**The City of New York**

**Cyber Command**

Connected Devices Cyber Security Network Assessment

# Introduction

The purpose of this document is to capture detailed level information about the connected devices of the solution being procured by the City of New York’s Agency to determine the cyber security posture of the platform.

Please familiarize yourself with the City’s Application Security Policies, Standards, and Process, so that the prerequisites are ready and available to expedite the Cybersecurity’s team review. Please address comments and/or questions to [IoT@cyber.nyc.gov.](mailto:NYC3UTIoT@cyber.nyc.gov.)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Project Contact Information | | | |
| **City Agency Name/Business Owner (the IoT owner):** | Enter Agency Name | **Date Submitted Cyber Command:** | Select Date |
| **City Agency Representative Name:** | Enter Agency Representative Name | | |
| **Vendor Company Name:**  **Application Name:**  **Main Contact Name:  Technical Contact Name:**  **Email: Phone(s)** | Enter Company Name  Enter Application Name  Enter Contact Name  Enter Technical Contact Name  Enter Email  Enter Phone | **City Agency Representative Contact:**  **Email: Phone(s)** | Enter Email  Enter Phone |
| 1. **Describe the IoT Solution and the Business Case** | | | |
| Describe the Solution | | | |

|  |  |
| --- | --- |
| **Application Criticality Questionnaire (To be filled out by City Agency)** | |
| This section of the questionnaire is to be completed by the City Agency Application’s Technical Team. All information must be truthful and will be used to determine the Application’s Overall Cyber Security posture. | |
| **Information Classification:** | **please click and select** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Operational Impact Analysis[[1]](#footnote-1)** | | | |
| **Security Objective** | **LOW** | **MODERATE** | **HIGH** |
| **Confidentiality**  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy & proprietary information. | The unauthorized  disclosure of information  should be expected to have a **limited adverse effect** on organizational operations, assets, or individuals. | The unauthorized disclosure of information should be expected to have a **serious adverse effect** on organizational operations, assets, or individuals. | The unauthorized  disclosure of information  should be expected to have a **severe or catastrophic adverse effect** on organizational operations, assets, or individuals. |
| **please click and select** | | | |
| **Integrity**  Guarding against improper  information modification  or destruction,  including ensuring  information non-repudiation  and authenticity. | The unauthorized  modification or destruction of information should be expected to have a **limited adverse effect** on organizational operations, assets, or individuals. | The unauthorized modification or destruction of information should be expected to have a **serious adverse effect** on organizational operations, assets, or individuals. | The unauthorized  modification or  destruction of information  should be expected to have  a **severe or catastrophic adverse effect** on organizational operations, assets, or individuals. |
| **please click and select** | | | |
| **Availability**  Ensuring timely and reliable access to and use of information. | The disruption of access to  or use of information or an  information system should  be expected to have a  **limited adverse effect** on  organizational operations,  assets, or individuals. | The disruption of access to  or use of information or an  information system should  be expected to have a  **serious adverse effect** on  organizational operations, assets, or individuals. | The disruption of access to  or use of information or an  information system should  be expected to have a  **severe or catastrophic**  **adverse effect** on  organizational operations, assets, or individuals. |
| **please click and select** | | | |

**Connected Device Security Questions:**Please answer all questions. If a question is not applicable, please note it as such in as your response “Not Applicable”.

|  |  |
| --- | --- |
| 1. Device Connectivity | |
| **CONNECTIVITY:** | |
| **How is the device connected to the backend data center?**  **Note: Please provide connectivity details (encryption key sizes, protocols & their version numbers used, tunnels, etc.) in the network architecture diagram.** | Describe |
| **LAYER 1:** | |
| **Is the device connected locally to other devices (e.g. via gateway or local/mesh network)?**  **Does the device communicate locally with other endpoints?**  **Can the device be managed locally?** | Describe |
| **LAYER 2:** | |
| **What Layer 2 connectivity is used on the device (LTE, Bluetooth, Wi-Fi, wired etc.) to connect to Internet?**  **If wired connectivity is used, are there redundant paths to the Internet?** | Describe |
| **How is Layer 2 secured (for example WPA2 or WPA3 for Wi-Fi)?** | Describe |
| **If LTE connectivity is used, are there dual SIM cards in the device?**  **What carriers do the SIM cards belong to?**  **Are the SIM cards generic or have private APN’s?**  **If the SIM card has a private APN then what kind of connectivity exists between the carrier’s data center, and backend data center?**  **Can the 4G/LTE device be downgraded to connect to 2G or 3G?**  **5G Capability?** | Describe |
| **Is the device protected from LTE level attacks (e.g. connecting to rogue eNodeB, and disclosing ESN, IMSI, IP address etc.)?**  **Does the device have an intrusion detection/prevention system to detect and prevent LTE level attacks?** | Describe |
| **Describe the device behavior after losing wireless connectivity or rebooting after power loss?** | Describe |
| **LAYER 3:** | |
| **List the endpoint security controls on the device: (e.g. malware detection, HIDS, WIPS, IDS, etc.).**  **Is there a security control that will prevent the device from breaking out on to the Internet?** | Describe |
| **How is the device protected from DDoS?** | Descirbe |
| **Is secure boot implemented in the device?** | Descirbe |
| **Is there HSM to store security credentials in the device?**  **What credentials are stored on the device?**  **How are the credentials loaded and or renewed?**  **Are credentials unique per device?** | Describe |
| **Is the interface between the device and backend network using any proprietary protocols and security algorithms?** | Describe |
| **If there are only outbound connections (no inbound connections), how does the device reconfigure, troubleshoot, and upgrade?**   1. **Can these actions be done remotely? If not, please elaborate:**   **List all inbound and outbound connections that originate from and terminate into the device.**  **What protocols and version numbers (e.g. TLS 1.2) are used?**  **Where are the servers connected to and what data is exchanged?** | Describe |
| **Are there any connections that are always-on or established on-demand?**  **If on-demand, what are the triggers that establish and tear down the connection(s)?** | Describe |
| **Please identify the key lengths and security algorithms (hash, encryption, public key) on each connection between the device and the network.**  **How often are the keys refreshed?**  **Who owns and manages the keys?** | Describe |
| **Is there a mutual authentication between the device and backend server for each connection?**  **Please identify the authentication credentials used for each connection.**  **If authentication is done via certificates, then what checks are done in the device on the server certificate fields?**   1. **How many certificates are stored in the device?** 2. **What are the lifetimes of these certificates?** | Describe |
| **Explain the liveness check function between the device and backend server?**  **What is the highest liveness check message frequency?**  **What will happen if there is no liveness check from the device?**  **Are the liveness check messages bidirectional?** | Describe |

|  |  |
| --- | --- |
| 1. Device Security Questions | |
| **Are any physical ports exposed externally on the device?**   1. **If yes, please enumerate them.** | Describe |
| **Does the device have a keyboard, touch screen, screen for display, LEDs, etc., for input and/or output?**  **What information can be inputted into the device?**  **Is the data input by a customer/user validated locally in the device against errors?**  **Is** | Describe |
| **tIs IIs there a touch screen associated with this product.**   1. **Does any PII appear on the display and is it protected against shoulder surfing?** 2. **Can you access multiple applications from the screen or does a single application control the entire screen?** 3. **Is the interface a touch screen?** 4. **Are hand gestures enabled on thee touch screen?** 5. **Is there a keyboard associated with the screen?** | Describe |
| **Does the device need physical keys and/or screws to open the device?**  **What would be the reason to open the device?**   1. **What are the openings, if any, into the device?** | Describe |
| **What is the NEMA rating of the device?**  **Does the device utilize security screws and/or tamper-evident measures to assure the device has not been altered?**  **Please enumerate physical protections. (e.g. NEMA Classification, construction ruggedization, protection from environment like temperature, humidity, dust etc.)** | Describe |
| **Is the device accessible to the public?**  **If yes, how is the device protected from misuse or misconfiguration?** | Describe |
| **Is the device powered by battery or electrical outlet or solar etc.?**  **If powered by electrical outlet, is it power outlet surge protected?**  **If not, what is the source of power?**  **How long will the batteries last on a single charge?**  **Are there backup batteries in the device?**  **Is the health of the battery information relayed to the backend?**  **What is the life of the battery?** | Describe |
| **Is the device portable or secured to a location?**  **Please identify the location of the device. Is the device accessible physically?**  **Is the device mounted and its wiring secured to the location using tamper-resistant methods?** | Describe |
| **Agency to Respond: Is the device under asset management, configuration management and change management processes?**  **Do you have processes and polices in place to ensure that the latest patches & software upgrades are implemented, ensure end of life software is removed, ensure software upgrades do not lead to incompatible software versions (and hence security holes), comply with password management, comply with best practices like default passwords changed, unused ports disabled, remove unused accounts etc.?** | Describe |
| **Is there a single point of failure in the device and its connectivity path to backend data center?** | Describe |

|  |  |
| --- | --- |
| 1. Device Monitoring Troubleshooting Questions | |
| **Is the device troubleshooted remotely and/or locally? Are the activities logged and events generated?**  **Is there a separate account to track per technician’s activity?**  **What is the technician able to do on the device?**  **Is the technician authenticated via MFA?**  **Does the device support MFA/SSO?** | Describe |
| **Agency to Respond: If the device can be troubleshooted locally, is there a scanning station (e.g. USB ) used to scan systems and peripherals that will be connected to the device?** | Describe |
| **Are logs generated? List all common fields.**  **What events are generated by the device? How often are they sent out?** | Describe |
| **Is there a single point of failure in the device and its connectivity path to backend data center?** | Describe |

|  |  |
| --- | --- |
| 1. Remote Device Management Questions | |
| **How do you detect/prevent device spoofing?**  **What is the process to onboard a new device?**  **What is the process to detect a stolen device?**  **What is the process of activating a device on the network?**  **When a new device is added to the network, does it automatically register itself with device management service?** | Describe |
| **Does the device have detection/prevention against device spoofing?** | Describe |
| **Is the device under MDM?**  **If yes, who is the vendor for MDM?** | Describe |
| **How do firmware upgrades happen?**  **Are upgrades automatic or manual?**   1. **Are the updates done in person or remotely?** 2. **Please describe the upgrade process**   **Please describe the upgrade process.** | Describe |
| **Is the device accessible for forensics collection remotely and/or locally?**  **What can be collected?** | Describe |
| 1. **Data Security Questions** | |
| **Is all data leaving the device encrypted?**  **Is any data transmitted to or from the connected device contain any sensitive/regulated information/PII?**  **Please identify all information leaving or entering the device.** | Describe |
| **If the device is misconfigured, what damage can it cause and what sensitive data will it reveal?** | Describe |
| **What data is stored on the device, even temporarily? If yes, for how long?**  **Is it encrypted? Please provide details of the data fields.**  **Can data be extracted from the device when it is deployed in service and once it is removed from service?** | Describe |
| **What card reader security controls, if any, are in place? [e.g. to protect against counterfeit cards, expired or stolen cards, cards with malicious code on their chips, protection from skimmers etc.]** | Describe |
| 1. **Generic Connected Device Questions** | |
| **How many devices does the agency plan to procure? Please list model number and quantity for each.** | Describe |
| **How many customers are using this service and where?**  **Is the City Agency using this service currently and for how long?** | Describe |
| **What is the OS running on the device and what is its version number?** | Describe |
| **Describe how the devices are managed?**  **Who are the users accessing thee device(s) [general public, City. Agency Employees]?**  **Will the Agency be using a mobile application too access the service?**  **Will the mobile application be accessed on an “Agency/DoITT issued” mobile device?** | Describe |
| **What steps have you taken in ensure backward compatibility of device hardware/software, and future upgrades, for next 3-5 years?** | Describe |
| **Are there any certifications the device has qualified for?**  **Are there any regulations that this service is subject to?** | Describe |
| **What documentation and training do you have available to use the device/service?**  **Please provide documents/links.** | Describe |
| **What is the roadmap of this device/service?** | Describe |
| **Is the connected device or its components reaching end of life? Is the maintenance support ending for the device or any of its components?** | Describe |
| **What is the process to verify the integrity of the software loaded on the device and that the software does not pose a security threat / vulnerability?**  **What is the assurance process to determine that there is no malicious code introduced via the third-party software?** | Describe |
| **What timers are used in device for external communication and what values are they set to?** | Describe |
| **Does the device undergo periodic vulnerability testing?**  **Is there a pen test or SOC2 report available for NYC3 to review? *NOTE: the report(s) must be less than a year old.*** | Describe |
| **Does the web-based device management application undergo periodic penetration testing?** | Describe |

**Appendix A: Network Diagram**

Provide a global network architecture diagram illustrating relevant details and identifying components, make, model/regions, include, Call Flows, firewalls, NAT, PGWs, IDS/IPS, DMZ, Securezone, Network Segmentation etc., from the connected devices to the servers and its’ supporting infrastructure. Include a global view of any services or applications (new or existing) that this service/product will depend on. Include third party or external data sources, administration access etc.

Please insert relevant global view diagram (picture or Visio Diagram) below:

|  |
| --- |
| Click here to paste the network diagram(s) |

# 

1. For additional guidance see: <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>

   2 Data owner is a senior-level official who bears overall responsibility and accountability for that data [↑](#footnote-ref-1)