Analytical Work Grant Application

QUALITY INFRASTRUCTURE INVESTMENT PARTNERSHIP

TITLE of ACTIVITY TO BE FINANCED: CYBERSECURITY TOOLKIT FOR SMART CITIES

SECTION A – BASIC DATA

1. **Task Team Leader(s)**	Jessica Carolina Grisanti	
2. **Managing Unit**	SURGP	
3. **Submitting GP**	URL	
4. **Date of submission**	12/20/2023	
5. **Proposed Grant amount (US$)**	$250,000 (co-funded with $200,000 from the Cybersecurity TF)	
6. **Proposed duration of grant (months)**	24 Months	
7. **Region**	☐ AFR ☐ EAP ☐ ECA ☐ LAC ☐ MNA ☐ SAR ☒ Global	
8. **Elements of QII that will be enhanced by the Grant**	☒ QII.1 Sustainable Growth and Development ☐ QII.2 Economic Efficiency in view of Life Cycle Cost ☐ QII.3 Environmental Considerations ☐ QII.4 Resilience against Natural Disaster ☐ QII.5 Social Considerations ☒ QII.6 Infrastructure Governance	
9. **Infrastructure Sector supported by the Grant (Check <u>one</u> that is most relevant)**	☐ Digital Development ☐ Energy and Extractives ☐ Governance ☐ Transport ☒ Urban, Disaster Risk Management, Resilience and Land ☐ Water	
10. **Name(s) of primary counterpart(s)/Implementing Agency:**	Counterpart Name: Global with the first pilot in Lima, Peru	Agency To be determined

SECTION B – DESCRIPTION of GRANT ACTIVITY TO BE FINANCED

Note: *All questions are mandatory unless stated otherwise**.***

B.1 Describe the objective of the QII Grant and its effect on the supported WB operation.

Provide a grant specific objective statement and describe how the activities will support the achievement of the objective.

The objective of the grant is to develop a Cybersecurity Toolkit for Smart Cities (STSC) by leveraging Sectoral Cybersecurity Maturity Model (SCMM) and other cybersecurity tools being developed by the Digital Development GP (DD GP) (e.g. Cybersecurity Risk Assessment Framework (CRAF), Cybersecurity Good Practice Note (CGPN)) and tailoring them specifically for smart cities and to the city context, and then piloting them under GSCP3 (Global Smart City Partnership Program Phase 3, P181073), and refining the toolkit further for scale-up across various urban service sectors and their smart systems such as Intelligent Transport System (ITS), urban land and housing information system, and urban data platform.

B.2 Describe what question(s) the proposed analytical work will address.

No	Key Question to be Addressed
1	What are the most pressing cybersecurity risks or needs in the cities of developing countries? What is the level of awareness and preparedness of cities regarding cybersecurity risks and solutions?
2	How can a sectoral maturity and risk assessment, notably for urban transport, inform a city-level cybersecurity strategy and roadmap? Which part of the SCMM methodology can be adjusted to the city context? How do we adjust the Layers of Assessment (LoA), Dimensions and Factors in SCMM?
3	What are the concrete actions that cities can implement to address and prevent cybersecurity risks and enhance their cyber resilience?

Please provide a comprehensive assessment of the context, how the key questions identified above will be addressed with the grant, proposed methodology and the specific value that the QII Grant will provide to the global knowledge on QII. Please focus on the impact, by describing how this analytical work will contribute to enhancing the knowledge and implementation of the QII Principles selected in Section A, Question 8.

The objective of the proposed work is to develop and pilot a Cybersecurity Toolkit for Smart Cities through the Global Smart City Partnership Program (GSCP). GSCP provides technical and operational support to the World Bank Group (WBG) teams and clients by mobilizing smart city experts to meet their demands. Since 2018, GSCP has supported over 50 engagements on smart cities across digital development, transport, urban and other key infrastructure sectors. Building on five years of successful implementation, GSCP has transitioned to its third phase (GSCP3) through a concept review in May 2023. One of the strong recommendations at the review meeting was to strengthen digital safeguards for smart city investments, particularly by addressing cybersecurity risks that can undermine the advancement of smart cities. It is also an opportune time to benefit from and contribute to the WBG-wide momentum on mainstreaming cybersecurity with useful tools such as Sectoral Cybersecurity Maturity Model (SCMM) in place. Recognizing that the current SCMM methodology was developed for sectoral assessments at the national level, the proposed activity will focus on applying it to the sub-national, city level so that the client cities can better understand the threats, risks and opportunities of emerging technology and develop strategies, institutional arrangements and capacities to address cybersecurity issues, which is a critical foundation for their smart city endeavors. SCMM builds on a premise that cyber resilience is intricately interlinked to

various components of a system within a sector and is not simply the sum of the individual capacity of its constituent parts – i.e. the model offers a holistic approach that considers both the individual components contributing to sectoral cyber resilience and their correlations and dependencies, seeing a sector as a system and filling the gap in the existing assessment tools with a national or organizational focus, which lacks such integrated view (World Bank. 2023. Sectoral Cybersecurity Maturity Model).

With the SCMM's emphasis on a holistic approach, it is naturally fit for understanding city-level cybersecurity risks. City development requires a holistic approach to city infrastructure and services, effectively integrating strategies and investments across various sectors within cities. The true potential of smart cities comes from an effective use of data and digital technologies for facilitating the integration of sectoral planning and service provision and therefore achieving city-wide (cross-sectoral) innovation or transformation. If a sector is a system as noted in the Sectoral Cybersecurity Maturity Model (World Bank 2023), a smart city aspires to be a functioning system of systems (GSCP Smart City Engagement Guidance Note. 2023). From a cybersecurity perspective, it will then be necessary to examine risks and maturity across multiple sectors and adjusting and applying SCMM to the subnational, city level as a microcosm of the national level, with an expansion of the existing model.

In addition to SCMM, GSCP will take advantage of the new Cybersecurity Risk Assessment Framework (CRAF) that is about to be finalized by DD GP and ITS. While the SCMM focuses on readiness or maturity in terms of government institutions, regulations and measures, CRAF addresses technical sides of the digital technology investments from the cyber risk perspective. Cybersecurity incidents could, for instance (a) disrupt the delivery of critical services such as a utility's levels of production and distribution, (b) present a 'distributed denial of service' (DDoS) attack that could overload e-government systems and disrupt access to their services, or (c) deploy ransomware that could cause harm to populations in developing nations by holding sensitive systems or information hostage with the threat of leaking them or selling private data. Hence, CRAF will assess the technical and procurement risks such as industrial standards, maintenance practices and third party "back door" access. As smart city projects introduce digitalization and digital transformation in critical infrastructure such as energy, water, health and transport, proper risk assessment is critical in implementation of the project.

For smart city engagement, the GSCP Guidance Note provides two approaches: (i) a top-down approach starting from development of a smart city strategy that can guide sectoral activities downstream; and (ii) a bottom-up approach starting with a specific sector with strong data and digital systems and interconnecting them with those of other sectors to develop an integrated system at the city level. Applying this to cybersecurity assessment, the proposed work consists of two interlinked activities. Using a pilot case in Lima, where GSCP will support 'Lima Traffic Management and Sustainable Transport (LTM), P178842' selected under its Round 8 call for proposals in November 2023, the team will adjust and apply the existing SCMM and upcoming CRAF for urban mobility as a leading sector of smart cities (bottom-up). Building on this experience, the team will concurrently develop a more standard, broader cyber assessment tool for smart cities, which can cover various city functions and service sectors. Below is the summary of the proposed activities.

Activity 1 is to develop a Cybersecurity Toolkit for Smart Cities by leveraging Sectoral Cybersecurity Maturity Model (SCMM) and other cybersecurity tools being developed by the DD GP (e.g. Cybersecurity Risk Assessment Framework (CRAF), Cybersecurity Good Practice Note (CGPN)) and tailoring them specifically for smart cities and to the city context. Activity 2 will pilot the Cybersecurity Toolkit for Smart Cities through GSCP regular call for proposal for EOIs. Activity 3 includes producing knowledge products (completion report, case studies) and disseminating the conceptual framework, methodology, key elements of the new model at a webinar, BBLs and various annual events including the World Smart City Expo in Korea and Smart City Expo World Congress in Spain.

B.3 Describe a dissemination plan for the proposed analytical work.

As we develop the Toolkit and pilot it in in GSCP supported projects the team will raise awareness on cybersecurity issues, SCMM and CRAF with GSCP client teams and countries. As the key output of the work, the Cybersecurity Toolkit for Smart Cities will be publicized as a knowledge product and will be presented in the annual event such as the World Smart City Expo in Korea and the World Smart City Congress in Spain. The team will inform and engage with QII and Cybersecurity Multi-Donor Trust Fund (MDTF) at major dissemination events.

B.4 Explain how the Grant could potentially influence the preparation/implementation of WB operations

Once we develop the Cybersecurity Toolkit for Smart Cities will help GSCP to provide replicable support in assessing the cybersecurity circumstance and potential threats and to recommend solutions in selected sectors. As smart technologies advance in different sectors and converge in the city administration, and the number of cities that are interested or engaged in smart city project grows, the potential risk regarding the cybersecurity keeps getting higher. As such assessing the maturity and risk of cybersecurity of smart city projects will be critical and the impact of the new tool will be extensive. Specifically, a WB operation named "Lima Traffic Management and Sustainable Transport (LTM), P178842", which is seeking for a support to assess cybersecurity risks for LTM system and find solutions, poses as a good pilot for the new tool among the selected GSCP support recipients in November 2023. GSCP will also collaborate with the task team to identify and leverage any synergies related to smart traffic management in Lima, which have been enhanced with the support from the Public – Private Infrastructure Advisory Facility (PPIAF).

B.5 Describe each activity to be financed by the Grants using the template below

ACTIVITY 1	
Activity Name:	**Developing a Cybersecurity Assessment Toolkit for Smart Cities**
Relevant Key Question(s) from Section B, Question 1 *(check all that apply)*	1 ☒ 2☒ 3 ☐ 4☐
Estimated Costs:	$ 150,000 (QII contribution)
Description *(provide a clear objective, scope of work and methodology)*	
The activity 1 consists of (i) Stock taking and desk review of the frameworks and tools available at the WB to better understand what is applicable at the local level, the gaps and how can they be use together; and (ii) develop the toolkit. The existing SCMM is designed to capture and assess different aspects of sectoral cybersecurity maturity across **three Layers of Assessment** (LoAs), which correspond to three different categories of stakeholders: National Entities (LoA1), Sectoral Supervisory Authorities (LoA2), and Sector Key Entities (LoA3). National Entities refer to central government or agencies that are in charge of overarching rules or regulation with regards to cybersecurity. Sectoral Supervisory Authorities means the ministries or agencies that overlook the specific sectors, such as Department of Transport, Federal Housing Agency or else. Sector Key Entities refer to those who operate the daily services in the critical infrastructure sectors such as telecommunication companies, bus service companies, commercial banks, etc. For each LoA, the SCMM evaluates five Dimensions (or areas of assessment), namely: Cybersecurity Governance, Cyber Risk Management,	

Cybersecurity Measures, Cyber Capacity Building, and Incident Response and Crisis Management. Each of these Dimensions comprises of twelve Factors and a number of Indicators that help assessors to judge the level of maturity of each factors, which provide a more granular level of analysis and a set of guiding questions to structure the data gathering.

On the other hand, CRAF, which is being developed in DD GP in cooperation with ITS, is designed to assess the technical risks, political and governance risks and procurement risks. Technical risks refer to vulnerabilities such as non-adherence to best practice design or industry standards as insufficient technology maintenance (e.g. missing software patches or upgrades) can create vulnerabilities in critical infrastructure or systems that enable incidents, potentially disrupting service delivery and compromising personal information. Political and governance risks refer to gaps in institutional, legal or governance frameworks that enable attackers to compromise infrastructure or systems. This risk could also involve the misuse of World Bank-funded tools and software in ways that do not comply with personal data privacy and protection norms – in what is called misuse of 'dual-use technologies' and can present significant reputational risk to the Bank. Procurement risks refer to purchase of infrastructure or technology that have hidden intentional or unintentional "backdoor access," enabling unauthorized third parties to access government servers, systems and data. Software upgrades could patch as well as introduce such a vulnerability.

As smart city projects require WB teams to analyze the current status (readiness and maturity) of the subject field of the clients and the potential risks embedded in the smart city investments, the new cybersecurity toolkit for smart cities will be focused on identifying strength, weakness, and risk factors with practical findings on the cybersecurity environment in city administration – technical (hard and software), regulatory, institutional/governance and human capacity. The adjusted model will review and modify the key elements of the existing tools for conducting city-level assessments.

The team plans to **hire a capable consulting firm or a consultant** that is specialized in both cybersecurity and public service domains of cities. The firm or person will undertake the development of the tool, support the pilot testing in selected cities, and ensure the quality of user experience after the development and throughout piloting. The Korean partners of GSCP such as MOLIT (Ministry of Land, Infrastructure and Transport), NIA (National Intelligence Association) and Korea Agency for Infrastructure Technology Advancement (KAIA) will be invited to participate in the best design of a tool.

Relevance to QII Principles:
(Please select the QII aspect that is most relevant to the proposed activity and explain word limit – 150)

QII.1 - Sustainable Growth and Development
Grant will help GSCP team to develop the Cybersecurity Assessment tool for Smart Cities, which will provide a solid foundation for sustainable growth and development of smart cities with digitalized and interconnected service platforms where cybersecurity is critical. The new tool will address cybersecurity issues in various angles such as administrative levels (national vs local vs government sponsored agencies), different service sectors (transport, waste, electricity, energy, et cetera) and different administrative measures (regulations and capacity building).

Expected Outputs:
(Please provide specific deliverables (and interim deliverables if applicable) from the planned activity by populating the table provided. Deliverables may include, for example, guidelines, manuals, plans, publications, reports, seminars, systems, trainings, workshops, etc.

No	Description of Deliverables	Quantity	Planned Delivery Date *(months from grant award)*

1-1	Joint stocktaking workshops between SCMM team, CRAF team and GSCP team	2	3 months
1-2	Contract with a consultant or consulting firm	1	3 months
1-3	Prototype of Cybersecurity Assessment Tool for Smart Cities	1	18 months
1-4	Finalize "Cybersecurity Assessment Tool for Smart Cities" including conceptual framework, methodology, and guidelines	1	24 months

Expected Intermediary Outcomes:
(Please provide an outcome statement for each output to be produced, focusing on the short to medium term effects of the grant's outputs in beneficiary's behavior, knowledge, skills, status, or way of functioning. The outcome statement must be specific, measurable, achievable, relevant, and time-bound)

No	**Outcome Statement**	**Timeline** *(year/months from grant award)*
1-1	Enhanced understanding of cybersecurity, SCMM and CRAF in GSCP team and experts group via participation in the stocktaking workshops and collaboration on the cybersecurity assessment tool. Indicator: 30 relevant participants attend workshops	1 year
1-2	Establishment and endorsement of replicable and effective GSCP support tool in cybersecurity of smart city projects.	2-5 years
1-3	Laying groundwork for cross-sectoral collaboration between DD and URL on smart city and beyond is established via the expanded application of the toolkit and continuous knowledge exchange. Indicators: 3 DD/URL projects applying the toolkit -2 webinar sessions on the cross-sectoral collaboration	3-5 years

ACTIVITY 2	
Activity Name:	Piloting the toolkit to GSCP projects
Relevant Key Question(s) from Section B, Question 1 *(check all that apply)*	1 ☐ 2☒ 3 ☒ 4☐
Estimated Costs:	$ 75,000 QII contribution

Description *(provide a clear objective, scope of work and methodology)*

Activity 2 consists of (i) identifying projects/city to pilot the toolkit; ii) conducting the existing SCMM procedure and CRAF to the projects, (iiI) pilot the toolkit; produce a report that summarizes the piloting excesses and lessons learned and iii) report that will summarize key recommendations from the pilot to incorporate in the toolkit.

GSCP will identify projects to pilot the toolkit through GSCP regular call for proposal process. The program currently utilizes a call for proposal for EOIs to identify projects to be supported under GSCP3 Component 1 (Technical Assistance to Smart City Strategic and Investment Planning). The Program is expected to support 12 lending operations/ASA that have smart city components, which can presents opportunities for piloting the toolkit.

The program just closed round 8 for call proposal and the GSCP team selected a WB project named "Lima Traffic Management and Sustainable Transport (LTM), P178842", which is seeking for a support to

cybersecurity measure for LTM system, as a pilot subject for the SCMM from the most recent round of call for proposal. With GSCP call for proposals planned in April and October 2024, the program will have an opportunity to pilot which will help further refine and finalize the toolkit.

Under this activity the team aims to identify gaps and challenges hindering the ability of the sector to reach a higher level of cybersecurity maturity, then starts to organize them into an assessment report that will include among other sections:

• An executive summary providing the main findings and high-priority recommendations;
• An overview of the main aspects related to the digitalization and cybersecurity of the sector under analysis, including a presentation of the specific country and sectoral context;
• A list of all the entities involved in the assessment
• A thorough explanation of the key findings, with particular attention to maturity gaps; and
• A thorough explanation of the high-level recommendations

The team will also formulate a set of tailored recommendations to strengthen the cyber capabilities and resilience of the sector. Subsequently, the team will incorporate all the relevant assessment results to produce the new model or tool tailored for Smart Cities. The new tool will not only address the maturity of the client countries but also assess the risks embedded in the smart city investments.

Relevance to QII Principles:
(Please select the QII aspect that is most relevant to the proposed activity and explain word limit – 150)

QII.1 - Sustainable Growth and Development
Grant will help GSCP team to develop the SCMM for smart cities, which will provide a solid foundation for sustainable growth and development of smart cities with digitalized and interconnected service platforms where cybersecurity is critical. The new model will address cybersecurity issues in various angles such as administrative levels (national vs local vs government sponsored agencies), different service sectors (transport, waste, electricity, energy, et cetera) and different administrative measures (regulations and capacity building).

Expected Outputs:
(Please provide specific deliverables (and interim deliverables if applicable) from the planned activity by populating the table provided. Deliverables may include, for example, guidelines, manuals, plans, publications, reports, seminars, systems, trainings, workshops, etc.

No	Description of Deliverables	Quantity	Planned Delivery Date *(months from grant award)*
2-1	Report documenting application of toolkit to selected pilot cases	2	12 months
2-2	Application of the SCMM to pilot cases	2	18 months
2-3	Application of CRAF to pilot cases	2	18 months
2-4	Summary report of key lessons learned and recommendations for toolkit application	1	24 months

Expected Intermediary Outcomes:
(Please provide an outcome statement for each output to be produced, focusing on the short to medium term effects of the grant's outputs in beneficiary's behavior, knowledge, skills, status, or way of functioning. The outcome statement must be specific, measurable, achievable, relevant, and time-bound)

No	Outcome Statement	Timeline *(year/months from grant award)*
2-1	cybersecurity plans for pilot cities are established via the application of the cybersecurity toolkit to the 2 identified pilot cases	2 years
2-2	Lessons learned and key recommendations from the summary report result in updates to the toolkit that lead to its Establishment as a replicable and effective GSCP support tool in cybersecurity of smart city projects	3 years

ACTIVITY 3	
Activity Name:	Dissemination and Mainstreaming of the Cybersecurity Toolkit for Smart Cities
Relevant Key Question(s) from Section B, Question 1 *(check all that apply)*	1 ☐ 2☒ 3 ☒ 4☐
Estimated Costs:	$ 25,000 (QII Contribution)

Description *(provide a clear objective, scope of work and methodology)*

As the new toolkit for smart cities is developed or finalized and gets ready to be launched, the team will disseminate the conceptual framework, methodology, key elements of the new model at webinar, BBLs and various annual events including the World Smart City Expo in Korea and Smart City Expo World Congress in Spain. In addition, the team will collaborate with the SCMM team and other relevant teams to expand the use of the new tool as well as the branding of GSCP.

Relevance to QII Principles:
(Please select the QII aspect that is most relevant to the proposed activity and explain word limit – 150)

QII.1 - Sustainable Growth and Development
Grant will help GSCP team to develop the SCMM for smart cities, which will provide a solid foundation for sustainable growth and development of smart cities with digitalized and interconnected service platforms where cybersecurity is critical. The new model will address cybersecurity issues in various angles such as administrative levels (national vs local vs government sponsored agencies), different service sectors (transport, waste, electricity, energy, et cetera) and different administrative measures (regulations and capacity building).

Expected Outputs:
(Please provide specific deliverables (and interim deliverables if applicable) from the planned activity by populating the table provided. Deliverables may include, for example, guidelines, manuals, plans, publications, reports, seminars, systems, trainings, workshops, etc.

No	Description of Deliverables	Quantity	Planned Delivery Date *(months from grant award)*
3-1	Showcasing the SCMM and the new tool for Smart Cities in the world smart city event such as the World Smart City Expo in Korea or the Smart City Expo World Congress in Spain	2	20

Expected Intermediary Outcomes:

(Please provide an outcome statement for each output to be produced, focusing on the short to medium term effects of the grant's outputs in beneficiary's behavior, knowledge, skills, status, or way of functioning. The outcome statement must be specific, measurable, achievable, relevant, and time-bound)

No	Outcome Statement	Timeline *(year/months from grant award)*
3-1	Raising awareness of cybersecurity in smart city stakeholders around the globe such as mayors, government officers, smart city engineers and research institutes Indicators: - Number of clients/participants satisfied with knowledge sharing and dissemination activities -5 Follow-up discussions with interested stakeholders to advance the SCMM work	2 years
3-2	Increase in usage of the new assessment tool for cybersecurity in smart cities Indicator: Applications of the toolkit in five cities	2-5 years

B.6 Describe additional and innovative aspects of the QII Grant proposal.

Describe new, experimental solution to accelerate development impact, such as new technology, product, policy, or other approach; or adaptation of an established approach to accelerate development impact within a different sector or context which proves to be innovative and experimental.

The proposed activity attempts to adapt Sectoral Cybersecurity Maturity Model (SCMM) and other cybersecurity tools that are already developed under the collaboration of WB and Tel Aviv University to the context of Smart City development. For those cities that pursue Smart City vision where data and information flow seamlessly within the digitalized (internal) systems or (interactive) platforms in critical infrastructure and service sectors, cybersecurity has emerged as a critical risk. As such, the output of the activity, SCMM for Smart Cities, will secure a safe path to Smart City goal that enables sustainable and inclusive growth.

B.7 Does the proposed activity include a component relating to digital transformation in critical infrastructure?

☒Yes ☐No

If yes, please explain.

Cybersecurity is one of the building blocks to ensure that digitalized services in critical infrastructure such as public transport, roads or railways, energy, water, and urban and geospatial planning are running securely. GSCP promotes smart city development, which entails an evolution of major infrastructure and service areas through digitization and digitalization processes towards digital transformation at the city level through an integrated digital and institutional system of city functions. Cybersecurity has posed one of the most critical and relevant agenda for the program and its goal to support our clients' ambition of digital transformation in cities. By developing cybersecurity maturity and risk assessment model, GSCP can raise the efficiency, safety and social trust of the digital system and further enhance the digital transformation in urban infrastructure management.

SECTION C – ADDITIONAL JUSTIFICATION AND CONSIDERATIONS

C.1 Describe the reasons why the proposed activities cannot be engaged through normal World Bank business or other relevant similar facilities (e.g.; WB supervision/preparation budget, Project Preparation Facility, PPIAF, GFDRR, etc.)1. Describe co-financing and collaboration opportunities to create synergies for improved service delivery (if any).

Cybersecurity is an emerging agenda which requires specialized skills and expertise. GPURL and particularly GSCP has a well stablished engagement with cities and local government that are currently investing on the smart systems and overall smart cities agenda, but cybersecurity is not always a top priority in those investment. Therefore, this is a great opportunity to strengthen the smarty city engagements and develop safe and sustainable projects.

Moreover, the Cybersecurity MDTF jointly with QII Partnership is set up to build cyber and digital security capability and capacity through knowledge, technical assistance and practical tools and therefore is best positioned to further the agenda within the World Bank. The proposed activities are aiming to be co-funded by Cybersecurity MDTF ($150,000) and QII Partnership ($250,000) in total $400,000 for the urban sector (including urban transport) where the existing tools have not yet been introduced or applied. The activities will be planned and executed by GSCP team under Global Practice for Urban, Resilience and Land (GPURL) with the support of Cybersecurity/SCMM team under Digital Development (DD) Global Practice, creating synergies between two practices (i.e. urban and digital) and navigating possibilities of collaboration beyond the smart city agenda. GSCP will also co-finance the activity through GSCP team and experts' time and travel (if needed), particularly for Activity 2 (piloting).

C.2 Provide details of client demand, global director awareness and support for the technical assistance activities, and any other factors that will help achieve the grant objectives.

While the cybersecurity is a nascent agenda within GPURL, there is sufficient awareness on the importance of having digital safeguards in our operations with rapid penetration of digital technologies. More importantly, GSCP clients have always raised questions on cybersecurity and data privacy and protection in our engagement on smart cities, which the team has been less equipped to respond thus far. In this context, the proposed activity will meet the client demand externally and have full support of the GPURL Global Director and Global Unit Practice Manager internally (endorsement email attached). GPURL Global Director emphasizes that we develop, through cross-GP efforts, a methodology and tool to help replicate and scale up GSCP services to WBG teams and clients. To this end, GSCP just started a process of developing a smart city readiness assessment tool (Digital Ecosystem Assessment Tool for Smart Cities) again in collaboration with DD GP (with a grant support from the Korea Green Growth Trust Fund). The proposed activity, SCMM and Cybersecurity Risk Framework for Smart Cities will be part of the overall effort to standardize and scale up GSCP support and closely interlinked with the overall smart city readiness assessment tool. Finally, GSCP has an established and well-known mechanism of providing smart city TA to WBG teams and clients, which will help achieve the grant objective of developing and piloting the cybersecurity assessment tools for smart cities. Recently, one of the GSCP beneficiary projects selected under the Round 8 call for proposal (in November 2023) has requested for examining cybersecurity risks and opportunities in Lima Traffic Management System. This already offers an immediate opportunity for the grant-funded activities.

[1] Please avoid using constraints on budget as a sole rationale. Rather, it should focus on the added value of the grant to the operation.

C.3 Explain major anticipated risk(s) to Grant implementation and explain risk management strategies that will be utilized.

Potential Risks - Please use the dropdown list and explain [Word limit – 50]	**Risk Level**	**Mitigation Measures** - Please use bullet points [Word limit – 100]
Sector Strategies and Policies Smart city development or urban development in general involves multiple sectors and strategies which can complicate cybersecurity assessment	Substantial	As proposed, the team will start with a concrete entry point, urban transport, to better understand cybersecurity issues in urban areas and identify ways to expand the assessment to others sectors within a city. GSCP portfolio includes a few other key sectoral digital systems that can benefit from cybersecurity assessment (e.g. housing, land, urban planning) which provides an opportunity for testing and expansion of the assessment. The team will also ensure to engage various stakeholders within a city across sectors in developing the assessment tool.
Institutional Capacity for Implementation and Sustainability Cybersecurity assessment requires specialized skills and experience and finding adequate experts (either firm or individual) with a developing country experience can be a challenge	Moderate	The Cybersecurity team in DD GP has a roaster of individual consultants who have worked on developing SCMM for different sectors and more broadly in various contexts (region/country). The DD team also has experiences in working with academic institutions and consulting firms which can help refine the scope of work and procure adequate expert services (particularly for Activity 1).

C.4 Team members

Name	**Role**	**Field of expertise**
Jessica Grisanti	TTL	Urban Specialist-Smart Cities
Sung Up Yoon	Core team member	Urban Specialist-Smart Cities
Oleg Petrov	Core team member	Senior Digital Development Specialist – cybersecurity
Oscar Avila Molina	Consultant	Cybersecurity expert
Francisco Galera	Consultant	Smart Mobility expert

SECTION D: DETAILED COST TABLE, BY ACTIVITY (QII Contribution only)

Add additional activities as necessary.

ITEM	Activity 1:	Activity 2:	Activity 3:	Activity 4:	Funding Request by Item
Contractual Services (firm consultancy services, training, workshops)	$150,000	Click here to enter amount	Click here to enter amount	Click here to enter amount	**$150,000**
ETC & ETT Contracts	Click here to enter amount	Click here to enter amount	Click here to enter amount	Click here to enter amount	**Click here to enter amount**
Media, Works, Conf (press conference, printing, publishing, VC, translation	Click here to enter amount	Click here to enter amount	$10,000	Click here to enter amount	**$10,000**
Staff Costs* (in TRS)	$25,000	$10,000	$5,000	Click here to enter amount	**$40,000**
STC & STT Appointments	Click here to enter amount	$30,000	$10,000	Click here to enter amount	**$40,000**
Travel Expenses* (staff)	Click here to enter amount	$5,000	Click here to enter amount	Click here to enter amount	**$5,000**
Travel Expenses (consultants)	Click here to enter amount	$5,000	Click here to enter amount	Click here to enter amount	**$5,000**
Total Cost by Activity**	**$175,000**	**$50,000**	**$25,000**	**Click here to enter amount**	**$250,000**

* *Note that Task Team Supervision costs (staff time costs plus travel) should **not** exceed 20% of the total grant funding request*

** *The total cost by activity should correspond with the estimated costs by activity in Section B–Q2*