Foreign Entity of Concern Requirements in the One Big Beautiful Bill Act

INL/RPT-25-89586

Center for Securing Digital Energy Technology (CSDET)

Digital Assurance Brief #3

NOVEMBER 2025

Idaho National Laboratory

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

INL/RPT-25-89586

Foreign Entity of Concern Requirements in the One Big Beautiful Bill Act

Digital Assurance Brief #3 - Technical Assistance for Digital Assurance (TADA) Program

NOVEMBER 2025

Idaho National Laboratory
National & Homeland Security
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

CONTENTS

ACRONYMS

BABA	Build America, Buy America
BPS	Bulk Power System
CIP	NERC Critical Infrastructure Protection
DOE	U.S. Department of Energy
FBOM	Firmware Bill of Materials
FEOC	Foreign Entity of Concern
FERC	Federal Energy Regulatory Commission
FIE	Foreign-Influenced Entity
HBOM	Hardware Bill of Materials
IRA	Inflation Reduction Act
INL	Idaho National Laboratory
IIJA	Infrastructure Investment and Jobs Act
IRS	Internal Revenue Service
ITC	Investment Tax Credit
IBR	Inverter-Based Resource
LLTF	Large Load Task Force
MW	Megawatt
NDAA	National Defense Authorization Act
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OBBB	One Big Beautiful Bill Act
OT	Operational Technology
PFE	Prohibited Foreign Entity
PRC	People's Republic of China
SBOM	Software Bill of Materials
SFE	Specified Foreign Entity
UFLS	Under Frequency Load Shedding
U.S.	United States

Page intentionally left blank

Foreign Entity of Concern Requirements in the One Big Beautiful Bill Act

Digital Assurance Brief #3

1. EXECUTIVE SUMMARY

Disclaimer: This analysis is based on information available as of November 2025. Additional guidance is expected to clarify details from OBBB.

The One Big Beautiful Bill Act (OBBB), enacted July 4, 2025, makes billions of dollars in federal energy tax credits conditional on supply chain independence from foreign suppliers and other foreign entities of concern. The OBBB simultaneously creates powerful economic incentives to reshore energy supply chains to the United States and allied nations. Through such incentives, the OBBB elevates digital assurance and supply chain verification from voluntary best practices into critical capabilities for demonstrating tax credit eligibility. The OBBB uses tax credit eligibility requirements to simultaneously address national security concerns regarding foreign supply chain dependencies and incentivize domestic energy manufacturing.

The OBBB attempts to achieve these objectives through Foreign Entity of Concern (FEOC) restrictions that make tax credit eligibility conditional on supply chain independence from the People's Republic of China (PRC) other countries of concern[1]. Organizations seeking investment tax credits (ITC) (Section 48E), production tax credits (Section 45Y), manufacturing tax credits (Section 45X), or carbon capture incentives (Section 45Q) must now prove supply chain independence through three independent eligibility tests. First, the "material assistance" test prohibits sourcing significant project value from Prohibited Foreign Entities (PFEs), with required non-FEOC content thresholds rising over time [1]. Second, the "direct control" test disqualifies projects where FEOCs hold 25 percent or greater ownership stakes, capturing minority interests that convey strategic influence [2]. Finally, the "effective control" test extends beyond equity ownership to capture operational dependencies including remote firmware access, intellectual property licensing, and cloud hosting arrangements with FEOC entities [2]. Failure of any single test disqualifies projects from claiming or retaining credits; Internal Revenue Service (IRS) oversight extends six-years and includes a ten-year recapture authority.

PRC dominance of critical supply chains creates considerable implementation challenges. Chinese manufacturers control 70-90 percent of global lithium-ion cell manufacturing capacity [3], as well as 65-86 percent of global shipments of inverters and associated power electronics [4]. Alternative suppliers in allied nations cannot absorb demand within OBBB timelines, and Treasury guidance clarifying detailed compliance requirements may not arrive until December 2026, one year after enforcement begins [5]. Additionally, there are increasing concerns that supply chains cannot reorient as quickly as necessary [6], with suppliers expressing difficulties in disclosing component origins. Reports suggest that some developers are warehousing components pending regulatory clarity [6].

Digital assurance capabilities provide the operational pathway forward. The United States (U.S.) Department of Energy's (DOE) cybersecurity principles, Idaho National Laboratory's (INL) procurement guidance, and National Institute of Standards and Technology's (NIST) supply chain risk management standards provide the architecture to demonstrate FEOC conformity. Organizations embedding comprehensive digital assurance practices such as granular supplier documentation, traceable component origin, continuous vendor monitoring, and operational independence verification into standard workflows will demonstrate credit eligibility and drive investor confidence.

[1] Named countries of concern include Russia, Iran, and North Korea, in addition to the PRC. The PRC is called out in text here due to the strong prevalence of PRC components in electric energy systems.

However, FEOC compliance is not a one-time documentation exercise but an ongoing operational capability requiring cross-functional integration across procurement, operational technology (OT) security, cybersecurity, and legal functions. Organizations that treat digital assurance as continuous verification rather than point-in-time certification will maintain compliance as supply chains evolve, vendor relationships change, and equipment undergoes lifecycle updates. Those that delay may face retrofit costs, audit exposure, and credit recapture risk. Organizations that embed digital assurance capabilities, however, will transform FEOC compliance from an administrative exercise into a competitive advantage that reduces systemic supply chain vulnerabilities which threaten grid reliability.

This brief details how organizations should operationalize these requirements through baseline compliance audits, interim documentation systems, supply chain diversification strategies, and long-term institutional integration of digital assurance capabilities that turn compliance burdens into competitive advantages.

2. EVOLUTION OF FOREIGN SUPPLIER DEPENDENCE

The U.S. electric grid's transformation from analog to digital control over the past four decades created deep dependencies on globalized electronics supply chains concentrated in the PRC. Federal modernization funding accelerated deployment of smart meters, automated distribution systems, and networked protection and control platforms beginning in 2009, embedding digital components throughout grid infrastructure [7]. The recent proliferation of battery storage, distributed generation, and advanced metering and control further tied grid operations to semiconductors, controllers, power electronics, and software systems, technologies where PRC manufacturers dominate global production. The PRC develops, manufactures and distributes a significant portion of the technologies that enable modern grid operations, including digital energy controllers and most semiconductor packaging facilities [3].

This offshoring creates systemic vulnerabilities: concentrated supply chains establish single points of failure for critical infrastructure, while reliance on a strategic competitor raises both cybersecurity and geopolitical risks. Recent reshoring initiatives including the CHIPS Act, Build America Buy America Act (BABA), and the Inflation Reduction Act's (IRA's) tax credits will likely require years to close these dependency gaps. Compliance with domestic content rules has proven administratively burdensome, with developers reporting difficulty tracing component origins, accessing supplier cost data, and securing certifications, especially under BABA and the IRA bonus credit [8]. FEOC restrictions build upon this regulatory landscape by making supply chain independence an economic prerequisite for federal tax credits, adding another layer of documentation requirements to an already complex compliance environment.

3. BACKGROUND: FEOC RESTRICTIONS IN OBBB

FEOC restrictions in OBBB represent the latest evolution of a multi-year legislative trajectory responding to national security concerns about foreign control – and particularly FEOC control – of energy infrastructure. Executive Order 14017 (February 2021) initiated comprehensive federal review of critical supply chain vulnerabilities in semiconductors, large-capacity batteries, and critical minerals [9]. The National Defense Authorization Act (NDAA) 2019 prohibited federal procurement of information and communications technology from designated foreign vendors, establishing precedent for component-level restrictions [10]. NDAA 2024 extended these prohibitions specifically to six major PRC battery manufacturers banning their products from federal procurement contracts [10]. The BABA Act mandated domestic content requirements for federally funded infrastructure projects, introducing percentage-based thresholds for U.S. manufacturing [11]. The Infrastructure Investment and Jobs Act (IIJA) introduced FEOC eligibility criteria for DOE grant programs, leading the concept of foreign entity restrictions in digital energy funding [12].

The IRA (2022) established the direct template later expanded by OBBB. Section 30D of the IRA applied FEOC restrictions specifically to electric vehicle tax credits, prohibiting battery components from "foreign entities of concern" and establishing phase-in thresholds for domestic content [13]. More recently, Executive Orders 14154 [11], 14156 [14], and 14262 [15]declared national energy emergencies and mobilized Defense Production Act authorities for supply chain resilience, demonstrating executive branch alignment with legislative efforts. State governments have enacted parallel restrictions, with Texas [16], Florida [17], Michigan [18], Tennessee [19], and Idaho [20] prohibiting entities from countries of concern from owning or controlling critical infrastructure including electric generation and transmission facilities. This policy evolution reflected bipartisan recognition that incentivizing advanced energy technology deployment required corresponding measures to prevent subsidizing adversaries or those which present foreign-sourcing risk.

4. FEOC: THE MECHANISM

The OBBB expands the FEOC framework established under the IRA by creating a unified definition of Prohibited Foreign Entities (PFEs). PFEs include both Specified Foreign Entities (SFEs) and Foreign-Influenced Entities (FIEs). An SFE is an organization incorporated in, headquartered in, or owned or controlled by the governments or nationals of China, Russia, Iran, or North Korea, or listed on U.S. restricted-party registers. In contrast, a Foreign-Influenced Entities (FIEs) is a firm that is not an SFE, but which exhibits qualifying levels of ownership, debt, or operational dependence on them.

These expanded definitions recognize that foreign influence operates through multiple mechanisms

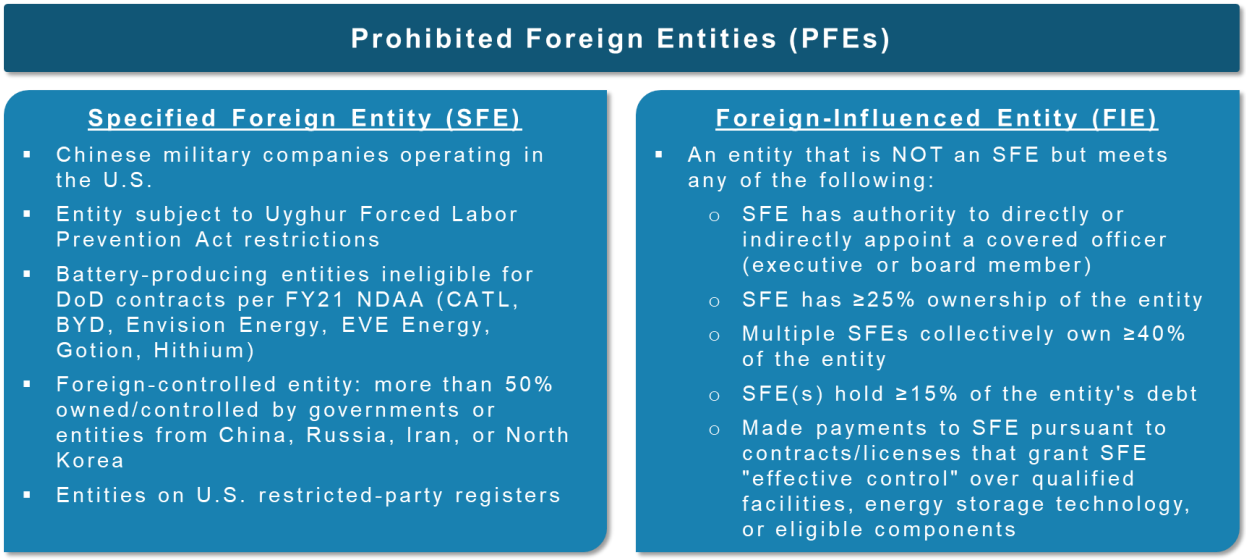

Figure 1. Definitions of PFEs, SFEs, and FIEs

beyond direct equity ownership, requiring corresponding breadth in compliance verification. Three independent tests enforce these requirements:

The “material-assistance” test determines project-level eligibility based on the proportion of total manufactured-product costs attributable to PFEs. Project costs for the material-assistance test refer only to the direct material costs of manufactured products and components used in a facility, excluding services, licensing fees, or financing expenses [21]. For qualified generation facilities, PFE-sourced costs may not exceed 40 percent for projects beginning construction in 2026, declining to 25 percent after 2029 [22]. For energy-storage systems, the limit begins at 45 percent in 2026 and falls to 25 percent after 2029 [22].

The “direct control” (or ownership-and-control) test deems an entity to be an FIE – and therefore an PFE - if an SFE owns, directly or indirectly, at least 25 percent of its equity, if multiple SFEs together

own 40 percent or more, or if SFEs hold 15 percent or more of the entity's total debt [2]. These thresholds apply to both direct and indirect ownership or financing relationships, including intermediary or layered corporate structures that confer equivalent control or economic benefit [21]. The test recognizes that minority ownership positions, when paired with board representation or preferential voting rights, can still provide effective influence over strategic decisions.

An entity also qualifies as an FIE if a SFE exercises *effective operational control* through contractual or technological arrangements rather than ownership [2]. Examples include long-term technology-licensing or data-hosting agreements granting a foreign party access to operational data, remote firmware-update privileges for grid-connected devices, or service contracts giving veto or dispatch authority [2].

FEOC compliance operates under continuous verification rather than a single point-in-time assessment. The IRS may reassess FEOC status for six years after initial tax filing, requiring developers to maintain comprehensive documentation of supplier relationships, ownership structures, and operational arrangements throughout this period [2]. The ten-year credit recapture provision creates extended liability: if prohibited FEOC relationships emerge through vendor acquisitions, contract modifications, or ownership changes, previously claimed credits become subject to repayment plus a 20 percent penalty [23].

This enforcement architecture makes FEOC compliance central to maintaining long-term project financial viability and thereby transforming digital assurance from voluntary best practice into mandatory evidence demonstrating supply chain independence, operational autonomy, and component origin. Organizations must prove not only that they avoided FEOC suppliers during initial procurement, but that they maintain FEOC independence throughout the oversight period as supplier circumstances, ownership structures, and service arrangements evolve.

5. COMPLIANCE CHALLENGES

OBBB's FEOC requirements strengthen incentives for domestic manufacturing but are accompanied by implementation challenges. Mandatory enforcement begins January 1, 2026, but Treasury safe-harbor guidance clarifying detailed compliance procedures is not required until December 31, 2026, leaving nearly a full year where developers bear full liability without regulatory clarity. This guidance gap combines four structural challenges that can slow the deployment of advanced digital technologies for the electric grid:

- **Supply chain reorientation cannot match policy timelines:** Forward-thinking developers began shifting procurement away from FEOC suppliers during 2024, but these diversification efforts cannot reorient supply chains as quickly as necessary. CATL alone controlled approximately 37 percent of global lithium-ion cell production in 2023, with limited immediate alternatives offering equivalent capacity, performance, and pricing [24, 25]. Alternative suppliers in Japan, South Korea, and emerging U.S. facilities may not be able to keep up with U.S. demand within OBBB's implementation timeline. BESS projects face the highest exposure due to concentrated manufacturing, with grid communications equipment similarly dependent on semiconductors and sensors where Asian supply chains dominate.
- **Documentation complexity exceeds current capabilities:** The Material Assistance test requires granular component-level documentation to track manufacturing origin, but detailed Software Bills of Materials (SBOMs), Hardware Bills of Materials (HBOMs), and subcomponent origin declarations needed to calculate thresholds accurately are often lacking. Open-source software components present challenges. Such software may include contributions from developers in foreign countries of concern, yet lacks the corporate ownership structures FEOC definitions presume, The Effective Control test demands evidence of operational independence, but standard equipment purchase agreements rarely address these issues with sufficient specificity.

- **International financing structures create hidden exposure:** Many distributed generation developments utilize tax equity partnerships, syndicated project finance, or offshore holding companies where ownership attribution requires complex legal analysis. Projects could inadvertently become FEOC-exposed if minority investors are acquired by FEOCs during the six-year IRS oversight period, requiring continuous monitoring of investor corporate structures and contractual provisions preventing ownership transfers that would jeopardize compliance.
- **Extended recapture periods alter project finance:** The ten-year credit recapture provision requires lenders and tax equity investors to evaluate FEOC risk not just at project closing but throughout the recapture period, potentially affecting financing costs and documentation requirements as compliance obligations extend beyond initial project commissioning.

6. MARKET IMPACTS

The compliance challenges described above impact the market in four distinct ways that are already affecting investment decisions and project timelines:

- **FEOC compliance shifts risk from suppliers to project owners**: Developers must obtain detailed supplier certifications, validate subcontractor relationships, and monitor corporate ownership structures during construction and initial operations. Utilities and independent generators then assume ongoing compliance risk throughout the six-year IRS oversight window and ten-year recapture period, requiring continuous monitoring of vendor relationships and operational dependencies. This requires new organizational capabilities most developers and utilities lack. Legal teams must understand supply chain architectures, procurement professionals must evaluate cybersecurity implications, and asset managers must track potential FEOC exposure throughout equipment operational life.
- **Vendor relationships create ongoing exposure:** Projects may become FEOC-exposed if vendors are later acquired by foreign entities, modify service contracts to include FEOC-controlled subcontractors, or migrate software platforms to cloud hosting involving FEOCs. Many inverter and BESS manufacturers retain remote access for firmware updates, creating potential supply chain vulnerabilities. Recent investigations of critical infrastructure targeting campaigns have highlighted firmware as a particularly challenging attack vector [24]. Firmware Bills of Materials (FBOMs), analogous to SBOMs but documenting firmware provenance and update chains, remain uncommon in energy equipment procurement, limiting visibility into firmware supply chain risks [25]. Project must negotiate contractual provisions ensuring owner control or implement air-gapped systems that sacrifice remote monitoring capabilities.
- **The compliance burden may lead to a consolidation of market power:** Vertically integrated developers with in-house supply chain management capabilities gain competitive advantages. Smaller developers lacking dedicated compliance staff face disproportionate documentation costs and difficulty obtaining supplier disclosures, potentially consolidating the market around larger firms and slowing deployment of distributed energy projects where smaller developers have historically driven innovation.
- **High compliance costs may incentivize foregoing credits rather than achieving compliance:** Limited non-PFE manufacturing capacity for critical components such as battery cells and power electronics enables compliant suppliers to command pricing premiums during the transition period. When combined with substantial documentation costs, ongoing monitoring expenses, and regulatory uncertainty pending December 2026 Treasury guidance, some developers may determine that total compliance costs exceed tax credit value. Organizations may forego credits entirely, resulting in infrastructure deployment without the digital assurance practices the policy was designed to encourage.

7. DIGITAL ASSURANCE: FROM VOLUNTARY BEST PRACTICE TO REGULATORY REQUIREMENT

The compliance challenges and market impacts described above require organizations to develop systematic approaches to demonstrating FEOC independence. While OBBB does not mandate cybersecurity requirements, organizations can leverage digital assurance capabilities to generate the documentation architecture needed for FEOC compliance. The fundamental insight is that proving FEOC independence requires the same technical infrastructure needed to secure supply chains against cyber threats: granular supplier documentation, traceable component origin, continuous vendor monitoring, and operational independence verification.

- **Established frameworks provide architecture:** DOE CESER principles [26], INL procurement guidance [27], and NIST C-SCRM standards [28] define the documentation and verification processes for demonstrating FEOC conformity. For utilities, North American Electric Reliability Corporation (NERC) Critical Infrastructure (CIP)-013 supply chain risk management programs provide the operational foundation while FEOC requirements extend existing vendor risk assessments to address foreign entity concerns.
- **Cybersecurity capabilities serve dual purpose:** Organizations verifying firmware update delivery paths can adapt similar controls used to prevent malicious code injection, although these capabilities serve distinct purposes. Network segmentation preventing unauthorized remote access demonstrates both cybersecurity protection and FEOC operational independence. However, many energy assets rely on authorized vendor remote access for operations and maintenance, requiring organizations to distinguish between prohibited FEOC control relationships and legitimate service arrangements with FEOC vendors. Effective Control compliance builds directly on NERC CIP-005 perimeter controls, CIP-010 configuration management, and CIP-013 vendor access governance.
- **SBOMs and HBOMs become prerequisites for compliance:** SBOMs enumerate code origins and license relationships that might create Effective Control exposure. HBOMs trace manufacturing origins through subassemblies to establish Material Assistance compliance. Firmware Bills of Materials (FBOMs) provide visibility into firmware origin, particularly relevant for inverters and battery systems [25]. Emerging frameworks such as the OpenSSF Supply Chain Integrity Working Group's SLSA provide standardized approaches for software supply chain verification [29]. While these documentation frameworks provide the conceptual architecture for FEOC compliance, industry capability to generate comprehensive bills of materials remains inconsistent, particularly for firmware and complex subassembly chains. This creates a gap between regulatory requirements and current practice.
- **Vendor assessments expand beyond cybersecurity:** Standard security assessments require additional analysis covering ownership structures, manufacturing facility locations, remote access protocols, data hosting arrangements, and intellectual property licensing terms.
- **Continuous origin tracking maintains compliance:** Tracking systems must identify triggering events during operations such as supplier acquisitions by foreign entities, contract modifications introducing FEOC subcontractors, vendor migration to FEOC-controlled platforms, or new service agreements creating payment obligations to foreign entities.
- **Cross-functional integration replaces silos:** Legal teams must understand supply chain architectures, procurement professionals must assess cybersecurity implications, engineering staff must document operational independence, and asset managers must monitor vendor changes. This level of cross-functional coordination may require investment in new

workflows, training, and collaboration mechanisms for organizations without established integration processes

- **Compliance capability is competitive advantage:** Early adopters implementing comprehensive digital assurance programs achieve faster project approvals, lower financing costs, and investor confidence. This alignment between FEOC compliance and operational excellence mirrors DOE's broader infrastructure strategy: capabilities that demonstrate tax credit eligibility simultaneously improve cybersecurity posture, reduce supply chain vulnerabilities, and enhance grid reliability.

8. RECOMMENDATIONS

Immediate Actions (2025): Baseline Compliance

- [Utilities] Conduct comprehensive inventories of digital assets identifying component origins and manufacturers, collecting HBOMs, SBOMs, and FBOMs for critical systems using standardized formats such as SPDX or CycloneDX, ensuring SBOMs meet NTIA Minimum Elements requirements including supplier names, component names, version strings, dependency relationships, and author information, and integrating foreign entity assessments into procurement processes with ongoing verification throughout equipment lifecycle.
- [Vendors] Provide comprehensive HBOMs/SBOMs identifying all components with country of origin and manufacturer details, disclosing sub-tier supplier relationships, and maintaining current documentation throughout product lifecycle including component changes or substitutions.
- [Utilities] Develop internal risk assessment frameworks for evaluating supplier foreign entity status and component origins while federal and state designation criteria are being finalized.

Near-Term Actions (2025-2026): Interim Framework Development

- [DOE] Publish clear frameworks for assessing PFE, FIE, and FEOC status including effective control determinations addressing ownership thresholds, intellectual property licensing arrangements, vendor access rights, and firmware development locations.
- [DOE] Leverage DOE national laboratory expertise to develop and deliver training programs for state agency and utility personnel on foreign entity assessment, supply chain risk management, and technical implementation of digital assurance controls.
- [Utilities] Integrate FEOC verification into NERC CIP-013 workflows embedding foreign entity screening into existing vendor risk management and change control processes rather than creating parallel compliance programs.
- [Utilities] Prohibit uncontrolled vendor remote access to OT systems requiring access only through utility-managed secure gateways that enable monitoring and session termination, with contracts mandating full disclosure of subcontracted cloud services and sub-tier dependencies.
- [Vendors] Implement secure remote access frameworks aligned with NERC CIP requirements with authenticated and encrypted connections, multi-factor authentication, utility visibility and audit capabilities, real-time monitoring or session termination, and elimination of always-on remote access in favor of just-in-time access provisioning for scheduled maintenance activities with automatic session expiration.
- [Vendors] Provide advance vulnerability notification under confidentiality agreements before public disclosure, enabling utilities to assess risk and implement mitigations or compensating controls while maintaining vendor confidentiality protections.

Medium-Term Actions (2026-2028): Supply Diversification and Institutional Maturation

- [DOE] Facilitate development of trusted supplier certification program in partnership with industry partners, enabling market-driven certification while maintaining consistency with federal requirements. Provide procurement preference and eligibility benefits for certified suppliers.
- [Utilities] Integrate cybersecurity and supply chain transparency requirements into request for proposals with adequate negotiation time, establishing safe harbors for security-driven updates that don't void warranties, and requiring documented commitments to lifecycle security support including vulnerability management throughout operational life.
- [DOE] Create funding mechanisms and peer learning forums specifically for state agency implementation of supply chain security programs, enabling states to build internal expertise while sharing implementation experiences and troubleshooting common challenges. Such resources can reduce compliance barriers that disproportionately affect smaller organizations, helping mitigate market consolidation toward well-resourced firms with in-house due diligence capabilities.
- [Utilities] Implement containment controls for already-deployed systems with foreign entity components including network segmentation isolating systems from enterprise networks, enhanced monitoring for unauthorized communication attempts or configuration changes, and integration into existing OT security programs and NERC CIP-013 compliance frameworks.
- [Utilities] Prioritize remediation of authentication vulnerabilities across deployed digital grid-edge assets with hard-coded passwords and insecure defaults, implementing Known Exploitable Vulnerability (KEV) catalog for patch prioritization, and deploying monitoring for industrial protocols including Modbus, DNP3, and IEC 61850.

Long-Term Actions (2026 and Beyond): Institutionalization and Competitive Advantage

- [Vendors] Pursue trusted supplier certification demonstrating transparent supply chains, secure-by-design practices, and vulnerability management programs as competitive differentiation.
- [Vendors] Guarantee minimum security support periods appropriate to equipment type. Typically, this is 20-30 years for hardware components, with documented software lifecycle plans including migration paths, end-of-support notifications, and technical enablement for asset owner implementation of compensating controls when software reaches end-of-life while hardware remains operational.

9. CONCLUSION

FEOC requirements in the OBBB significantly alter energy project development by making federal tax credit eligibility conditional on supply chain independence from countries of concern. The OBBB achieves two policy objectives simultaneously: creating economic incentives to reshore energy manufacturing and establishing enforceable supply chain verification standards for federally subsidized projects. The compliance documentation demanded by these FEOC restrictions elevates digital assurance practices into essential capabilities for organizations seeking to demonstrate tax credit eligibility.

Digital assurance capabilities provide a framework for addressing FEOC compliance requirements by serving dual purposes: strengthening cybersecurity while generating compliance evidence through SBOMs, HBOMs, vendor risk assessments, origin declarations, and continuous origin tracking systems. However, industry maturity varies considerably. While some vendors can produce standardized, comprehensive documentation, many lack established processes. Standards for these documentation frameworks continue to evolve, with adoption remaining inconsistent across manufacturers and equipment types.

Though digital assurance best practices have strong alignment with FEOC verification requirements, implementation challenges may create near-term obstacles. Non-domestic dominance of controllers and power electronics means alternative suppliers cannot absorb demand within OBBB timelines. The post-OBBB environment is likely to reward organizations who recognize that FEOC compliance is a structural prerequisite for accessing federal energy incentives. Digital assurance capabilities provide the framework for demonstrating legal compliance. Organizations that institutionalize these practices early may establish competitive advantages through demonstrated governance capabilities. However, the compliance burden creates market entry barriers consolidating power around firms with sophisticated institutional capabilities.

REFERENCES

[1] J. Davis, M. Sykes, N. C. Klugman, J. Jentz, S. Moradi and P.-T. Peng, "New law changes IRA Tax Credits," White & Case, 8 August 2025. [Online]. Available: https://www.whitecase.com/insight-alert/amendments-to-ira-tax-credits-congressional-budget-bill-july-6.

[2] X. Fishman, D. Elizalde, Z. Ureki and J. McGee, "Unpacking the FEOC Provisions in H.R. 1, the One Big Beautiful Bill Act," Bipartisan Policy Center, 28 July 2025. [Online]. Available: https://bipartisanpolicy.org/explainer/unpacking-the-feoc-provisions-in-the-one-big-beautiful-bill-act/.

[3] U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response, "Battery Energy Storage Systems Report," 1 November 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2025-01/BESSIE_supply-chain-battery-report_111124_OPENRELEASE_SJ_1.pdf.

[4] Wood Mackenzie, "Global PV inverter shipments grew by 10% in 2024 to 589 GWac," Wood Mackenzie, 10 July 2025. [Online]. Available: https://www.woodmac.com/press-releases/global-pv-inverter-shipments-grew-by-10-in-2024-to-589-gwac.

[5] K. Martin, D. Burton, H. Lefko and G. Jacques, "Working Through The FEOC Maze," Norton Rose Fulbright, 8 July 2025. [Online]. Available: https://www.projectfinance.law/publications/2025/july/working-through-the-feoc-maze/.

[6] J. Leonti and V. Morrison, "What's Next for US Energy Storage After OBBBA and Amid Continued Tariff Risk?," 23 September 2025. [Online]. Available: What's Next for US https://www.troutman.com/wp-content/uploads/2025/09/Whats-Next-for-US-Energy-Storage-After-OBBBA.pdf.

[7] U.S. DOE Office of Electricity Delivery and Energy Reliability, "Smart Grid Investment Grant Program Final Report," December 2016. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/03/f34/Final%20SGIG%20Report%20-%20Executive%20Summary.pdf.

[8] A. Fischer, "Navigating the challenges of domestic content compliance," PV Magazine USA, 5 March 2025. [Online]. Available: https://pv-magazine-usa.com/2025/03/05/navigating-the-challenges-of-domestic-content-compliance/.

[9] The White House, "Executive Order on America's Supply Chains," Biden White House Archives, 4 February 2021. [Online]. Available: https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

[10] 115th Congress (2017-2018), "H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019," 2018. [Online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

[11] The White House, "Executive Order 14154: Unleashing American Energy," 20 January 2025. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/01/unleashing-american-energy/.

[12] U.S. Department of Energy, "Build America, Buy America," [Online]. Available: https://www.energy.gov/management/build-america-buy-america. [Accessed 1 November 2025].

[13] U.S. DOE Office of Manufacuring and Energy Supply Chains , "Foreign Entity of Concern Interpretive Guidance," U.S. DOE, [Online]. Available: https://www.energy.gov/mesc/foreign-entity-concern-interpretive-guidance. [Accessed 1 November 2025].

[14] The White House, "Executive Order 14156: Declaring a National Energy Emergency," 20 January 2025. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/01/declaring-a-national-energy-emergency/.

[15] The White House, "Executive Order 14262: Strengthening the Reliability and Security of the United States Electric Grid," 8 April 2025. [Online]. Available: https://www.whitehouse.gov/presidential-actions/2025/04/strengthening-the-reliability-and-security-of-the-united-states-electric-grid/.

[16] "Texas Government Code, Chapter 2275: Prohibition on Contracts With Certain Foreign-Owned Companies in Connection With Critical Infrastructure," Texas Constitution and Statutes, [Online]. Available: https://statutes.capitol.texas.gov/?tab=1&code=GV&chapter=GV.2275&artSec=. [Accessed 1 November 2025].

[17] "CS/CS/SB 264 (2023): Interests of Foreign Countries," Florida Senate, 2023. [Online]. Available: https://www.flsenate.gov/Session/Bill/2023/264/BillText/c1/HTML. [Accessed 1 November 2025].

[18] "House Bill 4233 of 2025," Michigan Legislature, 2025. [Online]. Available: https://legislature.mi.gov/Bills/Bill?ObjectName=2025-HB-4233. [Accessed 1 November 2025].

[19] Gibson Dunn, "The Rise of State Laws Restricting Foreign Entities from Acquiring Property: Another Front in U.S.-China Tensions and the Constitutional Challenge of Florida SB 264 in Shen v. Simpson," Gibson Dunn, 12 September 2023. [Online]. Available: https://www.gibsondunn.com/rise-of-state-laws-restricting-foreign-entities-from-acquiring-property-another-front-in-us-china-tensions/.

[20] "Idaho Statutes, Title 55, Chapter 1, Section 55-103: Who May Own Property," Idaho Statutes, [Online]. Available: https://legislature.idaho.gov/statutesrules/idstat/Title55/T55CH1/SECT55-103/. [Accessed 1 November 2025].

[21] KPMG LLP, "Incentives and credits tax provisions in “One Big Beautiful Bill Act”," 28 July 2025. [Online]. Available: https://kpmg.com/kpmg-us/content/dam/kpmg/taxnewsflash/pdf/2025/05/kpmg-report-credits-one-big-beautiful-bill-may-15-2025.pdf.

[22] D. Burton, "A practical discussion of the One Big Beautiful Bill’s (OBBB) Foreign Entity of Concern (FEOC) rules," 1 October 2025. [Online]. Available: https://www.projectfinance.law/media/6082/nrf-presentation-a-practical-discussion-of-feoc-rules-10012025-revised-100125-2504922632.pdf.

[23] C. Chance, "One Big Beautiful Bill Act: The Impact on the Clean Energy Production Tax Credit and Investment Tax Credit," July 2025. [Online]. Available: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2025/07/one-big-beautiful-bill-act-the-impact-on-the-clean-energy-production-tax-credit-and-investment-tax-credit.pdf.

[24] D. Parr, "Li-ion Battery Market 2026-2036: Technologies, Players, Applications, Outlooks and Forecasts," IDTechEx, October 2025. [Online]. Available: https://www.idtechex.com/en/research-report/li-ion-battery-market/1132. [Accessed November 2025].

[25] Solar Builder, "Global LI-ion Battery Capacity to Expand by 7% by 2036," Solar Builder, 20 November 2025. [Online]. Available: https://solarbuildermag.com/energy-storage/global-li-ion-battery-capacity-to-expand-7-by-2036/.

[26] R. McKerchar, "Pacific Rim: Inside the Counter-Offensive—The TTPs Used to Neutralize China-Based Threats," Sophos, 31 October 2024. [Online]. Available: https://news.sophos.com/en-us/2024/10/31/pacific-rim-neutralizing-china-based-threat/ .

[27] Eclypsium, "Vulnerabilities in Netgear Firmware-Based IoT Devices In The Enterprise," Eclypsium, 16 July 2025. [Online]. Available: https://eclypsium.com/blog/vulnerabilities-in-netgear-firmware-based-iot-devices-in-the-enterprise/ .

[28] U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response, "Supply Chain Cybersecurity Principles," U.S. Department of Energy, June 2024. [Online]. Available: https://www.energy.gov/sites/default/files/2024-06/DOE%20Supply%20Chain%20Cyber%20Princples%20June%202024.pdf .

[29] E. M. Stewart, R. V. Stolworthy, S. Gribbin, T. L. Briggs and M. J. Culler, "Securing Digital Energy Infrastructure: Procurement, Contracting, and Supply Chain Risk Management Guidance," October 2024. [Online]. Available: https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_133245.pdf.

[30] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook and M. Fallon, "NIST Special Publication 800 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," May 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf.

[31] Open Source Security Foundation, "Supply Chain Integrity Working Group (wg-supply-chain-integrity)," Github, [Online]. Available: https://github.com/ossf/wg-supply-chain-integrity. [Accessed 1 November 2025].