# Project 3: Government Mobile Apps Security Assessment & Strategy

For this research report you will research and then present your findings about cybersecurity issues specific to mobile applications. You will also provide a set of recommendations for best practices (your “strategy”) for security architectures and designs for mobile apps.

Mobile applications are important because they allow citizens and other stakeholders to access information and services through the federal government’s digital government initiatives. For more information about requirements to provide mobile friendly websites and mobile apps see this blog posting from GSA.GOV <https://www.gsa.gov/blog/2018/08/07/collaborating-for-better-design-technology-and-user-experience> and the text of the Connected Government Act Public Law 115-114 <https://www.congress.gov/115/plaws/publ114/PLAW-115publ114.pdf>

Note: this assignment requires inclusion of diagrams or graphics that help to explain the information provided in your analysis and strategy. You are not required to create these on your own. Instead, you should look for useful graphics/diagrams in the readings and use those to support your work. You must cite the source for each piece of artwork used in your project. Put a figure caption under the diagram or chart and then place the in-text citation at the end of the caption. See the example at the end of this file.

## Research:

1. Review the Weekly readings.
2. Review the 2017 changes in US Laws regarding the requirement for mobile friendly government websites.
	1. <https://www.congress.gov/115/plaws/publ114/PLAW-115publ114.pdf>
	2. <https://www.nextgov.com/ideas/2018/01/what-digital-government-cx-pros-should-know-about-connected-government-act/144987/>
	3. <https://www.fedscoop.com/bill-mobile-friendly-government-websites-cruises-senate/>
3. Research the “best” of federal mobile apps to see examples of the type of apps that other agencies have created in the past.
	1. *Discover Six of the Government's Best Mobile Apps* [*https://www.prnewswire.com/news-releases/discover-six-of-the-governments-best-mobile-apps-300236300.html*](https://www.prnewswire.com/news-releases/discover-six-of-the-governments-best-mobile-apps-300236300.html)
	2. *The Best Government Mobile Awards!* [*https://www.mobile-webaward.org/mwa/winners\_detail.asp?yr=all&award\_level=best&category=Government*](https://www.mobile-webaward.org/mwa/winners_detail.asp?yr=all&award_level=best&category=Government)
	3. *7 Essential Mobile Apps for Federal Employees in 2019* [*https://www.waepa.org/resources/7-essential-mobile-apps-for-federal-employees-in-2019/*](https://www.waepa.org/resources/7-essential-mobile-apps-for-federal-employees-in-2019/)
	4. *CDC Mobile APPS (Centers for Disease Control and Prevention)* [*https://www.cdc.gov/mobile/mobileapp.html*](https://www.cdc.gov/mobile/mobileapp.html)
4. Research the federal government’s perspective on mobile app security architectures and design recommendations. Here are three sources to help you get started:
	1. *App Developers: Start with Security*
	<https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security>
	2. *Mobile Security Reference Architecture*
	<https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2013/05/Mobile-Security-Reference-Architecture.pdf>
	3. *How to build a secure mobile app: 10 tips*<https://www.techrepublic.com/article/how-to-build-a-secure-mobile-app-10-tips/>
	4. *2019 Mobile Security R&D Program Guide*<https://www.dhs.gov/sites/default/files/publications/2019_mobilesecurity_rd_programguide_vol3.pdf>
	5. *Why your agency (likely) doesn’t need a mobile app* <https://18f.gsa.gov/2018/02/13/why-your-agency-doesnt-need-a-mobile-app/>
5. Research industry recommendations for mobile app security. Begin with the following sources:
	1. *OWASP Mobile Security Project* <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project>
	2. *Top 10 Mobile Risks* (click on tab) <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks>
	3. *Mobile app security: Always keep the back door locked* <https://arstechnica.com/security/2013/02/mobile-app-security-always-keep-the-back-door-locked/>
6. Find five or more best practice recommendations for ensuring the security of mobile apps. These recommendations must include security for the platform (mobile device), the data on the device, and the transmission path between the device and the mobile application server. Your focus should be upon recommendations that can be implemented as part of a strategy for reducing risk.

## Write:

Write a five to seven page report in which you summarize your research and present your “best practices” based strategy for reducing risk and ensuring security for government provided mobile apps and their users. You should focus upon clarity and conciseness more than length when determining what content to include in your paper. At a minimum, your report must include the following:

1. An introduction or overview of mobile apps for digital government. Include 5 or more examples of mobile apps recognized as being innovative or “best of category” applications for delivering government information and services to mobile devices. This introduction should be suitable for an executive audience.
2. A separate section in which you discuss the federal government’s requirements and recommendations for mobile app security architectures and the associated design recommendations. Write this section for non-technical managers; you will need to translate from tech-speak to manager-speak. Include at least three diagrams or pictures in this section and remember to include the appropriate in-text citations for the source (append to the figure caption).
3. A separate section in which you discuss industry’s recommendations for security architectures and risk reduction for mobile app security. Write this section for non-technical managers; you will need to translate from tech-speak to manager-speak. Include at least three diagrams or pictures in this section and remember to include the appropriate in-text citations for the source (append to the figure caption).
4. A section in which you present 5 or more *best practice* recommendations for building security (the confidentiality, integrity, availability, authenticity, and non-repudiation for Mobile Applications) into mobile applications used to deliver government information and services. Present these strategies as recommendations for reducing risk.
5. A separate section in which you summarize your research and recommendations.

## Submit for Grading

Submit your work in MS Word format (.docx or .doc file) using the Project 3 Assignment in your assignment folder. (Attach the file.)

## Additional Information

1. Consult the grading rubric for specific content and formatting requirements for this assignment.
2. Your 5- to 7-page research report should be professional in appearance with consistent use of fonts, font sizes, margins, etc. You should use headings and page breaks to organize your paper.
3. Your paper should use standard terms and definitions for cybersecurity.
4. The CSIA program recommends that you follow standard APA formatting since this will give you a document that meets the “professional appearance” requirements. APA formatting guidelines and examples are found under Course Resources. An APA template file (MS Word format) has also been provided for your use CSIA\_Paper\_Template(TOC+TOF,2021).docx.
5. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s page count.
6. You should write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
7. You must credit your sources using in-text citations and reference list entries. Both your citations and your reference list entries must follow a consistent citation style (APA, MLA, etc.).

**Example Diagram with Citation and Reference List Entry**



Figure 1. Enterprise Core Services (Adapted from Figure 1 in CIO Council, 2013, p. 5)

Federal CIO Council & Department of Homeland Security. (2013). *Mobile security reference architecture.* Retrieved from https://s3.amazonaws.com/sitesusa/wp-content/‌uploads/sites/‌1151/‌downloads/‌2013/05/Mobile-Security-Reference-Architecture.pdf