Draft - Sustainable infrastructure recommendations - for discussion only (not final and subject to change)

Recommendation 1: The federal government should consider the development of Smart City/Infrastructure Extension Partnerships (SCIEP).

Description:

The federal government should consider funding and establishing a nationwide network of “smart city/infrastructure” extension partnerships (SCEP) that will provide cities, counties, regional agencies, and states with expertise, resources, information and tools in planning, developing, and optimizing the use of “smart technologies”. The SCEP would be analogous in concept to the Manufacturing Extension Partnerships (MEP) and the Agricultural Extension Offices. The network can be operated in partnership with private organizations, universities, and other public agencies.

Justification:

- Municipalities, agencies and other organizations lack the internal expertise, tools, resources to innovate, plan and use these IoT and its associated technologies in their operations.
- Small to medium size municipalities, agencies and utilities lack the same capabilities, resources and access as the larger counterparts. They are often the ones that are the most “behind the curve”, slow to innovate, and in most need of assistance.
- IoT and smart city/infrastructure expertise in the private sector is limited, unevenly distributed, and fragmented. In addition, IoT is an emerging technology and knowledge is rapidly being developed. Municipalities, agencies and utilities may not easily find and engage these resources.
- The public procurement processes to engage private sector resources are burdensome. Municipalities and agencies may not have the budget, the empowerment, and priorities to engage these resources. A different way to engage these resources is needed.

Implementation Considerations:

- Smart cities and IoT are broad in scope and discipline. SCIEP should be a multidisciplinary center, with expertise spanning technical, operations, cybersecurity, etc.
- Public/private/academia partnership
- Potential collaboration with regional consortiums

Potential implementation barriers:

- Limited expertise in the market and industry; resources and expertise may be difficult to secure

Possible participating agencies:

Draft - Sustainable infrastructure recommendations - for discussion only (not final and subject to change)

As sustainable infrastructure is broad and cuts across the scope of multiple federal agencies, there should be participation, support and coordination from multiple agencies, including:

- Department of Energy (renewable energy, electrification, etc.)
- Department of Transportation (intelligent traffic, roads, highways, autonomous vehicles, etc.)
- Department of Commerce/NIST (standards, cybersecurity, GCTC, regulatory, etc.)
- Department of Homeland Security/CISA (cybersecurity, etc.)

Federal considerations:

- SCIEP should be put in place and operational to support sustainable infrastructure projects funded through the Bipartisan Infrastructure Law and the Inflation Reduction Act
- Role of states should be defined. In particular, some BIL and IRA funding may be given to states to manage and allocate.

Recommendation 2: The federal government should consider the specification and utilization of IoT and "smart" technologies into infrastructure and other projects that are funded in full, or partially, with federal funding.

Description:

The federal government should consider the specification and utilization of IoT and "smart" technologies into infrastructure and other projects that are funded in full, or partially, with federal funding. Every year, the federal government, through its many agencies, supports and funds billions of dollars of infrastructure planning, construction and operation projects. These projects include projects owned by non-federal stakeholders (municipalities, utilities, agencies, states, etc.) and federal stakeholders (federal facilities, infrastructure, etc.).

The federal government should take this opportunity to specify and incorporate IoT and smart technologies into infrastructure projects spanning the project lifecycle from design, construction, to commissioning and operation. For example, IoT technologies can be specified and used during the construction phase of infrastructure projects. Air quality sensors can be specified to monitor vehicle emissions and dust and particulate matter generated during construction in order to comply with local air quality regulations. When AQ levels reach certain levels, mitigation measures can be implemented to minimize impacts to worker and community health. IoT sensors and intelligent traffic solutions can be specified into roadway projects to support future intelligent highway and autonomous vehicle projects. Remodeling or construction of new federal facilities, including airports, military bases and buildings can specify the use of various IoT solutions, such as smart building sensors and energy management systems, smart parking, and other technologies.

Justification:

- For many projects, including infrastructure and building projects, project owners don't know about IoT, or if they do, may not want to specify or incorporate the use of it for a variety of reasons, such as cost, lack of understanding of the value/benefit provided, or don't want the extra "complexity" that could add risk to the project. Unless someone (the federal government) mandates or specifies the use of IoT, project owners will not willingly incorporate IoT.
- The General Services Administration (GSA) and the U.S. Army Corps of Engineers specified the use of Building Information Modeling (BIM) in its projects. As a result, contractors had to comply with the requirement and used BIM tools, which enabled both the government and the contractor to reduce construction and project risks. A similar approach was used to accelerate the utilization of small and disadvantaged businesses in federally funded projects.

Implementation considerations:

- While it is easy to say "you shall incorporate IoT technologies", it is more difficult to specify what IoT technologies should be acceptable to be used. Some concrete and

specific IoT applications should be defined for inclusion in the project and funding requirements, based on project types. This may require coordination with other federal agencies in alignment with their objectives.

Potential implementation barriers:

- Project owners may have limited to no IoT awareness of knowledge
- Limited expertise and resources in marketplace to support IoT in the projects

Possible participating agencies

- All federal agencies that provide grants and funding for projects where IoT may be incorporated

Federal considerations:

- The SCIEP may be a resource to assist and facilitate the adoption and use of IoT in federally funded projects and grants.
- IoT may introduce cybersecurity vulnerabilities into the project or system, so some minimal requirements for cybersecurity should be defined and specified for the IoT and smart technologies to be incorporated.

Recommendation 3: The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects.

Description:

The federal government should consider funding models for sustaining and support beyond the initial acquisition and building of new projects. While many grants for projects help offset the initial cost of capital procurement, integration and development, the cost of operating the asset or system is left to the municipality or agency. Some municipalities may have the resources, funding models, or mechanisms to find the resources to sustain the operation and maintenance of this asset or system. However, many municipalities and agencies do not have these mechanisms (budget, taxes, etc.), and may forgo these types of projects.

Justification:

- Initial procurement, acquisition and construction costs of an asset or infrastructure is one part of the expenses. However, operating and maintaining an asset over its useful life can be expensive, and municipalities and agencies may not have sufficient resources and funds for this. For example, one county used CARES Act funding to build out a network of 300 public WiFi access points to support student remote learning during the pandemic. However, the county, in its pre-pandemic operating budget, did not have this additional support funding. Moving forward, the county is faced with finding funding, or shut down the network.
-

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- All federal agencies that provide grants and funding for projects where IoT may be incorporated

Federal considerations:

- tbd

Recommendation 4: The federal government should consider "student loan forgiveness" programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies. (some overlap with recommendation 1)

Description:

The federal government should consider "student loan forgiveness" programs in exchange for providing critical emerging technology (IoT, data science, cybersecurity, etc.) skills to municipalities and agencies. These programs, analogous to the National Health Science Corps, provide expertise to municipalities, agencies and utilities, especially smaller ones, that can help them to adopt, and accelerate the implementation and execution of these "smart solutions".

Justification:

- Cities lack the critical resources, skills and capabilities to work with innovative and emerging technologies, from data science, AI, cybersecurity, to IoT and more). These skills are in-demand, hard to find, and difficult for cities to attract due to competition from the private sector.
- This problem is magnified for smaller municipalities and agencies, and those in rural areas, who are already struggling with a "brain drain". This uneven access to talent prevents smaller cities and agencies from taking advantage of innovative and emerging technologies to address its needs.
- It is difficult for municipalities and public agencies to attract the future digital talent they need, and at the scale that they need to make an impact.

Implementation considerations:

- These resources can work directly with cities and agencies
- These resources can work in the SCIEPs

Potential implementation barriers:

- For the critical skills like cybersecurity and data science, it may still be hard to attract someone to this program since there is fierce competition from the private sector
- There is a lack of sufficient numbers of certain skills, especially working with cybersecurity, AI, ML, etc. There may not be enough of these skillsets.

Possible participating agencies:

- Department of Energy (renewable energy, electrification, etc.)
- Department of Transportation (intelligent traffic, roads, highways, autonomous vehicles, etc.)
- Department of Commerce/NIST (standards, cybersecurity, GCTC, regulatory, etc.)
- Department of Homeland Security/CISA (cybersecurity, etc.)

Federal considerations:

- Consider this in conjunction with the SCIEP (Recommendation 1) and specification of IoT into federally funded projects (Recommendation 2).

Recommendation 5: The federal government should facilitate and support the development of smart city and sustainable infrastructure reference architectures. (some overlap with recommendation 2)

Description:

The federal government should facilitate and support the development of smart city and sustainable infrastructure reference architectures. These reference architectures may include a broader integration of entities that are not normally considered, such as utilities, smart regions, counties, and other communities (rural areas, etc.).

Justification:

- There is no standardized definition of a smart city. Even among cities, what they call a smart city varies. For example, some would say digitizing processes and doing transactions online makes them a smart city, while another may set up a public WiFi network and call themselves a smart city.
- Most smart cities are a bunch of “point solutions” set up by different departments and agencies that don’t integrate together or share common infrastructure.
- Smaller cities have needs that may be different than their larger counterparts. The architectures they need may be different from those of larger cities. However, without a reference architecture, a piecemeal approach may lead to the situation where smart cities are built such that it would be difficult to integrate together, or may lead to a city of smart solutions instead of a smart city of solutions working together.
- There is not a starting point vision or model that municipalities can begin to build with. For example, a true “smart city” is an interconnected system of cities, utilities (city owned or not), buildings, communities and businesses that interact. Most smart city efforts are disparate silos of initiatives not integrated together.
- A broader reference model/architecture helps to identify potential areas of collaboration between entities, as well as identify areas of “sharing” and economies of scale.

Implementation considerations:

- The NIST GCTC has already established a structure and model to create, engage and support industry/academia/government partnerships. This infrastructure can be tailored to execute on this
- This effort should consider inclusion of public entities such as counties, states, and other regional agencies and utilities.

Potential implementation barriers:

- tbd

Possible participating agencies:

- NIST - GCTC

- NSF - Smart and connected communities

Federal considerations:

- Consider the early efforts done by NIST to define a smart city framework, and continue to build on that
- There are various efforts across a variety of private and non-profit organizations that may have created similar models. However, reference models need to be translated into something actionable that cities and agencies can act on (e.g. blueprints, etc.)

Recommendation 6: The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies. (combinable with recommendation 2?)

Description:

The federal government should consider offering grants to support smart city projects that target small and midsize cities and agencies. Many smart city projects today are done by larger cities that have the capabilities, resources, budgets and the capacity to implement and support these projects. There are a few smaller cities that are doing innovative smart city projects, but most smaller cities are not doing this.

Justification:

- A majority of American cities are smaller cities. For example, while there are 10 cities with a population greater than one million, there are 4,005 cities with a population between 5,000 and 50,000, 476 cities with a population between 50,000 and 100,000, 238 cities between 100,000 and 250,000.[1]
- Equitable access to benefits for smaller cities. Smaller cities have limited levels of in-house expertise, resources, capabilities and budgets as compared to their larger city counterparts. These smaller cities are highly dependent on outside funding sources for many projects. Without outside funds, these types of IoT and smart city projects will not happen for smaller cities. There are a lot of cities (large and small) that run pilots that never advance to the next stage because of a lack of funding even if the pilot is successful.
- Smaller cities and agencies are accustomed to grants and other funding mechanisms to finance projects.

Implementation considerations:

- The value of the grants for smart city projects for smaller cities can be extended by funding smart region projects that involve multiple small cities. These are projects that address issues that cut across city borders (e.g. air quality, transportation, resilience, etc.), and that no one city can do effectively on their own. This makes the cost-benefit and ROI metrics more attractive.
- While there may be some common smart city “use cases” for both large and smaller cities, in general, the types of projects and outcomes for smaller cities may be very different than those for larger cities.
- There are no “one size fits all” smart city projects. Each city, even in the same geographic region, has its own set of priorities that may be different from its neighbor. Expect a wide range of disparate projects to be considered for funding.

[1] “Places of 50,000 or more, City and Town Population Totals, July 1, 2021” U.S. Census Bureau, https://www.census.gov/data/tables/time-series/demo/popest/2020s-total-cities-and-towns.html

Draft - Sustainable infrastructure recommendations - for discussion only (not final and subject to change)

Potential implementation barriers:

- The ROI and other project feasibility criteria for metrics of success for smaller cities will be a lot different than for larger cities. A new set of evaluation criteria will be used to consider potential projects for funding.
- Smaller cities, especially those in semi-rural and rural regions, lack the pre-requisite digital and communications infrastructure to support smart city/region sustainable infrastructure type projects.

Possible participating agencies:

- All federal agencies that provide grants and funding for projects where IoT may be incorporated

Federal considerations:

- Smaller cities have limited resources and capabilities.The SCEP may be a resource to assist and facilitate the adoption and use of IoT in federally funded projects and grants for these smaller cities.
- Some portions of projects that are funded from the Bipartisan Infrastructure Law and the Inflation Reduction Act should be considered for this.
- Maximize returns on BIL broadband infrastructure investments by piggybacking smart city grants in those regions
- tbd

Recommendation 7: The federal government should facilitate and support the adoption of smart city and sustainable infrastructure standards. (some overlap with recommendation 5)

Description:

The federal government should facilitate and support the adoption of smart city and sustainable infrastructure standards in projects.

Justification:

- Smart city projects incorporate a variety of technologies which may incorporate different standards, and create issues around interoperability. For example, traffic systems employ various standards, and these systems do not interoperate with each other.
- Many utility companies utilize SCADA systems. These proprietary systems may not easily integrate with other systems, including more modern IoT solutions.
- Municipalities do not have budgets to change out systems. The solutions they procure need to be futureproofed.

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- All federal agencies that provide grants and funding for projects where IoT may be incorporated

Federal considerations:

- Consider this recommendation in conjunction with Recommendation 5 (reference architectures), recommendation 2 (federal funding) and recommendation 6 (grants for small to mid size municipalities and agencies).

Draft - Sustainable infrastructure recommendations - for discussion only (not final and subject to change)

TSERONIS - Recommendations

Recommendation 8: The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies.

Description:

The Federal Government should establish a Smart City Officer (SCO) within each of the twenty-four (24) CFO Act agencies. The SCO will serve as a business executive and technology strategist, developing and governing a comprehensive strategic, tactical, and operational roadmap intended to communicate how existing and future projects are/can support organizational mission, inform resourcing decisions, and identify enterprise-wide investment opportunities. Moreover, the SCO will establish and maintain a community-of-interest comprising C-Level executives, e.g., CIO, CTO, CFO, CAO, and CDO, to organize, manage, and steward a body of knowledge from which community members can draw.

Specific Objectives:

- Identifying the key stakeholders involved in the creation of a smart city and IoT strategy. This includes government agencies, private sector organizations, academic institutions, and community groups
- Developing a clear and concise vision for your smart city that aligns with your overall city goals. This should involve defining what you want to achieve with your smart city and what metrics you will use to measure success
- Prioritizing the projects that will have the greatest impact on your community and help you achieve your smart city goals. This could include projects related to transportation, energy, public safety, and more
- Develop a comprehensive IoT infrastructure: Develop a comprehensive IoT infrastructure that includes sensors, devices, and networks that can collect and analyze data. This infrastructure should be scalable and flexible to accommodate future growth and changes
- Use advanced analytics to turn the data collected by your IoT infrastructure into insights that can be used to make informed decisions. This includes analyzing data on traffic patterns, energy consumption, and other holistic key performance indicators
- Foster collaboration between stakeholders to ensure that everyone is working towards the same goals. This includes creating partnerships between government agencies, private sector organizations, and academic institutions
- Ensure that your IoT infrastructure is secure and protected from cyber and physical threats. This includes implementing encryption and other security measures to protect sensitive data
- Engage communities of interest and practice in the development of your smart city and IoT strategy. This includes soliciting feedback and input from residents and community groups to ensure that your strategy meets their needs and expectations.

Justification:

- tbd

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- The 24 CFO Act agencies

Federal considerations:

- Consider this recommendation in conjunction with Recommendation 1 (SCIEP) recommendation 11 (smart city program office).

Recommendation 9: The Federal Government should update Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy.

Description:

The Federal Government should update Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience requiring a sector-specific Internet of Things (IoT) data strategy.

This strategy should address the following:

- \Data collection: This includes the sensors, devices, and gateways that are used to collect data from the physical world. It's important to determine what data is necessary for the use case and how frequently it should be collected.
- Data storage: The data collected from IoT devices needs to be stored in a way that is scalable, secure, and easily accessible. This may involve using a combination of on-premises and cloud-based storage solutions.
- Data analysis: IoT data often contains large amounts of noise and unstructured data, so it's important to have tools and techniques to analyze the data and extract meaningful insights. This may involve using machine learning algorithms, data visualization tools, or other analytics software.
- Data integration: IoT data often needs to be integrated with other data sources, such as enterprise systems or third-party data feeds. It's important to have a strategy for integrating this data to provide a holistic view of the business.
- Data governance: IoT data can be sensitive and may need to be handled in compliance with various regulations and privacy laws.
- Data sharing: IoT data may need to be shared with other stakeholders, such as customers, partners, or regulatory bodies. It's important to have a strategy for sharing data that protects sensitive information while still enabling collaboration and innovation.

Justification:

- tbd

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- tbd

Federal considerations:

- tbd

Recommendation 10: The Sector Risk Management Agencies (SRMAs) shall collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience.

Description:

The Sector Risk Management Agencies (SRMAs) shall collaborate with sector partners and develop IoT performance metrics intended to strengthen critical infrastructure security and resilience. By monitoring and analyzing these metrics, operators of critical infrastructure can optimize the performance of their systems and minimize the risk of disruptions or failures.

Some general metrics that are commonly used in critical infrastructure monitoring could include:

- Availability: This metric measures the percentage of time that the critical infrastructure is operational and available for use. It is a key metric in ensuring that the infrastructure is meeting the uptime requirements.
- Response time: This metric measures the time taken by the infrastructure to respond to a request or an event. Response time is a critical factor in determining the effectiveness of critical infrastructure systems.
- Throughput: This metric measures the amount of data that is transferred through the critical infrastructure in a given period. This metric is especially important for infrastructure that handles large amounts of data such as power grids and transportation systems.
- Reliability: This metric measures the ability of the critical infrastructure to perform consistently over time. It is important to ensure that the infrastructure is appropriately reliable and able to perform its intended functions even in adverse conditions.
- Security: This metric measures the appropriate level of security of the critical infrastructure. It is critical to ensure that the infrastructure is protected from cyber threats and other security vulnerabilities.
- Scalability: This metric measures the ability of the infrastructure to expand its capacity and capabilities as needed. Scalability is important in ensuring that the security and resiliency aspects of infrastructure are able to meet the increasing demands of its users over time.
- Energy efficiency: This metric measures the energy consumption of the critical infrastructure. It is important to ensure that the infrastructure is energy-efficient to reduce operating costs and minimize the impact on the environment.

Justification:

- tbd

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- tbd

Federal considerations:

- tbd

Recommendation 11: The Federal Government should establish a Smart Cities executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States.

Description:

The Federal Government should establish a Smart Cities executive office of the President to ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States.

The benefit of this recommendation would include:

- Coordination and Integration: Smart cities involve the integration of multiple technologies, systems, and stakeholders. A program office can provide a centralized coordination mechanism to ensure that all the elements are integrated seamlessly.
- Strategic Planning: A program office can help cities develop a comprehensive strategic plan for their smart city initiatives. This includes identifying goals, prioritizing initiatives, and developing a roadmap for implementation.

- Stakeholder Engagement: Smart city initiatives involve multiple stakeholders, including government agencies, private sector entities, and citizens. A program office can facilitate engagement with these stakeholders, ensuring that their needs and expectations are incorporated into the smart city planning process.

- Resource Allocation: A program office can help cities allocate resources effectively by identifying funding sources, prioritizing projects, and optimizing resource utilization.

- Performance Monitoring and Evaluation: A program office can monitor the performance of smart city initiatives, identify areas for improvement, and evaluate the effectiveness of the overall program. This can help cities to continuously improve smart city initiatives and achieve their goals.

Justification:

- tbd

Implementation considerations:

- tbd

Potential implementation barriers:

- tbd

Possible participating agencies:

- tbd

Federal considerations:

- Consider this recommendation in conjunction with Recommendation 1 (SCIEP) recommendation 8 (smart city officer at federal agency).