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 and Sustainability Extension Partnerships (SCSEP).

Description:

The federal government should consider funding and establishing a nationwide network of "smart city and sustainability extension partnerships (SCSEP) 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 SCSEP 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 in 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, sustainable infrastructure and IoT are broad in scope and discipline. SCSEP should be a multidisciplinary center, with expertise spanning technical, operations, cybersecurity, etc.
- The expertise lies across a variety of areas and could be implemented through partnerships with public (state, local) agencies, industry, and universities
- There are a small number of regional "smart city" type consortiums across the country. Consider establishing partnerships or collaboration with these consortiums to support or enable these capabilities.
- The USDA agriculture extension offices and the US DoC manufacturing extension partnerships models as starting points. They have built infrastructure and processes. In some rural areas, perhaps this is how these capabilities of the SCSEP are delivered through.

Potential implementation barriers:

- Limited expertise in the market and industry; resources and expertise may be difficult to secure
- Establishing a new extension office infrastructure will take time and resources
- There is not a clear or obvious federal agency owner for this.

Possible participating agencies:

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:

- SCSEP 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.
- Consider whether some of these activities can be performed through the existing extension offices and infrastructure, or through partnerships with regional consortiums or states

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.

The federal government, through its procurement and funding activities, can influence and facilitate action. For example, 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 (SB and SB8a) in federally funded transportation projects.

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.
- There are a lot of reasons for the lack of adoption. However, compliance is a critical tool to help spur adoption of IoT on government and government funded projects. The specification and adoption of IoT on these projects signals to the market the

government's interest and confidence in these technologies, which helps spur adoption in the non-government projects. It builds and reinforces capabilities in the marketplace (suppliers and workforce) to develop and support these technologies.

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. Without this list, the contractors will be left on their own to interpret what is meant by IoT, and in some cases, will do the minimum possible just to comply or comply with things that meet the definition but not make any sense.
- A broader vision and understanding of how IoT is to incorporated, used and operated is needed by project owner, government and operators in order to develop the requirements and specifications

Potential implementation barriers:

- Project owners may have limited to no IoT awareness of knowledge
- Limited expertise and resources in government and marketplace to support IoT in the projects
- Specification of IoT may add complexity and cost to the project, the requirements, and to the timeline
- No pre-defined acceptable or allowable IoT is be considered and specified for the different types of projects

Possible participating agencies

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

Federal considerations:

- The affected federal agencies should create a reference list or reference model, by project type (e.g. building, freeway or road project, etc.) of the types of IoT to be considered. This may require coordination with other federal agencies in alignment with their objectives, and working with industry and/or consultants to develop a reference set of IoT
- IoT may introduce cybersecurity vulnerabilities into the project or system. Require NIST cybersecurity frameworks are taken into consideration for specification of IoT into projects.
- The federal agencies should work with industry stakeholders to develop a list of what are the IoT elements to be incorporated or considered on projects by project type
- Consider incorporation of IoT solutions on federal government owned facilities, including those owned, managed, and operated by the GSA. For example, federal owned buildings should specify and use "smart" building systems, from building controls, energy

management and renewable energy, access control, etc. Select buildings or facilities can be “reference models” that can be used as models to be emulated by other federal facilities.

- Consider the incorporation of IoT in cities, facilities where BIL funds were used to build out broadband infrastructure. This provides an additional ROI on infrastructure.
- The SCSEP may be a resource to assist and facilitate the adoption and use of IoT in federally funded projects and grants.

Recommendation 3: The federal government should encourage other models to help select adopting organizations sustain and support in evaluating project feasibility

Description:

The federal government should consider models to help select adopting organizations sustain and support beyond the initial acquisition and building of new projects incorporating IoT technologies. While 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 organization, municipality or agency. Some select organizations have the resources, funding models, or mechanisms to find the resources to sustain the operation and maintenance of this asset or system. However, many other organizations, especially the smaller ones, or those in rural and tribal areas, that benefit from these technologies the most, do not have these mechanisms (budget, taxes, etc.), and may forgo these types of projects, or only operate the IoT applications short term until the funds run out. Similarly, current agency grant application evaluation criteria may screen out those that don't meet the financial requirements for sustaining operations.

Justification:

- Many grant programs are developed around financially supporting the initial procurement, acquisition and construction costs plus one or two years of operation of an asset or infrastructure. It is then expected that the grantee supports the ongoing operation afterwards after the grant funding period. However, operating and maintaining an asset over its useful life can be expensive, and some organizations, municipalities and agencies may not have sufficient resources and funds for this.

- IoT technologies may require additional levels of support that buyers may not have accounted for. For example, in addition to the cost of maintaining the physical IoT devices, there is software and data needs to be maintained. Depending on the device types, IoT can collect a lot of data that needs to be analyzed, stored and integrated with other software systems. The buyers may need to retain and maintain the data, hire the data science skills to build models and analyze the information, and staff to create programs based on the data.

- IoT technologies enable new business and operating models. These models impact project and service economics. For example, IoT technologies enable "as a service" and "pay per use" offerings, which is new in the market. However, these models have a high initial upfront cost, and a long, recurring cost recovery. This makes the ability of the organization to offset the operations and maintenance costs more challenging.

Implementation considerations:

- Extended Funding: For existing grant programs, consider extending funding for operations from one to two years for applicants that meet specific criteria of those that

can benefit from IoT but could not otherwise sustain it (rural areas, tribal areas, small cities and towns, etc.)

- Regional models: Incorporate models that encourage regional partnerships. For example, one small community may not have the means to sustain a small IoT application. But if multiple adjacent communities apply for a grant together, they may be able to leverage some economies of scale to purchase and set up the application, but may be able to employ synergies and cost sharing to maintain the application together.
- Innovative partnerships: Incorporate criteria that encourage and reward innovative approaches to sustaining operations. For example, one city was able to sustain operations by implementing a “support a AQ node” and getting corporate sponsors in the business community to support the maintenance and operation of the network.

Potential implementation barriers:

- IoT funding may be embedded into a broader funding or project package, and it may not be easy to separate the two.
- Non-traditional and innovative funding models may be challenging to track and evaluate

Possible participating agencies:

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

Federal considerations:

- A subset of organizations that receive federal funding and subject to recommendation 2 is part of this recommendation
- The SCSEP can be a resource that provides some support to help these adopting organizations operate and sustain their IoT solutions

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 exacerbated for smaller municipalities and agencies, and those in rural and tribal 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:

- Leverage model used by the National Health Science Corps
- These resources can work with non-profit organizations that support government agencies (e.g. FUSE Corps).
- Identification of specified work roles/skills needs (cybersecurity, data analytics, software development

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 SCSEP (Recommendation 1) and specification of IoT into federally funded projects (Recommendation 2).

Recommendation 5: The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models.

Description:

The federal government should facilitate and support the development and use of smart city and sustainable infrastructure reference models that capture and document the ecosystem. Smart cities are complex ecosystems of communities, neighborhoods, districts, buildings, other cities, utilities, and businesses that co-exist, collaborate occasionally and interoperate with each other. Reference models capture the various components of the ecosystem and provide a blueprint for design and planning, collaboration, coordination and communication in smart city efforts, sharing and economies of scale.

These reference models include technical and operations frameworks and architectures, operational concepts, and draft requirements and reference standards. The reference models serve as a template that planners can use to plan, design and build their smart city projects, and if followed, provides a path for interoperability, scalability, integration and security. Furthermore, these models incorporate best practices and facilitate collaboration between various stakeholders, accelerate adoption and scaling, and are replicable.

A broader reference model/architecture helps to identify use cases, potential areas of collaboration between entities, as well as identify areas of “sharing” and economies of scale.

Justification:

- The smart city market is fragmented and broad. In addition, the applications in the market span a lot of different areas, from transportation to energy to things like resilience, public safety, economic vitality, to operations. These applications may have different standards and practices.
- Most smart city projects are DIY and not replicable for the needed mass adoption scales
- Most smart city (and other brownfield projects) efforts are “one off” approaches with disparate “point solutions” piecemealed together by different departments and agencies. This results in inconsistent and disjointed smart cities with IoT applications that don’t integrate together or share a common infrastructure. This leads to problems with integration, interoperability, data silos, replication of infrastructure, scaling, potential cybersecurity vulnerabilities and privacy issues, and higher costs. This may also lead to a lack of interoperability with nearby cities (in a region or in a county).
- While there are various efforts around smart city standards and models, many of these are either in development, are incomplete, unknown to adopters, or are not easily consumable by city planners and designers. There is no standardized reference model of a smart city that planners can use as a starting point.
- Existing reference models focus on cities. Smart cities can be communities, counties, and regions and states. Real life smart cities are an ecosystem of diverse stakeholders. Existing models don’t show those, and their collaborations and dependence.

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

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.
- There is not a one size fits all “reference model and architecture”. There is one for small cities, large cities, as well as “smart regions”, utilities, buildings, etc..
- Key participants in developing the reference model include government (states), federal, industry (and industry and standards bodies), and academia.
- There are various efforts around models and standards. Consider projects that are funded using federal money to incorporate the use of these reference models.
- NIST has developed the Smart City Framework v1.0 (https://pages.nist.gov/smartcitiesarchitecture/) but that is a starting point for building on something that is more usable by city planners

Potential implementation barriers:

- Complexity of coordinating various stakeholders together to define a reference model or architecture
- There may be work in these models undertaken by consortiums or industry. Integrating and aligning existing parts of models may be challenging.

Possible participating agencies:

- NIST - GCTC
- NSF - Smart and connected communities
- DoE
- DoT

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.)
- This recommendation may support Recommendation 2

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 as they don't have the same access and measures for raising funds as larger cities. 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.

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.
- Consider the incorporation of IoT in cities, facilities where BIL funds were used to build out broadband infrastructure. This provides an additional ROI on infrastructure.

[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 IoT standards. (some overlap with recommendation 5)

Description:

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

Justification:

- Smart city and sustainable infrastructure 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. Solar inverters on solar power systems have varying standards. In addition, smart city and sustainable infrastructure projects span a variety of application areas, from transportation to energy, to public safety and more. Each of these incorporate specific application areas standards that may need to be converged and interoperate.
- 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:

- Depending on the agency (DoE, etc.), there are already existing definitions of standards.
- Consider incorporating the need for open standards, industry consortium, or standards body developed standards as part of the requirements for federal funded projects

Potential implementation barriers:

- Different agencies within the federal government have different definitions and standards. For example, for air quality, the EPA has a set of standards that may be different than the ones used by USDA, DoE, etc. The federal government agencies should standardize around their definitions and requirements for air quality.

Possible participating agencies:

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

Federal considerations:

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

- 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).
- Consider specifying that projects that use federal funding adhere to some agreed to set of standards

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

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

This positions 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

Implementation Consideration

- Once assigned via the Agency Head, e.g., Cabinet Secretary, the SCO will be required to develop a 90-day plan to include resources necessary to carry out the SCO program

Barriers

- Lack of funding to support the SCO, notably in terms of staff needed (federal and contractor) and communications/outreach

Possible participating agencies

- The 24 CFO Act agencies, with consideration being given to the non-CFO Act agencies

Federal Considerations

- Ensure that the SCO in each agency will participate in a Community of Practice, like the Federal CIO Council format, which, in turn, will serve to convene SCOs across all agencies

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

Existing Presidential Policy Directives are outdated and should be updated to reflect the current risk associated with critical infrastructure reliability, resilience, security, and sustainability

Implementation Consideration

- Development of the language and context should include input from the National Security Council, the Office of Management and Budget, and Intelligence Communities.
- Once developed, the language could/should be shared with additional communities of interest/practice, e.g. NERC, FERC, ISACs.

Barriers

- Lack of coordination among the key stakeholders, based on disparate missions
- Most of the critical infrastructure assets/systems are owned and operated by private sector entities, thus, requiring crucial conversations with said infrastructure owners/operators

Possible participating agencies

- All SRMAs

Federal Considerations

- Continuous and comprehensive asset visibility is a basic precondition for any organization to effectively manage critical infrastructure risk. Accurate and up-to-date accounting of assets residing on federal networks is also essential.
- Enhancing visibility into agency assets and associated vulnerabilities, focusing on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration.

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

The expansive development and adoption of IoT assets and systems should map to IoT performance metrics intended to strengthen critical infrastructure security and resilience

Implementation Consideration

- Agency Chief Technology Officer and associated program office could serve as the nexus for convening peer stakeholders, e.g. CIO, CDO, CPO.
- Defining the performance metrics will need to be in conjunction with owners/operators of critical infrastructure assets/systems (both IT and OT).

Barriers

- Lack of coordination from the Executive Office
- Minimal support from designated agency leadership
- Lack of branding
- Lack of coordination, stakeholder engagement, resource allocation, and performance monitoring

Possible participating agencies

- The 24 CFO Act agencies, with consideration being given to the non-CFO Act agencies

Federal Considerations

- Ensure that the SCO in each agency will participate in a Community of Practice, like the Federal CIO Council format, which, in turn, will serve to convene SCOs across all agencies

Recommendation 11: The Federal Government should establish a Smart Cities Program Office within the 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

This central office will ensure that the federal government, state, and local government entities can effectively plan, implement, and manage smart city initiatives across the United States

Implementation Consideration

- The SCPO will align with the U.S. Chief Technology Officer Team to maximize the benefits of IOT and corresponding data for critical infrastructure sectors.

- The SCPO will develop a 360-day approach/plan addressing how the Federal Government can help cities develop a corresponding strategic roadmap for their smart city (and IoT) initiatives. This includes identifying goals, prioritizing initiatives, and developing a roadmap for implementation.

Barriers

- Lack of coordination from the Executive Office
- Minimal support from designated agency leadership
- Lack of branding
- Lack of coordination, stakeholder engagement, resource allocation, and performance monitoring

Possible participating agencies

This office should be aligned with the Office of Science and Technology Policy to:

- work with federal departments and agencies and with Congress to create bold visions, unified strategies, clear plans, wise policies, and effective, equitable programs for IoT and Smart Cities modernization
- engage with external partners, including industry, academia, philanthropic organizations, and civil society; state, local, Tribal and territorial governments; and other nations
- ensure equity, inclusion, and integrity in all aspects of IoT implementations

Federal Considerations

- Ensure that the Coordination and Integration with the NIST (FWIoT and GCTC) protocols are in place, i.e. IoT implementations involve the integration of multiple technologies, systems, and stakeholders. A SCPO can provide a centralized coordination mechanism to ensure that all the elements are integrated seamlessly.

Recommendation 12: The federal government should specify and utilize energy efficient and sustainable 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 energy efficient 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.).

There are already a number of existing technologies that can spur the transition to a more energy efficient economy: renewable generation (i.e., solar/wind) energy storage, microgrids, transportation/building electrification, and demand response. Many of these technologies complement each other. As an example: Solar Panels can be installed with an Energy Storage System that can store the energy sources for usage at a later time. Installing Energy Storage Systems with EV Charging Equipment can also help respond to large fluctuations and/or peaks in grid demand by discharging from the battery when the demand for EV charging exceeds the capacity of the electricity network. They can also shift charging times to when electricity is cheaper and more abundant.

They can also help to promote the energy transition in the private sector.

Justification:

- There is an overall worldwide trend across governments and nations to decarbonize and reduce greenhouse gas emissions. The Intergovernmental Panel on Climate Change, the United Nations body for assessing science related to climate changes, had produced a special report on the impacts of global warming of 1.5 degrees C (https://www.ipcc.ch/sr15/chapter/spm/). The US is behind with respect to other countries and nations on this target.
- While there has already been Federal Funding through the Bipartisan Infrastructure Law (BIL) and the Inflation Reduction Act (IRA) it needs to serve as a catalyst for the broader energy transition in the private sector.

Implementation considerations:

- Energy Savings Performance Contracts (EPSCs) are a mechanism to allow federal agencies to procure energy savings and facility improvements with no up-front capital costs or special appropriations from Congress. An EPSC is a partnership between an energy and an energy service company.
- Building Energy Use Benchmarking is another effective mechanism that measures energy performance of a single building over time as compared to other similar buildings. It facilitates opportunities for improvement.

- Adoption of building and energy codes that include language like automated demand response technologies and EV-Ready/EV-Capable language that will provision these facilities to accommodate future demand response programs and EV Charging equipment.

- The GSA Federal Acquisition Regulation (FAR) could have base level energy efficiency requirements for procurement in federally owned or operated buildings.

Potential implementation barriers:

- Funds: Costs to wide scale conversion to an energy efficient economy are significant

- Supply Chain: In some cases, there are existing supply chain issues (i.e., distribution transformers, mining limitations for batteries,) that the manufacturing community is working to overcome.

- Legacy Equipment: Some of the existing legacy equipment such as boilers, furnaces, hot water heaters, and stoves have a long operating lifetime.

Possible participating agencies

- All federal agencies that provide grants and funding for projects where energy efficient technologies may be incorporated.

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

Recommendation 13: The federal government should support existing industry standards development activities with respect to energy efficient technologies that are used in sustainable infrastructure.

Description:

The federal government should support existing industry standards development activities with respect to energy efficient technologies that are used in sustainable infrastructure. This is particularly relevant if these standards activities are addressing known gaps and solving market fragmentation issues.

It would be good to survey the standards landscape to better ascertain where these efforts are occurring as several activities are already underway. There are also several roadmap activities underway that are identifying needed gaps. A noteworthy example of this is the ANSI Electric Vehicle Standards Panel that is currently developing a roadmap of codes & standards needed to deploy Electric Vehicles at scale. That activity is a cross-sector body fostering collaboration and coordination on standardization matters among public- and private-sector stakeholders to enable the safe, mass deployment of electric vehicles and associated infrastructure in the United States with international coordination, adaptability, and engagement: https://www.ansi.org/standards-coordination/collaboratives-activities/electric-vehicles

Justification:

- Standards efforts that are not coordinated, aligned cause confusion in the market.
- Harmonized standards provide consistent guidance for design, operations, and maintenance. They can also facilitate market entry. When feasible international harmonization of standards should be pursued.

Implementation considerations:

- The Federal Government can call out existing standards in applicable legislations and regulations.
- The Federal Government can support the private sector in relevant standards development activities.

Potential implementation barriers:

- Resources: The standards development process can be time consuming, particularly when trying to achieve consensus. Once standards are published, they typically need to undergo maintenance (revisions, updates) within a certain time frame. This time frame increases when international harmonization is being pursued.

Possible participating agencies

- NIST, DHS, DOT, DOE, CISA, among others.