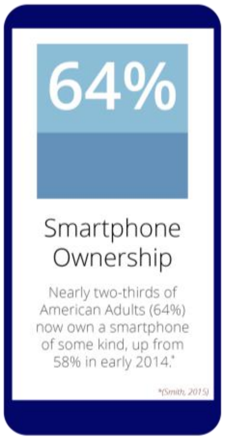
MOBILE APPLICATION PLAYBOOK (MAP)

U.S. Department of Homeland Security (DHS)
Office of the Chief Technology Officer (OCTO)

Table of Contents

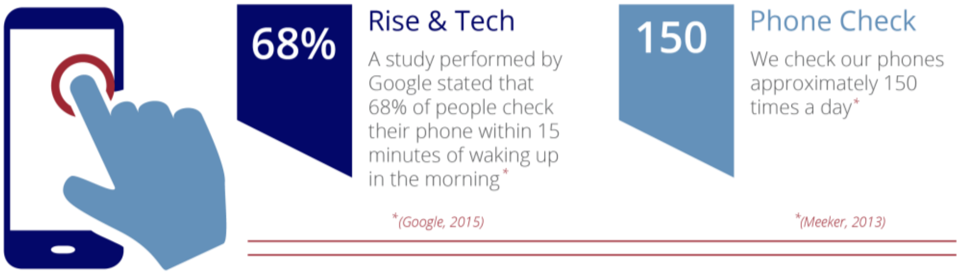
Executive Summary


64%
Smartphone Ownership
Nearly two-thirds of American Adults (64%) now own a smartphone of some kind, up from 58% in early 2014.*

*(Smith, 2015)

There are approximately 7.5 Billion mobile connections to date according to GMSA's real-time tracker[1]. The number of active mobile connections exceeded the number of humans alive around the 7.19 Billion mark[2]. Mobile devices are multiplying five times faster than the human race[3]. With the rise in mobile devices this has changed the way we search, consume and inform each other.

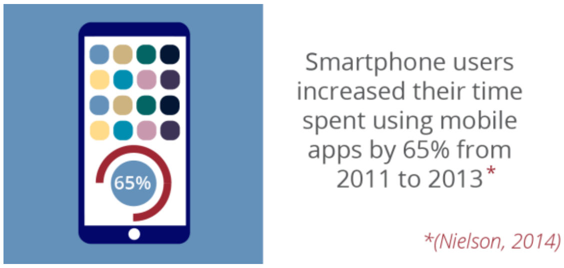
Mobile devices are used for more than calling, texting, or internet browsing as 40% of smartphone users have used their phone to look up government services or information in the last year[4]. Both commercial and federal entities are realizing the critical need to utilize enterprise mobile strategies to delivery both public service offerings as well as perform internal business functions.


68%
Rise & Tech
A study performed by Google stated that 68% of people check their phone within 15 minutes of waking up in the morning*
150
Phone Check
We check our phones approximately 150 times a day*

*(Google, 2015)

*(Meeker, 2013)

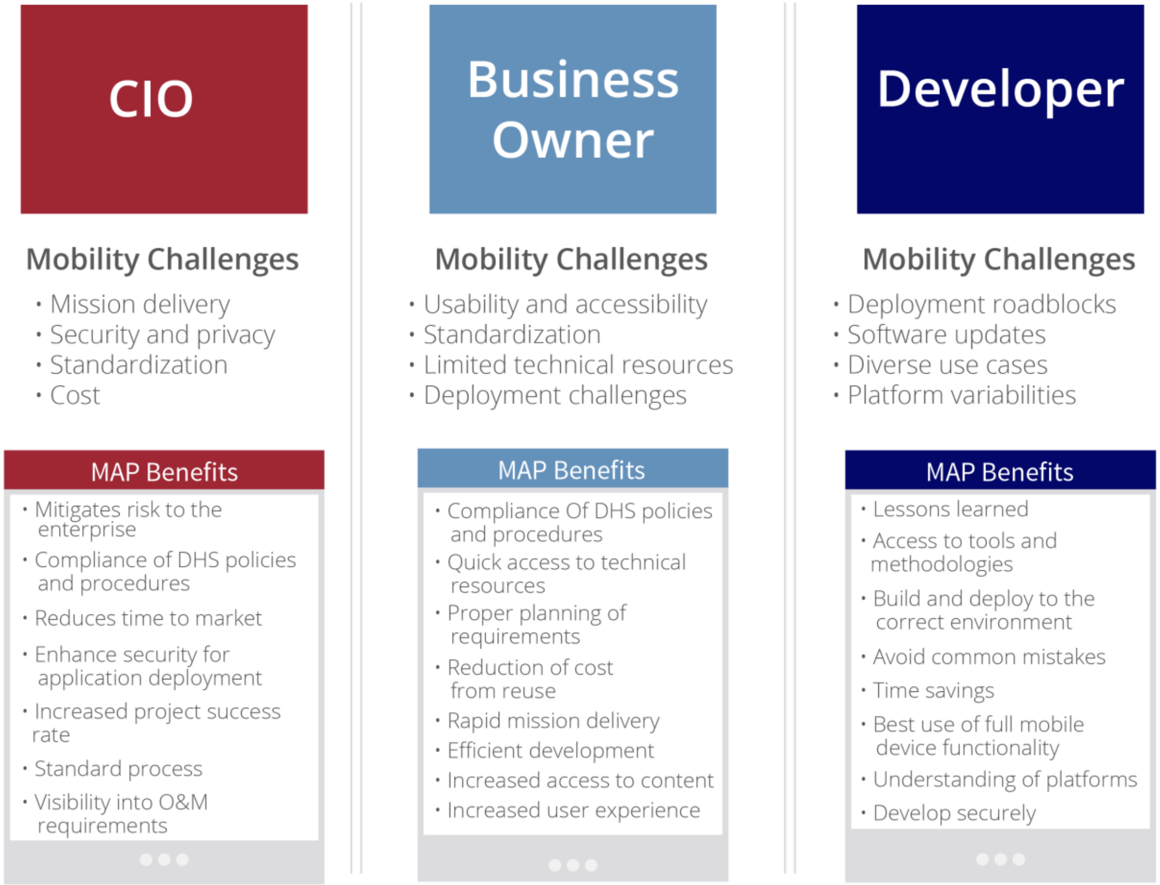
As the importance of the mobile channel increases, government employees and the general public will look to Federal Agencies to offer low cost, high quality, and secure mobile applications. Considering the data that mobile phones can gather and access (GPS location, contact lists, text messages, etc.) building and maintaining secure applications for end users is essential. Federal Agencies must streamline the process for building, deploying, and maintaining safe mobile applications to rapidly deliver functionality to their end users while complying with agency rules and regulations. The Mobile Application Playbook (MAP) is a DHS sponsored reference guide to assist application owners and developers in the planning, management, and execution of mobile application projects.


65%
Smartphone users increased their time spent using mobile apps by 65% from 2011 to 2013*

*(Nielson, 2014)

[1] (GSMA Intelligence, 2015)
[2] (Boren, 2014)
[3] (Boren, 2014)
[4] (Smith, 2015)

The MAP is a critical tool to utilize during the entire lifecycle of the mobile application. The Playbook informs readers of the process for developing and managing applications that run on smartphones and other mobile devices from the initial concept to design, development, testing, deployment, and ongoing maintenance and operations. MAP addresses the challenges of mobile application development and deployment within the government, provides solutions and processes that benefit CIOs, Business Owners, and Developers.



CIO

Mobility Challenges

- Mission delivery
- Security and privacy
- Standardization
- Cost

MAP Benefits

- Mitigates risk to the enterprise
- Compliance of DHS policies and procedures
- Reduces time to market
- Enhance security for application deployment
- Increased project success rate
- Standard process
- Visibility into O&M requirements

Business Owner

Mobility Challenges

- Usability and accessibility
- Standardization
- Limited technical resources
- Deployment challenges

MAP Benefits

- Compliance Of DHS policies and procedures
- Quick access to technical resources
- Proper planning of requirements
- Reduction of cost from reuse
- Rapid mission delivery
- Efficient development
- Increased access to content
- Increased user experience

Developer

Mobility Challenges

- Deployment roadblocks
- Software updates
- Diverse use cases
- Platform variabilities

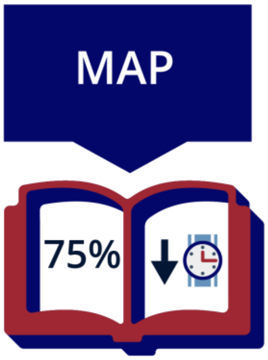
MAP Benefits

- Lessons learned
- Access to tools and methodologies
- Build and deploy to the correct environment
- Avoid common mistakes
- Time savings
- Best use of full mobile device functionality
- Understanding of platforms
- Develop securely

MAP is a living document with input from multiple Federal Agencies and industry partners. Within DHS, OCTO works collaboratively with the Mobile Device Security (MDS) Program within the Science and Technology Directorate (S&T) to identify and respond to the evolving threats and security challenges in the mobile space.

Mobilizing your Mission with MAP

MAP enables your team to focus on delivering mission critical mobile applications while reducing risk and complying with the DHS policies and procedures. MAP is a DHS sponsored guide, tailored to the unique requirements of mobile computing within the DHS environment. This playbook provides DHS organizations and components a well-documented set of steps for planning and deploying mobile applications quickly and securely while following all necessary gate reviews.



The use of MAP reduced one mobile application deployment timeline by 75%, decreasing the time to market by 9 months.

How to engage with DHS OCTO if you need assistance?

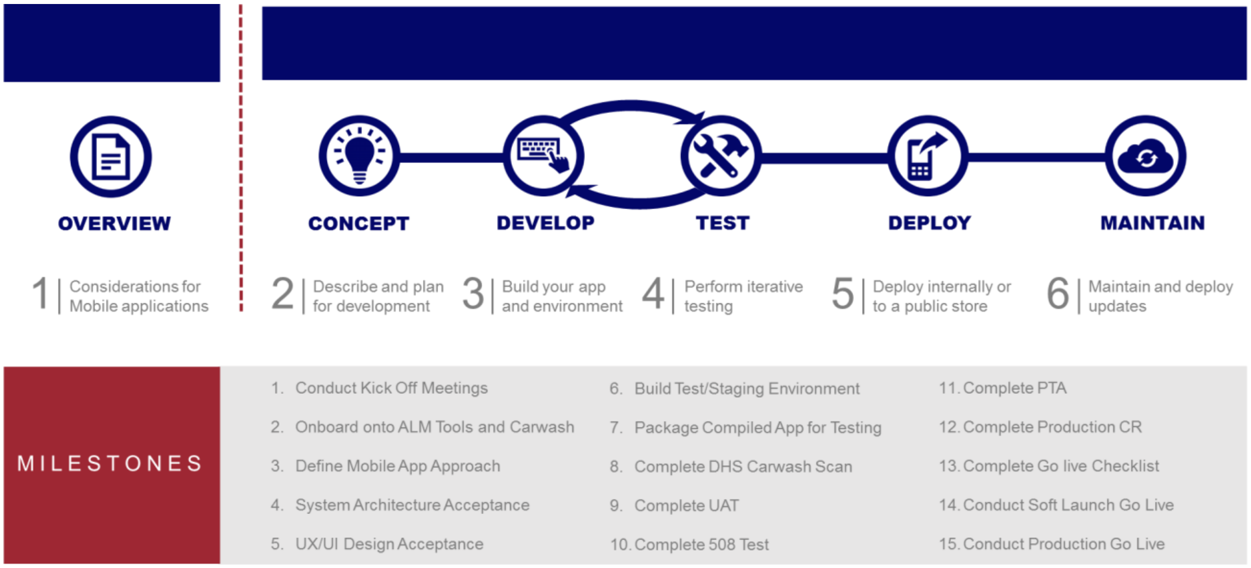
The contact information for the team is located in Appendix VII: . The best way to get started is to reach out to the team and schedule an initial discussion regarding the mobile application development requirements of your organization. OCTO takes a consultative approach and helps each mobile business owner, project manager, or developer tailor an approach that works best for their DHS component and customer base.

How to use the Mobile Application Playbook?

Whether you are internally developing an application or attempting to deploy a 3rd party application, use the MAP to gain information about the steps of the application development lifecycle that apply to you. For each phase of the application lifecycle, the MAP includes detailed steps for your business owners, project managers, and developers to follow. Each section also contains key checklist items to follow, and links to resources to further support your development or deployment efforts. Review the checklists and resources to get an understanding of each lifecycle phase, or use the detailed steps to get a deeper understanding and receive detailed guidance and recommendations. The appendices at the end of the playbook include further information about certain topics, as well as helpful information like a contact list and the challenges of mobility in the government. Read the document all the way through, or browse and use the information that is helpful for you. If you have any feedback or suggestions on MAP please send those comments to DHSOCTO@hq.dhs.gov.

Mobile Application Phases

The following provides an overview of the mobile application development phases and major milestones to ensure efficient delivery of your mobile application. The phases identified below are to guide you through your development from conception through deployment, regardless of where you are in your development lifecycle. Start from the beginning, or pick up where ever you are in your development effort.



OVERVIEW
CONCEPT
DEVELOP
TEST
DEPLOY
MAINTAIN
1 | Considerations for Mobile applications
2 | Describe and plan for development
3 | Build your app and environment
4 | Perform iterative testing
5 | Deploy internally or to a public store
6 | Maintain and deploy updates
MILESTONES

1. Conduct Kick Off Meetings
2. Onboard onto ALM Tools and Carwash
3. Define Mobile App Approach
4. System Architecture Acceptance
5. UX/UI Design Acceptance
6. Build Test/Staging Environment
7. Package Compiled App for Testing
8. Complete DHS Carwash Scan
9. Complete UAT
10. Complete 508 Test
11. Complete PTA
12. Complete Production CR
13. Complete Go live Checklist
14. Conduct Soft Launch Go Live
15. Conduct Production Go Live

Phase 1: Overview

This section will inform you about the mobile landscape and critical considerations for your business unit. For example, do you need a native mobile application, or will a responsive website suffice? Should you develop a hybrid mobile application, or develop in iOS and Android native code?

Phase 2: Concept

Create detailed requirements and designs for the mobile application use case, UI/UX, and interfaces. The two goals of this phase are to 1) create a thorough understanding of the mobile project so that it can be realistically planned and scheduled, and 2) develop a design to a sufficient level of detail to where the application can be built. Ensure that you have all of the necessary tools to manage your project and track progress using a methodology such as Agile.

☐	**Milestone 1:**	**Conduct Kick-off Meeting with OAST/508, Privacy, and Security Teams**
☐	**Milestone 2:**	**Onboard onto Application Lifecycle Management (ALM) Tools and Carwash**

❑ **Milestone 3:**	**Define Mobile Application Approach – i.e. Native vs. Hybrid, iOS/Android**
❑ **Milestone 4:**	**System Architecture Acceptance**
❑ **Milestone 5:**	**UX/UI Design Acceptance**

Phase 3: Develop

Build the mobile application, its interfaces, and server based components. The goal of this phase is to iteratively build a working application to be deployed to desired environment(s).

❑ **Milestone 6:**	**Build Test/Staging Environment**
❑ **Milestone 7:**	**Package Compiled Application for Testing**

Phase 4: Test

Thoroughly test your application and ensure coordination with applicable stakeholders (Users, Security, OAST/508, and Privacy).

❑ **Milestone 8:**	**Complete DHS Carwash Scan**
❑ **Milestone 9:**	**Complete User Acceptance Testing (UAT)**
❑ **Milestone 10:**	**Complete 508 Test**
❑ **Milestone 11:**	**Complete Privacy Threshold Analysis (PTA)**

Phase 5: Deploy

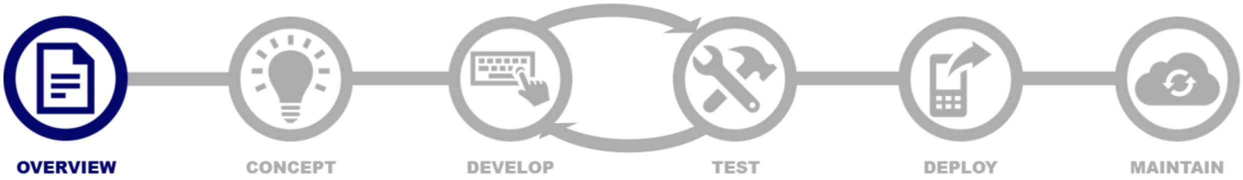
Depending on the intended distribution method for your application, this phase will require you to submit your compiled application to the public app stores (iTunes and Google Play) and/or work with your organization's mobile application store.

❑ **Milestone 12:**	**Complete Production CR**
❑ **Milestone 13:**	**Complete Go Live Checklist**
❑ **Milestone 14:**	**Conduct Soft Launch Go Live**
❑ **Milestone 15:**	**Conduct Production Go Live**

Phase 6: Maintain

Whether you are performing bug fixes or functionality enhancements, ensure that you follow the necessary processes and gate reviews for each new release of the mobile application.

Overview of the Mobile Landscape



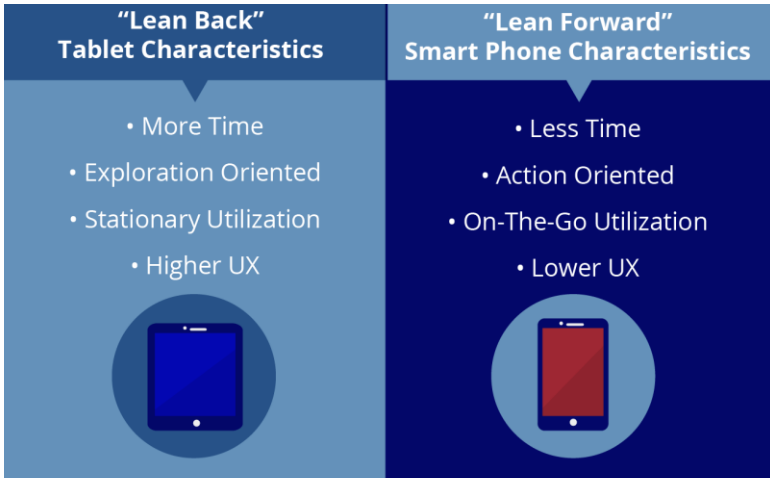
Critical Considerations for your Business Unit

Responsive Web Design vs. Mobile Application

The first critical consideration involves deciding if your business unit needs to develop a responsive website or a native application. If you are able, it is highly recommended that you build both in order to reach the entire mobile audience. However, most business units do not always have the available resources to develop both. Therefore it is critical that you understand the advantages of both options when addressing your mission priorities. Responsive websites are designed so that the website formats according to the devices that it is being accessed from. Responsive website design is normally less costly than developing a native application and they provide the ability for the website's URL to be found on search engines unlike native mobile applications. Native mobile applications are downloaded from either the App Store or Google Play and one of the significant benefit is the ability to access the features of the phone or mobile device such as the camera and GPS. Mobile applications also provide the additional capability to send out push notifications to the mobile device.

Smartphone vs. Tablet

Developing for the smartphone vs. the tablet are often being regarded as separate initiatives.   Their respective orientation (i.e., 'lean back' orientation on tablet vs. 'On the Go' orientation on smartphone) continue to serve more distinct than common use cases as the use of tablet devices continues to further proliferate in the marketplace. Users expect and demand to take advantage of the larger screen real-estate and user experience (UX) potential available with a tablet.

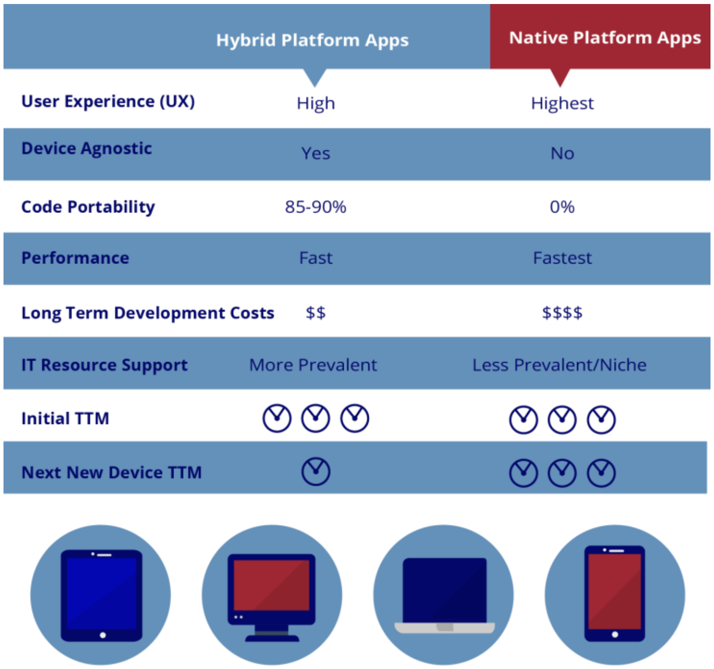


"Lean Back" Tablet Characteristics	"Lean Forward" Smart Phone Characteristics
• More Time	• Less Time
• Exploration Oriented	• Action Oriented
• Stationary Utilization	• On-The-Go Utilization
• Higher UX	• Lower UX

Hybrid vs. Natively Developed Apps

The platform on which to develop mobile apps for smartphones and/or tablets is another critical decision for an organization. Several years ago prevailing industry thinking was that native mobile development (i.e., developing iOS mobile apps in Apple's Swift, and Android mobile apps in Android Studio, etc.) was the most prudent way to develop for any use case or industry need. Emerging hybrid mobile app platforms i.e., device-agnostic platforms that promised a 'write once, deploy to any mobile device' capability) at the time lacked high (UX) support and limited access to mobile device-specific APIs to take advantage of specific mobile device features/performance.

As the mobile app development marketplace has matured, the gap has significantly narrowed. While native mobile application development still provides the most superior UX and performance in a mobile app, hybrid platforms have matured, making that gap closer to negligible. More open mobile-device API sets are offered by the most prevalent mobile device manufacturers (i.e., such as iOS and Android, who comprise the 'Big 2' mobile devices at 94%+ current US market share (comScore, 2015)). With the prolific use of the JavaScript language as an effective code bridging mechanism, hybrid mobile app development platforms have narrowed the gap for UX, performance, and native device feature use. Adding in the benefits of high code portability and more prevalent (and less divergent) IT resource support available in the marketplace, any perceived gaps in UX or performance can be greatly offset by decrease in time to market (TTM) and long term mobile app support costs afforded by a hybrid mobile app development platform.

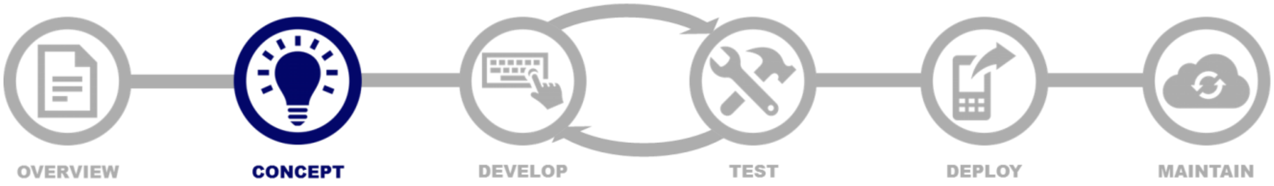


	Hybrid Platform Apps	Native Platform Apps
User Experience (UX)	High	Highest
Device Agnostic	Yes	No
Code Portability	85-90%	0%
Performance	Fast	Fastest
Long Term Development Costs	$$	$$$$
IT Resource Support	More Prevalent	Less Prevalent/Niche
Initial TTM	◷ ◷ ◷	◷ ◷ ◷
Next New Device TTM	◷	◷ ◷ ◷

Checklist

- ❑ Analyze and understand the best mobile solution for your business unit's needs (Responsive Website, Respective Orientation, Hybrid Application, Native Mobile Application)

Concept



The concept phase includes meeting with key stakeholders and building the details around your use case, technology dependencies, and UI/UX. In this phase, thoroughly document the requirements and onboard onto Application Lifecycle Management tools to create your backlog and start tracking your tasks and progress.

Key Steps

Step 1a: Conduct Kick-off Meeting with Security Team

- Contact your organization's Security Team to ensure that you are considering the necessary requirements for your application
- Ensure that you have a ISSO assigned to your application
- Your ISSO will help your through the process of getting your application certified and approved for use and distribution

Step 1b: Conduct Kick-off Meeting with OAST/508 Team

- The Office of Accessible Systems & Technology (OAST) provides strategic direction, governance, technical support, and training to ensure DHS employees and customers with disabilities have equal access to information and data.
- Link to OAST Home Page
- Ask the OAST Team about Mobile Developer Best Practices

Step 1c: Conduct Kick-off Meeting with Privacy Team

- The DHS Privacy Office works to protect the privacy of all individuals and to ensure compliance with Freedom of Information Act (FOIA) requirement for the Department.
- Link to Privacy Office Home Page
- Ask the Privacy Team about the Mobile Application Instruction

□ **Milestone 1:** **Conduct Kick-off Meeting with OAST/508, Privacy, and Security Teams**

Step 2: Use Case Design

- Develop a written description of how users will perform tasks using your mobile application.
- Identify, from the user's point of view, the mobile application's behavior as it responds to a user request. Each use case is represented as a sequence of simple steps, beginning with a user's objective and ending when the objective is fulfilled.
- Use case design will help determine critical aspects such web responsive vs. native mobile app, hybrid mobile app vs. native mobile app, and public deployment vs. internal deployment.

Step 3: Gain Access to Application Lifecycle Management Tools

- Use Application Lifecycle Management tools to manage your project, track your requirements, track your bugs, manage your source code, collaborate with your team, and run scans on your application
- DHS OCIO OCTO offers free Application Lifecycle Management Shared Services (ALMSS) through the DHS Carwash service.
- Click here to access the DHS Carwash page in the DHS IT Services & Hardware Catalog
- Click here for access to the Carwash User Guide from a DHS network
- Click here for access to the Carwash User Guide for users with OMB Max accounts

❑ **Milestone 2:** **Onboard onto Application Lifecycle Management (ALM) Tools and Carwash**

Step 4: Populate your Agile Backlog in your ALM Suite

- Create user stories to gather your business requirements for development and track your progress to the "definition of done" for each story
- DHS OCIO OCTO offers Agile Guidance through the DHS Agile Center of Excellence
- Click here to access the DHS Agile Center of Excellence
- Click here to access the DHS Agile Guidebook
- Click here to access the DHS Agile Instruction

Step 5: Develop Physical System/Architecture View

- The physical systems view documents all of the physical features of the system such as the specific technology platforms and components.
- The physical systems view communicates decisions about the hardware and systems software used to deliver the mobile application.
- Examples include handset platforms (iPhone, Android, Blackberry, etc.), server platforms (mainframe, cloud, etc.), and systems software used (app servers, DB servers, etc.)

❑ **Milestone 3:** **Define Mobile Application Approach – i.e. Native vs. Hybrid, iOS/Android**

❑ **Milestone 4:** **System Architecture Acceptance**

Step 6: Identify Technology Requirements and Dependencies

- Develop a list of the high level technology requirements for the mobile application.
- Include a list of which specific mobile devices (e.g., iOS – iPhone 6s, iPhone 6, iPhone 5s; Android – Samsung Galaxy S6, Samsung Galaxy S6 Edge, etc.) are targeted for deployment and support.

Step 7: Design UX/UI

- Design graphics for all screens of the mobile application
- Create wireframes and mock-ups to show the user experience for your application

❑ **Milestone 5: UX/UI Design Acceptance**

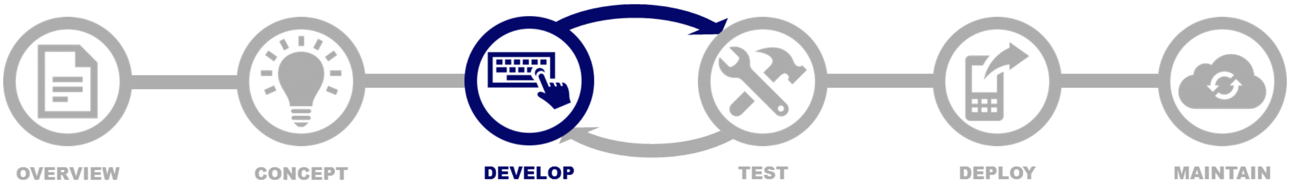
Checklist

❑ Meet with Security Team
❑ Meet with Privacy Team
❑ Gain access to ALM tools
❑ Create Systems Architecture
❑ Design UI/UX
❑ Meet with 508 Team
❑ Develop Use Case
❑ Populate your backlog
❑ Identify Technology Dependencies

Resources

✓ **OAST Home Page**
✓ **DHS Carwash**
✓ **Privacy Office Home Page**
✓ **DHS Agile Center of Excellence**

Develop



The Develop phase includes setting up your application development tools, setting up your environments, developing the application, and performing debugging. Develop in an iterative fashion and package your application for testing at the end of your development increment. Whether you perform a development and test increment every day, week, or month, consider the following steps:

Key Steps

Step 1: Setup your developer tool kits, depending on your development platform (hybrid vs. native)

- Hybrid
    - If using JavaScript based framework, develop using HTML, CSS, and JavaScript
    - If using any other framework, use their documentation and references to ensure correct use
- Native iOS
    - Most applications in iOS have been written in the Objective-C programming language however there is an increasing number of applications that are being written in Swift, Apple's new programing language that makes programming easier and more flexible.
    - Developers typically use Xcode to develop their apps
- Native Android
    - Most Android applications are written in the Java programming language
    - Developers typically use Android Studio to develop their apps

Step 2: Prepare Development Environments

- Set up the development and testing environments for use by the application development team
- For mobile applications that will eventually be public facing, consider testing software such as Crashlytics to setup your distribution tool for user acceptance testing and crash analytics
- For mobile applications to be deployed to Government Furnished Equipment (GFE) mobile phones, inquire with your organizations Mobile App Store provider and your Mobile Device

Management (MDM) provider to learn about testing and pre-production (staging) environments

- For applications accessing back-end systems and data, ensure that you have a testing or staging environment to have the Mobile Application interact with non-production data during development

❑ **Milestone 6: Build Test/Staging Environment**

Step 3: Create story boards and screen layouts

- XCode, Android Studio, and most mobile development tools have a "story board" function which enable developers to create screens and define content for each

Step 4: Iteratively develop code

- Associate code with story boards or layout files for iOS and Android native development
- In some cases hybrid applications may not have story boards or layout files
- Build out functionality and tie your application to any data or external sources as necessary

Step 5: Perform debugging

- For iOS, use Xcode to simulate an iOS device running the application directly on your machine
- For Android, use the emulator to run the application or connect a phone or tablet
- For Hybrid applications, use Safari and Chrome to debug web views in iOS and Android apps

Step 6: Upload your code into a source code repository

- At the end of each development iteration (daily, weekly, etc), ensure that you commit your code into a source code repository

Step 7: Package your application into an ipa or apk for distribution

- For testing and distribution purposes, your mobile application must be compiled into either an ipa (iOS) or and apk (Android)

❑ **Milestone 7: Package Compiled Application for Testing**

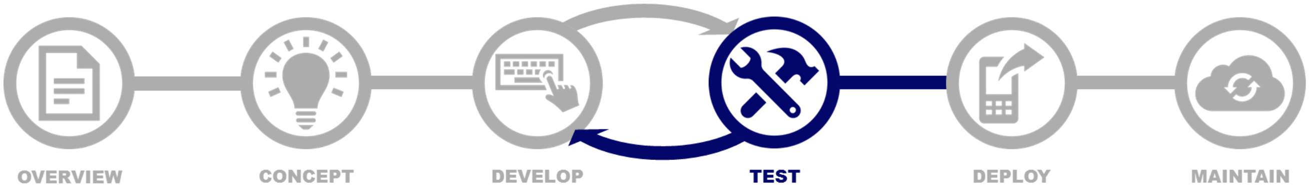
Checklist

❑ Setup your developer tool kits
❑ Create story boards and screens
❑ Upload to a source code repository
❑ Prepare testing/staging environment
❑ Perform debugging
❑ Package your app (ipa/APK)

Resources

- ✓ Android Design Center
- ✓ Android accessibility developer tools
- ✓ Apple Developer Support
- ✓ iOS accessibility developer tools

Test



The Test phase includes finalizing your test conditions, distributing the application to your test groups, and receiving feedback for inclusion within your next development cycle or your deployment.

Key Steps

Step 1: Finalize Test Conditions/Cases

- Complete the list of conditions/cases to be tested with regard to aspects such as application functionality, usability, accessibility, security, and performance
- Certain methodologies like Test Driven Development (TDD) promote testing plans to be made prior to development

Step 2: Identify and create re-usable automated test scripts

- Unit testing
- Quality testing
- Security testing
- Talk to the Carwash Team to discuss what tests can be automated with the Carwash framework

Step 3: Identify groups for distribution

- Quality Assurance Team for basic functionality testing
- User groups for User Acceptance Testing (UAT)
- 508 Team for accessibility testing
- Carwash Team for security testing/scanning

Step 4: Prepare for test group access

- Setup any user accounts needed to access and authenticate to the application
- Ensure test groups have devices
- Ensure test group device compatibility with application

Step 5: Provide instructions to test groups

- Document test steps (consider using ALM tools such as Jira/Confluence to track test cases – contact the Carwash Team for more information)
- Document access/log in steps
- Define specific screens or fields to test
- Define and document any instructions for data submission

Step 6: Distribute mobile application

- Carwash – Upload your source code and binary to your Carwash Source Code repository
- Users groups/508 -
  - For mobile applications that will eventually be public facing, consider testing software such as Crashlytics to distribute - Using Crashlytics for UAT
  - For internal/sensitive mobile applications, inquire with your organizations Mobile App Store provider and your Mobile Device Management (MDM) provider to learn about options for distributing within testing and pre-production (staging) environments

Step 7: Check-in with test groups throughout testing

- Offer demos or training once application is distributed and in hand of the test group
- Be available for ad hoc question and answer
- Use a tracking system and ALM tool suite to document and monitor responses from your ongoing tests

Step 8: Evaluate results and determine necessary actions

- Review test results
  - Prioritize results and determine what will be accomplished in your next development cycle
  - Consider pushing bugs and compliance issues (security/508) to the top of the list
  - If all results are positive, move onto the deployment phase of the lifecycle

❑ **Milestone 8:**	**Complete DHS Carwash Scan**
❑ **Milestone 9:**	**Complete User Acceptance Testing (UAT)**
❑ **Milestone 10:**	**Complete 508 Test**
❑ **Milestone 11:**	**Complete Privacy Threshold Analysis (PTA) * if production ready**

Checklist

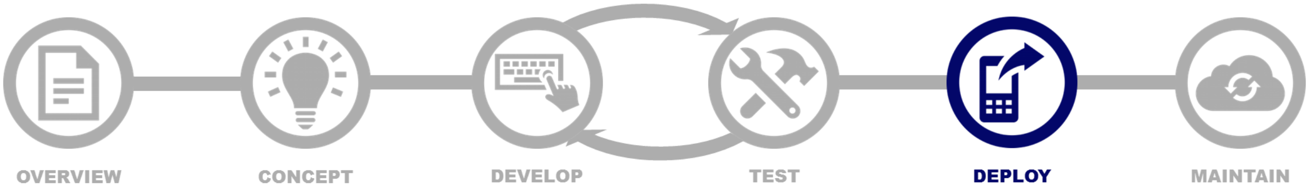
❑ Finalize Test conditions/cases
❑ Identify test groups for distribution
❑ Provide instructions to test groups
❑ Create automated tests
❑ Prepare for test group access
❑ Distribute mobile application

- ❑ Check-in with test groups
- ❑ Evaluate results and determine actions

Resources

- ✓ Using Crashlytics for UAT

Deploy



The Deploy phase includes steps to distribute your test results to the necessary parties, complete your CR, sign your application, and distribute to your intended users. Whether deploying internally or to a public app store, consider the following steps:

Key Steps

Step 1: Distribute test results to necessary parties

- Send your Carwash results to the Privacy Team along with your PTA
- Send your Carwash results to your Security Team and ISSO
- Send the 508 results from OAST to your product/system owner
- Send the UAT results to your product/system owner

Step 2: Prepare Change Request (CR) and have it approved at the CCBs

- Prerequisites for your CR include the PTA, ISSO approval, product owner approval, OAST approval
- Present your CR at your component CCB
- Present your CR at the Enterprise CCB if need be (ICCB information here)

□ **Milestone 12: Complete Production CR**

Step 3: Get licenses for Android and iOS deployments

- Apple
  - **Apple Developer Enterprise Program License** - This license is used to create proprietary apps designed and distributed exclusively to your organization's employees.
  - **Apple Developer Program License** - This license is used by organizations for creating apps for distribution on the App Store for iPhone, iPad, Mac, and Apple Watch.
- Android
  - **Google Play Publisher License** - This license is used to publish apps on the Google Play store.

Step 4: Digitally “Sign” your application for deployment

- Learn about iOS app signing here
- Learn about Android app signing here

Step 5: Complete Go Live checklist

- Did you perform all necessary actions throughout this Playbook and hit all of your Milestones? Complete the Go Live checklist to make sure

❑ **Milestone 13: Complete Go Live Checklist**

Step 6: Deploy the mobile application – Soft Launch

- The intent of a soft launch is to release your application to a controlled set of users, or to release it without a press release or public announcement. This method provides time for review and live testing of the production application.
- Ensure that you have an approved CR for your release
- Tell a few of your users and stakeholders about your release, and let them try it out
    - iTunes or Google Play - There is typically a delay between the date of release and the appearance of the application in the respective store:
        - iTunes: 10-14 days for a new application, 3-7 for an update
        - Google: 12hrs to 1 day for a new application or an update
    - For internal/sensitive mobile applications, inquire with your organizations Mobile App Store provider and your Mobile Device Management (MDM) provider to learn about options for distributing to a small user group for your soft launch

❑ **Milestone 14: Conduct Soft Launch Go Live**

Step 7: Deploy Go Live

- Ensure that your Soft Launch was successful and that the application worked correctly in the production environment
- For public facing applications, point your users to the newly deployed application in the app store
- For internal/sensitive mobile applications, inquire with your organizations Mobile App Store provider and your Mobile Device Management (MDM) provider to learn about opening the Soft Launch to all intended

❑ **Milestone 15: Conduct Production Go Live**

Step 8: Announce your release

- Communicate the release of your application

- ○ Consider a press release (public or internal depending on your app)
- ○ Claim the success for your work

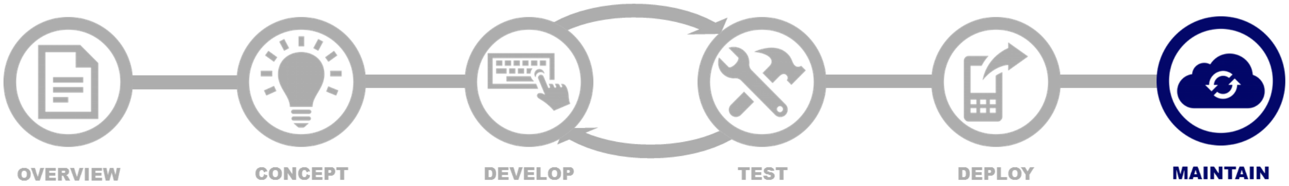
Checklist

□ Distribute test results
□ Get licenses for iOS and Android
□ Complete Go Live checklist
□ Deploy Go Live
□ Present your CR
□ Sign your app for deployment
□ Deploy Soft Launch
□ Announce your release

Resources

✓ **ICCB information here**
✓ **Learn about Android app signing**
✓ **Learn about iOS app signing**
✓ **Complete the Go Live checklist**

Maintain



The Maintain phase includes steps for monitoring your application, communicating with your users, understanding how platform changes affect your app, and planning for sun setting and decommissioning.

Key Steps

Step 1: Setup and perform monitoring

- Monitor your application and gather analytics such as user downloads for each platform and number of crashes
- Monitor your back-end systems
    - Server traffic
    - Server utilization
    - Server performance

Step 2: Capture feedback from users

- Solicit feedback from users on a regular basis
- Consider a survey tool, or reach out directly if you know your user base

Step 3: Monitor and respond to platform/framework updates

- Pay attention to updates that could affect your application:
    - New releases on the platform (iOS/Android)
        - Monitor iOS news pages to learn more about Apple developer news and try Beta versions of OS
        - Monitor Android developer resources to learn more about upcoming changes
    - New hardware releases
    - Sun setting of hardware or software
- Perform testing on all new software or hardware releases

Step 4: Monitor and respond to new vulnerabilities

- Pay attention to any new listed vulnerabilities

- Consider following organizations such as OWASP
- Request re-scans from the Carwash Team to ensure your application's security posture has not changed

Step 5: Monitor and respond to bug fixes and modifications

- Provide the ability for users to submit bugs and feature request
- Monitor, respond to, and prioritize user submissions

Step 6: Communicate changes with users

- Inform your user of content changes
- Inform users of any upcoming releases or modifications to the applications

Step 7: Sunset/decommission plan

- Develop communication strategy to inform all necessary stakeholders
- Communicate to any necessary users and stakeholders
- Remove your application from the production environment

Checklist

□ Setup and perform monitoring
□ Respond to platform updates
□ Communicate changes with users
□ Capture feedback from users
□ Monitor vulnerabilities, updates, and bug fixes
□ Sunset your application

Resources

✓ **iOS news pages**
✓ **OWASP**
✓ **Android developer resources**
✓ TBD

Appendix I: MAP Checklist

Action Items	Yes	No	Comments
1. Conduct Kick-off Meeting with Security and document milestones (when scans required, risk acceptance, FISMA, etc.)			
2. Conduct Kick-off Meeting with OAST/ 508 Team and document milestones (building 508 in, testing, etc.)			
3. Conduct Kick-off Meeting with Privacy Team and document milestones (document required identified)			
4. Develop Use Cases			
5. Gain Access to the ALM tools			
6. Onboard onto Carwash			
7. Create Systems Architecture			
8. Populate your backlog			
9. Identify technology dependencies			
10. Design UI/UX			
11. UI/UX Design Acceptance			
12. Setup your developer tool kits			
13. Create story boards and screens			
14. Upload to a source code repository			
15. Prepare testing/staging environment			
16. Preform debugging			
17. Package your app (ipa/APK)			
18. Finalize test conditions/cases			
19. Create automated tests			
20. Identify test groups for distribution			
21. Prepare for test group access (setup user accounts, access to devices)			
22. Provide instructions to test groups			
23. Distribute mobile application			
24. Check-in with test groups			
25. Evaluate results and determine actions			
26. Complete DHS Carwash Scan			
27. Complete User Acceptance Testing (UAT)			
28. Complete 508 Test			
29. Complete Privacy Threshold Analysis (PTA) *if production ready			

Action Items	Yes	No	Comments
30. Distribute test results (PTA, Security Team, ISSO, Product/ System Owner)			
31. Present your Change Request to the CCB			
32. Get licenses for iOS and Android			
33. Sign your app for deployment			
34. Complete go live checklist			
35. Deploy soft launch			
36. Deploy go live			
37. Announce your release			

Appendix II: List of Resources

- OAST Home Page
- Privacy Office Home Page
- Access the DHS Carwash Page in the DHS IT Services & Hardware Catalog
- Access to the Carwash User Guide from a DHS Network
- Access to the Carwash User Guide for Users with OMB Max accounts
- DHS Agile Center of Excellence
- DHS Agile Guidebook
- DHS Agile Instruction
- Android Design Center
- Apple Developer Support
- Android Accessibility Developer Tools
- iOS Accessibility Developer Tools
- Crashlytics
- Using Crashlytics for UAT
- ICCB Information
- iOS App Signing
- Android App Signing
- Go Live checklist
- iOS News
- Android News
- OWASP
- Link to Enterprise Architecture SharePoint Page
- Link to OAST On-line Classes
- Link to OAST Contract Analyzer

Appendix III: Carwash Overview

OCTO provides a core set of Application Lifecycle Management tools and application scanning tools that are tailored to meet the needs of mobile application development efforts.

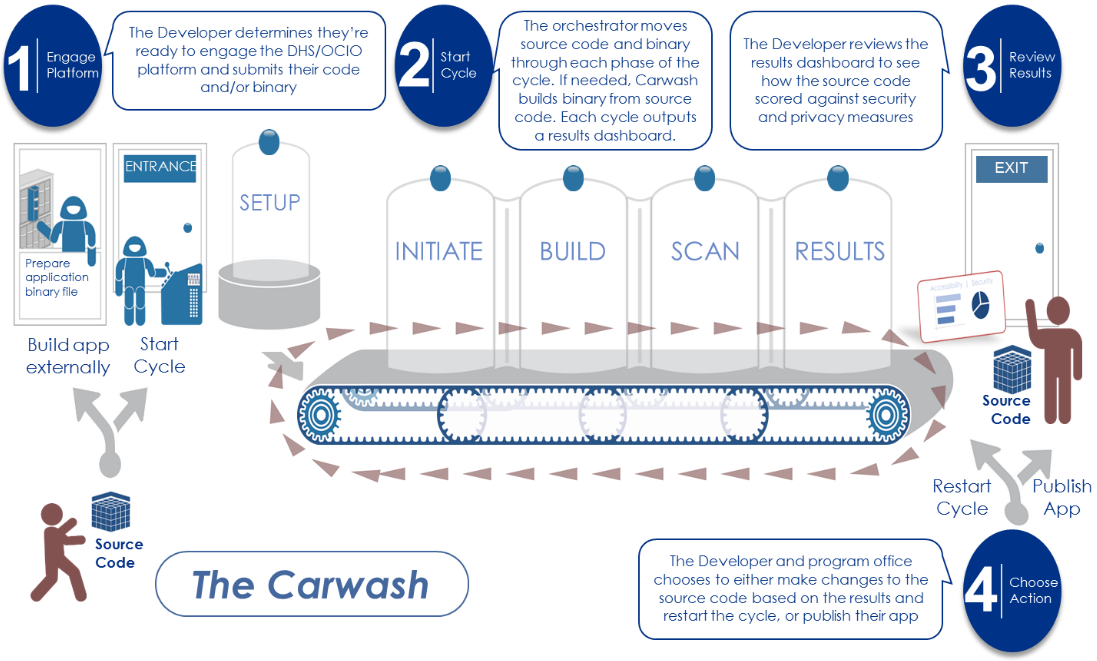
Carwash Wiki

General Toolsets

- Issues (Jira) – A full-featured issue and risk tracking system
- Content (Confluence) – A wiki-like team collaboration and publishing space
- Source (Stash) – Project source code repositories, and shared repositories for the storage of in-development efforts
- Automate (Bamboo)– A continuous integration (CI) orchestrator to support build, test, and deploy
- Mobile Content Management & Engagement Platform
- Open source and GOTs/COTs Scanning Tools

Carwash Scanning Process

OCTO tenants can view in-depth reports generated by each of the mobile scanners.



1 Engage Platform

The Developer determines they're ready to engage the DHS/OCIO platform and submits their code and/or binary

2 Start Cycle

The orchestrator moves source code and binary through each phase of the cycle. If needed, Carwash builds binary from source code. Each cycle outputs a results dashboard.

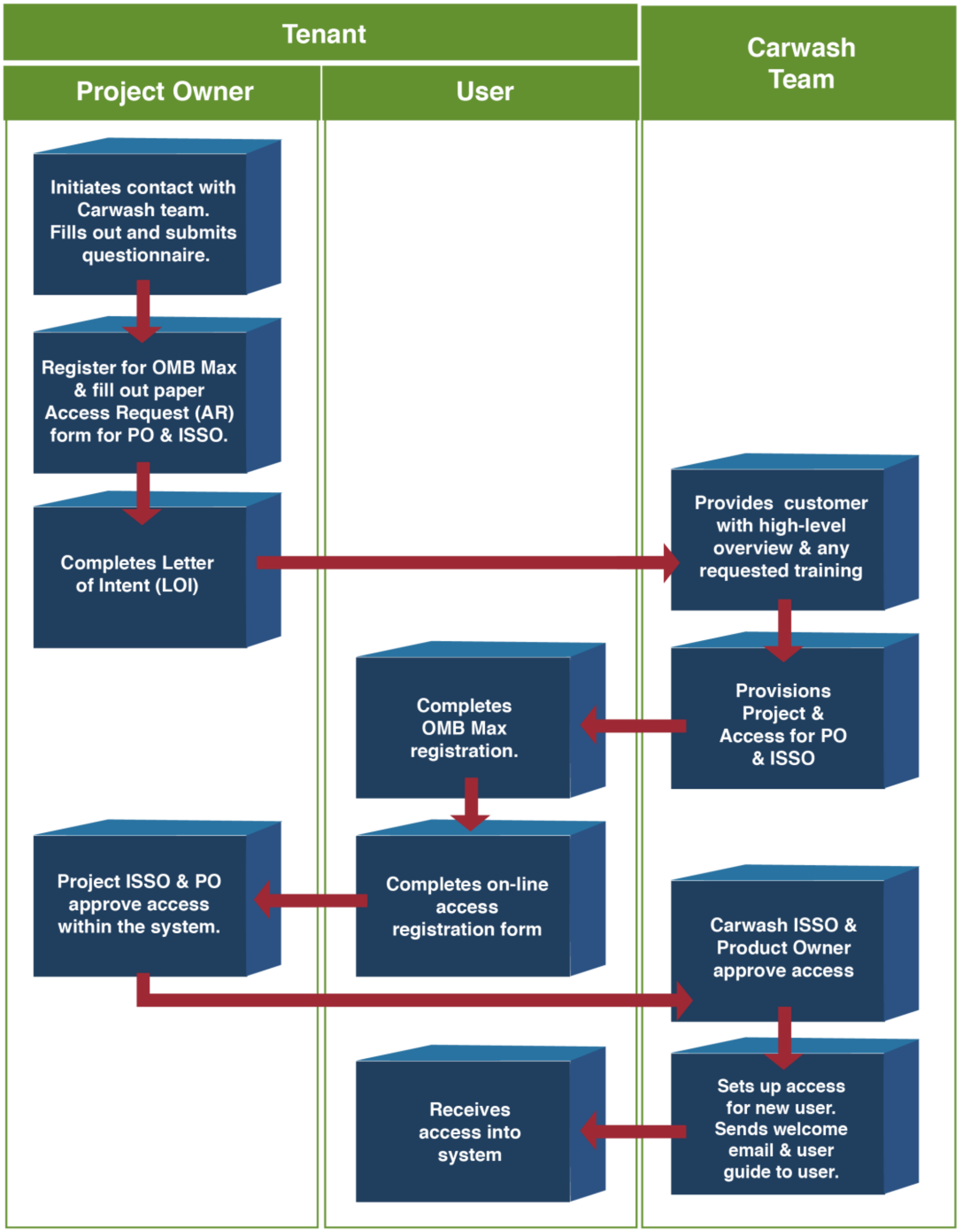
The Developer reviews the results dashboard to see how the source code scored against security and privacy measures

3 Review Results

The Developer and program office chooses to either make changes to the source code based on the results and restart the cycle, or publish their app

4 Choose Action

Carwash On-boarding


Tenant
Project Owner
User
Carwash Team
Initiates contact with Carwash team. Fills out and submits questionnaire.
Register for OMB Max & fill out paper Access Request (AR) form for PO & ISSO.
Completes Letter of Intent (LOI)
Provides customer with high-level overview & any requested training
Provisions Project & Access for PO & ISSO
Completes OMB Max registration.
Completes on-line access registration form
Project ISSO & PO approve access within the system.
Carwash ISSO & Product Owner approve access
Sets up access for new user. Sends welcome email & user guide to user.
Receives access into system

Appendix IV: UAT Distribution – Using Crashlytics

The DHS Office of the Chief Technology Officer (OCTO) uses the following approach to deploy mobile application to user groups for user acceptance testing purposes. This approach will be used until a Mobile Device Management (MDM) or Mobile Application Management (MAM) solution is available to distribute the application to the user's devices.

The steps below document the list of application distribution tasks to implement in order to distribute the application to the user acceptance test team.

Step 1: Create an enterprise distribution certificate for the app
Enable the application to be signed using the valid Enterprise License purchased from the respective application store. Create an enterprise distribution certificate for the OCTO app (Choose Enterprise distribution, NOT Ad-Hoc).

- Sign into the apple web site
- Create a bundle identifier (for example: gov.OCTO.mobile.OCTOapp)
- Create a license distribution cert: (there are directions on the developer site for this)

Step 2: Add an admin developer to the license to distribute the application

- Sign into the respective vendors public application store site
- Add the email address for the license under team members section of the vendors site

Step 3: Add the distribution certificate to the application

- Go into X-Code (the IOS developers platform, or go to the Android equivalent)
- Add the certificate

Step 4: Build the app for Archive

- Enable the application to be executed using the certificate.
- Go into X-Code (the IOS developers platform, or go to the Android equivalent)
- Build the app for archive

Step 5: Distribute the application using a free cloud-based service called Crashlytics.

- Sign up for the Crashlytics service by going to https://try.crashlytics.com
- Sign up for the Crashlytics service using the email from step 1
- Upload the app to the Crashlytics service

Step 6: Add pilot users to the application distribution list in the Crashlytics service

- In the Crashlytics pulldown, click the import CSV button to add users

Step 7: Push the app out to the users

- Logon to the Crashlytics site using the email address associated with the developers license
- Follow the prompts to push the application out to the list of users
- The pilot user will receive an email with a link that enables them to accept the profile and install the app
- When the user accepts the profile on their machine by clicking on a button within the email, the application will be installed on the device

Appendix V: 508 Lessons Learned

Adherence to the guidelines of the Section 508 team is best done as part of a multi-phase approach-taking place during the entire development process. To minimize the costs of compliance the following document will lay out the steps to be taken in the process of app development.

Before Development

- Request and receive the Section 508 acceptance criteria. This list should be inclusive of all required criteria for acceptance collated into one list.
- These criteria should be reviewed by all development team members including, but not limited to: Graphic Design, Development, and Quality Assurance.
- Criteria should be used during the wire framing and concept art stage to assure all graphic assets are in compliance.
- Development staff should review the compliance matrix and ensure items such as VoiceOver notifications are part of the development estimate.
- Have the 508 team review the designs to avoid expensive rework during later testing phases.

During Development

- Development staff should use compliance matrix such that items such as Voice-Over notifications developed on-line.
- Graphic Arts staff should produce ALL graphic assets necessary to complete the visual design in line with 508 approved designs.

Pre-Release

- Quality Assurance Staff should test the compliance of the app using the same technology as the 508 offices, and review the app for compliance to the initial matrix. Defects should be logged via the developer's defect tracking process.
- Development staff should close open issues in a timely manner.

Link to OAST On-line Classes

Link to OAST Contract Analyzer

Appendix VI: Development/Deployment Options

The DHS environment is complex, and one-size fits all approach does not meet the needs of every component. Mobile development and implementation must be flexible but adhere to some standards and guidance to ensure success. There are a number of different paths to success, with varying degrees of OCTO support. As an organization, you can either choose to do everything yourself, or engage with OCTO to see how they can support your need.

Options	Description
Do it yourself	The "Do it yourself" option leverages OCIO's experience encapsulated in the MAP to help your organization deliver its mobile application. OCIO provides the instructions - the playbook, and access to tools such as ALMSS/Carwash. Your organization plans, delivers, and operates the application. What you get: • Playbook • Access to Tools & Platforms (Carwash/ALMSS) • Consultation regarding best practices and lessons learned
Outsourced to OCTO	Outsource the work to OCTO. Pay OCTO to do it all. OCTO plans, delivers, and operates the application. What you get: • End-to-End Implementation of your mobile application to include application development, platform, and infrastructure hosting • Playbook • Access to Tools, Platforms & Hosting • Consultation regarding best practices and lessons learned

Appendix VII: Contacts

Name	Organization	Email	Phone
Office of the Chief Technology Officer Team	OCTO	DHSOCTO@hq.dhs.gov.	N/A
Doug Hansen	OCTO	Doug.Hansen@HQ.DHS.GOV	202-447-0790
Carwash Team	OCTO	Carwash@hq.dhs.gov	N/A
OAST Team		accessibility@dhs.gov	N/A
EA COE Team		EACOE.Facilitator@HQ.DHS.GOV	
Vincent Sritapan	S&T- MDS	Vincent.sritapan.hq.dhs.gov	540-604-9509

Appendix VIII: DHS S&T Mobile Device Security (MDS) Overview

Within DHS, OCTO works collaboratively with the Mobile Device Security (MDS) Program within the Science and Technology Directorate (S&T) to identify and respond to the evolving threats and security challenges in the mobile space.

Vision of MDS

The Department of Homeland Security (DHS) workforce has become increasingly mobile, driving the need for secure mobility solutions and a coordinated approach and framework to guide the selection and implementation of common enterprise mobility solutions. To promote the safe and secure adoption of mobile technology in DHS and the federal government, the DHS Science and Technology Directorate (S&T) Cyber Security Division (CSD) within the Homeland Security Advanced Research Project Agency (HSARPA) created the Mobile Device Security (MDS) Program, *and adopted the following vision to guide its research efforts:*

Context

Mobile Technology, recognized as a cornerstone of the 2012 White House Federal Digital Government Strategy (DGS), seeks to enable "access to quality digital government information and services anywhere, anytime, on any device." The DGS acknowledges new and unique security and privacy challenges must be met to accelerate the adoption of mobile technology into the federal government. In addressing DGS challenges, interagency efforts resulted in development of security requirements for mobile computing and identification of major barriers and gaps that impede mobile adoption. The mobile challenge areas identified were Mobile Device Management, Mobile Application Management, Identity and Access Management, and Data Protection. Though progress has been made in these areas, more needs to be done to address current and especially emerging challenges. Two factors conspire to create the urgent need for secure enterprise solutions. First, the use of mobile solutions is rapidly increasing across the Department and the federal government. Secondly, mobile threats present an increasingly common and more sophisticated threat to data stored or processed on DHS devices. Threats to mobile devices, applications, and data have grown dramatically in the past few years. A recent analysis of threats1 highlighted several key developments, including the following. Elements of a Mature Mobile Ecosystem

- Malware grew substantially in the U.S., driven by an increase in threats holding devices and data hostage in exchange for payment (ransomware).
- Mobile threat sophistication is increasing. Certain malware has even entered the marketplace pre-installed on certain devices, indicating a compromised supply

chain. Malware self-defense mechanisms are also gaining sophistication, evading attempts to detect and defeat the application.

- A mature mobile ecosystem comprises many elements, as shown below. Each of these areas presents security challenges and opportunities for additional study and mobile security research and development (R&D).

Objectives of MDS

To respond to the evolving threats and security challenges in the mobile space, S&T CSD has developed and will transition programs directed at several strategic objectives and initiatives. Through this work, S&T will ensure DHS is poised to bridge current capability gaps and deploy solutions that effectively, efficiently, and securely enable the mission of the Department. The MDS Program has established three overarching objectives as it seeks to achieve the program vision:

Link to Additional Resources on MDS

Appendix IX: The Challenges of Mobile Government

As more and more citizens and Federal employees are adopting mobile devices the demand to develop 'mobile first' applications is at an all-time high. However choosing to go mobile can also bring about several unique challenges that Federal Agencies haven't had before including:

- **Security** – Security presents unique challenges due to proprietary business data on mobile devices. As a result, user authentication and both data at rest and data in motion must be highly secure and protected.
- **Privacy** –For public facing applications, privacy advocates are particularly concerned with the use of location settings, which could be used by the Government to find the location of mobile users.
- **Accessibility** – Federal mobile applications may be subject to one or more accessibility standards such as Section 508.
- **Reliability of Mobile Networks** – Mobile Networks do not have guaranteed reliability and can be slower in providing the required connection. As a result, mobile apps must handle a variety of technology issues to include limited bandwidth, offline behavior, and memory management and device recognition.
- **Standardization** – The lack of mobile platform standardization due to the large market of devices and hardware/software solutions makes the architectural decision-making process more difficult. IT departments frequently support more than one device platform Examples include the following:
    - Device type - tablet, smartphone, or wearable
    - Operating system - IOS, Android, Windows Mobile, Blackberry
    - OS Version / application type - native, HTML 5 or hybrid
- **New Types of Data** – Mobile applications have capabilities to capture and transmit new types of data that have traditionally not been considered by federal IT. This data includes but is not limited to location, voice, image, and video data – in additional to traditional text data.
- **Content & User Experience Management** – With increasing demands for dynamic rich content and user experiences, hybrid mobile applications and mobile content management platforms are becoming increasingly popular.
- **Software Distribution** – Frequent OS changes and updates result in more frequent application updates. Dynamic updating of applications is important, given the frequency of device software changes.
- **Lack of Technical Resources** –Due to the diversity of hardware and software platforms, organizations are pressed to find skilled developers to comply with the heterogeneous mobile app landscape and the unique requirements of the public sector.

- **Deployment & Infrastructure Challenges** – Applications for the general public are simply delivered to the public app stores, but deployment to restricted internal user groups are more complicated and require the use of Mobile Device Management (MDM) and Mobile App Management (MAM) (private app stores) technology and infrastructure.
- **Diverse Use Cases** – Mobile applications enable a variety of scenarios not contemplated by traditional personal computing users.   There is a gap in what capabilities a mobile-friendly website provides (through a mobile-browser only experience) and the experience in a mobile application.

It is imperative that an organization understand the challenges of choosing to go mobile. These challenges can be address but need to be accounted for initially to ensure effective and efficient planning

Appendix X: MAP Benefits

The MAP will help you accelerate your time to market, reduce costs, and reduce risks when delivering mobile applications. The MAP achieves these benefits by enabling customers building mobile applications to:

1. **Effectively Navigate the DHS Organization** – Complete your project on time, and on-budget. DHS is a complex organization and significant collaboration and cooperation is required to successfully complete a project. You must ensure that all of the appropriate organizations are aligned to deliver your mobile application, including, Security, Privacy, Office of Accessible Systems & Technology, Information Technology, and Enterprise Architecture.
2. **Comply with DHS Policies and Procedures** – Prevent your project from being stopped by an inadvertent misunderstanding of DHS policy or DHS organizational requirements. The Playbook helps you understand your organizational responsibilities at the start of the project, and ensures that your mobile application meets applicable federal and organization standards.
3. **Access Proven Tools and Methodologies** – Your mobile application development team benefits from using tools and methodologies that are proven to work within the DHS environment (ALMSS/Carwash).
4. **Build and Deploy to the Correct Environment** – Business lines should think to leverage work already performed to establish a full production environment for developing and deploying mobile Apps. These environments can include a mobile distribution lifecycle, and mobile content management solution with a full authority to operate, thereby reducing the number of steps required by project teams to complete security related activities associated with the Federal Information Security Management Act (FISMA). A DHS environment with an Authority to Operate (ATO) significantly reduces the number of compliance activities required on the part of project teams to deliver mobile applications. And reduces the overall time required to deploy.
5. **Use Best Practices and Lessons Learned** – Leverage best practices and lessons learned – Your mobile application development team will understand what has worked successfully in the past, provides ability to learn from the mistakes of the past, and benefit from the experiences of others who have delivered mobile applications within the DHS environment. See 508 Lessons Learned.
6. **Access Knowledgeable Staff** – Your mobile application development team has the opportunity to interact with and learn from OCTO staff, which has successfully delivered enterprise mobile applications within the DHS environment.

Appendix XI: References

Adrian Mettler, Y. Z. (2014, August). *SSL Vulnerabilities: Who listens when Android applications talk?* Retrieved from FireEye: https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html

Boren, Z. D. (2014, October 7). *There are officially more mobile devices than people in the world.* Retrieved from Independent: http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html

comScore. (2015, February 9). *comScore Reports December 2014 U.S. Smartphone Subscriber Market Share.* Retrieved from comScore: https://www.comscore.com/Insights/Market-Rankings/comScore-Reports-December-2014-US-Smartphone-Subscriber-Market-Share

Google. (2015, August). *Smartphone Users.* Google Consumer Surveys.

GSMA Intelligence. (2015, 10 21). *Global Data*. Retrieved from GSA Intelligence: https://gsmaintelligence.com/

Lawson, M. (2015, September). *Win Every MicroMoment with a Better Mobile Strategy.* Retrieved from Thing with Google: https://www.thinkwithgoogle.com/articles/win-every-micromoment-with-better-mobile-strategy.html

Meeker, M. (2013, May 29). *2013 Internet Trends Report*. Retrieved from Kleiner Perkins Caufield & Byers: http://www.kpcb.com/blog/2013-internet-trends

Smith, A. (2015, April 1). *U.S. Smartphone Use in 2015.* Retrieved from PewResearchCenter: http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/