Project 3

[Name of the Writer]

[Name of the Institution]

Project 3

Mobile apps are becoming important for every industry including digital government. There are different mobile apps for the digital government which include MyTSA, WISER, Dolphin & Whale, USDA, Find a health center, FEMA, White House, etc. These are some top digital government mobile apps which can be used for different purposes (GovLoop, 2015). These applications are recognized as innovative and best for delivering information about the government. Such apps are very important for everyone and create new ways for a citizen to learn about different things.

Mobile apps are becoming not only necessary for individual or business companies but also for the federal government. However, there are huge concerns about security for the federal government mobile apps. Mobile apps security is a major concern which can cause vulnerabilities that can put sensitive government data and different resources at risk. NIST provided the guidelines to face security issues for the federal government. The federal government requires some serious security because they do have data of millions of people and it is their responsibility to secure that data (NIST Drafts Mobile App Security Guidelines, 2019).

It is important for federal agencies to find out what a mobile app really does before using it. They should be aware of security risks and privacy issues. There are many applications which can access more data of the user, and they don't even know about that which is why they fall victim of a cyber attack. Usually, the government takes advantage of third-party mobile applications to improve productivity, but they should not do that and built their own mobile apps. Government agencies should understand the security risks of mobile apps and should create a strategy to mitigate them. They need to provide training to employees regarding the privacy and security of apps and review the mobile app testing results to fulfill the objectives.

Mobile applications also required security just like web applications and desktop applications. Mobile app security requires security models that help to protect the data and information from an unauthorized person or people. The appropriate authentication methods are essential for the security of mobile applications. Antivirus and firewalls also play a key role in the security of mobile apps. It is the requirement for the security of mobile apps that connectivity options must be limited. One of the best methods these days use for mobile apps is the OTPs method which allows only a specific person to access the data and ensures the security of an individual. There are different methods which can help in protecting the mobile apps. However, it is important to implement those methods while creating mobile apps because different mobile apps require different security. A developer must be able to sort out the security of the software at the time of development (Mobile security reference architecture, 2013).

The security of mobile apps depends on their security needs. Mobile applications which are used to deliver government information and services requires a high amount of security because the data of government is always confidential. However, it is important to ensure the security of mobile apps at the time of development. Application developers can easily create mobile apps quickly with the help of different SDKs. It is the duty of the developer to check the security of apps at each phase of development. In the development team, there must be someone who is responsible for the security of the applications, who understands different between platforms and don't rely on a single platform to protect the security of the users. It is important to generate the credentials securely of mobile apps (Mobile security reference architecture, 2013).

There are different APIs which are used for the development of mobile apps, and they all have different functionality. Sometimes developers use APIs in their apps without searching on them which create problems for them as each API have different security features and developer must ensure that the security measures of the API they are implementing meet their requirement. A developer must use different encryption techniques at the time of development and encrypt sensitive data like username, passwords, contact, email, etc. of the user. It is also important to secure the servers and apply security measures to protect them. Application security also depends on the security of servers as the security of servers is very complex and required research (Federal Trade Commission, 2017).

A developer must take steps to secure the apps from vulnerabilities, cross-site scripting, and injection attacks. It is important for the developer not to use code from third parties because the third-party code isn't safe and is the biggest threat to the security of the applications. A developer must think like an attacker while building a mobile app because that is the only way they can find vulnerabilities in their application easily. It is also essential to secure data transmission between sender and receiver, and use tokens to handle sessions. A developer must implement tamper protection to protect the users and ensure the reputation of an app as a trustworthy application. These are some important recommendations which need to be considered at the time of development to ensure the security of the mobile app (Federal Trade Commission, 2017).

Mobile applications security has become a huge concern for everyone as there are many tricks which are attackers using to easily access the sensitive of the users from different mobile apps. The biggest risk these days is to the government agencies because their data is not secure these days and hackers easily access their data to make use of that for their own purposes. Usually, terrorists, these days try to access confidential data of federal agencies to observe their activities. However, there are different methods which can help agencies to protect their data and make their apps more secure.

**References**

Mobile security reference architecture (2013). S3.amazonaws.com. Retrieved from <https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf>

App Developers: Start with Security. (2017). Federal Trade Commission. Retrieved from <https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security>

NIST Drafts Mobile App Security Guidelines - InformationWeek. (2019). InformationWeek. Retrieved from <https://www.informationweek.com/government/mobile-and-wireless/nist-drafts-mobile-app-security-guidelines/d/d-id/1306815>

19 of the Coolest Government Mobile Apps | GovLoop. (2015). GovLoop. Retrieved from <https://www.govloop.com/community/blog/cool-gov-mobile-apps/>