TED M. ROSS
GENERAL MANAGER
CHIEF INFORMATION OFFICER

JOYCE J. EDSON
EXECUTIVE OFFICER

JEANNE M. HOLM
ASSISTANT GENERAL MANAGER

ANTHONY MOORE
ASSISTANT GENERAL MANAGER

LAURA ITO
ASSISTANT GENERAL MANAGER

CITY OF LOS ANGELES

CALIFORNIA

ERIC GARCETTI
MAYOR

ITA
INFORMATION TECHNOLOGY AGENCY

CITY HALL EAST
200 N MAIN ST, ROOM 1400
LOS ANGELES, CA 90012
213.978.3311

ita.lacity.org

June 17, 2019 REF: EXE-178-19

Budget and Finance Committee
c/o Richard Williams, Office of the City Clerk
Room 395 City Hall
Los Angeles, CA 90012

Subject: **POTENTIAL CYBER SECURITY THREATS & NECESSARY STEPS (CF NO. 14-1635-S7 – IMPLEMENTATION OF THE HOME-SHARING ORDINANCE, MOTION 6)**

Dear Councilmembers:

Pursuant to City Council Motion, Council File No. 14-1635-S7, the Information Technology Agency (ITA) is submitting the following report on the potential cyber security threats, necessary steps to ensure that host data is protected, and potential liabilities for the City.

Background

The City Planning Department is contracting with Host Compliance LLC to provide consulting and software services related to permitting, compliance monitoring, and enforcement of the City's ordinances, regulations, and tax rules associated with short-term rentals. To perform its role as an electronic platform supporting the Home-Sharing Ordinance, the Host Compliance solution will collect Personally Identifiable Information (PII) such as state-issued IDs, Vehicle Registration, Property Tax Bills, Address, Date of Birth, Phone Number, Electronic Payment Information, etc.

Potential Cyber Security Threats to City

The Host Compliance system is a web-based, online system hosted through Amazon Web Services (AWS). The system is intended to allow both host users and City administrators secure access to the solution via the Internet. The system is not hosted on City infrastructure and would not be maintained within the City network. This changes the nature of cyber threats to the platform. In addition, the system uses limited interfaces (APIs) to City systems (e.g. publicly available property data). With this in mind, the following are key potential categories of cyber threats that could affect Host Compliance:

- Exploiting Application-Level Security – These cyber-attacks try to exploit the input data screens of the application to steal data or disrupt system (e.g. SQL Injection or Cross-site Scripting).

- Exploiting System-Level Security – These cyber-attacks try to exploit operating system or web server vulnerabilities to steal, exfiltrate, or hold ransom data (e.g. WannaCry).

- Intercepting Communications - A cyber-attack that seeks to insert itself between the communications of the user (client) and the Host Compliance server (e.g. Session Hijacking or Eavesdropping).

- Denial of Service – A coordinated cyber-attack on Host Compliance's system resources intended to overwhelm and debilitate the system (e.g. TCP SYN flood attack).

Host Compliance Existing Cyber Security Controls
The Information Technology Agency (ITA) and City Planning discussed the vendor's security and access controls. The following are key controls being provided by the vendor:

1. Data Encryption - All collected host data is encrypted both in transit and at rest.

2. 3rd Party Payment Processing - All electronic payment information is processed and handled by a Payment Card Industry Data Security Standard (PCI DSS) compliant third-party Service Provider and has been audited by an independent PCI Qualified Security Assessor (QSA). This means that Host Compliance does not store or process sensitive credit card information.

3. Meets FedRAMP & FISMA Standards - Host Compliance infrastructure is hosted on Amazon Web Services (AWS) and complies with a variety of IT security standards including Federal Information Security Management Act (FISMA), Department of Defense Assurance Certification and Accreditation Process (DIACAP) and the Federal Risks and Authorization Management Program (FedRAMP). These are mandated cyber security standards required by the federal government for use by all federal agencies using Cloud infrastructure addressing data encryption, data breach notification, denial of service attack prevention, etc.

4. Information Security Policies - Host Compliance has enacted a number of data privacy and security policies (e.g. Physical & Environmental Security, Crisis Management, Damage Restoration Plans, etc).

The controls listed above are industry-recognized for data security and privacy.

Additional Recommended Steps to Protect Host Data
In addition to the existing security controls listed by the vendor above, the Information Technology Agency recommends requiring the vendor to allow City Planning and Information Technology Agency to conduct periodic or as-needed vulnerability assessment of Host Compliance system.

Potential Liability to the City in Case of Data Breach
The City's contract with the vendor recognizes the risk of a data breach and contains various protections, including language requiring the vendor to indemnify the City in the event of a data breach and a requirement that the vendor obtain appropriate insurance coverage.

Respectfully submitted,

Ted Ross
General Manager

ec: Trina Unzicker, CAO
Timotny Plummer, CLA