# Securing the Modern Grid: Federal Investments, Digitization, and Supply Chain Strategy

INL/RPT-25-89606

Center for Securing Digital Energy Technology (CSDET)

NOVEMBER 2025

Megan Culler
Remy Stolworthy

*Idaho National Laboratory*

Patrick Heeter
Alex Tylecote
Todd Ponto
Josh Kmiec
Luke Martin

*ScottMadden, Inc.*

Idaho National Laboratory

*Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy*

INL/RPT-25-89606

# Securing the Modern Grid: Federal Investments, Digitization, and Supply Chain Strategy

**Megan Culler**
**Remy Stolworthy**
**Idaho National Laboratory**

**Patrick Heeter**
**Alex Tylecote**
**Todd Ponto**
**Josh Kmiec**
**Luke Martin**
**ScottMadden, Inc.**

**November 2025**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517**

*Page intentionally left blank*

# EXECUTIVE SUMMARY

Across the United States (U.S.) grid expansion and modernization is underway, paving the way for accelerated load growth and intelligent resource management. Digitization of the grid is supported by several state and federal programs, providing support for utilities installing advanced metering infrastructure (AMI), AI-powered analytics systems, battery energy storage systems (BESS), and distributed energy resource management systems (DERMS) to transform the grid from a one-way power delivery system into an intelligent, responsive network that will enable faster load growth and power expansion of data centers for advanced artificial intelligence (AI) applications.

The digital transformation of America's grid presents opportunity for increased efficiency and resiliency but also introduces new digital risks that require careful management. Digital equipment often contains several vulnerabilities such as unencrypted communication protocols, and persistent remote access capabilities that could be exploited to manipulate device settings, coordinate service disruptions, or inject false data into grid operations. These digital risks become particularly important as the grid must rapidly scale to support AI-driven data centers, which the administration has identified as essential for maintaining U.S. technological leadership and economic competitiveness. These vulnerabilities are compounded by supply chain realities: Chinese manufacturers currently produce 70-90% of essential grid components including inverters, batteries, and control systems [1], with the U.S. lacking domestic manufacturing capacity for critical assets like extra-high voltage transformers [2].

Recent federal legislation has established Foreign Entity of Concern (FEOC) restrictions to address these risks, requiring projects to achieve escalating thresholds of non-FEOC content to receive tax credits while utilities work to expand sourcing channels for their supply chains and strengthen security measures. These restrictions arrive precisely when utilities face unprecedented electricity demand growth driven by the rapid growth in data centers, creating a considerable challenge: rapidly expanding infrastructure while navigating complex compliance requirements while lacking viable alternatives for many critical components.

Idaho National Laboratory (INL) and its partners have developed practical approaches to help utilities navigate these intersecting challenges as they leverage federal investment to strengthen and grow the grid. These solutions include Cyber-Informed Engineering (CIE) principles [3] that build resilience directly into systems, the Cirrus tool for secure cloud migration [4], and enhanced procurement guidance [5] that embeds security requirements throughout equipment lifecycles. Federal initiatives, such as the Technical Assistance for Digital Assurance (TADA) project, provide direct support to utilities implementing these approaches while facilitating knowledge sharing across the industry [6].

While these tools and frameworks cannot eliminate all risks inherent in foreign supply chain dependencies, they offer pragmatic pathways for strengthening security posture without sacrificing the deployment momentum essential to meeting surging electricity demand. Ultimately, securing America's digital energy infrastructure demands dedicated coordination across multiple fronts: building domestic supply chains, implementing robust digital assurance practices, and maintaining the aggressive modernization timeline necessary for reliability, resilience, and energy independence.

# CONTENTS

# FIGURES



# TABLES

*Page intentionally left blank*

# ACRONYMS

| | |
|---|---|
| ADMS | Advanced Distribution Management Systems |
| AI | Artificial Intelligence |
| AMI | Advanced Metering Infrastructure |
| API | Application Programming Interface |
| BESS | Battery Energy Storage Systems |
| BIL | Bipartisan Infrastructure Law |
| BMS | Battery Management Systems |
| CCE | Consequence-driven Cyber-Informed Engineering |
| CESER | Office of Cybersecurity, Energy Security, and Emergency Response |
| CIE | Cyber-Informed Engineering |
| DER | Distributed Energy Resources |
| DERMS | Distributed Energy Resource Management Systems |
| DMS | Distribution Management System |
| DMZ | Demilitarized Zone |
| DNP3 | Distributed Network Protocol 3 |
| DOE | U.S. Department of Energy |
| DPA | Defense Production Act |
| ESP | Energy Services Platform |
| EV | Electric Vehicle |
| FEOC | Foreign Entity of Concern |
| FERC | Federal Energy Regulatory Commission |
| FLISR | Fault Location/Isolation/Service Restoration |
| FOA | Funding Opportunity Announcements |
| FPGA | Field-Programmable Gate Array |
| FY | Fiscal Year |
| GIS | Geographic Information System |
| GPS | Global Positioning System |
| GRIP | Grid Resilience and Innovation Partnerships |
| GW | Gigawatt |
| HBOM | Hardware Bills of Materials |
| IBR | Inverter Based Resources |
| IPP | Independent Power Producers |
| IIJA | Infrastructure Investment and Jobs Act |

| | |
|---|---|
| kV | Kilovolt |
| MACR | Material Assistance Cost Ratio |
| ML | Machine Learning |
| MW | Megawatt |
| NDAA | National Defense Authorization Act |
| NERC | North American Electric Reliability Corporation |
| NERC CIP | North American Electric Reliability Corporation Critical Infrastructure Protection |
| NIST | National Institute of Standards and Technology |
| OBBB | One Big Beautiful Bill |
| OEM | Original Equipment Manufacturer |
| OLCM | Online Condition Monitoring |
| OMS | Outage Management System |
| PCS | Power Conversion Systems |
| PFE | Prohibited Foreign Entities |
| PLC | Power Line Carrier |
| PUC | Public Utility Commission |
| R2AP | Resilience and Reliability Assessment Program |
| RF | Radio Frequency |
| SAIDI | System Average Interruption Duration Index |
| SBOM | Software Bills of Materials |
| SCADA | Supervisory Control and Data Acquisition |
| SGC | Smart Grid Chip |
| TADA | Technical Assistance for Digital Assurance |
| TSMC | Taiwan Semiconductor Manufacturing Company |

*Page intentionally left blank*

# Securing the Modern Grid: Federal Investments, Digitization, and Supply Chain Strategy

## 1. INTRODUCTION

The modernization of the United States (U.S.) electric grid is accelerating under a wave of federally funded initiatives aimed at enhancing resilience, growing grid capacity, and supporting deployments of artificial intelligence (AI) technologies. In January 2025, the Administration declared a National Energy Emergency executive order and issued the Unleashing American Energy executive order, establishing a policy framework to expedite energy infrastructure development and remove regulatory barriers to grid expansion [7]. This was reinforced in April 2025 with the Strengthening the Reliability and Security of the United States Electric Grid executive order, which grants emergency authority to maintain grid stability amid rapidly increasing electricity demand [8], and in July 2025 with the Accelerating Federal Permitting of Data Center Infrastructure executive order, which streamlines infrastructure development for AI-driven technologies [9].

At the heart of this transformation lies a growing reliance on digital energy equipment, ranging from advanced battery storage systems and power conversion devices to grid-edge sensors and control platforms. These technologies are essential for enabling real-time monitoring, adaptive control, and secure operation of a dynamic and rapidly expanding grid.

However, the rapid scale-up of digital energy infrastructure has exposed critical vulnerabilities in the energy sector's supply chains. Many of the components essential to grid modernization are sourced from global suppliers, raising concerns about digital risk, reliability, and national security. The limited domestic manufacturing capacity for key digital assets, such as semiconductors and embedded control systems, further compounds these risks, especially as geopolitical tensions and trade uncertainties continue to disrupt global supply flows.

This report examines the scale and scope of digital energy equipment deployment in federally supported grid expansion projects, with a particular focus on the systemic challenges posed by supply chain insecurity. By analyzing current initiatives and identifying persistent gaps, this report aims to inform policy and programmatic strategies that can safeguard the digital backbone of America's future energy system.

### 1.1. State & Federal Energy Investment Programs

The digitization of the U.S. energy grid is being actively supported through a growing portfolio of federal and state investment programs that aim to modernize infrastructure, enhance security, and improve operational intelligence. These programs provide a mix of direct grants, low-interest loans, and tax credits to accelerate the deployment of digital grid technologies such as advanced metering infrastructure (AMI), distributed energy resource management systems (DERMS), and grid-edge control devices. The DOE, for example, administers the Grid Resilience and Innovation Partnerships (GRIP) program, which includes dedicated funding for technologies that enable capacity-growing, data-rich, flexible grid performance [10]. Similarly, the Smart Grid Investment Matching Grant Program under Section 40107 of the Bipartisan Infrastructure Law (BIL) supports utilities in deploying digital control systems and sensors to improve grid visibility and responsiveness. Many grants require a certain percentage of matching funds contributed from the applicant to complete the project. Loan programs can also play a critical role, offering repayment mechanisms upon a project's successful completion and demonstrated benefit to the grid. These loans help reduce the financial burden of upfront investments, making it easier for smaller utilities and cooperatives to keep up with growth and modernize their systems

Tax incentives also play a critical role in scaling digital energy infrastructure. The Inflation Reduction Act (IRA) introduced or expanded several tax credits that reward energy projects incorporating domestic content and digital control capabilities. These credits are structured to be accessible to both public and private entities, with “direct pay” options for tax-exempt organizations and “transferability” provisions for developers. Following the January 2025 Unleashing American Energy executive order, the Administration paused certain IRA and Infrastructure Investment and Jobs Act (IIJA) disbursements and directed federal agencies to conduct 90-day reviews to ensure funding alignments with national energy priorities, including grid reliability, energy dominance, and domestic energy infrastructure development [7] Additionally, the DOE’s Office of Manufacturing and Energy Supply Chains has issued guidance to ensure that digital components used in federally funded projects meet domestic sourcing thresholds, reinforcing both supply chain security and economic competitiveness.

At the state level, energy offices and public utility commissions are increasingly aligning their programs with federal priorities by offering complementary incentives for digitalization. These include matching grants for grid modernization, security readiness assessments, and streamlined permitting for projects that integrate advanced digital controls. Some states have also begun to condition funding on compliance with cyber risk frameworks or supply chain transparency requirements, particularly for digital assets that interface with critical grid operations. Together, these federal and state programs form a layered investment ecosystem that not only funds physical infrastructure but also embeds intelligence, resilience, and security into the digital core of the evolving energy system.

The IIJA established domestic content requirements through "Build America, Buy America" provisions, requiring that all iron, steel, manufactured products, and construction materials used in many IIJA funded infrastructure projects be produced in the United States, with limited waivers available [11; 12]. As of 2025, these requirements have significantly impacted procurement of digital equipment components, many of which continue to rely on global supply chains [13].

The One Big Beautiful Bill Act (OBBB), enacted in 2025, further tightened these requirements by introducing Foreign Entity of Concern (FEOC) provisions that restrict eligibility for variable energy tax credits under the IRA. Under OBBB, projects must demonstrate escalating levels of non-FEOC content. These provisions target critical digital infrastructure elements, reinforcing the administration's emphasis on domestic manufacturing and supply chain security

## 1.2. Importance of Digital Equipment in Modernizing U.S. Energy Infrastructure

Digital equipment forms the technological backbone of grid modernization, enabling the transformation from a one-way power delivery system to an intelligent, responsive network capable of managing complex, bidirectional energy flows. The DOE identifies these technologies as essential for improving reliability, resilience, and security while facilitating the integration of new generation sources and widespread load growth. AMI, distribution automation systems, and grid-edge intelligence provide utilities with real-time visibility and control capabilities that were impossible with traditional analog infrastructure. The economic imperatives driving grid modernization make digital equipment deployment not merely beneficial but essential for achieving national energy objectives.

Utilities worldwide are investing heavily in digital transformation, with 71% prioritizing grid modernization to manage the complexity of distributed energy resources (DERs) [14]. Federal policymakers recognize that comprehensive digitalization represents the critical path to building an electric grid capable of supporting economic growth and resilience goals while delivering reliable, affordable power to all Americans. Recognizing AI's critical role in grid modernization, the White House's July 2025 America's AI Action Plan [15] and the accompanying Accelerating Federal Permitting of Data Center Infrastructure executive order specifically directs federal agencies to develop AI-enabled grid technologies and accelerate digital infrastructure deployment through coordinated efforts across

DOE, Department of Commerce (DOC), and other agencies [9]. This builds upon the April 2025 Strengthening the Reliability and Security of the United States Electric Grid executive order, which empowers DOE to take emergency actions under Section 202(c) of the Federal Power Act to prevent grid failures, develop uniform methodologies for analyzing reserve margins, and maintain critical generation resources amid surging electricity demand from AI, data centers, and expanded manufacturing [8].

## 1.3. Challenges of Digital Equipment

The modernization of America's energy infrastructure through digital technologies represents a fundamental shift from traditional analog systems to interconnected, software-defined networks that promise enhanced reliability through real-time monitoring, improved resilience via DER integration, and operational efficiency from data-driven optimization. However, this transformation expands the attack surface while supply chain dependencies on foreign manufacturers create potential backdoors for adversarial exploitation.

The digital energy ecosystem now involves numerous stakeholders - utilities, independent power producers (IPPs), developers, integrators, original equipment manufacturers (OEMs), and third-party service providers - all requiring various levels of system access, creating cascading vulnerabilities where each stakeholder's security becomes everyone's risk [16]. Recent ransomware and supply chain attacks demonstrate how compromising a single stakeholder - whether through social engineering of maintenance staff or exploiting vendor access - can cascade across the entire ecosystem [16]. The challenge compounds as stakeholders often operate across multiple sectors, with battery OEMs supplying solar and wind components using shared platforms, meaning a single compromise can impact multiple infrastructure types [16].

Grid digitalization has also dramatically increased connectivity touchpoints - from web application programming interfaces (APIs) and virtual private network (VPN) connections to wireless access points and cloud platforms. As demonstrated by recent cyberattacks on critical infrastructure globally, the consequences of compromised digital equipment could extend beyond individual utilities to impact national security, economic stability, and public safety, making the imperative to secure digital equipment not merely a technical requirement, but a strategic necessity for maintaining grid reliability and national resilience. The July 2025 America's AI Action Plan [15] acknowledges cyber risks found alongside dramatic modernization, and integration of digital tools in critical infrastructure projects. The White House has recommended that Department of Homeland Security (DHS) establish an AI Information Sharing and Analysis Center (AI-ISAC) and promote secure-by-design principles for AI systems deployed in critical infrastructure, recognizing that digital equipment security is fundamental to both grid resilience and national AI competitiveness [17].

## 1.4. Report Purpose & Scope

This report examines the scale and security implications of digital energy deployment, focusing on the intersection of rapid grid modernization efforts supported by federal funding and the evolving supply chain security landscape. The analysis assesses digital equipment supply chains serving federal programs, evaluates the impact of Foreign Entity of Concern (FEOC) restrictions on project implementation, examines risks from digital grid technologies, and provides actionable recommendations for securing critical infrastructure while maintaining deployment momentum.

The scope examines key technologies such as AMI, distribution automation and management systems (ADMS), smart inverters, and battery energy storage systems (BESS). The report considers projects recently receiving federal support with particular attention to FEOC restrictions beginning July 4, 2025, across all 50 states participating in federal programs.

# 2. GRID DIGITIZATION OVERVIEW

As the U.S. power grid evolves to accommodate a more complex and decentralized energy landscape, digitization has emerged as a necessary shift to enable reliable, abundant energy delivery. The increasing integration of distributed generation and large and controllable loads like data centers has introduced new operational challenges that traditional grid infrastructure was not designed to manage. In response, utilities and grid operators are turning to digital technologies, such as advanced sensors, real-time data analytics, and automated control systems, to enhance visibility, flexibility, and responsiveness across the grid.

Digitization supports grid capacity growth by enabling optimized use of existing infrastructure and accelerating the integration of new assets. Technologies like distributed energy resource management systems (DERMS), digital substations, and advanced metering infrastructure (AMI) allow operators to monitor and manage load in real time, optimize power flows, and reduce the need for costly upgrades. These capabilities are especially critical as electrification increases demand and as federal and state policies push for faster interconnection of generation and large load projects. Digital tools also support predictive maintenance and outage management, improving reliability and reducing operational costs.

Adoption of digital grid technologies is accelerating, driven by both policy incentives and operational necessity. Federally funded programs are prioritizing projects that incorporate digital infrastructure. At the same time, industry-led initiatives and state-level modernization plans are embedding digitization into long-term grid planning. As these trends converge, digital capabilities are no longer viewed as optional enhancements but as essential components of a resilient, efficient, and future-ready energy system.

As of 2022, utilities had installed 119.3 million advanced meters nationwide (72.3% penetration), with adoption rates varying from 87% in the West South-Central region to below 50% in Middle Atlantic and New England areas [18]. This federal investment transforms grid infrastructure from basic meter reading to AI-powered optimization and real-time dynamic line rating systems, bridging the technological gap between early adopters and regions using legacy systems. The following use-cases demonstrate the types of digital tools being implemented and how they are being utilized by utilities through federal funding to achieve measurable improvements in reliability, operational efficiency, and grid resilience.

## 2.1. Use Cases

Federal awarded projects demonstrate widespread interest and planning for digital technologies across the U.S. electric grid. Analysis of IIJA GRIP project submissions reveals four key categories of digital technology implementation: smart meters and AMI, AI-powered analytics systems, Advanced Distribution Management Systems (ADMS), and DERMS. Other technologies may have digital components even if their primary purpose is not digital by nature. For example, BESS have digital components embedded to perform power conversion management for charging discharging and network connectivity to receive dispatch signals. Even traditional components like transformers have seen increased digitization in modern offerings. This section focuses on the use cases that have digital technology embedded as part of their core capability, i.e. the technology would not exist without digitization.

Figure 1 below illustrates the scale and overlap of these technology deployments, showing that ADMS/DERMS implementations represent the largest investment at $550 million in original project scale, followed by AI/ML applications at $317 million, and AMI deployments at $88 million, with significant integration occurring between these systems as indicated by the overlapping areas. These deployments range from foundational upgrades replacing old manual meters with radio frequency (RF) smart meters to sophisticated AI applications for grid optimization and management. The following use cases from projects selected in 2024 for federal support demonstrate how utilities are successfully

deploying digital equipment to enhance grid reliability, enable distributed generation integration, and improve operational efficiency across their service territories.

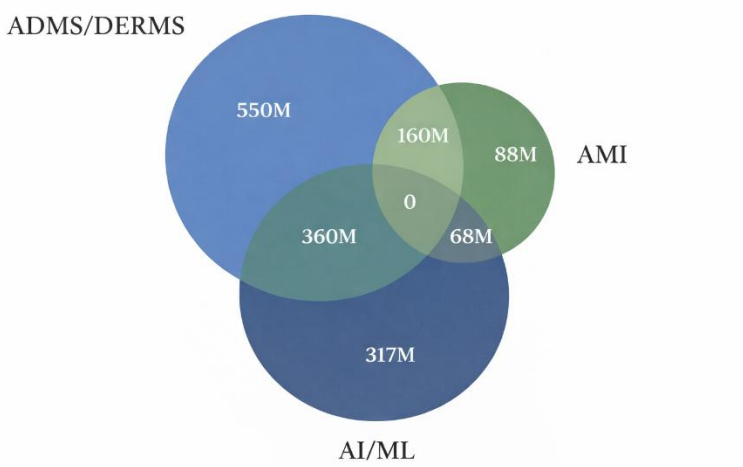


*Figure 1. IIJA Funding by Digital Technology Type (USD)*

### 2.1.1. Smart Meters & Advanced Metering Infrastructure (AMI)

The widespread adoption of smart metering systems represents a significant shift in how utilities manage and monitor infrastructure. These digital devices collect energy usage data at frequent intervals (often hourly or faster) and transmit it wirelessly to utilities while providing customers with real-time consumption insights. Unlike traditional analog meters requiring manual readings, smart meters use RF networks or fiber optics for near instant, two-way data exchange.

Example AMI deployments demonstrate the scale of grid modernization underway. Examples include projects selected to deploy over 714,000 smart meters collectively, from municipal utilities to rural cooperatives covering territories as large as 4,700 square miles [19]. For example, Arkansas Valley Electric Cooperative proposed to deploy advanced smart meters across a sprawling 4,700 square-mile territory, delivering sub-one-minute usage intervals and edge computing capabilities by leveraging their existing fiber-to-the-home network transforming rural infrastructure into a sophisticated data network [20]. (See Appendix A for complete AMI deployment examples). These AMI deployments transform meters from basic billing tools into real-time smart grid networks, enabling near-instant outage reporting, remote operations, conservation voltage reduction, and demand response programs. By serving as both data collection points and edge controllers, these systems create self-healing grids that improve reliability, reduce costs, enhance customer engagement through usage data access, and provide the visibility needed for DER integration, ultimately accelerating the shift to resilient, customer-centric grid operations. (See Appendix A for detailed project examples.)

### 2.1.2. AI-Powered Systems

AI and machine learning (ML) are emerging as critical tools in grid modernization. Capable of analyzing large streams of data, AI algorithms can forecast demand, detect anomalies, and recommend optimized actions. These capabilities complement and enhance digital meters and sensors projects. AI is being used for several purposes; to predict outages, prioritize vegetation management using satellite imagery, model wildfire risks, reduce interconnection timelines, and evaluate the reliability impact of distributed energy resources (DERs) [21]. From this analysis it is apparent that AI systems are being deployed alongside AMI and supervisory control and data acquisition (SCADA) upgrades, turning the grid into a data-rich environment where algorithms support near real time analysis and enhanced forecasting.

Several projects demonstrate innovative AI applications across widely varied utility settings. Examples include proposed deployment of 18,000 Nvidia-powered AI modules for real-time grid edge visibility, satellite imagery systems that forecast wildfire risk days in advance, and AI platforms that reduce interconnection timelines from 30 to 12 months [19]. For instance, Tri-County Electric Cooperative proposed to deploy AI-powered satellite imagery that can forecast wildfire risk 4 days in advance, combined with analytics platforms that aggregate real-time meter and SCADA data for predictive outage forecasting demonstrating how AI transforms raw data streams into actionable intelligence [22] (See Appendix A for complete AI deployment examples.) Utilities are applying edge analytics to meter data, imagery, and control systems to predict outages, manage vegetation, and shorten interconnection studies. Early results show faster interconnection timelines, enhanced decision-making, optimized grid loads, and more precise investments while maintaining reliability. Federal support is accelerating the practical use of AI across utilities nationwide. (See Appendix A for detailed project examples.)

### 2.1.3. Advanced Distribution Management System (ADMS) & Distributed Energy Resource Management Systems (DERMS)

DERMS are software platforms that enable utilities to monitor, control, and optimize distributed energy resources (DERs), including rooftop solar, battery storage, and smart appliances. These systems synthesize data across thousands of individual DERs into manageable virtual power plants, providing real-time visibility and control through algorithms that balance grid reliability with economic optimization. Leveraging these assets intelligently enables more load growth overall with fewer upgrades to the larger grid system. Implementation of advanced DERMS platforms synchronize many kinds of communication relationships between SCADA systems to modern AMI devices. By integrating with ADMS, DERMS transforms passive distribution grids into active networks capable of bidirectional power flows, automated dispatches, and market optimization.

DERMS deployments span from single utilities to multi-state cooperatives. Examples include projects selected to consolidate 12 legacy systems into unified ADMS platforms, deploy multi-tenant DERMS across 42 distribution cooperatives serving over 1 million customers, and integrating over 200 megawatts (MW) of controllable load across 200,000 square miles [19]. For example, Tri-State Generation and Transmission Association is deploying a multi-tenant DERMS platform across 42 distribution cooperatives serving over 1 million rural customers in four states, integrating 200 MW of controllable load and 1,000 MW of utility-scale variable energy resources across 200,000 square miles - demonstrating how DERMS transforms scattered resources into coordinated grid assets. [23] (See Appendix A for complete DERMS deployment examples.) ADMS and DERMS work in tandem to give operators clear grid visibility while grouping distributed resources into controllable assets that support voltage and load management. These integrated systems enable faster service restoration, defer capital upgrades, and create new value from distributed resources, with documented improvements including 5% System Average Interruption Duration Index (SAIDI) reduction and millions in annual transmission upgrade deferrals [24]. (See Appendix A for detailed project examples.)

## 3. SUPPLY CHAIN CHALLENGES, RISKS, & IMPACTS

The deployment of digital equipment confronts evolving supply chain challenges that have shifted from pandemic-era disruptions to new pressures driven by unprecedented electricity demand growth and increasingly stringent domestic content requirements. Understanding this evolution is critical for implementing effective mitigation strategies under current federal programs.

## 3.1. Supply Chain Challenges & Disruptions

Long-standing risks in the digital equipment supply chain were rapidly intensified during the COVID-19 pandemic in 2020-2021, when backlogged demand collided with clogged logistics networks, creating severe shortages for grid infrastructure (e.g. transformer lead times were extended from 12 to over 52 weeks in the course of a single year) [25].This exposed dependency on foreign suppliers, particularly China, which controlled 80-90% of inverter production [26] and 70% of battery cells [27]. Federal legislation responded with frameworks to reduce foreign dependencies driven by multiple strategic imperatives: enhancing national security by reducing vulnerability to adversarial control, strengthening domestic manufacturing capacity for economic competitiveness, and ensuring supply chain resilience against future disruptions. The IIJA (2021) implemented Build America, Buy America provisions, while the IRA (2022) created domestic content bonus credits. While the fiscal year (FY)2021 National Defense Authorization Act (NDAA) established the framework for identifying Chinese military companies operating in the United States, the FY2024 NDAA [28] prohibited six Chinese battery companies from federal procurement, and FY2025 presidential actions have promoted further growth of American supply chains for critical energy sectors.

New supply chain pressures now compound earlier challenges. Data centers driven by AI could account for almost half of U.S. electricity demand growth by 2030, creating competition for already constrained digital equipment supplies to help accelerate grid growth [29]. FEOC requirements have dramatically reduced eligible suppliers while the OBBB's expansion of FEOC definitions to include companies with 25% foreign ownership eliminates many previously acceptable vendors, forcing utilities to reconfigure procurement strategies to receive tax credits.

These requirements brought increased scrutiny to fundamental vulnerabilities in the digital equipment supply chain that persist today:

- **Digital control systems**: The overwhelming majority of power electronics, control systems, and smart grid components remain manufactured overseas, with Chinese companies dominating market share.
- **Supply chain opacity**: Complex multi-tier supplier relationships, white-labeling practices, and cross-sector component sharing continue to obscure the true origins of critical equipment.
- **Persistent foreign influence**: The digital nature of modern infrastructure requires ongoing connections to vendors for firmware updates, remote diagnostics, and technical support.
- **Rapid market evolution**: The influx of federal funding has attracted new market entrants, with dozens of new players entering various segments between 2021-2024.

## 3.2. Foreign Entity of Concern (FEOC) Procurement

Foreign Entity of Concern (FEOC) restrictions across federal grid programs require utilities and project developers to navigate increasingly complex procurement requirements while maintaining critical modernization timelines. These evolving regulations, which encompass tax credits and federal procurement policies, necessitate comprehensive adjustments to equipment sourcing strategies and vendor relationships to ensure both compliance and grid resilience.

The OBBB signed into law on July 4, 2025, expanded FEOC definitions beyond the Inflation Reduction Act's initial framework [30]. While companies remain free to purchase from FEOCs, they forfeit federal tax credits when doing so. Under the OBBB, Prohibited Foreign Entities (PFE) encompass two categories:

1. Specified Foreign Entities - including Chinese military companies, entities subject to Uyghur forced labor restrictions, and entities controlled by China, Russia, North Korea, or Iran.

2. Foreign-Influenced Entities, which captures companies where PFEs can appoint officers, hold 25% or more ownership, control 40% in aggregate, hold 15% of debt, or exercise "effective control" through contractual arrangements [30].

The NDAA for FY2024 had already signaled this direction by banning six BESS companies from federal Department of Defense procurement: CATL, EVE Energy Company, BYD Company, Gotion High Tech Company, Envision Energy, and Hithium Energy Storage Technology, establishing precedent for the broader restrictions now implemented through the OBBB [28].

### 3.2.1. Implementation Challenges

The OBBB's material assistance tests require projects beginning construction after December 31, 2025, to calculate a Material Assistance Cost Ratio (MACR = (T-P)/T × 100%) that measures non-PFE content in manufactured products [30]. Threshold percentages vary by technology and escalate over time: qualified facilities must achieve 40-60% non-PFE content (2026-2029), energy storage technology (under 48E) requires 55-75%, while battery components (under 45X) range from 60-85% over the same period [30].[1] Projects must obtain supplier certifications under penalty of perjury confirming products were not produced by PFEs, creating comprehensive verification requirements throughout the supply chain [30].

The OBBB establishes stringent enforcement mechanisms with an extended six-year IRS statute of limitations for material assistance determinations - double the normal assessment period - and accuracy-related penalties of 20% when taxpayers understate liability by more than 1% due to FEOC violations [30]. Suppliers providing false certifications face penalties of $5,000 or 10% of the related credit amount, whichever is greater, for certifications provided after December 31, 2025 [30].

### 3.2.2. Impact on Digital Equipment Industries

The FEOC restrictions under the OBBB have profound implications for the solar, storage, and inverter industries, where Chinese manufacturers maintain dominant market positions. Among the top global inverter manufacturers, several qualify as Specified Foreign Entities under the OBBB definitions [31]. Even non-Chinese manufacturers face compliance challenges due to material assistance from prohibited entities [32], [33], [34].

The BESS sector faces some of the most acute challenges, with prevalent manufacturers appearing on Department of Defense procurement prohibition lists [35]. International manufacturers also source critical components from China or maintain manufacturing operations there [36, 37]. The solar sector reveals similar dependencies, with well-known manufacturers operating in Xinjiang amid forced labor concerns [38] or maintaining substantial Chinese manufacturing facilities [39]. Implementation of FEOC restrictions creates immediate procurement challenges as companies must rapidly reconfigure supply chains to meet escalating thresholds, beginning at 40-60% non-FEOC content in 2026 and increasing to 60-85% by 2029 [30]. With companies affected by FEOC restrictions controlling substantial market share, finding alternative suppliers presents a considerable challenge [40].

## 3.3. Vulnerabilities within Grid Components

Many grid modernization projects deploy not only highly visible digital platforms such as AMI, ADMS/DERMS, and AI/ML-enabled systems, but also technologies that are not primarily digital in function yet now incorporate substantial digital elements, particularly in more recent designs. BESS, modern inverters, and large power transformers increasingly incorporate embedded processors, networked

[1] Section 48E provides investment tax credits (ITCs) for complete energy storage systems installed as part of energy projects, while Section 45X provides production tax credits (PTCs) for the domestic manufacturing of individual battery components such as cells and modules. The higher FEOC thresholds for 45X battery components (60-85%) compared to 48E energy storage technology (55-75%) reflect the administration's emphasis on securing the domestic manufacturing supply chain for critical battery components themselves, rather than just the assembly of complete storage systems.

sensors, and software-driven control systems. These features enable advanced monitoring, automation, and integration with grid management platforms, but they also make these assets part of the digital threat surface. Even when their primary function is mechanical or electrical, their digital subsystems create security and supply chain considerations comparable to more overtly digital systems.

Digital equipment deployment introduces a larger digital attack surface that foreign supply chain dependencies amplify into national security risks. Common technical vulnerabilities across critical digital grid equipment─such as BESS, inverter-based resources (IBRs), AMI, and DERMS - include unencrypted communication protocols [41], vulnerable APIs [42], and persistent remote access capabilities that enable both immediate attacks and long-term compromise [43]. These systems are not always designed with security in mind, and competition to innovate new technologies at lower costs disincentivizes the time and cost to include security reviews and features.

Research has shown evidence that exploitation of these vulnerabilities has the potential to enable several categories of attacks: firmware manipulation during vendor maintenance windows [44, 45, 46], compromise of cloud APIs and management platforms [47, 48], equipment damage through parameter manipulation such as inducing thermal runaway or overheating [49, 50], and establishment of persistent backdoors by nation-state actors, like Volt Typhoon, for long-term reconnaissance and pre-positioning [51, 52, 53].

While security research has identified potentially catastrophic consequences from exploiting these vulnerabilities, particularly when combined with foreign manufacturing control and mandatory vulnerability disclosure to adversarial governments, these scenarios remain largely theoretical at this stage, with most validated only in laboratory settings rather than observed in operational grid environments. Nevertheless, the convergence of these risk factors warrants the defensive strategies and procurement practices detailed in Section 6.

### 3.3.1. China’s Vulnerability Disclosure Process

Understanding China’s vulnerability disclosure process is important given that current grid infrastructure is current from (or being procured from) China. Foreign control of manufacturing, combined with China's 2021 vulnerability disclosure law, creates significant security concerns. This law, issued by the Cyberspace Administration of China (CAC), mandates companies to report security flaws to the Chinese government before patching. The key requirements of this law for the purposes of this report are the following [54]:

- Article 7, (2): Obligates vendors to report all identified vulnerabilities to the Ministry of Industry and Information Technology (MIIT) within two days.
- Article 9, (1): Forbids security researchers from disclosing bug details before the vendor has had a reasonable opportunity to patch the issue, with exceptions requiring MIIT approval.
- Article 9, (7): Restricts the disclosure of vulnerability details to overseas organizations or individuals, except for network product providers.
- Article 10: Requires all network operators and product vendors to register their vulnerability reporting platforms with MIIT.

These requirements can create an asymmetric advantage where adversaries possess both the means of production and advance knowledge of exploitable weaknesses. The convergence of these factors enables sophisticated attack scenarios where nation state actors could pre-position capabilities during manufacturing, maintain access through legitimate service channels, and execute coordinated disruptions timed to coincide with grid contingencies or geopolitical tensions.

### 3.3.2. Battery Energy Storage Systems (BESS) & Inverters

While Section 2 focused on AMI, AI systems, and ADMS/DERMS as primary examples of digital equipment deployment, BESS and inverters are equally critical components of grid modernization projects. These systems contain sophisticated digital control systems, including battery management systems, power conversion controls, and cloud-connected monitoring platforms, that create similar vulnerabilities requiring examination.

Security researchers have documented vulnerabilities in inverter systems that highlight risks across grid-connected power electronics [55]. In 2025, multiple vulnerabilities were identified across several major manufacturers, affecting cloud APIs, mobile applications, and communication gateways [54]. Some gateway devices were found to permit unauthorized firmware modification, though actual deployment and exposure levels vary significantly [55]. Previous disclosures have revealed other weaknesses such as hardcoded passwords, insecure cloud interfaces, and unencrypted communications, issues observed across various suppliers in the solar and distributed energy sectors [55]. Additionally, tens of thousands of solar management interfaces were identified as internet-accessible, although not all were confirmed to be exploitable or unauthenticated [55].

While formal vulnerability assessments specific to BESS remain limited, these systems often share common hardware, software architectures, and control platforms with inverter technologies. Vulnerability disclosures in integrated control platforms illustrate potential crossover risks, suggesting that similar weaknesses could exist in BESS deployments, though such risks remain largely theoretical in operational contexts.

This challenge is further compounded by supply chain concentration across these sectors. A significant share of inverter and battery component manufacturing is concentrated among a small number of foreign entities, many operating in jurisdictions with limited transparency or differing security disclosure requirements. In the inverter market, a majority of global production originates from a few large suppliers located in East Asia, while domestic manufacturing capacity remains limited but is gradually expanding.

Similarly, the battery sector shows extreme concentration: in 2024, 70% of U.S. battery storage imports originated from [56] China and six Chinese companies control 62.5% of the global market for lithium-ion manufacturing [40]. Foreign dependency (where according to an INL Center for Securing Digital Energy Infrastructure (CSDET) supply chain analysis, the vast majority of power conversion systems approved for use in California contain at least one component manufactured in China) combined with white labeling practices (when a product or service produced by one company is rebranded and marketed by another company as its own) and China's mandatory vulnerability disclosure law creates multiple attack pathways. Even companies that want to promote security and be good actors for their customers may present risk when subject to the laws of a government adversarial to U.S. interests [54]. Such concentration, combined with white-labeling practices (where a product is rebranded and sold under another company’s name) and foreign vulnerability disclosure laws, creates multiple potential exposure pathways. Even well-intentioned suppliers may be compelled to share sensitive information under foreign legal frameworks, inadvertently increasing cyber risk.

While real-world attacks exploiting these vulnerabilities have not been documented, security researchers theorize that a highly skilled adversary with system access could potentially cause operational disruptions. These theoretical scenarios include manipulating device settings, causing localized service disruptions, or disrupting monitoring and control functions. However, it's important to emphasize that such attacks remain hypothetical rather than observed in practice and would require significant technical expertise and system access to execute.

The convergence of documented vulnerabilities in related systems, extreme supply chain concentration, and foreign manufacturing control creates risk conditions that require careful management through the security measures and procurement practices outlined in Section 6 of this report.

### 3.3.3. ADMS & Advanced Metering Infrastructure (AMI)

ADMS platforms must integrate hardware, software, and data components across complex systems, including outage management systems (OMS) and distribution management systems (DMS) which create interoperability and security challenges, especially with multi-vendor deployments [57]. As discussed above, such multi-vendor integration requirements create supply chain risk through foreign manufactured components throughout the metering infrastructure that sophisticated actors can exploit.

Among the most cited vulnerabilities AMIs suffer from is weak encryption, which can compromise the confidentiality and integrity of transmitted data [58]. Many also employ insecure communication protocols, such as the Modbus protocol, that are not adequately secure, leaving the transmitted data vulnerable to interception and manipulation, along with other weaknesses such as poor authentication mechanisms [58]. Common threats exploiting these vulnerabilities include data tampering or manipulation, unauthorized access, privacy breaches, and denial-of-service or distributed DoS attacks [58].

### 3.3.4. Transformers

Modern transformers increasingly integrate digital monitoring and control systems essential for grid modernization. Newer transformers utilize Online Condition Monitoring (OLCM) systems that turn these devices into connected grid infrastructure and expand the attack surfaces beyond traditional vulnerabilities. Products like ETOS®, Sensformer, and TXpert™ monitor voltage regulation, temperature, dissolved gas analysis, and bushing conditions [59].

Security researchers have identified potential vulnerabilities with OLCM systems that could theoretically be exploited by an adversary. These include unencrypted DNP3 and Modbus communication protocols inadequate authentication mechanisms, and remote access vulnerabilities [59]. Researchers have proposed attack scenarios where adversaries could manipulate OLCM systems to falsify temperature readings causing overheating, inject false tap changer commands to destabilize voltage, or mask developing faults until catastrophic failure occurs [59].

The United States lacks domestic manufacturing for extra high voltage transformers (>345 kV), creating foreign dependence for assets that transport 60 to 70% of electricity [2]. Custom transformers cost $2 to 10 million with long lead times having been experienced by many utilities, preventing rapid replacement. The discovery of backdoor electronics in Chinese transformers revealed prepositioned access capabilities [2]. Researchers propose that attackers could manipulate OLCM systems to falsify temperature data causing overheating, inject false tap commands destabilizing voltage, or mask developing faults until catastrophic failure, transforming individual transformer compromises into regional blackouts given the inability to quickly source replacements [2].

### 3.3.5. Communications & Networking

All digital equipment ─ from AMI and ADMS to BESS and AI analytics platforms ─ relies on communications and networking infrastructure for data transmission, remote monitoring, and control functions. This fundamental dependency makes the security of communications networks critical to the overall resilience of grid modernization efforts.

Grid communications infrastructure faces hard-to-replace foreign dependencies in critical chipsets. Most baseband processors originate from Qualcomm and MediaTek─HiSilicon (China) is a dominant player [60]; TSMC controls 92% of advanced chip production [61]. Unlike other equipment where

alternatives exist, these chipset monopolies create unavoidable vulnerabilities across EMS/SCADA systems, distribution automation, and AMI networks.

Field assessments have revealed systemic configuration failures for networked grid equipment overall: missing demilitarized zones (DMZs) with direct internet exposure, plaintext passwords, unencrypted protocols, and third-party management creating backdoors [62]. Nation state actors systematically exploit these weaknesses: Volt Typhoon ─ a Chinese state-sponsored group that targets critical infrastructure for pre-positioning and persistence - compromises distribution automation routers, Salt Typhoon ─ another Chinese threat group focused on telecommunications infrastructure - infiltrates utility internet service providers, while Dragonfly ─ a Russian-linked group known to target system integrators maintaining persistent access [62]. Additionally, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)-013-01 regulation only covers bulk electric system components, leaving distribution level communications unregulated. The convergence of irreplaceable chip dependencies, configuration failures, and active exploitation creates scenarios where adversaries could eliminate visibility and control across entire distribution networks.

# 4. HOW THE CURRENT ADMINISTRATION IS ADDRESSING SUPPLY CHAIN RISKS & IMPACTS

The Trump administration has undertaken several initiatives to secure equipment supply chains and address vulnerabilities identified in the report. The January 2025 "Unleashing American Energy" executive order declares a national energy emergency and directs agencies to expedite approvals for energy infrastructure, invoking Defense Production Act (DPA) authorities to accelerate domestic production of critical energy equipment including for the electricity grid [7].

## 4.1. Executive Orders Establish Framework for Energy Dominance

President Trump declared a national energy emergency on January 20, 2025, through Executive Order 14156, invoking the National Emergencies Act to accelerate energy infrastructure development [63]. This emergency declaration notably excludes wind and solar power from the federal definition of "energy," instead focusing on crude oil, natural gas, refined petroleum products, uranium, coal, biofuels, geothermal heat, hydroelectric power, and critical minerals.

The administration's energy supply chain strategy centers on three core executive orders signed between January and April 2025. Executive Order 14154, "Unleashing American Energy," aims to position the U.S. as the leading producer and processor of non-fuel minerals and rare earth elements while strengthening supply chains for allies and reducing influence of adversarial states [7]. Executive Order 14262, "Strengthening the Reliability and Security of the United States Electric Grid," addresses electricity demand from AI data centers and domestic manufacturing by streamlining DOE emergency authorities and preventing generation resources over 50 MW from leaving the bulk-power system if it reduces grid capacity [8].

## 4.2. Manufacturing Initiatives Prioritize Domestic Production Through Tariffs & Incentives

The administration's domestic manufacturing strategy combines aggressive tariffs with targeted investments in critical equipment production. Major transformer manufacturing investments have materialized despite supply chain challenges, with Siemens Energy committing $150 million to a Charlotte, North Carolina facility producing 24 large power transformers initially and scaling to 57 units annually by 2027 [63]. Hitachi Energy invested $22.5 million in Virginia facilities creating 120 jobs [64], while Eaton announced a $340 million investment in South Carolina for three-phase transformer production beginning 2027 [65].

Build America, Buy America Act (BABA) requirements remain in effect with enhanced enforcement, mandating 100% domestic manufacturing processes for iron and steel, greater than 55% domestic content for manufactured products, and entirely domestic production for construction materials in all federal energy projects for applicable entities [12].

## 4.3. Cybersecurity Requirements Target Foreign Equipment Risks

Executive Order 14306 establishes verification protocols for grid equipment through mandatory post-quantum cryptography standards and U.S. Cyber Trust Mark labeling requirements by 2027 [66]. These measures directly address the supply chain infiltration risks discussed in Section 3.3, where foreign-manufactured components pose persistent security threats.

The administration prohibits acquisition, importation, transfer, or installation of bulk-power system equipment from foreign adversaries, with the Secretary of Energy authorized to determine transactions posing unacceptable risk to national security. The prohibition on bulk-power system equipment from foreign adversaries under the 2020 executive order “Securing the United States Bulk-Power System”, implemented by the DOE, reduces dependency on potentially compromised components [67]. The Federal Energy Regulatory Commission (FERC) Order No. 907's Internal Network Security Monitoring, requiring implementation by October 2028, creates detection capabilities for supply chain compromises that may have already occurred [68]. However, these requirements add compliance costs potentially slowing deployment of needed infrastructure.

# 5. CONCLUSION

The Infrastructure Investment and Jobs Act's $65 billion investment in grid modernization represents an important initiative towards the transformation America's energy infrastructure through deployment of digital equipment across 105 GRIP projects nationwide installing AMI, AI-powered analytics, BESS, DERMS, and other systems. While this digital transformation promises enhanced reliability and resilience, it introduces significant cybersecurity vulnerabilities this report has identified.

At the same time, FEOC manufacturers currently control 70-90% of essential components for grid modernization. Chinese companies dominate production of inverters, batteries, and control systems. This concentration creates risks beyond traditional supply chain concerns, as foreign entities with manufacturing control and advance knowledge of vulnerabilities through their government's disclosure requirements can pre-position capabilities or exploit known weaknesses during critical grid events.

Policymakers have responded with increasingly stringent restrictions, culminating in the OBBB FEOC provisions that require projects to achieve 40-85% non-FEOC content by 2026-2029 and exclude companies with as little as 25% ownership by prohibited entities, thereby dramatically reducing the pool of eligible suppliers for utilities. These requirements dramatically reduce the pool of eligible suppliers precisely when utilities face the first significant electricity demand surge in decades, driven by the explosion in data center investments that could account for nearly half of demand growth by 2030.

# 6. REFERENCES


1. U.S. Department of Energy. Battery Energy Storage Systems: Supply Chain Assessment. DOE/LP/NNL--2024--365849, November 2024. Available at: https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf
2. Baker, G., Webb, I., Burkes, K., & Cordaro, J. "Large Transformer Criticality, Threats, and Opportunities." Journal of Critical Infrastructure Policy 2, no. 2 (2021): 82-95. https://centerforsecuritypolicy.org/wp-content/uploads/2022/06/LARGE-TRANSFORMER-THREATS-OPPORTUNITIESJCIP-PUBLISHED-VERSION.pdf
3. Idaho National Laboratory. Cyber-Informed Engineering: Strategy Guidance Framework, Version 1.0. INL/RPT-22-67122. Idaho Falls, ID: Idaho National Laboratory, 2022. Available at: https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf
4. Idaho National Laboratory. Cirrus: Cloud Infrastructure Resource for Resilience and Uninterrupted Services. Idaho Falls, ID: Idaho National Laboratory, 2024. Available at: https://inl.gov/cirrus
5. U.S. Department of Energy. Enhanced Cybersecurity Procurement Guidelines for Grid Modernization Equipment. Technical Report OSTI-2473239. Washington, DC: Office of Scientific and Technical Information, 2024. Available at: https://www.osti.gov/biblio/2473239
6. Idaho National Laboratory. Technical Assistance for Digital Assurance (TADA): Supporting Secure Digital Transformation in the Energy Sector. Center for Securing Digital Energy Technology. Idaho Falls, ID: Idaho National Laboratory, 2024. Available at: https://inl.gov/csdet-technical-assistance-and-training/
7. Executive Order 14156. Declaring a National Energy Emergency. January 20, 2025. Available at: https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-american-energy/
8. Executive Order. Strengthening the Reliability and Security of the United States Electric Grid. April 8, 2025. Available at: https://www.whitehouse.gov/presidential-actions/2025/04/strengthening-the-reliability-and-security-of-the-united-states-electric-grid/
9. Executive Order 14318. Accelerating Federal Permitting of Data Center Infrastructure. July 23, 2025. Available at: https://www.whitehouse.gov/presidential-actions/2025/07/accelerating-federal-permitting-of-data-center-infrastructure/
10. Infrastructure Investment and Jobs Act. Pub. L. No. 117-58, 135 Stat. 429 (2021). Available at: https://www.congress.gov/117/plaws/publ58/PLAW-117publ58.pdf
11. U.S. Department of Energy. Bipartisan Infrastructure Law Programs. Available at: https://www.energy.gov/bil/bipartisan-infrastructure-law-programs
12. U.S. Department of Energy. Build America, Buy America. Available at: https://www.energy.gov/management/build-america-buy-america
13. U.S. Department of Energy Grid Deployment Office. Grid Resilience and Innovation Partnerships (GRIP) Program. Available at: https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program
14. Utility Dive. Utilities See AI as Tool for Grid Modernization but Lack Expertise, Survey. Available at: https://www.utilitydive.com/news/utilities-see-ai-as-tool-for-grid-modernization-but-lack-expertise-survey/803980/

15. White House. America's AI Action Plan: Accelerating Innovation and Infrastructure for National Competitiveness. Washington, DC: Executive Office of the President, July 2025. Available at: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf
16. Stewart, Emma, Ginger Wright, Ben Lampe, Megan Culler, and Remy Stolworthy. Application of Cyber-Informed Engineering for Protecting BESS. White Paper. Idaho National Laboratory, Idaho Falls, ID, January 2025. Available at: https://inl.gov/content/uploads/2024/03/BESS-CIE-White-Paper_vFINAL.pdf
17. Cybersecurity Dive. White House Artificial Intelligence Action Plan Includes Cybersecurity Initiatives Under Trump Administration. Industry Dive, July 2025. Available at https://www.cybersecuritydive.com/news/white-house-artificial-intelligence-action-plan-cybersecurity-trump/753856/
18. Federal Energy Regulatory Commission. Annual Assessment of Demand Response. November 2024. Available at: https://www.ferc.gov/sites/default/files/2024-11/Annual%20Assessment%20of%20Demand%20Response_1119_1400.pdf
19. INL Analysis of IIJA GRIP 1 & 2 Projects See Appendix A
20. Arkansas Valley Electric Cooperative Corporation. Beyond AMI to True Grid Intelligence with Distribution Automation. Technical Volume, Concept Paper TA2-052-E, GRIP Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP
21. https://www.osti.gov/servlets/purl/2997112
22. National Energy Technology Laboratory. Tri-County Electric Cooperative, Inc. (TCE). U.S. Department of Energy, February 2024. Available at: https://netl.doe.gov/sites/default/files/2024-02/Tri-County%20Electric%20Cooperative,%20Inc.%20(TCE).pdf
23. Tri-State Generation and Transmission Association. Technical Volume. GRIP Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP
24. American Electric Power. Technical Volume. Grid Resilience and Innovation Partnerships (GRIP) Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP
25. Wall Street Journal. Power Companies Enter Peak Hurricane Season Lacking Enough Transformers. August 1, 2022. Available at: https://www.wsj.com/business/logistics/power-companies-enter-peak-hurricane-season-lacking-enough-transformers-11659351601
26. Wood Mackenzie. Global PV Inverter Shipments Grew by 56% in 2023 to 536 GWAC. Available at: https://www.woodmac.com/press-releases/2024-press-releases/global-pv-inverter-shipments-grew-by-56-in-2023-to-536-gwac/
27. Carnegie Endowment for International Peace. Winning the Battery Race: How the United States Can Leapfrog China to Dominate Next-Generation Battery Technologies. October 2024. Available at: https://carnegieendowment.org/research/2024/10/winning-the-battery-race-how-the-united-states-can-leapfrog-china-to-dominate-next-generation-battery-technologies?lang=en
28. U.S. Congress. National Defense Authorization Act for Fiscal Year 2024. H.R. 2670, 118th Congress. Washington, DC: U.S. Government Publishing Office, 2023. Available at: https://www.congress.gov/bill/118th-congress/house-bill/2670
29. International Energy Agency. Energy and AI: A New Era for the Energy Sector. Paris: IEA, 2025. Available at: https://www.iea.org/reports/energy-and-ai/

30. White & Case LLP. "New Law Changes IRA Tax Credits." Alert, July 4, 2025. See H.R. 1, the "One Big Beautiful Bill Act," 119th Congress (2025). Available at: https://www.whitecase.com/insight-alert/amendments-to-ira-tax-credits-congressional-budget-bill-july-6
31. INL analysis based on market data and company disclosures, "Top Inverter/Solar/Storage Companies in the U.S. under the BBB FEOC definition (2024-2025)," June 2025.
32. BBC News. Tesla's Battery Supply Chain and CATL Partnership. 2025. Available at: https://www.bbc.com/news/articles/c3d4k1derzgo
33. SolarEdge Technologies. Manufacturing and Supply Chain Overview. Investor Presentation, 2025.
34. Electrawise. SMA Acquisition of Zeversolar. 2012. Available at: https://www.electrawise.com.au/sma-acquisition-of-zever-solar/; SolPlanet, "SMA China Partners with CMIG New Energy," 2025, https://solplanet.net/ma-china-partners-with-cmig-new-energy-to-expand-residential-pv-market-in-china
35. U.S. Congress. National Defense Authorization Act for Fiscal Year 2024. H.R. 2670, 118th Congress. Available at: https://www.congress.gov/bill/118th-congress/house-bill/2670/text
36. Teslarati. LG Energy Solution Lithium Supply Agreement with Chinese Supplier. 2025. Available at: https://www.teslarati.com/lg-energy-solution-lithium-supply-agreement-chinese-supplier/
37. Panasonic Corporation. Panasonic Factory in Dalian, China Begins Mass Production. Press Release, March 13, 2018. Available at: https://news.panasonic.com/global/press/en180313-3
38. U.S. Customs and Border Protection, "Withhold Release Orders and Findings," addressing Xinjiang production concerns, 2025.
39. Canadian Solar Inc. Form 20-F Annual Report. 2025. Available at: https://investors.canadiansolar.com/static-files/916becde-db76-4c6e-a7c0-5a42392b5a57; See also: MIT Technology Review. "Canadian Solar IRA Manufacturing in US." April 23, 2024. Available: https://www.technologyreview.com/2024/04/23/1091665/canadian-solar-ira-manufacturing-us/
40. Market analysis based on Wood Mackenzie, "Global Energy Storage Supply Chain Assessment," Q2 2025; BloombergNEF, "Battery Manufacturing Capacity by Region," 2025. Available at: https://www.woodmac.com/reports/power-markets-global-battery-energy-storage-supply-chain-trends-2025-report-150410525/
41. U.S. Department of Energy. Resilient Communication Systems. June 5, 2025. Available at: https://www.energy.gov/sites/default/files/2025-06/Resilient%20Communication%20Systems_20250605_Final_Amended.pdf
42. DERSec. Solar Vulnerability Summary v2.0. Available at: https://dersec.io/reports/DERSec-Solar-Vulnerability-Summary-v2.0-Final.pdf
43. U.S. Department of Energy. Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid. October 2022. Available at: https://www.energy.gov/sites/default/files/2022-10/Cybersecurity%20Considerations%20for%20Distributed%20Energy%20Resources%20on%20the%20U.S.%20Electric%20Grid.pdf
44. Forescout. Grid Security: New Vulnerabilities in Solar Power Systems Exposed. Available at: https://www.forescout.com/blog/grid-security-new-vulnerabilities-in-solar-power-systems-exposed/
45. SANS Institute and Electricity Information Sharing and Analysis Center. [Title missing]. Available at: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

46. Dragos. FrostyGoop ICS Malware Intelligence Brief. July 2024. Available at: https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf

47. CISA. MAR-17-352-01 HatMan - Safety System Targeted Malware (Update B). Available at: https://www.cisa.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%20-%20Safety%20System%20Targeted%20Malware%20%28Update%20B%29.pdf

48. Cybernews. Solarman Vulnerability: Solar Grid Exposed. Available at: https://cybernews.com/security/solarman-vulnerability-solar-grid-exposed/

49. MDPI. Cyber-Physical Cloud Battery Management Systems: Review of Security Aspects. Energies 9, no. 7 (2024): 382. Available at: https://www.mdpi.com/2313-0105/9/7/382

50. IEEE. Cyberphysical Security of Grid Battery Energy Storage Systems. IEEE Access. 2016 Available at: https://ieeexplore.ieee.org/ielaam/6287639/9668973/9787060-aam.pdf

51. CISA. Cybersecurity Advisory AA24-038A. Available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

52. U.S. Department of Energy. Resilient Communication Systems. June 5, 2025. Available at: https://www.energy.gov/sites/default/files/2025-06/Resilient%20Communication%20Systems_20250605_Final_Amended.pdf

53. Security Week. China's Volt Typhoon Hackers Dwelled in US Electric Grid for 300 Days. Available at: https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days/

54. The Record. Chinese Government Lays Out New Vulnerability Disclosure Rules. Recorded Future News, 2021. Available at: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules

55. Forescout. Grid Security: New Vulnerabilities in Solar Power Systems Exposed. Available at: https://www.forescout.com/blog/grid-security-new-vulnerabilities-in-solar-power-systems-exposed/

56. U.S. Census Bureau. "USA Trade Online: U.S. Imports under HTS 8507600000 (Lithium-Ion Accumulators), HTS 8507600010 (Lithium-Ion Batteries for EVs), and HTS 8507600020 (Other Lithium-Ion Batteries)." Foreign Trade Division, U.S. Department of Commerce, 2024. https://usatrade.census.gov/

57. Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., and Wollman, D. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. NIST Special Publication 1108r4. National Institute of Standards and Technology, Gaithersburg, MD, 2021. Available at: https://doi.org/10.6028/NIST.SP.1108r4

58. Ismail, A., Bendiab, G., Neagu, D., and Djenouri, Y. Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review. Energies 18, no. 4 (2025): 1445. MDPI, Basel, Switzerland. Available at: https://doi.org/10.3390/en18041445

59. Rahimpour, Hossein, Joe Tusek, Ahmed S. Musleh, Boyu Liu, Alsharif Abuadbba, Toan Phung, and Aruna Seneviratne. A Review of Cybersecurity Challenges in Smart Power Transformers. IEEE Access, vol. 12, 2024. Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10804107

60. Globe Newswire. Baseband Processor Industry Report 2025: Open RAN Adoption Opens New Avenues for Disaggregated Baseband Architectures. June 20, 2025. Available at: https://www.globenewswire.com/news-release/2025/06/20/3102563/28124/en/Baseband-Processor-Industry-Report-2025-Open-RAN-Adoption-Opens-New-Avenues-for-Disaggregated-Baseband-Architectures.html

61. Quartz. Top Chip Producers Revenue Share FAB TSMC Samsung. Available at: https://qz.com/top-chip-producers-revenue-share-fab-tsmc-samsung-1851758309

62. Summary of Findings: Network Hunt Engagement Report, INL Center for Securing Digital Energy Technology. Forthcoming.

63. Siemens Energy. "Expanding U.S. Transformer Manufacturing and Service Footprint." Charlotte, NC: Siemens Energy USA, 2025. Available at: https://www.siemens-energy.com/us/en/home/stories/transformer-manufacturing-and-service-expansion-in-us.html

64. pv magazine USA. "Hitachi Energy Expands U.S. Transformer Production with $22.5 Million Investment in Virginia." Tucson, AZ: pv magazine USA, April 28, 2025. Available at: https://pv-magazine-usa.com/2025/04/28/hitachi-energy-expands-u-s-transformer-production-with-22-5-million-investment-in-virginia/

65. Manufacturing Dive. "Eaton Invests $340M in US Transformer Production." Washington, DC: Manufacturing Dive, 2025. Available at: https://www.manufacturingdive.com/news/eaton-transformer-production-shortage-investment/740135/

66. The White House. "Executive Order 14306: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity." Washington, DC: The White House, June 6, 2025. Available at: https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity/

67. The White House. Executive Order: Securing the United States Bulk Power System. Trump White House Archives. Available at: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

68. Federal Register. Critical Infrastructure Protection Reliability Standard CIP-015-1: Cyber Security Internal Network Security Monitoring. July 2, 2025. Available at: https://www.federalregister.gov/documents/2025/07/02/2025-12309/critical-infrastructure-protection-reliability-standard-cip-015-1-cyber-security-internal-network

69. Gainesville Regional Utilities. GRUA Meeting Materials. April 17, 2024. Available at: https://www.gru.com/Portals/0/2024%20Updates/GRUA%204-17-24%20Meeting%20w%20Back-Up.pdf

70. National Energy Technology Laboratory. “Liberty Utilities (CalPeco Electric) LLC.” U.S. Department of Energy, February 2024. Available at: https://netl.doe.gov/sites/default/files/2024-02/Liberty%20Utilities%20(CalPeco%20Electric)%20LLC.pdf

71. Rappahannock Electric Cooperative. “Enabling EV and DER Adoption Through DERMS, AMI, and Fiber Integration.” Technical Volume, GRIP Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP

72. National Energy Technology Laboratory. “Sacramento Municipal Utility District.” U.S. Department of Energy, February 2024. Available at: https://netl.doe.gov/sites/default/files/2024-02/Sacramento%20Municipal%20Utility%20District.pdf

73. Latitude Media. “How one Michigan utility is using GRIP funding for edge computing.” Latitude Media News, 2024. Available at : https://www.latitudemedia.com/news/how-one-michigan-utility-is-using-grip-funding-for-edge-computing/

74. Renewable Energy World. “GridUnity selected to receive nearly $50M in federal funds for its solution to speed up interconnection.” Renewable Energy World, 2024. Available at:

https://www.renewableenergyworld.com/power-grid/smart-grids/gridunity-selected-to-receive-nearly-50m-in-federal-funds-for-its-solution-to-speed-up-interconnection

75. National Energy Technology Laboratory. “Commonwealth Edison Company.” U.S. Department of Energy, February 2024. Available at: https://netl.doe.gov/sites/default/files/2024-02/Commonwealth%20Edison%20Company.pdf
76. Portland General Electric. “Accelerating and Deploying Grid Edge Computing Technical Volume.” GRIP Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP
77. City of Naperville. “Technical Volume.” GRIP Program, accessed via National Energy Technology Laboratory FOIA, 2024. Available at: https://netl.doe.gov/home/foia/GRIP
78. United States Department of Energy. "Grid Resilience and Innovation Partnerships (GRIP) Program Projects." Grid Deployment Office. Available at: https://www.energy.gov/gdo/grid-resilience-and-innovation-partnerships-grip-program-projects
79. National Telecommunications and Information Administration. "Broadband Equity, Access, and Deployment (BEAD) Program." BroadbandUSA. https://broadbandusa.ntia.gov/funding-programs/broadband-equity-access-and-deployment-bead-program
80. National Telecommunications and Information Administration. "Enabling Middle Mile Broadband Infrastructure Program." BroadbandUSA. https://broadbandusa.ntia.gov/funding-programs/enabling-middle-mile-broadband-infrastructure-program
81. National Telecommunications and Information Administration. "Tribal Broadband Connectivity Program." BroadbandUSA. https://broadbandusa.ntia.gov/funding-programs/tribal-broadband-connectivity
82. United States Department of Energy. "Battery Materials Processing Grants." Manufacturing and Energy Supply Chains. https://www.energy.gov/mesc/battery-materials-processing-grants
83. United States Department of Transportation. "Strengthening Mobility and Revolutionizing Transportation (SMART) Grants Program." https://www.transportation.gov/grants/SMART

*Page intentionally left blank*

# Appendix A

The analysis completed in this section assessed the projects for IIJA GRIP projects that were approved **as of July, 2025**. Changes to these projects or new projects under similar funding sources are not assessed in this report.

## A-1. IIJA GRIP projects implementing AMI:

- **Gainesville Regional Utilities (GRU):** GRU's Meter Upgrade program proposed to replace approximately 220,000 electric, natural gas, and water meters by the end of 2025, with RF meters providing two-way communication, remote reading and connect/disconnect, and integration with customer information systems for improved billing accuracy and faster outage response [69].
- **TriCounty Electric Cooperative:** The Power Meter Squared & Green Tree project would upgrade 18,500 power line carrier (PLC) meters to RF mesh meters that communicate via an optical fiber network, with each meter featuring a super-capacitor allowing communications for ~60 seconds after power loss and supporting remote disconnect, demand response, conservation voltage reduction, and storage of 35 days of interval data, integrated with the co-op's SCADA and AI-based analytics platform for outage detection and extreme weather risk mitigation [22].
- **Arkansas Valley Electric Cooperative Corporation (AVECC):** Serving a 4,700 square-mile territory with roughly 62,600 active meters, AVECC planned to deploy Itron Gen5 Riva smart meters and fiber mini access points that will deliver sub-one-minute usage intervals, remote disconnect/control, DER readiness, bypass detection, and edge computing capabilities, leveraging the cooperative's existing fiber-to-the-home network [20].
- **Liberty Utilities (CalPeco Electric):** In the Lake Tahoe basin, Liberty proposed to replace approximately 33,000 manual and 14,000 walk-by automated meters with Itron Gen5 Riva smart meters that communicate over an RF mesh with cellular networks and run Linux-based distributed intelligence applications for outage detection, high impedance detection, and EV/solar identification, integrated with Itron's UtilityIQ head-end system [70].
- **Rappahannock Electric Cooperative (REC):** REC planned to transition from PLC technology to RF mesh AMI integrated with the NISC iVue platform, deploying smart meters across 180,000 connections over 22 counties to support time-of-use rates, DER participation, and enhanced grid operations through fiber network connectivity [71].
- **Sacramento Municipal Utility District (SMUD):** SMUD aims to deploy up to 200,000 Itron edge computing sensors beginning in September 2024, supporting eight distributed intelligence applications that will serve as the backbone for time-of-use rates, outage detection, DER integration, and edge computing capabilities within the municipal utility's smart grid ecosystem [72].

## A-2. IIJA GRIP projects implementing AI/ML Systems:

- **Consumers Energy:** Consumers Energy is targeting deployment of 18,000 Nvidia-powered AI modules (using Utilidata's Karman distributed AI platform) as meter collars or embedded meters to gain real-time grid edge visibility and determine where managed EV charging could serve as an alternative to traditional grid upgrades, with deployment planned for 2026 [73].
- **Tri-County Electric Cooperative:** Tri-County Electric proposed to deploy AI Dash satellite imagery software for vegetation management that can forecast wildfire risk 4 days in advance, combined with PwrMetrix AI/FireMetrix analytics platform that aggregates real-time data from RF meters, SCADA, and other systems to provide predictive outage forecasting and wildfire situational awareness across their South Carolina service territory [22].

- **GridUnity Inc.:** GridUnity proposed to deploy its DIGITAL platform with the Grid Analytics Learning Engine (GALE), an AI-powered cost estimation tool that streamlines interconnection studies by replacing fragmented communications between transmission organizations and owners with a centralized cloud-based workflow, aiming to reduce interconnection timelines from 30 months to 18 months initially, and eventually to 12 months [74].
- **Commonwealth Edison (ComEd):** ComEd proposed to deploy an Interoperable Control Framework in Rockford, Illinois that combines smart grid chips (SGCs) with distributed AI applications to train edge computing models using real-time grid data for demand forecasting, DER optimization, and automated grid control, alongside AI-based planning tools for DER integration and distributed intelligence functions running on next-generation AMI platforms [75].
- **Portland General Electric (PGE):** PGE proposed to deploy up to 90,000 SGCs powered by NVIDIA processors running Utilidata's distributed AI platform to analyze real-time waveform and grid edge data for predictive modeling, dynamic hosting capacity analysis, DER optimization, outage prediction, and autonomous grid control, with AI models achieving 90% accuracy in quantifying anomalies by 2027 [76].

## A-3. IIJA GRIP projects implementing DERMS:

- **American Electric Power (AEP):** AEP aims to deploy AspenTech/Open Systems International (OSI) Monarch ADMS with an integrated Operational DERMS module across seven operating companies serving 5.6 million customers in 11 states, consolidating 12 legacy systems (6 OMS and 6 DMS) into 2 unified ADMS instances that synthesize data from SCADA to AMI devices, enabling real-time DER visibility, automated fault location/isolation/restoration (FLISR), voltage optimization, and virtual power plant capabilities to improve SAIDI by 5% and deliver $1.9B in customer savings over 20 years [24].
- **Sacramento Municipal Utility District (SMUD):** SMUD's five-year "Connected Clean PowerCity" initiative includes 200,000 Itron edge-computing meters, layer an enhanced Open Systems International (OSI) DERMS onto the existing ADMS, modernize the Outage Management System (OMS), and install 100 miles of fiber, enable two-way management of solar, electric vehicles (EVs), battery storage, and smart appliances while providing fault location, automated restoration, and real-time market participation capabilities [72].
- **Tri-State Generation and Transmission Association:** Tri-State's "Cooperative Energy Ecosystem" proposed to deploy a multi-tenant DERMS platform across 42 distribution cooperatives serving more than 1 million rural customers in Colorado, Nebraska, New Mexico, and Wyoming, integrating over 200MW of controllable load (irrigation, thermostats, water heaters) and 1,000MW of utility-scale variable energy resources across 200,000 square miles, with an Energy Services Platform (ESP) for consumer engagement and PwrMetrix AI analytics for reliability benchmarking, targeting 4% demand response enrollment and $5.7M annual transmission upgrade deferrals [26].
- **Rappahannock Electric Cooperative (REC):** REC proposed to deploy a DERMS integrated with an AMI 2.0 upgrade (transitioning from power-line carrier to RF mesh meters) and fiber utility network across its 4,000-square-mile Virginia service territory, enabling real-time monitoring and control of DERs and EVs, virtual power plant capabilities, and enhanced grid resilience for 180,000 connections [71].
- **City of Naperville, Naperville Electric Utility (NEU):** NEU's three-year DERMS project would deploy a control room software platform that integrates with existing SCADA, OMS, Geographic Information System (GIS), and AMI systems to manage the city's rapid growth in solar (550+ producers), battery storage (20 installations), and electric vehicles (2,221+ EVs), enabling virtual power plant capabilities, demand response management, and increased hosting capacity to support Illinois' energy goals [77]

# Appendix B

The analysis completed in this section (shown in Table 1) assessed the projects funded under IIJA and BIL that were approved as of July 2025. Changes to these projects or new projects under similar funding sources are not assessed in this report.

*Table 1. Federal funding allocations for digital equipment programs under BIL/IIJA (2022-2026).*

| Program | Federal Allocation | Selections & Status | Typical Cost-Share |
|---|---|---|---|
| **Department of Energy (DOE) Grid Modernization Funds** | | | |
| **Grid Resilience & Innovation Partnerships (GRIP)** [78] three tracks (Grid Resilience, Smart Grid, Grid Innovation) | $10.5 billion across three funding mechanisms:<br>1. Grid Resilience Utility and Industry Grants ($2.5 billion)<br>2. Smart Grid Grants ($3 billion)<br>3. Grid Innovation Program ($5 billion) | Two funding rounds have now obligated $7.6 B for 105 projects across all 50 states; the FY24-25 FOA made $4.2 B available with awards announced April–June 2025 | 50 % (Smart Grid track), variable for others; small-utility set-asides and match waivers for resilience in disadvantaged communities |
| **High-Speed Broadband Programs (NTIA)** | | | |
| **Broadband Equity, Access, and Deployment (BEAD)** [79] | $42.45 B | As of 22 July 2025, all 56 states & territories have NTIA-approved Initial Proposals; challenge processes closed | Baseline 25 % match for deployment projects; waived in high-cost areas |
| **Middle-Mile Broadband** [80] | $1 B | $980 M awarded to 40 states/territories, building 20 000+ route-miles of fiber backbones | Match encouraged but not mandated (many recipients ~30 %) |
| **Tribal Broadband Connectivity** [81] | $3 B | Jan 2025 tranche recommended $162 M for four Tribal entities (round-2 of up to $1 B) | Varies by project; many Tribal governments contribute in-kind rights-of-way |
| **Battery Materials Processing & Manufacturing** | | | |
| **Battery Materials & Manufacturing Grants** [82] | $3 B total; $600 M / yr for FY 22-26 | Two complete rounds with 23 awardees. Round 3 notice of intent released 1/10/2025 to make $725 M available | 0% non-federal cost share for demonstration or commercial application projects. |
| **Digital Transportation Systems** | | | |

| Program | Federal Allocation | Selections & Status | Typical Cost-Share |
|---|---|---|---|
| **Strengthening Mobility and Revolutionizing Transportation (SMART)** [83] | SMART is a two-stage program. Stage 1 (up to $2M dollars and 18 months). Recipients of Stage 1 grants will be eligible to expand their projects through Stage 2 grants (up to $15M) | The SMART Grants program awarded 127 Stage 1 Planning and Prototyping Grants totaling over $200M across 45 states, DC, and Puerto Rico from FY2022-2024, plus eight Stage 2 Implementation Grants worth $85M across ten states. Of the $296M allocated for FY2022-2024, SMART has announced $289M in total awards, with additional Stage 2 rounds planned for 2025-2026. | SMART carries no federal match requirement |