English Dictionary defines “industrial base” as “The part of the economy of a country or region that is involved in producing goods in large quantities in factories.”
    - The concept of an industrial base is, therefore, inherently tied to production and commercial activity (versus government or regulatory activity). In a government context, activities associated with procurement of goods and services to support a critical national mission is a foundational parameter for establishing an industrial base.
- For Department of Defense, 10 U.S.C. §2500 establishes the National Technology and Industrial Base (NTIB), comprised of a domestic defense industrial base (DIB) and a global DIB
- **DIB definition** (per the DOD Dictionary):
    - The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.
- **Proposed ESIB Definition**:
    - The Department of Energy, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain energy sector systems, subsystems, components, or parts to meet US energy requirements.

Cyber Scoping for E.O. 14017

For purposes of this assessment, defining Cyber components as encompassing all **digital elements** in the energy sector supply chain:

- **Firmware** – The permanent software programmed into a read-only memory; provides the low-level control on a device for a device's specific hardware. Any component that has storage/memory or programmable controls operates firmware.

- **Software** – The applications that run on a system, that perform functions and process data.

- **Virtual Platforms and Services** – Cloud-based platforms, on the internet or on premise, that run applications, perform services, and store data.

- **Data** – The information used as inputs and outputs into processes and functions operated by software.

U.S. Cyber Supply Chain Threats, Risks, and Vulnerabilities

- **National Security risk** – The risk for damage to energy sector systems from national security threats is increasing
- **Criminal Activity risk** – Ransomware can be introduced through compromising software supply chain (similar to SolarWinds)
- **Reliance on Foreign Suppliers** – Cyber components systems globally sourced in an increasingly fragmented and dynamic digital supply chain
- **Opaque Supply Chains for Cyber Components** - Software and firmware code that operates digital components in energy sector systems is enormous and highly complex
  - Impossible to track the provenance and source of all code and manage the risk of supply chain compromise by ensuring that it stems from trustworthy sources
  - All software developers share, reuse code libraries
  - Open source code lacks provenance, often not maintained with security updates, creating cyber supply chain risk

U.S. Cyber Supply Chain Threats, Risks, and Vulnerabilities

- **Highly Dynamic Technology Marketplace** – Tech companies exist in a highly dynamic global marketplace characterized by a high degree of mergers and acquisitions (M&A) activity
  - Acquisitions re-brand, integrate digital components into larger product suites, obscuring the provenance of these subcomponents
  - Rapid changes in foreign ownership and control difficult to track
  - Assumption of control often means access to all source code, sensitive customer data, and continuing access to customer systems for maintenance
- **Concentrated Cyber Risk** – Critical infrastructure systems, including energy sector systems, frequently rely on a limited number of strategically important software components
  - Many examples of ubiquitous cyber components that, if compromised, could have an outsized impact on energy sector systems (similar to SolarWinds)
- **Fragmented and Inconsistent Oversight** - Digital portions of the supply chain are sourced from several critical infrastructure sectors
  - Some digital portions of the ESIB supply chain are regulated; many are not

Supply Chain for High-Integrity Data

Data

- Aggregated and curated data are a valuable global commodity
  - Now a critical part of digital supply chains
- Data has cyber supply chain risk like software - malicious manipulation can cause significant and nearly impossible-to-detect system failures.

Artificial Intelligence & Machine Learning

- AI/ML increasingly critical to national and economic security of the U.S.
- Growth in AI/ML research capability development/applied uses fueling commercial availability of data aaS, model development & training aaS, etc.
  - Increasing critical national need for massive, high-integrity datasets.

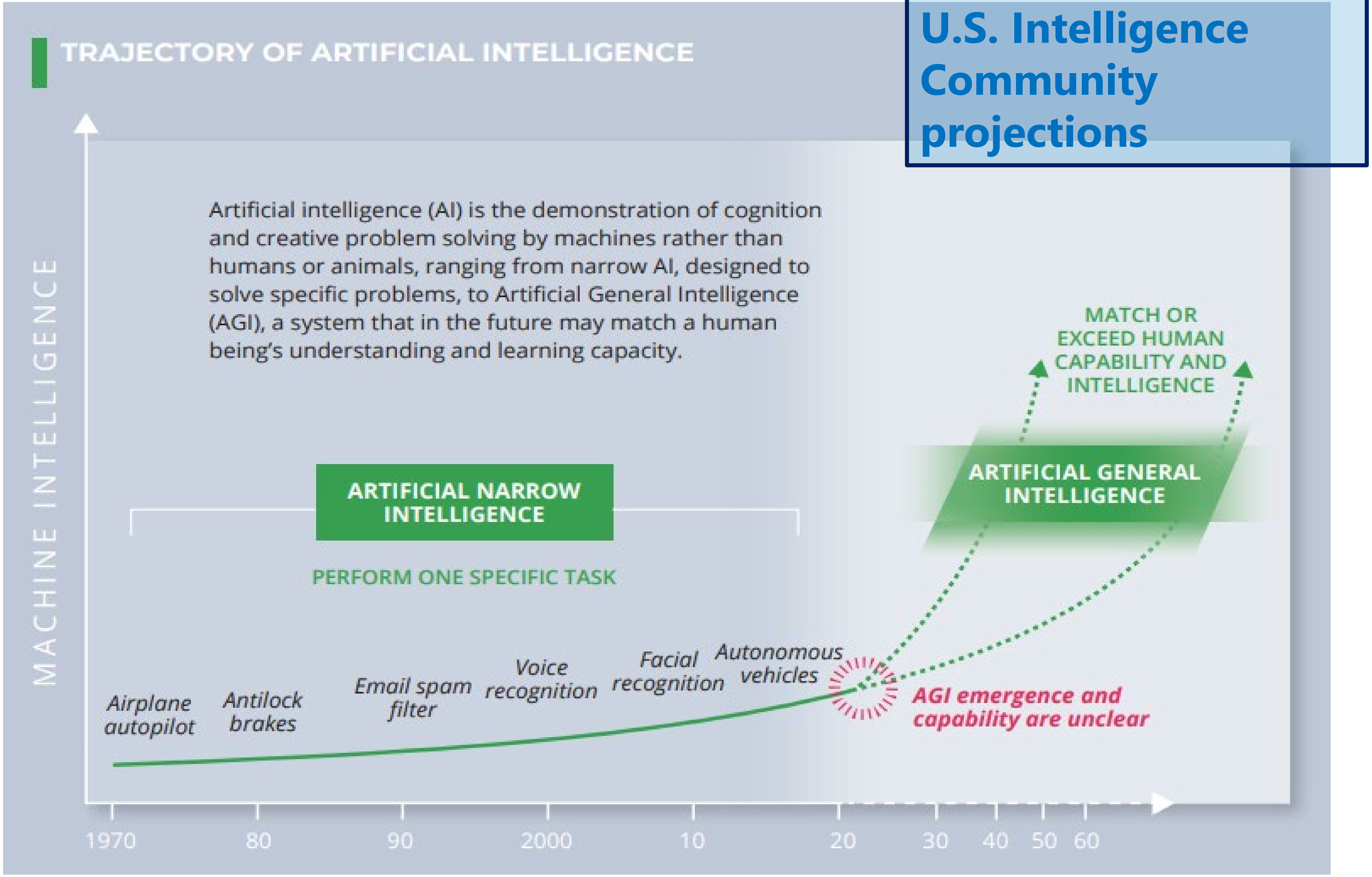
Energy Sector Industrial Base

- Energy Sector systems are data-heavy – Modelling, simulation, sensoring
- DOE National Labs are home to largest aggregate national R&D capability

Proposed Action:
Set foundation for policy on cybersecurity of data supply chains

Global Trends 2040

**March 2021
U.S. Intelligence Community projections**



TRAJECTORY OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is the demonstration of cognition and creative problem solving by machines rather than humans or animals, ranging from narrow AI, designed to solve specific problems, to Artificial General Intelligence (AGI), a system that in the future may match a human being's understanding and learning capacity.

MACHINE INTELLIGENCE
ARTIFICIAL NARROW INTELLIGENCE
PERFORM ONE SPECIFIC TASK
Airplane autopilot
Antilock brakes
Email spam filter
Voice recognition
Facial recognition
Autonomous vehicles
ARTIFICIAL GENERAL INTELLIGENCE
MATCH OR EXCEED HUMAN CAPABILITY AND INTELLIGENCE
AGI emergence and capability are unclear
1970
80
90
2000
10
20
30
40
50
60

https://www.dni.gov/index.php/gt2040-media-and-downloads

Feedback

Cheri Caddy
Senior Advisor for Cybersecurity
CESER/DOE

Cherylene.caddy@hq.doe.gov