INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2025-2028

SG20-TD1347-R1

STUDY GROUP 20

Original: English

Question(s): 6/20 Geneva, 12-21 May 2026

TD

Source: Co-Rapporteurs Q6/20

Title: A.1 justification for proposed draft new Recommendation ITU-T Y.sf-dpi-ssc "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities", Q6/20 meeting (Geneva, 12-21 May 2026)

Contact: Jie CHENG
China Mobile Communications Co. Ltd.
China
Tel: +86 13811723151
E-mail: chengjiewl@chinamobile.com

Contact: Xiongwei Jia
China Unicom
China
Tel: +86 156 1109 2296
E-mail: jiaxw9@chinaunicom.cn

Abstract: This TD contains A.1 justification for proposed draft new Recommendation ITU-T T Y.sf-dpi-ssc "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities", based on contribution SG20-C411R1 (Geneva, 12-21 May 2026).

A.1 justification for proposed draft new ITU-T Y.sf-dpi-ssc

Question:	Q6/20	**Proposed new ITU-T Recommendation**	Geneva, 12-21 May 2026	
Reference and title:	ITU-T Y.sf-dpi-ssc "Security Framework of Digital Public Infrastructure for Smart Sustainable Cities"			
Base text:	SG20-TD1348		**Timing:**	2028-Q4
Editor(s):	Ramy Ahmed Fathy, NTRA Egypt Ali Abbassene, Ministère de la Poste et des Télécommunications,Algeria Nura Falalu Nigerian Communications Commission (NCC), Nigeria (Federal Republic of)		**Approval process:**	TAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This draft Recommendation provides a security framework and a technical guidance to secure Digital Public Infrastructure (DPI) deployed in smart sustainable cities (SSC).

The scope of this draft Recommendation includes:

- Security threat and risk analysis relevant to DPI in SSC environments;
- Security framework applicable to DPI for SSC;
- Technical security guidelines for protecting DPI systems.

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

Digital Public Infrastructure (DPI) has emerged as a foundational digital layer for smart sustainable cities (SSCs), enabling essential functions such as digital identity, secure payments, data exchange, and public service delivery. These city-scale systems form the backbone of urban digital transformation, supporting millions of citizens in their daily interactions with public services, financial systems, and government institutions.

While DPI has traditionally been conceptualized and implemented at the national level, its deployment in SSC introduces distinct characteristics that fundamentally alter its technical architecture, operational requirements, and risk profile. The unique features of DPI for SSC include: Urban Density and Edge Distribution, Real-Time Operational Dependencies, Deep Physical-Digital Convergence, Multi-Stakeholder Complexity, Sustainability-Driven Data Intensity, Rapid Innovation and Pilot-to-Scale Dynamics.

The characteristics of DPI for SSC generate security challenges that exceed the boundaries of conventional cybersecurity frameworks developed for national-scale DPI or enterprise IT systems. The unique convergence of scale, speed, physicality, multiplicity, and innovation demands a framework that is simultaneously comprehensive and specific, providing actionable guidance for securing DPI in SSC.

This document establishes a Security Framework of Digital Public Infrastructure for Smart Sustainable Cities. The framework integrates threat and risk analysis, lifecycle-embedded security architecture, and actionable technical guidelines tailored to the SSC context. It provides city leaders, DPI architects, security practitioners, and technology vendors with a common reference for building and operating DPI that maintains confidentiality, integrity, and availability while sustaining the public trust essential for digital transformation.

Relations to ITU-T Recommendations or to other standards (approved or under development)**:**

ITU-T YSTR.DPI-BP, X.arch-design

Liaisons with other study groups or with other standards bodies:

IEC SyC Smart Cities, ISO TC 268, ITU-T SG17, ISO/IEC JTC 1/SC 27, GSMA, 3GPP, ETSI TC CYBER

Supporting members that are committing to contributing actively to the work item:

National Telecommunication Regulatory Authority (NTRA) (Egypt), Autorité de Régulation des Communications électroniques et des Postes (ARCEP) (Gabonese Republic), Autorité de Régulation des Technologies de Communication (ARTEC) (Madagascar (Republic of)), Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) (Côte d'Ivoire (Republic of)), Autorité de Régulation des Télécommunications et des Postes (ARTP) (Senegal (Republic of)), Conseil National des Télécommunications (CONATEL) (Haiti (Republic of)), General Authority of Communication and Informatics (Libya (State of)), Ministère de la Poste et des Télécommunications (Algeria (People's Democratic Republic of)), Ministère des Postes et Télécommunications (Cameroon (Republic of)), Ministère des Postes, Télécommunications et Nouvelles Technologies de l'Information et de la Communication (Democratic Republic of the Congo), National Communications Authority (NCA) (Ghana), Nigerian Communications Commission (NCC) (Nigeria (Federal Republic of)), Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) (Zimbabwe (Republic of)), Rwanda Utilities Regulatory Authority (RURA) (Rwanda (Republic of)), Tanzania Communications Regulatory Authority (TCRA) (Tanzania (United Republic of)), Ministère des Technologies de la Communication (Tunisia), Zambia Information and Communications Authority (Zambia)

Communication and Information Technology Regulatory Authority (CITRA) (Kuwait) , Telecommunications Regulatory Authority (Bahrain) , University of Dubai (United Arab Emirates)

Gap Analysis

1 Background

As cities increasingly rely on Digital Public Infrastructure (DPI) to deliver essential public services – including digital identity systems, electronic payment platforms, and cross-agency data exchanges – the security of these interconnected systems has become a critical concern. Urban DPI integrates heterogeneous digital assets spanning municipal sensor networks, utility providers, transport operators, emergency services, and citizen-facing platforms, creating an expansive attack surface that requires comprehensive protection.

Several ITU-T Recommendations address aspects of IoT and smart city security. ITU-T Y.4806 specifies security capabilities supporting safety of the Internet of things. ITU-T X.1205 provides an overview of cybersecurity, while ITU-T X.1361 defines a security framework for the Internet of things. ITU-T Y.4807 addresses the security requirements of IoT devices and gateways. ISO/IEC 27001 provides requirements for information security management systems, and the NIST Cybersecurity Framework offers a structured approach to managing cybersecurity risk.

However, none of these existing standards comprehensively addresses the security and risk management requirements specific to city-level DPI. Urban DPI operates across institutional boundaries, under multiple governance regimes, and at metropolitan scale, presenting unique challenges. While DPI has traditionally been conceptualized and implemented at the national level, its deployment in SSC introduces distinct characteristics that fundamentally alter its technical architecture, operational requirements, and risk profile. The unique features of DPI for SSC include: Urban Density and Edge Distribution, Real-Time Operational Dependencies, Deep Physical-Digital Convergence, Multi-Stakeholder Complexity, Sustainability-Driven Data Intensity, Rapid Innovation and Pilot-to-Scale Dynamics.

2 Discussion

Security is the foundational property that determines whether urban DPI can fulfil its potential as trusted public infrastructure. Without comprehensive, architecturally embedded security, digital investments in urban systems are exposed to cyber threats, privacy violations, and systemic failures that undermine public trust and service continuity.

Existing standardization efforts typically address individual aspects of IoT or security. IoT security standards (such as Y.4806 and Y.4807) focus on device-level and gateway-level security capabilities but do not define comprehensive defence-in-depth architectures for city-level DPI. General cybersecurity frameworks (such as X.1205 and ISO/IEC 27001) provide broad risk management guidance but do not address the specific requirements of urban public infrastructure, including federated governance, algorithmic fairness, and the structural avoidance of SPOFs. Smart city platform standards (such as Y.4200) address interoperability but do not specify security architectures, zero-trust models, or incident response requirements for municipal digital ecosystems.

The proposed Recommendation addresses this gap by defining a Security Framework of Digital Public Infrastructure for Smart Sustainable Cities. The framework integrates threat and risk analysis, lifecycle-embedded security architecture, and actionable technical guidelines tailored to the SSC context. It provides city leaders, DPI architects, security practitioners, and technology

vendors with a common reference for building and operating DPI that maintains confidentiality, integrity, and availability while sustaining the public trust essential for digital transformation.

This work was discussed and agreed at the ITU-T SG20RG-AFR meeting (Virtual, 30–31 March 2026) based on SG20RG-AFR-C9.

3 Proposal

This contains the gap analysis for a proposed new work item on " Security Framework of Digital Public Infrastructure for Smart Sustainable Cities". Attachment 1 provides a gap analysis comparing existing standards and activities of ITU-T and other standardization bodies related to ongoing works.

The scope of this draft Recommendation includes:

- Security threat and risk analysis relevant to DPI in SSC environments;
- Security framework applicable to DPI for SSC;
- Technical security guidelines for protecting DPI systems

This draft Recommendation applies to city-level digital ecosystems, focusing on protecting urban public services, municipal data exchanges, and citizen digital identities from cyber threats and systemic vulnerabilities.

Attachment 1 – Gap analysis

Table 1 provides gap analysis compared with other Standardization activities.

Table 1 – Gap analysis compared with other Standardization activities.

SDOs	**Number**	**Title**	**Summary**	**Gap analysis**
ITU-T SG20	**Published:** ITU-T Y.4200	*Requirements for the interoperability of smart city platforms*	This Recommendation defines the requirements for the interoperability of a smart city platform (SCP) and its reference points in order to ensure the correct functioning of city services.	Y.4200 addresses platform-level interoperability requirements between SCPs but does not define multi-layered security architectures, zero-trust access control models, incident response requirements, or structural resilience mechanisms for city-level DPI.

SDOs	Number	Title	Summary	Gap analysis
	Published: ITU-T Y.4201	*High-level requirements and reference framework of smart city platforms*	This Recommendation defines the reference framework and high-level requirements of smart city platforms (SCP). It is being revised to incorporate AI-related functionalities.	Y.4201 provides a general reference framework for SCP functionalities and interfaces but does not specify defence-in-depth security requirements, SPOF elimination strategies, or privacy-by-design safeguards, nor does it address zero-trust architectures, algorithmic fairness requirements, or supply chain security for urban DPI.
	Published: ITU-T Y.4459	*Digital entity architecture for IoT interoperability*	This Recommendation specifies a digital entity architecture addressing interoperability and security among IoT applications, including identity management and secure data exchange.	Y.4459 addresses IoT interoperability and security at the application level but does not define comprehensive city-level DPI security frameworks, including defence-in-depth architectures, zero-trust municipal access control, consent management, algorithmic fairness, or SPOF elimination strategies for urban digital ecosystems.
	Published: ITU-T Y.4806	*Security capabilities supporting safety of the Internet of things*	This Recommendation specifies security capabilities to support the safety of IoT systems, including threat analysis, security measures, and best practices for IoT deployment.	Y.4806 addresses IoT device and system safety but does not cover city-level DPI security architectures, zero-trust municipal access control, federated security governance, algorithmic bias mitigation, or the structural elimination of

SDOs	Number	Title	Summary	Gap analysis
				SPOFs in urban digital ecosystems.
	Published: ITU-T Y.4807	*Security of the Internet of things devices and gateways*	This Recommendation specifies security requirements for IoT devices and gateways, covering device authentication, secure boot, firmware integrity, and communication security.	Y.4807 focuses on device-level and gateway-level security but does not address city-wide DPI security architectures, multi-layered defence strategies for municipal platforms, privacy-by-design for citizen data, incident response coordination across agencies, or supply chain security for urban DPI ecosystems.
	Published: ITU-T X.1205	*Overview of cybersecurity*	This Recommendation provides an overview of cybersecurity, including definitions, taxonomies of security threats and vulnerabilities, and high-level guidance on network protection.	X.1205 provides a broad overview of cybersecurity concepts but does not define city-specific DPI security architectures, zero-trust requirements for multi-agency municipal environments, algorithmic fairness mandates, SPOF elimination strategies, or supply chain security requirements for urban digital ecosystems.
	Published: ITU-T X.1361	*Security framework for the Internet of things*	This Recommendation specifies a security framework for IoT, including security threats, security requirements, and security measures for IoT systems and services.	X.1361 provides an IoT security framework but does not address city-level DPI-specific concerns such as federated security governance, citizen identity protection, privacy-by-design for municipal services,

SDOs	Number	Title	Summary	Gap analysis
				consent management, or defence-in-depth architectures spanning multiple urban agencies.
	Published: ITU-T X.1362	*Simple encryption procedure for Internet of things environments*	This Recommendation specifies a simple encryption procedure for IoT environments, addressing lightweight cryptographic mechanisms suitable for resource-constrained devices.	X.1362 addresses encryption for constrained IoT devices but does not cover comprehensive city-level DPI security architectures, zero-trust models for municipal systems, algorithmic bias mitigation, SPOF elimination, or incident response coordination for urban digital ecosystems.
ISO/IEC	**Published:** ISO/IEC 27001	*Information security management systems — Requirements*	This document specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organisation.	ISO/IEC 27001 provides a general-purpose information security management framework but does not address city-specific DPI security requirements such as defence-in-depth for municipal platforms, federated security governance across urban agencies, algorithmic fairness, SPOF avoidance, or citizen identity protection in smart city environments.
	Published: ISO/IEC 27005	*Information security risk management*	This document provides guidelines for information security risk management, including risk assessment and treatment processes	ISO/IEC 27005 provides general risk management guidance but does not address city-level DPI-specific threats, zero-trust architectures for multi-agency municipal

SDOs	Number	Title	Summary	Gap analysis
			applicable to organisations of all types.	environments, privacy-by-design for citizen services, algorithmic fairness requirements, or structural resilience mechanisms for urban digital ecosystems.
NIST	**Published:** NIST CSF	*Cybersecurity Framework*	The NIST Cybersecurity Framework provides a structured approach to managing cybersecurity risk through five core functions: Identify, Protect, Detect, Respond, and Recover.	The NIST CSF provides a general-purpose risk management structure but does not address city-specific DPI security architectures, federated governance for municipal systems, algorithmic fairness, privacy-by-design for urban services, or structural SPOF elimination for smart city digital ecosystems.

___