COMMENTS ON NATIONAL STRATEGIC PLAN FOR ADVANCED MANUFACTURING

Docket No. OSTP-NSTC-2025-0001 / NIST-2025-0004

INTRODUCTION

The Global Data Alliance (GDA)[1] appreciates the opportunity to submit the following comments to the Office of Science and Technology Policy (OSTP) and the National Science and Technology Council (NSTC) Subcommittee on Advanced Manufacturing in response to the above-referenced Request for Information (RFI) on the development of a National Strategic Plan for Advanced Manufacturing ("Plan").

The GDA is a cross-sector coalition of companies that depend on the ability to access and transfer data across transnational digital networks to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders. GDA members are active in the following manufacturing sectors: automotive, aerospace, biopharmaceuticals, consumer goods, constructions, medical devices, transportation, telecommunications, and other AI- and advanced manufacturing technologies deployed across all sectors.

The GDA welcomes the Administration's commitment to revitalizing the United States advanced manufacturing base and restoring American leadership across critical industrial sectors. The GDA strongly supports this objective and submits these comments to highlight a set of policy challenges that, if not addressed in the Plan, risk undermining US advanced manufacturing competitiveness from within and from abroad.

Advanced manufacturing in the 21st century is inseparable from the digital infrastructure that enables it. AI-driven design, cloud-enabled production optimization, cross-border data flows, Digital Twins, computer-aided design and engineering (CAD/CAE), supply chain analytics, and real-time quality monitoring are not peripheral to advanced manufacturing — they are its operational core. The ability to move data securely and seamlessly across borders is therefore a foundational condition for US advanced manufacturing leadership.

The GDA's submission is organized around four distinct policy risks to US advanced manufacturing leadership that the Plan should specifically address:

- The harm to US advanced manufacturing from foreign cross-border data transfer barriers, data localization mandates, and other restrictions on cross-border access to technology, know-how, information, and data;

- The harm from foreign “digital sovereignty” requirements — protectionist measures that restrict market access for advanced products, services, and technologies from trading partners;
- The harm from discriminatory mandatory national standards or technical regulations that depart from prevailing international standards and WTO TBT Agreement safeguards; and
- The harm from digital protectionism at home, which — if pursued — risks fragmenting the open digital ecosystem upon which US advanced manufacturing competitiveness depends.

RECOMMENDATIONS

To protect and advance US advanced manufacturing leadership, the GDA urges OSTP and NSTC to incorporate the following recommendations into the National Strategic Plan for Advanced Manufacturing:

Recommendation 1: The Plan should recognize that open, secure cross-border data flows are a strategic input to US advanced manufacturing competitiveness and direct relevant Federal agencies to support international rules that protect US cross-border access to the knowledge, information, data, and digital tools that manufacturing depends on.

Recommendation 2: The Plan should direct the US government to actively identify and counter foreign “digital sovereignty” requirements – particularly via active diplomatic and other engagement – that discriminate against US-origin advanced manufacturing products, services, and technologies.

Recommendation 3: The Plan should call on the US government to defend and reinforce the international standards system — including WTO TBT Agreement disciplines — and ensure that foreign mandatory national standards or technical regulations that depart from international standards without adequate justification do not impede market access for US exported automotive, aerospace, biopharmaceutical, medical technology, and various AI-, quantum,- and ICT products and services.

Recommendation 4: The Plan should include a commitment not to pursue domestic digital protectionism in ways that would undermine the open, interoperable digital ecosystem upon which US advanced manufacturing competitiveness depends, and that could invite reciprocal measures from US trading partners.

Recommendation 5: The Plan should direct the US government to negotiate and implement international agreements with allies — including through the US-EU Joint Framework on Trade and Indo-Pacific economic engagement — that secure reciprocal, rule-based cross-border data access and that prohibit unjustified digital trade barriers in manufacturing-relevant sectors.

DISCUSSION

I. Cross-Border Data Flows as a Strategic Input to Advanced Manufacturing

Advanced manufacturing today is inherently data-intensive. AI-enabled production optimization, Digital Twins simulation, real-time supply chain monitoring, computer-aided design and engineering, predictive maintenance, and precision quality control all depend on the seamless cross-border movement of large volumes of data and on access to cloud-based analytical tools and enterprise software. The US manufacturing sector's ability to compete globally turns, in significant measure, on its ability to access and use this data — wherever in the world it originates.

Foreign data restrictions threaten this capability in measurable ways. Economic analyses by the World Bank, WTO, OECD, IMF, and independent researchers show that foreign cross-border data restrictions reduce GDP by an estimated 0.7–1.7%, reduce investment flows by approximately 4%, and impose productivity losses of approximately 4.5% on companies that depend on digital technologies. The World Bank has stated directly that "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies." These losses fall disproportionately on manufacturers, who rely on data flows at every stage of the value chain — from raw materials sourcing and R&D to production, quality assurance, logistics, and post-sale service.

The following sector-specific examples illustrate the breadth of this dependence:

- **Automotive (11 million US jobs; $105 billion in US exports):** The automotive sector depends on cross-border data flows for connected vehicle software updates, supply chain logistics, and the real-time monitoring of component performance across globally distributed manufacturing facilities. Restrictions on cross-border data access would impair the ability of US automakers to operate integrated global supply chains and to develop connected and autonomous vehicle technologies.
- **Aerospace (2.1 million US jobs; $90.6 billion in US exports):** Aerospace design and manufacturing involves collaborative R&D across multinational engineering teams, real-time monitoring of aircraft systems, and complex testing and certification processes that generate and transfer massive data sets across borders. Foreign data restrictions would disrupt these processes and increase costs for US aerospace manufacturers.
- **Semiconductors (1.6 million US jobs; $49 billion in US exports):** Semiconductor design involves an "innumerable number of cross-border data transfers" among hundreds of skilled engineers spread globally. The most advanced chips — with more than 50 billion transistors on a device smaller than a fingernail — cannot be designed without seamless cross-border data collaboration. Foreign data restrictions, including potential customs duties on electronic transmissions under consideration in several economies, would directly threaten US semiconductor competitiveness.
- **Medical Devices and Pharmaceuticals (3 million US jobs; $135 billion in US exports):** These sectors depend on cross-border access to clinical and health data for R&D, real-time patient monitoring, post-market surveillance, and the development of precision therapies. Cross-border data restrictions would impair every stage of the R&D and commercialization process for US medical technology companies.

- **Digital Twins and AI-Enabled Manufacturing:** Digital Twins technology — which allows US manufacturers to build, simulate, and measure performance in a virtual setting of their factories, products, and services — is particularly cross-border data dependent. Without reliable cross-border access to real-world operational data from globally distributed facilities, Digital Twins cannot replicate real-world conditions, nullifying one of the most powerful advanced manufacturing tools available.

Cross-border data restrictions harm US manufacturing industries in several concrete ways. First, data localization mandates force companies to fragment their global IT infrastructure, increasing costs and reducing the efficiency of cross-border manufacturing and supply chain operations. Second, restrictions on data transfers prevent manufacturers from deploying AI and analytics tools across their global operations, creating competitive disadvantages relative to overseas peers not subject to the same restrictions. Third, the unpredictability of foreign data policies increases compliance costs and deters investment in data-intensive production technologies.

The scale of the risk is significant. Approximately 40 million US jobs depend on international trade; 16 million US jobs are in software-related fields that underpin manufacturing operations; and the US manufacturing sector could need up to 3.8 million new workers in coming years, according to the National Association of Manufacturers. Foreign cross-border data restrictions — which have increased by 600% in the Asia-Pacific region alone in recent years — directly threaten the job creation potential of US advanced manufacturing in key export markets.

Moreover, the value of cross-border data access to US manufacturing extends beyond individual company operations. Cross-border data access enables supply chain risk monitoring across allied manufacturing networks, facilitates the coordination of R&D between US manufacturers and allied research institutions, and supports the defense industrial base's ability to maintain supply chain visibility and situational awareness — goals that the Departments of Defense, Energy, Agriculture, and Health and Human Services have each identified as national security priorities in their supply chain resilience reports issued pursuant to Executive Order 14017.

For these reasons, the National Strategic Plan for Advanced Manufacturing should explicitly recognize cross-border data access as a strategic enabler of US manufacturing competitiveness, and should direct relevant Federal agencies — including the Departments of Commerce, State, Defense, and Treasury, as well as USTR — to support international rules that protect US cross-border access to the knowledge, information, and digital tools upon which US manufacturers depend.

II. Foreign "Digital Sovereignty" Requirements as a Risk to US Advanced Manufacturing Leadership

Beyond data restrictions, US advanced manufacturing faces a growing threat from foreign "digital sovereignty" requirements — protectionist measures that restrict market access for advanced products, services, and technologies based on their national origin or on the origin of the digital tools and services embedded within them. These requirements, which are spreading across multiple major markets, threaten to exclude US-origin advanced manufacturing technologies from

global markets on grounds that have nothing to do with the safety, quality, or performance of those technologies.

As the GDA and BSA noted in their March 2026 submission on the US-EU Joint Framework on Trade, these measures take a variety of forms:

- **Ownership and control requirements:** Requirements that advanced technology products or services be owned or majority-controlled by nationals of the importing country, or that senior management or operational personnel hold national citizenship. These requirements discriminate against US-origin products and services on the basis of corporate nationality rather than on any functional criterion.
- **National origin exclusions in procurement and certification:** Eligibility conditions for government procurement or regulatory certification that broadly exclude products or services due to their "country of origin" or origin-based "dependency" arguments. Such measures can directly close government procurement markets — which account for 10–15% of GDP in most major economies — to US advanced manufacturing products and services. They also create barriers to regulatory approval for products whose certification depends on cross-border data access or cloud-based verification.
- **Insulation-from-foreign-jurisdiction requirements:** Requirements that service providers be "insulated from foreign legal jurisdiction" — a criterion that, by design, targets US providers subject to US legal requirements, including US national security and export control laws. This type of requirement creates a false and unacceptable choice between compliance with US law and access to overseas markets.
- **Mandatory use of locally developed technology:** Requirements that products incorporate locally developed components, software, or AI models — regardless of whether those components meet the same performance or security standards as US-origin alternatives. These measures are technology content rules in all but name, and directly discriminate against US manufacturers by mandating substitution of superior US-origin technology with inferior local alternatives.
- **Continuity of service risks:** Some trading partners have threatened or imposed measures designed to interrupt US companies' ability to provide continuity of service to customers in those markets, based on broader geopolitical disputes. This creates investment and market access risk for US advanced manufacturing exporters who depend on reliable software and digital service delivery to support their products in overseas markets.

These digital sovereignty requirements impose costs on US advanced manufacturing that extend far beyond the direct loss of market access. They fragment the global standards ecosystem, create compliance complexity for US manufacturers operating across multiple markets, undermine the interoperability of US-origin products and services with global supply chains, and increase costs for overseas customers of US advanced manufacturing products by restricting their ability to use best-in-class technology.

As noted in the GDA/BSA March 2026 Joint Framework submission, the transatlantic economy illustrates the cost of these dynamics: with daily trade flows averaging $4.0 billion and total

transatlantic investment stock of $4.8 trillion, even marginal increases in digital trade barriers impose substantial costs across interconnected manufacturing supply chains.

Several of these digital sovereignty measures may also implicate WTO disciplines. Requirements that condition market access, regulatory approval, certification, or government procurement on national origin of products or services, nationality of suppliers, or location of data or computing facilities can implicate WTO national treatment obligations under the GATT, the GATS, the TBT Agreement, the TRIPS Agreement, and the Agreement on Government Procurement (GPA), among others. The Plan should direct USTR and the Department of Commerce to identify and challenge such measures in available negotiating contexts.

The Plan should further direct the US government to negotiate affirmative commitments with trading partners — through bilateral trade frameworks, plurilateral digital economy agreements, and WTO disciplines — not to impose impermissible digital sovereignty requirements on US-origin advanced manufacturing products, services, and technologies. These commitments should include, as the GDA and BSA have recommended in the US-EU Joint Framework context, specific disciplines against: (1) conditioning market access or government procurement on national origin or other improper criteria; or (2) interrupting continuity of service for lawful digital tools.

III. Discriminatory National Standards and Technical Regulations as a Risk to US Advanced Manufacturing

A third major risk to US advanced manufacturing leadership comes from foreign mandatory national standards and technical regulations that depart from prevailing international standards and from the non-discrimination principles embedded in the WTO Agreement on Technical Barriers to Trade (TBT Agreement). The TBT Agreement requires countries to use international standards as the basis for technical regulations where relevant international standards exist, and prohibits technical regulations that create unnecessary obstacles to trade.

The Plan should address this risk because manufacturing's dependence on digital technology makes it particularly vulnerable to divergent standards. When countries impose mandatory national standards for AI, cybersecurity, connected devices, automotive technologies (e.g., autonomous vehicular technologies), industrial robotics, or other digitally-enabled or manufacturing technologies that depart from international norms, US manufacturers face a choice between: (1) developing costly, market-specific product versions; (2) forgoing market access; or (3) in some cases, transferring or disclosing sensitive IP as a condition of market access. None of these outcomes advances US manufacturing competitiveness.

The following forms of divergent standards are of particular concern:

- **AI and software standards:** Several major economies are developing mandatory national AI and software standards that diverge from international standards bodies such as ISO, IEC, and IEEE. Mandatory divergent AI standards impose market-specific compliance costs on US AI software and AI-enabled manufacturing product companies, and can effectively require US manufacturers to develop separate product versions for different markets. The US should lead in international AI standards bodies — including

ISO/IEC JTC1/SC42 on artificial intelligence — to ensure that international AI standards reflect US values and technical approaches.

- **Cybersecurity certification requirements:** Mandatory national cybersecurity certification schemes that depart from internationally recognized standards such as ISO/IEC 27001 and IEC 62443 fragment the global cybersecurity compliance landscape. Some such schemes condition certification on requirements — including source code disclosure, algorithm disclosure, or government back-door access — that have no basis in international standards and impose significant IP risks on US technology companies. Such requirements may constitute de facto barriers to trade and should be challenged under the TBT Agreement.
- **Mandatory source code and algorithm disclosure:** Technical regulations in several markets require disclosure of source code or encryption algorithms as a condition of market access. These requirements — which have no basis in international standards — impose significant IP risks on US advanced manufacturing technology companies and may constitute forced technology transfer. They also undermine cybersecurity by compelling disclosure of sensitive technical information to foreign governments.
- **Divergent product safety and certification requirements for connected devices:** Mandatory technical regulations for connected manufacturing equipment, autonomous industrial vehicles, robotic systems, and other advanced manufacturing products that depart from international standards without adequate technical justification impose fragmentation costs on US manufacturers. These costs are particularly acute for small and medium-sized US manufacturers, which lack the resources of large enterprises to maintain compliance with multiple divergent national standards regimes.

The Plan should reinforce the US government's commitment to the international standards system and direct relevant agencies to: (1) actively participate in and lead international standards bodies including ISO, IEC, IEEE, and ITU, particularly for AI, cybersecurity, additive manufacturing, robotics, and other advanced manufacturing technologies; (2) systematically challenge foreign technical regulations that depart from international standards without adequate justification under the TBT Agreement; and (3) engage trading partners bilaterally and multilaterally to promote the adoption of international standards in manufacturing-relevant technology sectors.

NIST's long leadership in standards development — including through the NIST Cybersecurity Framework, NIST AI Risk Management Framework, and NIST's participation in international standards bodies — positions it to play a central role in implementing this element of the Plan. The Plan should specifically direct NIST to: (1) expand its engagement in international standards bodies for AI and cybersecurity; (2) maintain alignment between US domestic standards and international standards; and (3) develop guidance for US manufacturers on navigating divergent foreign standards and seeking TBT challenges where appropriate.

The Plan should also commit that US domestic standards processes — including mandatory standards developed by Federal agencies for AI, cybersecurity, and other advanced technologies — will be: (1) aligned with international standards where relevant; (2) transparent and open to broad industry participation; and (3) developed through processes that comply with US obligations under the TBT Agreement. US credibility in challenging foreign discriminatory standards depends in part on the integrity of our own standards processes.

IV. The Risk to US Advanced Manufacturing from Digital Protectionism at Home

A fourth risk to US advanced manufacturing leadership — one that may be less intuitive but is no ess significant — comes from domestic digital protectionism. Well-intentioned domestic policies designed to promote US manufacturing capacity can, if poorly designed, impose costs on US advanced manufacturers that undermine rather than advance US competitiveness. The Plan should specifically guard against the following risks:

- **Data localization mandates:** Domestic requirements to store or process manufacturing-related data within US borders can increase costs for US manufacturers operating globally, prevent access to international cloud infrastructure and analytics capabilities, and invite reciprocal data localization requirements from US trading partners that would restrict US access to overseas markets and data. The GDA's prior submissions have documented that data localization mandates increase trade costs by up to 80% for affected businesses — costs that fall disproportionately on small and medium-sized manufacturers. Rather than the types of self-defeating localization mandates that some other countries promote, the United States should rely on existing legal frameworks to address legitimate data security concerns. To this end, the Plan should commit to cross-border data flows with trusted partners as a baseline policy position; adopting risk-based frameworks like the US-EU Data Privacy Framework where necessary; and turning to national security-focused frameworks (such as the US Department of Justice's Data Security Program, and the FTC's authority under the Protecting Americans' Data from Foreign Adversaries Act) in the case of bulk transfers of sensitive data to adversarial economies.
- **Origin-based procurement preferences that exclude allied suppliers:** Buy American requirements or procurement preferences that discriminate against allied-nation suppliers of advanced manufacturing technology — including enterprise software, cloud services, AI tools, and industrial machinery — can increase costs for US manufacturers that depend on best-in-class technology regardless of origin, and can invite reciprocal discrimination against US advanced manufacturing exports. The US government's own advanced manufacturing operations — including at national laboratories and defense facilities — depend on access to international technology. Where necessary, polices to promote domestic technology development should be performance-based and calibrated to genuine national security needs, not broad origin-based exclusions inconsistent with GPA obligations and allied relationships.
- **Overly broad technology export controls:** Export controls on advanced manufacturing technologies, AI, and related software are a legitimate and important national security tool. However, controls that are overly broad — extending beyond genuine national security risks to restrict the ability of US manufacturers to use and deploy advanced technologies in their global operations, or imposing significant compliance burdens on allied-nation technology transfers without commensurate national security benefit — can impose competitive disadvantages on US advanced manufacturers vis-à-vis overseas competitors not subject to equivalent controls. The Plan should call for a calibrated, risk-based, and allied-coordinated approach to technology export controls that protects

genuine national security interests while minimizing impact on US manufacturing competitiveness.

- **Failure to negotiate cross-border data access rules with allies:** Perhaps the most consequential form of domestic digital policy failure is the failure to negotiate with US allies to establish rules that protect future US cross-border data access. This failure creates a vacuum that adversaries are actively filling. China has announced pilot projects on cross-border data transfers with US allies including Chile, New Zealand, Singapore, and South Korea, and plans to "accelerate the establishment of mechanisms for cooperation regarding cross-border data transfers" with additional economies. If the United States does not negotiate with its allies to secure future cross-border data access on terms consistent with US values and law, it risks ceding that space to adversaries whose data governance model fundamentally conflicts with the open digital ecosystem that US advanced manufacturing depends on. Over 100 members of Congress have called on the US government to reengage on cross-border data negotiations with allies, citing the threat to "strong and resilient supply chains."

The GDA strongly supports the Administration's commitment to restoring and growing US manufacturing. However, the most effective way to achieve this goal is through investments that strengthen the US innovation ecosystem and promote competitive markets — not through measures that fragment the open digital ecosystem that US advanced manufacturing depends on. As the GDA and BSA argued in their March 2026 submission on the US-EU Joint Framework on Trade:

> *"Durable technological resilience is built on strong standards, transparent governance, and the freedom to operate in an open and interconnected digital ecosystem — not on the geographic origin of each technology element."*

The economic evidence confirms this point. World Bank analysis indicates that countries would gain an average of 4.5% in productivity from removing data restrictions — a benefit equivalent to an estimated $1.26–1.4 trillion in value creation when applied to US GDP. The Bureau of Economic Analysis estimates that the digital economy added $2.6 trillion to US GDP in 2022, with cross-border data transactions estimated to represent 25–40% of digital economy activity. McKinsey Institute analysis estimates that data transfers will add over $11 trillion to global GDP by 2025, of which the US — accounting for roughly 15% of global GDP — stands to capture an estimated $1.65 trillion. Digital protectionism at home would jeopardize a significant share of these gains.

The Plan should include an explicit commitment not to pursue domestic digital protectionism in ways that undermine the open, interoperable digital ecosystem upon which US advanced manufacturing competitiveness depends. It should further commit to policies that maintain US credibility as a champion of open, rules-based cross-border data access — credibility that is essential to the US government's ability to challenge foreign digital trade barriers on behalf of US manufacturers.

CONCLUSION

The GDA strongly supports the Administration's commitment to restoring American advanced manufacturing leadership and welcomes OSTP's effort to develop a comprehensive National Strategic Plan for Advanced Manufacturing. Achieving the Plan's goals will require not only domestic investment and workforce development, but also a proactive strategy to address the foreign digital barriers that are increasingly constraining US manufacturers' ability to compete in global markets and to access the cross-border data flows upon which their operations depend.

The National Strategic Plan for Advanced Manufacturing has an important opportunity to recognize four categories of digital policy risk to US manufacturing competitiveness — foreign cross-border data restrictions, digital sovereignty protectionism, divergent mandatory standards, and domestic digital protectionism — and to direct the US government to address them systematically through trade policy, international standards engagement, and bilateral and multilateral digital trade negotiations with US allies.

The GDA stands ready to support OSTP and NSTC in developing and implementing the Plan, providing technical expertise, economic data, and stakeholder engagement from GDA members across the full range of manufacturing-dependent industries. We thank OSTP and NSTC for the opportunity to submit these comments and look forward to continued engagement on the National Strategic Plan for Advanced Manufacturing.

---

[1] The GDA is a cross-sector coalition of companies that depend on the ability to access and transfer data across transnational digital networks to innovate and create jobs. Administered by BSA | The Software Alliance, the Global Data Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders. GDA members are active in the following sectors: agriculture, automotive, aviation, biopharmaceutical R&D, consumer goods, energy, finance, healthcare, hospitality, manufacturing, media, supply chain, and telecommunications. For more information, see https://www.globaldataalliance.org