DRAFT – Supply Chain Logistics Recommendations

Recommendation 1: The federal government should consider establishing a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management.

Description:

The federal government should consider establishing a comprehensive national IoT strategy that outlines clear goals and objectives for IoT adoption in supply chain management. This strategy should encompass regulatory frameworks, infrastructure development, education, and incentives for implementation.

Justification:

The justification for developing a national IoT strategy lies in the numerous benefits that IoT can bring to various industries, including supply chain management, as well as the overall economy and society. A comprehensive and coordinated national IoT strategy can help ensure that these benefits are fully realized and that potential challenges and risks are adequately addressed. Here are some key justifications for developing a national IoT strategy:

- Economic growth and competitiveness: A national IoT strategy for adoption in supply chain management can foster innovation, drive economic growth, and enhance the competitiveness of industries by promoting the widespread adoption and integration of IoT technologies. This can lead to increased productivity, reduced operational costs, and new business opportunities across various sectors.
- Enhanced efficiency and resilience of supply chains: IoT technologies can significantly improve supply chain efficiency, transparency, and resilience by enabling real-time monitoring, data-driven decision-making, and automation of processes. A national IoT strategy can provide guidance and support for businesses to adopt and integrate IoT solutions within their supply chains, thereby enhancing overall supply chain performance.
- Job creation and workforce development: The widespread adoption of IoT technologies will lead to the creation of new jobs and the need for skilled workers in areas such as data analytics, IoT device development, and cybersecurity. A national IoT strategy for adoption in supply chain management can help guide investments in education and workforce development to ensure that citizens are equipped with the necessary skills for the future IoT-driven job market.
- Addressing cybersecurity and privacy concerns: As IoT devices generate and process large amounts of data, there are inherent risks related to cybersecurity and data privacy. A national IoT strategy for supply chain management can help establish guidelines, standards, and best practices for IoT security and data protection, ensuring that the risks are adequately addressed and managed.
- Encouraging collaboration and standardization: A national IoT strategy can promote collaboration among businesses, academia, and government agencies, fostering innovation and knowledge sharing. Furthermore, it can help drive the development and adoption of IoT standards for supply chain management, which are essential for interoperability, security, and scalability of IoT solutions.
- Ensuring equitable access and benefits: A national IoT strategy can ensure that the benefits of IoT technologies are distributed equitably across enterprises engaged in supply chain management, addressing potential digital divides and promoting inclusive growth.

Implementation Considerations:

- Stakeholder engagement: Engage with key stakeholders, including businesses, academia, and government agencies, to identify priorities, needs, and challenges related to IoT adoption in

supply chain management. This collaboration will ensure the strategy is comprehensive, practical, and aligned with industry requirements.

- Focus on key areas: Prioritize areas within the supply chain where IoT can provide the most significant benefits and address the most pressing challenges, such as inventory management, transportation and logistics, and quality control.
- Support innovation and R&D: Foster innovation and R&D in IoT technologies by providing funding, incentives, and resources to businesses and research institutions. This will accelerate the development and commercialization of advanced IoT solutions tailored to supply chain management.
- Develop standards and guidelines: Establish standards and guidelines for IoT implementation in supply chain management, focusing on interoperability, security, and data privacy. This will facilitate seamless integration and adoption of IoT technologies across supply chains while addressing potential risks.
- Promote workforce development: Invest in education and workforce development programs to ensure that workers have the necessary skills and expertise to thrive in an IoT-driven supply chain environment.
- Encourage public-private partnerships: Foster collaboration between public and private sectors to promote IoT adoption in supply chain management, share knowledge, and address common challenges.
- Monitor progress and adapt: Establish mechanisms to monitor and evaluate the progress of IoT adoption in supply chain management, and adapt the national strategy as needed based on emerging trends, technologies, and challenges.

Potential implementation barriers: *(may need revision – these are more focused on overall barriers to adoption)*

- Funding constraints: Allocating sufficient funds to support IoT infrastructure, research and development, and workforce development initiatives can be a challenge, especially when competing with other national priorities.
- Interagency coordination: Developing a national IoT strategy requires close coordination among various federal agencies, which may have different goals, agendas, and regulatory frameworks. Ensuring a cohesive and consistent approach across agencies can be challenging.
- Resistance to change: Some stakeholders within the supply chain ecosystem may resist adopting IoT technologies due to concerns about job displacement, technological complexity, or fear of change. Overcoming this resistance requires effective communication, education, and change management strategies.
- Cybersecurity and data privacy concerns: Ensuring the security and privacy of the vast amounts of data generated by IoT devices is a significant challenge. Addressing these concerns requires investment in robust security measures and the development of comprehensive data protection policies and regulations.
- Standardization and interoperability: The IoT ecosystem consists of a wide variety of devices, platforms, and communication protocols. Developing and enforcing standards for interoperability can be a complex and time-consuming process, which may slow down the implementation of a national IoT strategy.
- Skilled workforce shortage: The rapid growth of IoT technologies and applications may outpace the availability of a skilled workforce in fields such as data analytics, IoT device development, and cybersecurity. Addressing this talent gap requires investments in education and workforce development programs.

- Legal and regulatory barriers: Existing laws and regulations may not adequately address the unique challenges posed by IoT technologies in supply chain management. Updating and harmonizing these legal and regulatory frameworks can be a complex and time-consuming process.
- Balancing innovation and regulation: Striking the right balance between promoting innovation and ensuring consumer protection, security, and privacy can be challenging. The federal government must carefully consider the potential trade-offs and unintended consequences of new regulations on IoT adoption and innovation.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Federal Trade Commission, the Department of Transportation, the Department of Energy, and the National Institute of Standards and Technology, among others.

Federal considerations:

- Aligning the strategy with broader national priorities and policies, such as economic growth, job creation, and environmental sustainability.
- Engaging with industry associations and international organizations to ensure that the strategy is in line with global trends and best practices.
- Coordinating efforts and resources across federal agencies to avoid duplication and ensure a cohesive approach.
- Providing financial and technical support to businesses, especially small and medium-sized enterprises, to help them overcome barriers to IoT adoption.
- Ensuring that the strategy addresses the concerns and needs of all stakeholders, including businesses, workers, consumers, and communities.

Recommendation 2: The federal government should consider creating industry standards and protocols.

Description:

The recommendation to consider creating industry standards and protocols is aimed at promoting the widespread adoption of IoT technology in supply chain management by ensuring interoperability, reliability, and security across various IoT systems and devices. By establishing a set of common standards and protocols, businesses can seamlessly integrate IoT solutions into their existing supply chain operations, facilitating data exchange, and enabling more efficient and informed decision-making processes.

Developing industry standards and protocols involves collaboration between government agencies, industry stakeholders, technology providers, and researchers to identify the key requirements and specifications for IoT systems in supply chain management. This may include addressing issues such as data formats, communication protocols, security measures, and device compatibility, among others.

To implement this recommendation, the government should support and participate in relevant standard-setting organizations and industry-led initiatives, working closely with stakeholders to develop consensus-based standards and protocols tailored to the unique needs and challenges of supply chain management. These standards should be flexible and adaptable, allowing for continuous innovation and improvement as technology evolves.

In addition, the government should promote the adoption of these standards and protocols through education and awareness campaigns, providing businesses with the necessary resources and guidance to successfully implement IoT solutions in their supply chain operations. By creating industry standards and protocols, the government can help to create a stable and unified foundation for IoT technology, driving its widespread adoption, and maximizing its potential benefits for businesses and consumers alike.

Justification:

The justification for creating industry standards and protocols in the context of IoT technology adoption, particularly for supply chain management, lies in several key benefits that they offer:

1. Interoperability: Industry standards and protocols ensure that IoT devices, systems, and platforms from different manufacturers can communicate and work together seamlessly. This is crucial for the successful integration of IoT technologies into complex supply chains, where multiple stakeholders and systems are involved.

2. Scalability: Standardization enables businesses to scale their IoT implementations more easily, as they can rely on a consistent set of protocols and guidelines when adding new devices or expanding their IoT networks. This lowers the risk of incompatibilities and simplifies the process of integrating new components.

3. Innovation and competition: Standards and protocols can stimulate innovation and competition by providing a level playing field for businesses and developers, regardless of their size or market share. This encourages the development of new products and services that adhere to established standards, ultimately benefiting consumers and the entire industry.

4. Cybersecurity and data privacy: By establishing robust security protocols and guidelines for data protection, industry standards can help address the inherent risks associated with IoT, such as cybersecurity threats and data privacy concerns. This fosters consumer trust and promotes the adoption of IoT technologies across the supply chain.

5. Simplified integration and maintenance: Industry standards and protocols streamline the process of integrating IoT technologies into existing systems and processes, reducing the time and resources required for implementation. Furthermore, standardized systems are typically easier to maintain and troubleshoot, as they follow a common set of guidelines and best practices.

6. Cost savings: Standardization can lead to cost savings for businesses by reducing the need for customized solutions and simplifying the procurement process. It also promotes economies of scale, as standardized components and devices can be produced more efficiently, leading to lower costs for manufacturers and end-users.

7. Regulatory compliance: Standards and protocols can serve as a foundation for government regulations and policies related to IoT and supply chain management. This helps ensure that businesses adhere to best practices for security, privacy, and environmental impact, enhancing the overall stability and sustainability of the IoT ecosystem.

By creating industry standards and protocols for IoT technologies in supply chain management, stakeholders can enjoy a range of benefits that ultimately lead to improved efficiency, security, and innovation within the industry. These standards serve as a crucial foundation for the widespread adoption and integration of IoT technologies, enabling businesses to fully realize their potential benefits while addressing potential challenges and risks.

Implementation Considerations:

Implementation considerations for creating industry standards and protocols for supply chain include:

1. Inclusiveness: Involve a diverse range of stakeholders, including businesses, technology providers, academia, and government agencies, in the development of standards and protocols. This ensures that the resulting guidelines are comprehensive, practical, and aligned with the needs and priorities of all relevant parties.

2. Prioritize critical areas: Focus on the most critical aspects of supply chain management where standardization can yield significant benefits, such as data exchange, device interoperability, security, and privacy.

3. Build on existing standards: Leverage existing industry standards and best practices as a starting point, and adapt or expand upon them as necessary to address the specific requirements of supply chain management.

4. Flexibility and adaptability: Design standards and protocols that are flexible and can be easily updated to accommodate new technologies, emerging threats, and evolving industry needs.

5. Promote adoption: Encourage and incentivize businesses to adopt the established standards and protocols through education, outreach, and support programs.

6. Ensure compliance: Develop mechanisms to monitor and enforce compliance with the established standards and protocols, including certifications, audits, and penalties for non-compliance.

Potential implementation barriers:

Possible barriers to implementing this recommendation include:

1. Resistance to standardization: Some businesses and stakeholders may resist standardization efforts due to concerns about the potential loss of competitive advantage, customization capabilities, or intellectual property rights.

2. Fragmentation: The IoT landscape is highly fragmented, with numerous vendors, platforms, and technologies. Achieving consensus and collaboration among all stakeholders can be challenging.

3. Cost and resource constraints: Developing and implementing industry standards and protocols can be resource-intensive, requiring significant investments in time, money, and expertise.

4. Rapid technological advancements: The IoT field is rapidly evolving, making it difficult to keep standards and protocols up-to-date and relevant.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC), the Department of Commerce, the Department of Transportation, and the Federal Communications Commission (FCC), among others.

Federal considerations:

In implementing industry standards and protocols for supply chain, the federal government should consider:

1. Providing a regulatory framework that supports standardization efforts while also promoting innovation and competition.

2. Collaborating with international organizations and foreign governments to ensure that the developed standards and protocols are globally relevant and can be harmonized with international guidelines.

3. Offering financial and technical support to businesses, particularly small and medium-sized enterprises, to help them adopt and comply with the established standards and protocols.

4. Monitoring and evaluating the effectiveness of the standards and protocols over time, and making adjustments as needed to address emerging challenges and opportunities.

By taking these factors into account, the federal government can facilitate the development and implementation of effective industry standards and protocols for IoT in supply chain management, driving the widespread adoption of IoT technologies and maximizing their benefits while mitigating potential risks.

Recommendation 3: The federal government should consider providing financial incentives.

Description:

The recommendation to establish and provide financial incentives aims to encourage businesses to adopt IoT technologies in their supply chain operations by reducing the initial investment costs and perceived risks associated with the implementation of IoT solutions. Financial incentives, such as tax breaks, grants, subsidies, or low-interest loans, can help lower the financial barriers for companies to experiment with and deploy IoT systems, leading to more widespread adoption and innovation in the sector.

By offering financial support, the government can promote the development and integration of IoT solutions into supply chain management, enabling businesses to capitalize on the various benefits IoT offers, such as improved efficiency, transparency, and resilience. Furthermore, financial incentives can stimulate private sector investment, drive the growth of IoT technology providers, and foster an ecosystem that encourages collaboration and innovation within the industry.

It is crucial, however, for the government to carefully design and target these financial incentives, ensuring that they align with strategic objectives and deliver measurable impact. By doing so, the federal government can effectively drive IoT adoption in supply chain management, unlocking its full potential to transform the industry and strengthen national competitiveness.

Justification:

The justification for providing financial incentives as a recommendation is to accelerate the adoption of IoT technology in supply chain management, particularly within the manufacturing sector. Financial incentives can lower the initial barriers to entry, making IoT adoption more feasible and attractive for businesses. The main reasons for this recommendation are:

1. Encouraging investment: Financial incentives, such as tax credits, grants, or low-interest loans, can help businesses offset the costs associated with implementing IoT solutions in their supply chains. This financial support can encourage companies to invest in IoT technology, even if they are initially hesitant due to the perceived risks or costs involved.

2. Stimulating innovation: Financial incentives can spur innovation in the IoT space for supply chain management by providing companies with the resources they need to experiment with new technologies and solutions. This can lead to the development of new IoT applications and the refinement of existing ones, ultimately contributing to the overall competitiveness of the manufacturing sector.

3. Enhancing competitiveness: By lowering the barriers to IoT adoption, financial incentives can help businesses in the manufacturing sector become more competitive on a global scale. Companies that leverage IoT technology can improve their supply chain efficiency, responsiveness, and resilience, allowing them to better compete with international rivals.

4. Creating jobs and economic growth: The implementation of IoT technology in supply chains can lead to job creation and contribute to economic growth. As companies adopt IoT solutions, they will require skilled workers to develop, implement, and maintain these systems. Financial incentives can help stimulate this job growth and support the development of a skilled workforce in the IoT sector.

5. Promoting sustainability: IoT technology can contribute to more sustainable supply chain practices, such as reducing waste, conserving resources, and minimizing emissions. Financial

incentives can encourage businesses to adopt IoT solutions that support these goals, ultimately promoting environmental sustainability and corporate social responsibility.

Implementation Considerations:

Implementation considerations for providing financial incentives for supply chain IoT adoption include the following:

1. Identifying appropriate incentives: The federal government should assess the most effective financial incentives to promote IoT adoption in the supply chain, such as grants, tax credits, low-interest loans, or subsidies. This may involve consulting with industry experts, conducting cost-benefit analyses, and evaluating the success of similar programs in other countries or sectors.

2. Defining eligibility criteria: Clear eligibility criteria should be established to ensure that the financial incentives are targeted at companies that can benefit the most from IoT adoption across supply chains, such as small and medium-sized enterprises or businesses in critical industries. Criteria may include company size, revenue, industry sector, or proposed IoT projects.

3. Coordinating among federal agencies: Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Small Business Administration, and the Department of Energy. These agencies should coordinate their efforts to ensure efficient and effective implementation of the financial incentives program. Collaboration with state and local governments may also be necessary to align initiatives and maximize the impact.

4. Monitoring and evaluation: The federal government should establish a system for monitoring and evaluating the effectiveness of the financial incentives program. This may include tracking key performance indicators, such as the number of IoT projects funded, the amount of private investment leveraged, and the impact on supply chain efficiency and sustainability. Periodic reviews should be conducted to assess the program's success and identify areas for improvement.

5. Addressing potential barriers: Possible barriers to implementing this recommendation may include budget constraints, lack of political support, or concerns about market distortion. The federal government should address these concerns by demonstrating the potential economic and environmental benefits of IoT adoption in supply chains, leveraging public-private partnerships to share costs, and ensuring that the financial incentives are designed to minimize market distortions.

6. Raising awareness and providing technical assistance: The federal government should consider implementing outreach campaigns to inform companies about the available financial incentives and the benefits of IoT adoption in supply chain management. Additionally, providing technical assistance to businesses in identifying, developing, and implementing IoT projects can help ensure the successful deployment of these technologies and maximize the impact of the financial incentives program.

Potential implementation barriers:

1. Budget constraints: Limited budgetary resources can restrict the federal government's ability to allocate sufficient funds for financial incentives. This may result in a smaller or less comprehensive program, reducing its overall impact on IoT adoption.

2. Political opposition: Financial incentives may face opposition from certain political groups or stakeholders who argue against government intervention in the market or perceive the incentives as favoring specific industries or companies.
3. Bureaucratic hurdles: The implementation of financial incentives may require collaboration and coordination among multiple federal agencies, which can introduce bureaucratic challenges and delays in rolling out the program.
4. Inefficient allocation of resources: There is a risk that financial incentives may be allocated to businesses that do not use the funds effectively or do not fully commit to IoT adoption, leading to an inefficient use of government resources.
5. Market distortion: Financial incentives may inadvertently create market distortions if they disproportionately benefit certain companies or industries, leading to an uneven playing field and potential resistance from competitors.
6. Difficulty in measuring impact: Assessing the direct impact of financial incentives on IoT adoption in supply chains can be challenging, as multiple factors contribute to a company's decision to invest in new technologies. This may make it difficult for the federal government to demonstrate the effectiveness of the incentives program and justify its continued funding.
7. Lack of awareness: Companies may not be aware of the available financial incentives or may not understand the potential benefits of IoT adoption in their supply chains, limiting the program's effectiveness in driving change.

Possible participating agencies:

1. Department of Commerce (DOC): The DOC, through its various bureaus, could support initiatives related to IoT adoption in supply chain management by offering grants, loans, or tax incentives to businesses investing in IoT technologies.
2. Small Business Administration (SBA): The SBA could provide financial assistance in the form of loans, grants, or other funding programs specifically targeted at small and medium-sized businesses looking to invest in IoT for their supply chain operations.
3. Department of Energy (DOE): The DOE might offer incentives to support IoT adoption in supply chain management for energy-related industries, such as smart grid technology, renewable energy production, and energy-efficient transportation.
4. Department of Transportation (DOT): The DOT could provide funding and incentives for IoT projects related to transportation and logistics within supply chains, such as smart transportation infrastructure or vehicle-to-vehicle communication.
5. National Science Foundation (NSF): The NSF could offer research grants or funding for projects aimed at developing and implementing innovative IoT technologies for supply chain management, fostering cutting-edge advancements in the field.
6. Department of Agriculture (USDA): The USDA might provide financial incentives for IoT adoption in the agricultural sector, helping to modernize supply chains, improve traceability, and increase overall efficiency in food production and distribution.
7. Environmental Protection Agency (EPA): The EPA could offer financial incentives to businesses that adopt IoT solutions to reduce their environmental impact, such as reducing waste, conserving resources, or minimizing carbon emissions within their supply chains.
8. Department of Defense (DoD): The DoD could support IoT adoption in supply chain management for defense-related industries, investing in technologies that improve the efficiency, security, and resilience of defense supply chains.
9. Department of Labor (DOL): The DOL might provide funding for workforce development and training programs focused on IoT technologies in supply chain management, equipping workers with the necessary skills to support IoT adoption.

Federal considerations:

1. Budget constraints: Financial incentives require budget allocations, and government resources are often limited. It is crucial to carefully evaluate the potential return on investment and prioritize IoT adoption projects that provide the highest impact on supply chain efficiency, resilience, and sustainability.
2. Targeting the right recipients: Financial incentives should be targeted at businesses or sectors that face the greatest barriers to IoT adoption or have the potential to drive significant improvements in supply chain performance. This may include small and medium-sized enterprises, which often face greater challenges in accessing resources for technology investments.
3. Balancing public and private investment: While financial incentives can help to spur IoT adoption, it is essential to strike the right balance between public and private investment. The government should encourage businesses to invest in IoT technology by providing a supportive policy environment and removing regulatory barriers, while also providing targeted financial incentives where appropriate.
4. Ensuring fairness and transparency: Financial incentives should be distributed in a transparent and equitable manner to avoid favoritism or distortion of competition. Criteria for eligibility and allocation of funding should be clearly defined and communicated to all relevant stakeholders.
5. Encouraging innovation: Financial incentives should be designed to promote the development and adoption of innovative IoT solutions, rather than supporting outdated or inefficient technologies. This can be achieved by offering incentives for research and development, pilot projects, or the adoption of cutting-edge IoT solutions.
6. Collaboration with industry and academia: The government should engage with industry stakeholders, research institutions, and other relevant parties to ensure that financial incentives are aligned with the needs and priorities of the supply chain sector. This will help to maximize the impact of incentives and foster long-term partnerships between the public and private sectors.
7. Flexibility and adaptability: As the IoT landscape evolves rapidly, the government should be prepared to regularly review and update its financial incentive programs to ensure their continued relevance and effectiveness. This may involve adjusting funding priorities, eligibility criteria, or the types of incentives offered.

Recommendation 4: The federal government should consider fostering public-private partnerships.

Description:

The recommendation to establish and foster public-private partnerships (PPPs) focused on IoT adoption aims to facilitate collaboration and knowledge sharing between government agencies, businesses, technology providers, and academia. By creating a platform that encourages the exchange of ideas, resources, and expertise, PPPs can help to accelerate the development, deployment, and adoption of IoT technologies in supply chain management.

Public-private partnerships can play a pivotal role in overcoming common challenges associated with IoT adoption, such as the lack of infrastructure, technical knowledge, and financial resources. By pooling resources and aligning efforts, PPPs can enable the development of innovative IoT solutions, pilot projects, and proof-of-concept initiatives that demonstrate the value and benefits of IoT in supply chain operations.

Additionally, PPPs can support workforce development and training programs, ensuring that businesses have access to skilled professionals capable of implementing and managing IoT systems. They can also facilitate the creation of regulatory frameworks and standards, promoting a conducive environment for IoT adoption across the supply chain industry.

To implement this recommendation, the government should actively engage with relevant stakeholders, identify shared goals and objectives, and establish mechanisms for ongoing collaboration and support. By fostering public-private partnerships focused on IoT adoption, the government can create a thriving ecosystem that drives innovation and competitiveness in the supply chain sector, ultimately realizing the full potential of IoT technologies.

Justification:

The justification for fostering public-private partnerships as a recommendation lies in the potential benefits of collaboration between the government and the private sector in promoting IoT adoption in supply chain management. Public-private partnerships can help overcome barriers to IoT implementation and unlock the full potential of this technology. The main reasons for this recommendation are:

1. Leveraging resources and expertise: Public-private partnerships allow both the government and private sector organizations to pool their resources, knowledge, and expertise. This collaboration can lead to more effective and efficient IoT implementation across supply chains, as well as the development of innovative solutions tailored to specific supply chain challenges.

2. Risk sharing: IoT adoption in supply chain management may involve significant investments and risks for businesses. Public-private partnerships can help share these risks, providing businesses with the confidence to invest in IoT technology and reducing potential financial burdens.

3. Accelerating technology adoption: By collaborating with the private sector, the government can help speed up the deployment of IoT solutions in supply chains. Public-private partnerships can facilitate the development and implementation of pilot projects, promoting the testing and scaling of innovative IoT solutions.

4. Addressing regulatory challenges: Public-private partnerships can help address regulatory and policy challenges associated with IoT technology. By involving private sector stakeholders in the decision-making process, the government can develop more informed and targeted regulations that support IoT adoption while addressing potential risks.

5. Fostering innovation: Collaborative efforts between the public and private sectors can create a fertile environment for innovation in IoT and supply chain management. Public-private partnerships can help identify and address gaps in the market, support research and development initiatives, and encourage the exchange of ideas and best practices.

6. Enhancing global competitiveness: Public-private partnerships can strengthen the competitiveness of the manufacturing sector on a global scale. By working together, the government and private sector can accelerate the development and deployment of IoT technology, enabling businesses to compete more effectively with international rivals.

7. Building trust and cooperation: Fostering public-private partnerships can help build trust and cooperation between the government and the private sector, which is essential for addressing complex challenges in supply chain management. A strong partnership can facilitate dialogue and encourage collaborative problem-solving, ensuring that the interests of all stakeholders are considered in the development and implementation of IoT solutions.

Implementation Considerations:

Implementation considerations for fostering public-private partnerships for supply chain IoT adoption include:

1. Identifying key stakeholders: The federal government should identify relevant private sector stakeholders, including businesses, industry associations, research institutions, and technology providers, who can contribute to the development and implementation of IoT solutions in supply chain management.

2. Establishing a collaborative framework: A formal framework should be established to facilitate collaboration between the public and private sectors. This may include creating joint working groups, industry forums, or innovation hubs, where stakeholders can share ideas, knowledge, and resources.

3. Defining clear goals and objectives: Public-private partnerships should have well-defined goals and objectives that align with the overall strategy for promoting IoT adoption in supply chain management. This will help ensure that all stakeholders are working towards a common vision and can measure their progress.

4. Developing joint projects and initiatives: The federal government and private sector stakeholders should collaborate on joint projects and initiatives that address specific challenges or opportunities in supply chain management. These could include pilot projects, research and development programs, or the development of new IoT standards and protocols.

5. Ensuring effective communication and coordination: Open and transparent communication between the public and private sectors is critical for successful collaboration. Regular meetings, progress reports, and information sharing mechanisms should be established to facilitate coordination and maintain momentum.

6. Monitoring and evaluation: The federal government should establish a system for monitoring and evaluating the effectiveness of public-private partnerships in promoting IoT adoption in supply chain management. This may involve tracking key performance indicators, such as the number of joint projects implemented, the amount of private investment leveraged, and the impact on supply chain efficiency and resilience.

Potential implementation barriers:

Possible barriers to implementing this recommendation include:

1. Mistrust between public and private sectors: A lack of trust between the government and private sector stakeholders can hinder collaboration and limit the effectiveness of public-private partnerships.

2. Differing priorities and objectives: Public and private sector stakeholders may have different priorities, objectives, and timelines, which can create challenges in aligning their efforts.

3. Intellectual property and data privacy concerns: Private sector stakeholders may be hesitant to share proprietary information or data with the government, hindering collaboration and knowledge sharing.

4. **Limited resources:** Both the government and private sector organizations may face resource constraints that limit their ability to participate in public-private partnerships.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Department of Transportation, the Department of Energy, and the Small Business Administration.

Federal considerations:

The federal government should consider addressing trust and communication issues, aligning priorities and objectives, protecting intellectual property and data privacy, and allocating resources efficiently to ensure the successful implementation of public-private partnerships for IoT adoption in supply chain management.

Recommendation 5: The federal government should invest in education and workforce development.

Description:

The recommendation to invest in and promote education and workforce development focused on IoT aims to address the growing demand for skilled professionals capable of designing, implementing, and managing IoT systems in supply chain operations. By investing in educational programs, training initiatives, and professional development opportunities, the government can ensure that businesses have access to a workforce equipped with the necessary expertise to harness the potential of IoT technologies.

Investing in IoT-focused education and workforce development involves developing curricula at various educational levels, ranging from K-12 to higher education and vocational training, to incorporate IoT concepts, technologies, and applications relevant to supply chain management. It also includes creating partnerships between educational institutions, industry stakeholders, and technology providers to facilitate internships, apprenticeships, and real-world projects that offer practical experience in IoT implementation.

In addition to formal education, promoting workforce development involves offering continuous learning opportunities, such as workshops, certifications, and online courses, for professionals looking to expand their IoT-related skills and knowledge. These initiatives can help ensure that the workforce stays up-to-date with the latest trends and innovations in the IoT landscape, thereby fostering the adoption of new technologies and driving competitiveness in the supply chain sector.

By investing in and promoting education and workforce development focused on IoT, the government can cultivate a skilled talent pool that is capable of navigating the complex challenges associated with IoT adoption, ultimately supporting the growth and success of the supply chain industry.

Justification:

The justification for the recommendation to invest in education and workforce development in the context of IoT adoption in supply chain management lies in the need to prepare the workforce for the technological advancements and skills required in the rapidly evolving industry. The main reasons for this recommendation are:

1. Addressing skills gap: The increasing adoption of IoT technologies in supply chain management will create a demand for workers with specialized knowledge and skills. Investing in education and workforce development can help address this skills gap, ensuring that companies have access to the talent they need to successfully implement IoT solutions.

2. Enhancing competitiveness: A well-trained and skilled workforce is a key factor in the competitiveness of the manufacturing sector. By investing in education and workforce development, the government can help businesses stay ahead of international competition and maintain a strong position in the global market.

3. Fostering innovation: A skilled workforce with a strong foundation in IoT technologies can drive innovation in supply chain management. By investing in education and training programs, the government can foster a culture of innovation and support the development of cutting-edge solutions.

4. Supporting digital transformation: As the manufacturing sector undergoes digital transformation, businesses need to adapt their operations and processes to incorporate new technologies, such as IoT. Investing in education and workforce development will equip workers

with the necessary skills to navigate this transition and support the successful integration of IoT solutions in supply chains.

5. Encouraging job creation: IoT adoption in supply chain management can create new job opportunities in fields such as data analysis, software development, and cybersecurity. By investing in education and workforce development, the government can ensure that workers are prepared to take advantage of these opportunities, supporting economic growth and job creation.

6. Promoting social inclusion: Education and workforce development programs can help promote social inclusion by ensuring that underrepresented and disadvantaged groups have access to the skills and training they need to participate in the IoT-driven job market.

7. Ensuring long-term sustainability: As the manufacturing sector continues to evolve, businesses will need to adapt to new technologies and industry trends. By investing in education and workforce development, the government can help ensure the long-term sustainability of the manufacturing sector and support businesses in their ongoing efforts to adopt and integrate IoT technologies in their supply chains.

Implementation Considerations:

Implementation considerations for investing in education and workforce development for supply chain IoT adoption include:

1. Identifying skill requirements: Conduct a thorough analysis of the specific skills and expertise needed to support IoT adoption in supply chain management, including technical, analytical, and managerial competencies.

2. Developing targeted curricula: Collaborate with educational institutions, industry stakeholders, and training providers to develop targeted curricula and training programs that address the identified skill requirements.

3. Expanding access to education and training: Implement policies and programs that ensure broad access to IoT-focused education and training, including financial aid, scholarships, and online learning options to reach underserved communities.

4. Encouraging industry-academia partnerships: Promote partnerships between industry and educational institutions to facilitate real-world learning experiences, internships, and collaborative research projects.

5. Focusing on reskilling and upskilling: Implement programs to reskill and upskill the existing workforce, enabling them to adapt to the changing requirements of IoT-driven supply chain management.

6. Promoting STEM education: Encourage interest in science, technology, engineering, and mathematics (STEM) education from an early age, laying the foundation for future workforce development in the IoT field.

7. Establishing performance metrics: Develop performance metrics and evaluation methods to assess the effectiveness of education and workforce development initiatives and make data-driven improvements as needed.

Potential implementation barriers:

Possible barriers to implementing this recommendation include:

1. Insufficient funding: Limited resources may constrain the government's ability to invest in education and workforce development programs at the desired scale.

2. Resistance to change: Some industry stakeholders may resist investing in new training and education programs due to concerns about costs, time constraints, or disruption to existing processes.

3. Difficulty in identifying skill requirements: Rapidly evolving technologies and market dynamics may make it challenging to accurately identify the specific skills needed for IoT adoption in supply chain management.

4. Skills mismatch: A mismatch between the skills taught in educational institutions and the skills required by industry can limit the effectiveness of education and workforce development initiatives.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Education, the Department of Labor, the National Science Foundation, and the Department of Commerce.

Federal considerations:

The federal government should consider allocating sufficient resources, fostering collaboration between industry and academia, ensuring broad access to education and training, focusing on reskilling and upskilling, promoting STEM education, and continuously evaluating and improving the effectiveness of education and workforce development programs in order to successfully implement this recommendation.

Recommendation 6: The federal government should consider strengthening cybersecurity measures.

Description:

The recommendation to strengthen cybersecurity measures focused on IoT across supply chain networks aims to address the growing concerns around data privacy, security, and the potential risks associated with the increased connectivity and interdependence of IoT systems. By implementing robust cybersecurity measures, the government can help ensure that businesses can confidently adopt IoT technologies in their supply chain operations without compromising the security and integrity of their networks and data.

Strengthening cybersecurity measures involves promoting the development and adoption of security best practices, guidelines, and standards specifically tailored to IoT systems in supply chain management. This includes securing data transmission, storage, and access, as well as protecting IoT devices and networks from unauthorized access, manipulation, and cyberattacks.

To implement this recommendation, the government should collaborate with industry stakeholders, cybersecurity experts, and technology providers to identify potential vulnerabilities and develop appropriate solutions that address the unique security challenges associated with IoT systems in supply chain operations. Additionally, the government should support research and development efforts aimed at advancing cybersecurity technologies and solutions tailored for IoT environments.

Training and awareness programs should also be promoted to ensure that businesses and professionals understand the importance of IoT security and are equipped with the knowledge and skills required to protect their systems and data. By strengthening cybersecurity measures focused on IoT across supply chain networks, the government can foster trust in IoT technologies and enable businesses to fully leverage their potential benefits while minimizing risks.

Justification:

The justification for the recommendation to strengthen cybersecurity measures in the context of IoT adoption in supply chain management lies in the increasing reliance on interconnected systems and devices, which may expose organizations to a higher risk of cyber threats. The main reasons for this recommendation are:

1. Protecting sensitive data: IoT devices and systems in supply chains generate and transmit vast amounts of data, including sensitive information about products, inventory, and logistics. Strengthening cybersecurity measures helps protect this data from unauthorized access, theft, or manipulation.

2. Ensuring operational continuity: Cyberattacks on IoT systems can disrupt supply chain operations, leading to delays, losses, and reputational damage. Enhanced cybersecurity measures help ensure the reliability and continuity of supply chain processes.

3. Maintaining trust: Trust is essential for the smooth functioning of supply chains, as organizations share sensitive information and collaborate on various processes. Strengthening cybersecurity measures helps maintain trust between supply chain partners by ensuring the confidentiality, integrity, and availability of data.

4. Compliance with regulations: As regulations related to data protection and cybersecurity evolve, organizations must ensure they meet the necessary requirements. Strengthening cybersecurity measures allows businesses to comply with these regulations and avoid potential legal and financial penalties.

5. Enhancing competitiveness: Organizations with strong cybersecurity measures in place are better positioned to compete in the global market, as they can assure their customers and partners of the safety and reliability of their supply chain operations.

6. Addressing evolving threats: As cyber threats become more sophisticated and targeted, organizations must continuously adapt and update their cybersecurity measures to stay ahead of potential attackers.

7. Fostering innovation: A secure environment enables organizations to safely experiment with new IoT technologies and solutions without the fear of exposing their systems and data to cyber risks. Strengthening cybersecurity measures, therefore, fosters innovation in supply chain management.

Implementation Considerations:

Implementation considerations for strengthening cybersecurity measures for supply chain include:

1. Develop a comprehensive cybersecurity framework: Create a framework that addresses various aspects of supply chain cybersecurity, including risk assessment, threat monitoring, incident response, and recovery plans.

2. Promote the adoption of best practices and standards: Encourage organizations to adopt industry best practices and internationally recognized standards, such as the NIST Cybersecurity Framework and the ISO/IEC 27000 series.

3. Encourage information sharing: Facilitate the sharing of threat intelligence, vulnerabilities, and best practices among supply chain partners and industry stakeholders to improve collective defense against cyber threats.

4. Invest in security technologies: Promote the adoption of advanced security technologies, such as encryption, intrusion detection systems, and artificial intelligence-based solutions, to protect IoT devices and systems.

5. Implement security-by-design principles: Encourage organizations to adopt a security-by-design approach, integrating cybersecurity considerations into the design and development of IoT devices and systems.

6. Raise awareness and provide training: Develop programs to raise awareness of supply chain cybersecurity risks and provide training for organizations and their workforce.

Potential implementation barriers:

Possible barriers to implementing this recommendation include:

1. Limited resources: Organizations may face resource constraints, including financial, technical, and human resources, which may limit their ability to strengthen cybersecurity measures.

2. Complexity of supply chains: The complexity of global supply chains, with numerous interconnected partners and systems, may make it challenging to implement comprehensive cybersecurity measures.

3. Resistance to information sharing: Organizations may be hesitant to share information about vulnerabilities or incidents due to concerns about revealing competitive information or damaging their reputation.

4. Evolving threats: Cyber threats are continuously evolving, which may make it difficult for organizations to stay ahead of potential attackers.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), the Department of Commerce, and the Federal Trade Commission (FTC).

Federal considerations:

The federal government should consider the following in implementing this recommendation:

1. Develop and promote the adoption of a comprehensive cybersecurity framework tailored to supply chain IoT adoption.

2. Support research and development efforts in security technologies and solutions.

3. Allocate resources to facilitate training and awareness programs.

4. Encourage collaboration and information sharing among industry stakeholders and government agencies.

5. Continuously monitor and update cybersecurity policies, regulations, and best practices to adapt to the evolving threat landscape.

Recommendation 7: The federal government should promote international collaboration.

Description:

The recommendation to promote international collaboration in IoT adoption across global supply chains aims to facilitate the sharing of knowledge, best practices, and resources between countries and regions, driving innovation and accelerating the widespread adoption of IoT technologies in supply chain operations worldwide. By engaging in international collaboration, governments can foster a global ecosystem that supports the development and deployment of IoT solutions, overcoming challenges related to interoperability, standardization, and regulatory compliance.

Promoting international collaboration involves creating platforms and forums where policymakers, industry stakeholders, technology providers, and researchers from different countries can come together to exchange ideas, discuss common challenges, and explore opportunities for joint projects and initiatives. This can lead to the development of harmonized regulations, standards, and guidelines that enable seamless integration of IoT systems across borders, fostering efficient and resilient global supply chain networks.

In addition, international collaboration can facilitate the pooling of resources and expertise to support research and development efforts, pilot projects, and capacity-building initiatives aimed at promoting IoT adoption in supply chain management. This can help bridge the digital divide between developed and developing countries, ensuring that businesses worldwide have access to the tools and technologies needed to harness the potential of IoT in their supply chain operations.

To implement this recommendation, the government should actively engage with international partners, participate in relevant forums and organizations, and seek opportunities to collaborate on IoT-related projects and initiatives. By promoting international collaboration in IoT adoption across global supply chains, the government can contribute to the development of a connected and resilient global supply chain ecosystem that benefits businesses and consumers alike.

Justification:

The justification for the recommendation to promote international collaboration in the context of IoT adoption in supply chain management lies in the inherently global nature of supply chains and the need for a coordinated approach to address common challenges. The main reasons for promoting international collaboration are:

1. Global nature of supply chains: Modern supply chains often involve multiple countries, making it essential for governments and organizations to collaborate across borders to ensure seamless, efficient, and secure operations.

2. Harmonization of standards and regulations: International collaboration can help develop and promote the adoption of common standards, protocols, and regulations, which can reduce inconsistencies and friction between countries, making it easier for organizations to operate globally.

3. Addressing global cyber threats: Cyber threats are not limited by geographical boundaries; therefore, international collaboration can enable the sharing of threat intelligence, best practices, and resources, improving collective defense against cyber attacks.

4. Leveraging global expertise: Collaborating with international partners allows countries to benefit from the expertise, technologies, and best practices developed by others, leading to more effective and efficient IoT adoption in supply chain management.

5. Fostering innovation: International collaboration can stimulate innovation by enabling the exchange of ideas, knowledge, and technologies among countries, research institutions, and businesses.

6. Building trust: Working together on common challenges can help build trust between countries, which is crucial for the smooth functioning of global supply chains.

7. Addressing social and environmental challenges: International collaboration can help address global social and environmental issues related to supply chain management, such as labor rights, environmental sustainability, and resource management.

Implementation Considerations:

Implementation considerations for promoting international collaboration for supply chain include:

1. Establish bilateral and multilateral agreements: Form strategic partnerships with key countries to facilitate collaboration on IoT-related supply chain initiatives, standards, and best practices.

2. Participate in international forums and organizations: Engage in existing forums and organizations dedicated to supply chain management, IoT, and cybersecurity to contribute to and benefit from global discussions and initiatives.

3. Share information and best practices: Promote the exchange of information, threat intelligence, and best practices related to IoT adoption and supply chain security among international partners.

4. Collaborate on research and development: Engage in joint research and development projects with international partners to foster innovation and develop new technologies for supply chain management.

5. Promote capacity building: Support capacity-building initiatives and programs to help countries strengthen their IoT infrastructure, develop relevant skills, and improve supply chain management practices.

6. Identify key international partners: Assess which countries are critical for collaboration based on their role in global supply chains, technological capabilities, and mutual strategic interests.

7. Leverage existing diplomatic channels: Utilize existing diplomatic relationships to initiate dialogue and cooperation on IoT adoption in supply chain management.

8. Coordinate with relevant federal agencies: Ensure that all relevant federal agencies are involved in the development and implementation of international collaboration initiatives.

Potential implementation barriers:

Possible barriers to implementing this recommendation:

1. Differing priorities and interests: Different countries may have varying priorities and interests, which could make it challenging to align objectives and collaborate effectively.

2. Trust and data privacy concerns: Sharing sensitive information and best practices may be hindered by trust and data privacy concerns among collaborating countries.

3. Regulatory and legal barriers: Differences in regulations, standards, and legal frameworks may impede collaboration efforts and create challenges in harmonizing policies.

Possible participating agencies:

DRAFT – Supply Chain Logistics Recommendations

Federal agencies that may be impacted by this recommendation include the Department of State, the Department of Commerce, the Department of Homeland Security, the National Institute of Standards and Technology, and the Federal Trade Commission.

Federal considerations:

1. Align collaboration efforts with national priorities and interests while respecting the priorities of partner countries.

2. Develop clear objectives and mutually beneficial goals for international collaboration initiatives.

3. Ensure effective communication and coordination among relevant federal agencies and international partners.

4. Establish mechanisms for monitoring and evaluating the progress and effectiveness of collaboration efforts.

5. Remain adaptable and responsive to the evolving global landscape and emerging challenges in IoT adoption and supply chain management.

Recommendations 8: The federal government should monitor and evaluate progress.

Description:

The recommendation to monitor and evaluate progress aims to ensure that IoT adoption efforts in supply chain management are on track, effectively addressing the identified challenges and opportunities, and delivering the desired outcomes. By regularly monitoring and evaluating the progress of IoT implementation, the government can identify areas of improvement, assess the impact of its policies and initiatives, and make informed decisions to optimize its strategies and investments in the future.

Monitoring and evaluating progress involves establishing a set of measurable indicators and targets that reflect the key objectives and desired outcomes of IoT adoption in supply chain management. These indicators may include the level of IoT technology adoption, efficiency gains, cost reductions, improvements in transparency and traceability, and advancements in cybersecurity, among others.

To implement this recommendation, the government should develop a comprehensive framework for data collection, analysis, and reporting, which includes input from industry stakeholders, technology providers, and relevant government agencies. Regular assessments should be conducted to track the progress of IoT adoption against the established targets, identify any gaps or challenges, and evaluate the effectiveness of the implemented policies and initiatives.

Based on the findings of these assessments, the government should adapt its strategies and actions to address the identified issues, optimize resource allocation, and maximize the impact of its efforts. By monitoring and evaluating progress, the government can ensure that its approach to driving IoT adoption in supply chain management remains agile, responsive, and results-oriented, ultimately contributing to the long-term success and competitiveness of the industry.

Justification:

The justification for the recommendation to monitor and evaluate progress in IoT adoption for supply chain management stems from the need to ensure the effectiveness of implemented strategies, measure their impact, and identify areas for improvement. Regular monitoring and evaluation are crucial for several reasons:

1. Assess effectiveness: Monitoring and evaluation help determine whether the implemented strategies and policies are achieving their intended goals and objectives.

2. Measure impact: Assessing the impact of IoT adoption in supply chain management is essential to understand the benefits, such as efficiency improvements, cost savings, and enhanced resilience.

3. Identify areas for improvement: By evaluating progress, the government can identify weaknesses or gaps in the implementation of IoT adoption strategies, enabling targeted improvements and adjustments to ensure better outcomes.

4. Allocate resources efficiently: Monitoring and evaluation provide insights into the effectiveness of various initiatives, helping the government make informed decisions on resource allocation and prioritize investments in areas with the most significant potential impact.

5. Enhance accountability: Regular assessment of progress helps ensure transparency and accountability for the government and other stakeholders involved in IoT adoption and supply chain management.

6. Facilitate knowledge sharing: Monitoring and evaluating progress can generate valuable knowledge and insights that can be shared with other stakeholders, helping to improve practices and drive further innovation in the field.

7. Inform future strategies: The insights gained from monitoring and evaluating progress can inform the development of future policies and strategies, ensuring they are more effective and better aligned with the evolving needs of supply chain management.

Implementation Considerations:

Implementation considerations for monitoring and evaluating progress for supply chain include:

1. Establish clear goals and objectives: Define specific, measurable, and time-bound goals and objectives for IoT adoption in supply chain management to enable effective monitoring and evaluation.

2. Develop relevant performance indicators: Identify key performance indicators (KPIs) that reflect the desired outcomes of IoT adoption and can be used to measure progress and impact.

3. Implement data collection and reporting mechanisms: Set up systems and processes for collecting, storing, and analyzing data related to IoT adoption and supply chain performance.

4. Conduct periodic assessments: Schedule regular evaluations of progress and impact, using the collected data and KPIs to assess the effectiveness of IoT initiatives in supply chain management.

5. Foster a culture of continuous improvement: Encourage feedback and learning from monitoring and evaluation results, using the insights to improve and refine policies and initiatives.

6. Collaborate with stakeholders: Engage with industry, academia, and other relevant stakeholders to gather their insights and perspectives, ensuring a comprehensive understanding of progress and challenges.

7. Assign responsibility: Designate a lead federal agency or interagency group responsible for overseeing the monitoring and evaluation process for IoT adoption in supply chain management.

8. Develop a monitoring and evaluation plan: Create a detailed plan outlining the goals, objectives, KPIs, data collection methods, and evaluation schedule.

9. Allocate resources: Ensure adequate financial, human, and technical resources are allocated to support monitoring and evaluation activities.

Potential implementation barriers:

Possible barriers to implementing this recommendation:

1. Lack of clear goals and objectives: Ambiguous or poorly defined goals can make it difficult to assess progress and impact.

2. Inadequate data collection and reporting mechanisms: Ineffective systems for collecting, storing, and analyzing data can hinder accurate and reliable monitoring and evaluation.

3. Resource constraints: Limited resources can impede the government's ability to conduct thorough and consistent monitoring and evaluation.

4. Resistance to change: Stakeholders may resist sharing information or adopting new practices based on evaluation results, limiting the impact of monitoring and evaluation efforts.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Department of Transportation, the Department of Homeland Security, the National Institute of Standards and Technology, and the Federal Trade Commission.

Federal considerations:

1. Ensure clear communication of goals, objectives, and expectations related to monitoring and evaluating progress in IoT adoption for supply chain management.

2. Collaborate with relevant stakeholders to gather their perspectives and insights, promoting a more comprehensive understanding of progress and challenges.

3. Be transparent in sharing the results of monitoring and evaluation, fostering trust and accountability among stakeholders.

4. Remain adaptable and responsive to new information and insights, using the results of monitoring and evaluation to continuously refine and improve policies and initiatives.

Recommendation 9: The federal government should select the most appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic IoT manufacturing supply chain.

Description:

These policies, incentives, and requirements are particularly relevant in the transportation sector as that becomes increasingly connected, electric, shared, integrated, seamless, and ultimately autonomous. Rapid advances in transportation technologies are already occurring that are further augmented by several communication and information technologies, including the Internet of Things (IoT). In addition, the sector is becoming increasingly electrified. The recommendations in this section can apply to all aspects of domestic IoT manufacturing.

Justification:

American manufacturers share the goal of fostering and strengthening domestic manufacturing and supply chain capabilities. With the recent influx of federal funding and executive orders in this sector, there is an increasing trend to support the "Buy American" concept Ensuring the Future Is Made in All of America by All of America's Workers. The justification for an appropriate mix of policies, incentives, and requirements to support sustainable and scalable growth in the domestic manufacturing supply chain market is provided below:

1. Absent significant time to build new manufacturing capacity, develop new supply chains, and train workers, tighter domestic preference requirements could create supply constraints and prevent the manufacturers from meeting even modest deployment goals.

2. In some cases, U.S. manufacturing capacity cannot meet increased demand that would be sparked by anticipated federal investment/incentives let alone current domestic demand.

3. In some cases, there are no domestic alternatives for components and subcomponents, limiting the ability of equipment providers to control their domestic content. US Manufacturers cannot force their component and subcomponent suppliers to relocate facilities to the U.S.

4. Compliance with federal domestic preference requirements is time consuming and costly particularly when it comes to the country of origin of components and subcomponents. This burden will increase as subcomponents become smaller and more integrated.

Implementation Considerations:

Implementation considerations for fostering and strengthening domestic manufacturing and supply chain capabilities include:

1. Phasing in domestic contact requirements. An extended phase in period is necessary in order to avoid supply shortages and provide domestic manufacturers and their suppliers with sufficient time to develop domestic manufacturing capabilities, build up supply chains, and train their workforce.

2. Accelerate domestic manufacturing with an investment tax credit for associated capital costs.

3. Provide clear rules governing domestic content requirements, including guidelines on how they apply across all funding and procurement programs. Further, this guidance should also be provided to implementing state agencies.

4. Avoid any rules that require determining the country of origin of subcomponents integrated into larger domestically manufactured components.

5. The component test should include all costs associated with the manufacturing of a product, such as labor, transportation, allocable overhead, and material. And clearly designate that the domestic labor used in the final assembly of a product is included in the component test.

6. Allow 100% of manufacture value added (MVA) or substantial transformation to be classified as domestic content in component tests.

7. Countries should be designated outside of the US from which materials and components can be procured and the component test for products substantially transformed in one of these acceptable countries can be waived. These could be countries that the US already has established trade agreements with such as: USMCA countries, European Union member states, The United Kingdom, and Indo-Pacific

Potential implementation barriers:

Possible barriers to implementing this recommendation:

1. Current Supply Chain constraints meeting domestic content requirements - while there are a number of North American manufacturing plants for EV components particularly batteries being developed and constructed, there is a ramp up time to get to full production.

2. Funding constraints: There is a huge initial capital cost investment to build up new domestic manufacturing plants.

3. Resource constraints: There will need to be an influx of skilled engineers and technicians to support this domestic buildup.

Possible participating agencies:

Federal agencies that may be impacted by this recommendation include the Department of Commerce, the Department of Transportation, Federal Highway Administration, the National Highway Traffic Safety Association, and the National Institute of Standards and Technology.