**报告编号：2019-XAPG-SXYD-03**

**互联网新技术新业务信息安全评估复核报告**

|  |  |
| --- | --- |
| **委托单位：** | 中国移动通信集团山西有限公司 |
| **业务名称：** | 和生活 |
| **完成时间：** | 2019年10月 |

**评估单位：国家计算机网络与信息安全管理中心**

**2019年10月**

**声明**

受中国移动通信集团山西有限公司委托，国家计算机网络与信息安全管理中心对中国移动通信集团山西有限公司和生活进行了新技术新业务初评报告的核查。

本次核查主要从系统架构和业务流程分析入手，全面查找和生活配置的不安全因素，查验业务系统是否存在信息安全隐患，保障业务信息安全。

本报告评估结论的有效性建立在被评估单位提供相关证据的真实性基础之上。

本报告中所给出的核查结论仅对被评估业务系统当时的安全状态有效。当评估工作完成后，由于业务系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行评估，本报告不再适用。

本报告中给出的核查情况评估结论不能作为对业务系统内部署的相关系统构成组件（或产品）的评估结论。

在任何情况下，若需引用本报告中的核查结果或结论都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实。

**评估复核情况确认签字表**

|  |  |
| --- | --- |
| **受评**  **单位** | 中国移动通信集团山西有限公司 |
| **复核**  **业务** | 和生活 |
| **评估**  **复核**  **依据** | 1、《工业和信息化部办公厅关于印发<2018年省级基础电信企业网络与信息安全工作考核要点与评分标准>的通知》（工信厅网安〔2018〕4号）  2、《互联网新技术新业务安全评估指南》（2018年修订版） |
| **复核**  **结果** | 根据工信部相关工作要求和标准，国家计算机网络与信息安全管理中心对和生活业务进行了复核，经评估一致认为：   1. 该业务存在部分信息安全风险，可进行改进，总体安全可控，但总体制度建设、制度规范需要进一步加强。 2. 后续需在数据传输存储、信息内容管理等多方面进行问题整改，同步配套更新安全保障措施。 3. 该业务评估报告结构较为严谨，但存在部分项目研判依据不准确，技术保障方面仍存在信息安全的薄弱环节。 |
| **评估单位**  **复核确认**  **（签字及盖章）** |  |
| **信息安全部门负责人**  **（签字及盖章）** |  |

附件：复核记录

1. **初评报告中部分研判不准确：**

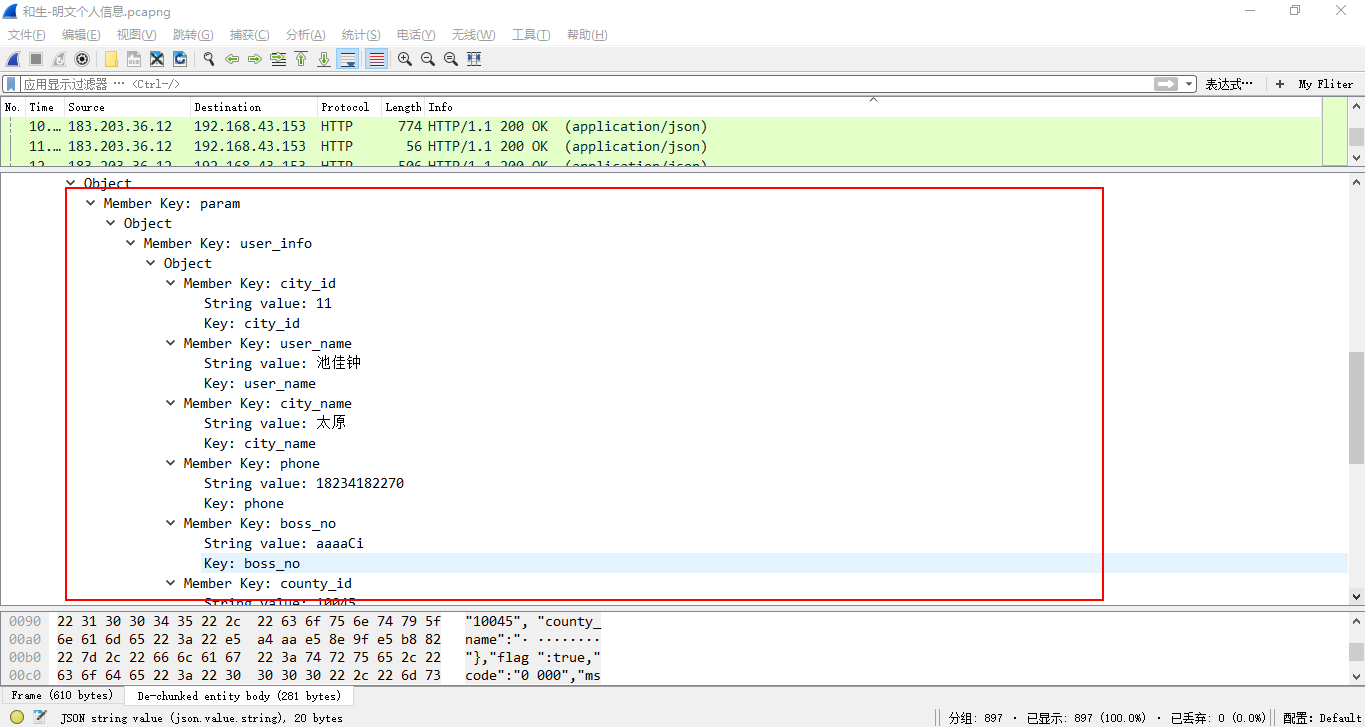
初评报告中存在部分内容研判不准确，对日常管理制度的评估不够全面，建议对报告进行完善统一，精简内容，加强评估报告的规范性。

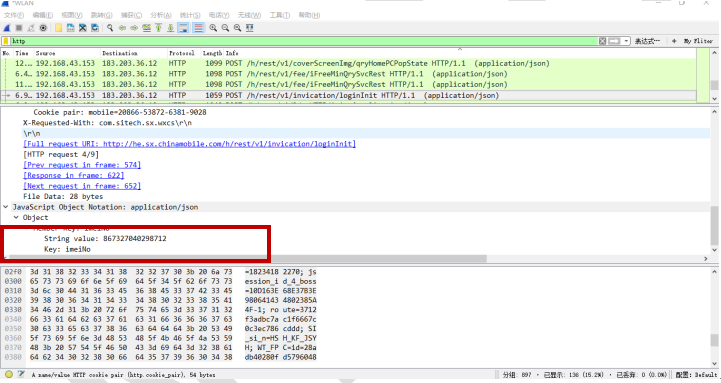
1. **复评中新发现的问题：**
2. **业务制度建设存在部分问题**

按照相关管理要求，山西移动建立了一系列管理办法保障业务安全。该业务平台目前管理制度为集团公司规范，需进一步按照业务需求，对应制度完善满足本业务保障需要的制度，需形成制度性文件保障业务安全。

1. **业务保障能力方面，存在部分保障安全风险**
2. **业务应用安全保障：**
3. 明文传输大量个人敏感信息，包括手机号 imei 姓名 单位地址 等等大量个人信息，未作任何加密措施，容易受篡改劫持；**风险程度：高；**

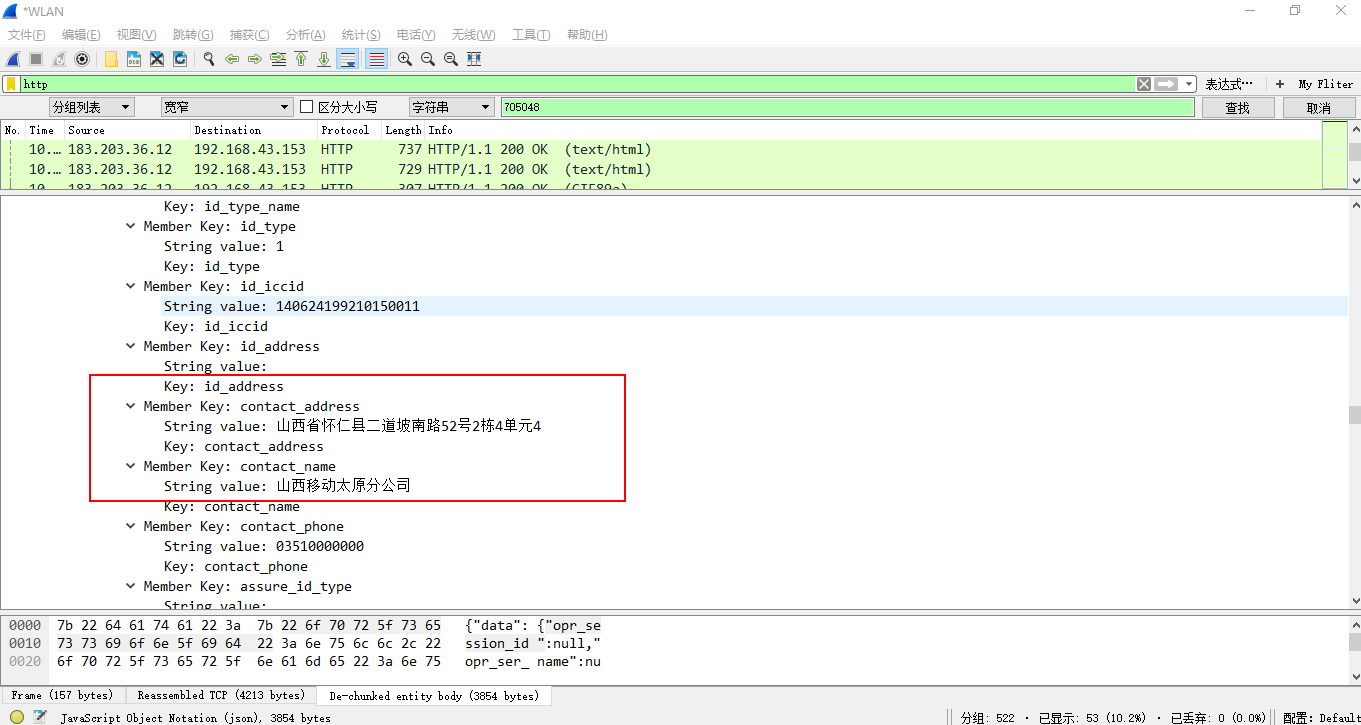
**建议：对个人敏感信息加密；**





1. 过度使用用户个人信息，超出业务必要范围，不符合最小化使用用户个人信息原则；**风险程度：高**

**建议：最小化采集传输用户信息，不使用、传输、采集非必要个人敏感信息；**



1. 多点登陆，无提示。**风险程度：中**

**建议：增加单点登陆校验，如：可采取优化SessionId等方式；**



1. 短信登陆，无验证码校验，且无发送次数限制，容易造成短信轰炸；**风险程度：中**

**建议：限制频繁试错与暴力破解，限制发送短信条数；**