K-15016/61/2016-SC-I
Government of India
Ministry of Urban Development

Nirman Bhawan, New Delhi
Dated: 19th May 2016
20

OFFICE MEMORANDUM

Subject: Cyber Security Model Framework for Smart Cities.

The undersigned is directed to convey that the National Security Council Secretariat, Government of India in consultation with the Industry (NASSCOM, DSCI) has prepared a Cyber Security Model framework which consists cyber security requirements which may be necessary to be incorporated while inviting proposals/offers from the companies implementing Information Technology and applications as part of project on Smart Cities. A copy of the Cyber Security requirements is enclosed.

2. It is requested that this Model framework may be considered while implementing solutions for setting up Smart Cities.

Encl.: As above.

(Sanjay Sharma)
Under Secretary to the Government of India
Tel. No. 23062908

The Principal Secretaries (UD)/
State Mission Directors/Municipal Commissioners
in respect of 98 Cities

Copy to:

1. PPS to AS (SC)
2. PS to JS (AMRUT)/JS (W&H)/JS (SBM)
3. PS to Director (SC-I)/Deputy Secretary (SC-III)

NATIONAL SECURITY COUNCIL SECRETARIAT
NEW DELHI

Cyber Security Requirement for Smart City – Model Framework

1. The Generic architecture of smart city generally consists of four layers – a sensing layer, a communication layer, a data layer and an application layer, and these four layers are overseen by the smart city security system. Architecture of Information Technology systems deployed in Smart city need to be open, interoperable and scalable.

The reference architecture of Information Technology (IT) infrastructure in Smart city suggested by National Institute of Standards and Technology (NIST) serves as a common starting point for system planning while promoting interoperable functional building blocks, which are required in a smart city.

2. The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Centre (DC) should talk to the applications hosted in the datacenter through only predefined APIs.

3. While it is necessary to converge multiple infrastructures into one Central platform for ease of management, it is mandatory that such applications hosted in the central data center support multi-tenancy with adequate authentication and Role based access control mechanism for each tenant pertaining to their respective infrastructure.

4. In multi-tenant architecture, there should be provisions for flow of normalized data only to respective tenant partition(s) in a predefined manner with adequate authentication and encryption mechanism.

5. The smart city architecture should be capable of managing heterogeneous data, which would be continuously communicated through numerous devices following different protocols. In order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow:

Between applications and back end systems: HTTP, SQL, FTP, SNMP, SOAP, XML, SSH, SMTP

Between back end systems and field devices: Message Queue Telemetry Transport (MQTT), XMPP, RESTful HTTP, Constrained Application Protocol (CoAP), SNMP, IPv4/6, BACnet, LONworks, Low Power Wide Area Network (LoRa), Fixed, 4G/5G, Wi-Fi, WiMax, 2G/3G From field devices: ZigBee oIP, ETSI LTN, IPv4/6, 6LowPAN, ModBus, Wi-Fi, 802.15.4, enOcean, LoRA, RFID, NFC, Bluetooth, Dash7, Fixed, ISM & short-range bands.

6. Data Layer (termed as City Digital platform/ fabric) should be capable of communicating with various types of sensors/ devices and their management platforms/applications for single/multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer, thus making it one true source of data abstraction, normalization, correlation and enable further analysis on the same. Adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality breach and unauthorized access.

7. The entire Information Technology (IT) infrastructure deployed as part of Smart city should follow standards like – ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180,BSI PAS 181, BSI PAS 182, for Wi-Fi access – PEAP (Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GPP), etc. as appropriate.

8. Application Program Interfaces (APIs) should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.

9. From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.

10. Wireless broadband plan and architecture for the specific City may be prepared detailing the existing Fiber System and other supporting infrastructure so as appropriately interfacing another or citywide wireless network.

11. All sensors deployed as part of IT and IT based systems in the Smart cities should talk only to the authorized wireless network, and do not hook on to the rogue networks. The guidelines to secure wi-fi networks as published by Department of Telecom must be followed.

12. Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPNs) or separate networks in the wired core, so that any traffic from the Internet users is not routed into the sensor networks and vice-versa.

13. All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted.

14. Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC ID, Device ID etc.

15. Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.

16. As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary

authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.

17. The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.

18. The sensors deployed in Smart city should be of low power consumption and should work on self-sufficient power sources.

19. All devices and systems deployed in Smart city should be hardened and have the ability to be upgraded remotely for firmware through encrypted image files with authentication mechanism to complete the operation.

20. All the sensors in the Smart city should connect to a completely separate network.

21. The data center should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data center in one zone, and the Internet facing side of the data center should be in another zone.

22. The Internet facing part of the data center should have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports.

23. The customer application servers should be accessed only by the web server that is hosted in a different zone of the data center.

24. The following should be implemented in the data centre - firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated Identity and access management system, etc.

25. Security Information and Event Management (SIEM) monitoring on all Smart City networks, devices and sensors to identify malicious traffic.

26. All "applications" and "apps" will undergo static and dynamic security testing before deployment and be tested with respect to security on regular basis at least once in a year.

27. All applications and "Apps" deployed as part of Smart city be hosted in India.

28. The said architecture provide:

(a) Automatic and secure updates of software and firmware etc.

(b) All systems and devices should provide auditing and logging capabilities.

(c) Ensure vendor compliance to remove any backdoors, undocumented and hard cored accounts.

(d) End-to End solution should be provided with annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of five years form the date of operations of the systems.

29. Appropriate teams may be set up to monitor cyber incidents and mitigation of same.

30. All the information on incidents be shared regularly with Indian Computer Emergency Response Team (CERT-In) and NCIIPC (National Critical Information Infrastructure Protection Centre) and take help to mitigate and recover from the incidents.