Smart City

Government of India
Ministry of Housing and Urban Affairs
Smart Cities Mission

Advisory No. 22 **Date: 22nd November, 2022**

Standard Operating procedure for cyber security of Smart City Infrastructure.

1. Background

The Projects being implemented by cities under Smart Cities Mission include ICT interventions that aim to leverage digital infrastructure for urban governance. One such initiative is Integrated Command and Control Centre (ICCC), which is envisioned to help address the needs of citizens in a holistic manner, by acting as a decision support system for city administration, thus channelizing citizen-centric governance.

It important that ICCCs adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. As use of advanced and integrated technology to deliver services to the citizens may expand cyber threat landscape of the city, therefore, city authorities must consider cyber security in a comprehensive manner, including that of field equipment and software systems.

To address the above concerns, the Ministry had released a model framework in 2016 for cyber security vide OM no. K- 15016/61/2016-SC-1 dated 20th May 2016, to be followed by the smart cities. Subsequently, based on experiences of the cities in working with various stakeholders viz., system integrators and technology providers, the Ministry released a Model RFP 2.0 in 2021 to guide cities on specific features, clauses, works, services, and infrastructure to be included in tenders, including cyber security provisions.

2. Pilot Assessment in Cities

Recently, a Pilot security assessment was conducted in 5 Smart cities by STQC (Standard Testing and Quality Control) directorate, Ministry of Electronics & Information Technology (MeitY) at the directions of Committees of Secretaries (CoS) *vide* MoM No. 082/2/4/2016-CA.IV/CA.V (Vol-III) dated 5.7.2022, for undertaking a security audit, in coordination with MHA and MeitY and to explore the possibility of using critical IT & Telecom products in strategic installations only from trusted sources in coordination with DoT and MeitY.

Based on the findings of Pilot security assessment conducted in 5 Smart cities, a Standard Operating Procedure (SoP) has been released by STQC directorate. The same is placed at Annexure – 1.

Smart Cities are therefore advised to take immediate steps to get the assessment of their ICCC infrastructure done in line with above mentioned SoP document, with a view of making the digital infrastructure of the city highly secure, as it is intended to handle sensitive data relating to the city and its citizens. The cities are advised to take this exercise on priority basis.

Annexure-I

Base line Security Measures ('must do' type)

A. At Sensor Layer:

1. All edge devices, including IoT and environmental sensors, shall be authenticated during installation using the network based on physical characteristics such as device ID and MAC ID.
2. Physical interface in edge devices shall be disabled to prevent software modifications.
3. Remote access to all edge devices shall be enforced with strong authentication mechanism.
4. Encryption shall be enforced for all communications to and from edge devices.

5. Edge devices shall be configured to connect to the authorized wireless network only.
6. The firmware of the edge device shall be updated, as and when necessary, however in a controlled manner following the principles of 'Trusted Electronic Value Chain.'
7. The default configuration of all end point devices/edge devices, including default passwords, should be changed to enhance security; the devices shall be hardened in line with the recommendations of OEM.
8. Under no circumstances the sensors or edge devices shall be accessible from public domain, ICCC shall mediate all citizen centric services.
9. The smart city service shall allow authenticated sensors only to operate in their systems.

B. At Communication Layer:

1. All the smart city services must run in isolated private networks. Data communication from these private networks shall only be through authorized gateway to ICCC

2. Segmentation shall be enforced in data center network.

3. All edge devices, including Wi-Fi, sensors and IoT devices, shall e placed on a separate firewall-monitored network.

4. Data Center network shall be secured through external firewall, web application firewall, and intrusion prevention and detection system.

5. Wireless network shall be securely configured.

6. All the devices (servers and network devices) on the network shall be hardened.

7. All the devices (servers and network devices) on the network shall be authenticated.

8. All data communication shall be encrypted. Encrypt inter-component communication with secure protocols such as HTTPS over TLS 1.2, SSH, SFTP, etc.

9. The remote connection to data center network shall always use encrypted channels (VPNs).

10. All unused network or telecommunication access points shall be disabled to prevent unauthorized access.

C. At Data Layer:

1. All servers and network devices used for data storage shall be hardened and regularly patched.

2. User authentication, followed by log generation shall be implemented on all databases.

3. The database access shall be restricted to the authorized users only.

4. The database server shall be deployed into a network segment which is separated from the Application server network and web server network.

5. Perform channel encryption to ensure security of data in transit.

6. The classified sensitive data shall be stored in encrypted form.

7. Regular backups of database and encrypt backup media shall be conducted as per formal policy as defined in Information Security Management System.

D. At Application Layer:

1. All Web-based applications shall be tested and hardened as per the requirements of OWASP ASVS (input validation at server side, authentication, session management, access control, error handling, logging, secure file upload, SSRF protection, web service security etc.)

2. All mobile apps shall be tested and hardened as per the requirements of OWASP MASVS.

3. Disable access to default web server pages.

4. Build authentication mechanisms for all applications and API.
