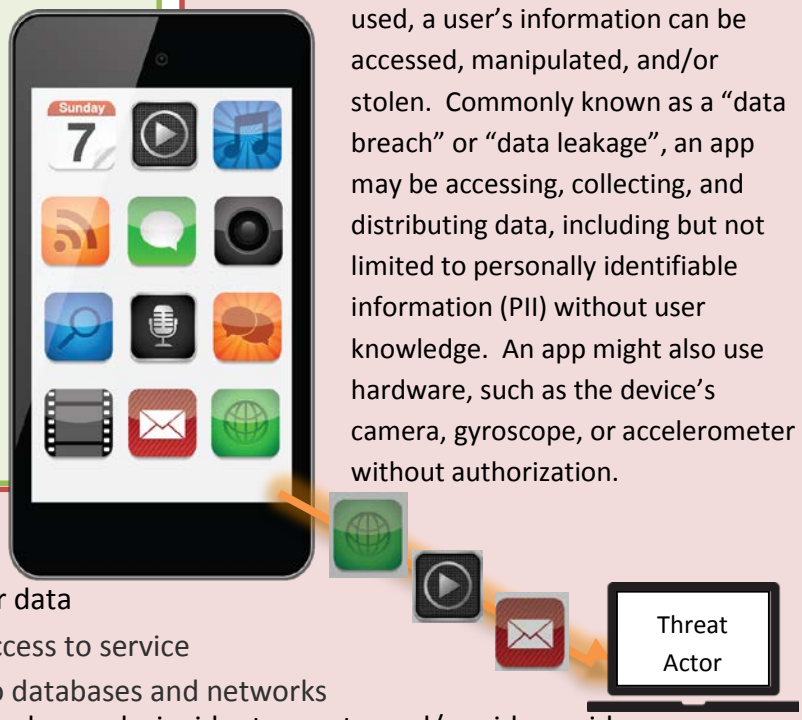
Homeland Security

Office of Emergency Communications

MOBILE APPLICATION ADOPTION BEST PRACTICES

As a first responder, you may be using mobile applications for daily operations or during emergencies. Next-generation mobile applications, also known as "apps", are enhancing responder safety, informing incident management, enabling mobility, and improving productivity. Yet, the current app ecosystem poses substantial risks to you, your data, and the network you and your colleagues rely upon to communicate.

Do You Know About…



….Mobile Application Risks?

Regardless of the mobile device and app being used, a user's information can be accessed, manipulated, and/or stolen. Commonly known as a "data breach" or "data leakage", an app may be accessing, collecting, and distributing data, including but not limited to personally identifiable information (PII) without user knowledge. An app might also use hardware, such as the device's camera, gyroscope, or accelerometer without authorization.

- hijack other applications
- steal, broadcast, and/or alter data
- deny the authorized users access to service
- allow unauthorized access to databases and networks
- access medical data, personnel records, incident reports, and/or video evidence
- report on sensitive information of the user, such as location information, to a third party
- violate or disrupt the confidentiality, integrity, and availability of all other legitimate apps through shared memory or other methods

An app with too much access to information and device function can be harmful, but an app with too little access can be less useful. This document and its appendix introduce an approach to balance app risks with app benefits and provide basic best practices and sample questions to consider during app adoption in the public safety community in the absence of formal network controls.

Please note: Apps present significant operation, security, interoperability, and performance risks. This document provides basic best practices for maintaining app security in the public safety community. These actions are designed specifically for you, the user, and should be used in conjunction with any policies that your agency has established. Not all actions may be possible based on your agency policies and/or network configuration. However, this guidance should be used in conjunction with or deferred in the case of more formal mobile application management functions and processes provided by your organization.

For more information on mobile device or mobile application adoption, please visit dhs.gov/maps.

Homeland Security

Office of Emergency Communications

Define Benefits and Seek Approval

Determine if Desired Function and Operation Will be Achieved

The app should work well with existing operational processes and procedures, using familiar data types and terminology. In addition, the app should retain data that meets both operational needs and any necessary evidentiary standards. The app should use universally familiar actions and provide technical support, in-app help, and/or support documentation. Conveniences such as easy installation, launch, operation and maintenance should also be considered when selecting an app.

Determine if the Application Will Meet Operational Demands

Evaluating the description by the developer, including screenshots or video demonstrations, may provide a better sense of the function of the app. Reading reviews from other users, especially other first responders, can provide a sense of usefulness, responsiveness, reliability, accuracy and ease of use. When looking at the reviews it is important to determine the version of the app reviewed, as functionality may change as the app is updated. Review available documentation to ensure the app will work on the intended device, i.e., proper operating system, processor speed, media capacity, wireless bandwidth, etc. It may also be important to ensure the app will wait long enough for network response in times of congestion.

Seek Leadership Approval

Every mobile app introduces risk into an operational and network environment, and checking with leadership, command staff, and/or information technology (IT) staff on the use of any device and/or app is important.* Regardless of whether or not the equipment in use is government or personally-owned, there may be certain limitations on the cost, type, or number of apps allowed for use. In addition, there may be a mobile enterprise strategy in place or certification requirements for apps that will need to be satisfied.

Avoid Security Threats

Limit Data Input and Output

Knowing what type of data could be compromised if the app is malicious or vulnerable to attack can assist with the decision to adopt the app. It is important to understand if an app can inadvertently send data to non-authorized places. Do not store or transmit sensitive information on any app that has not been approved for use by leadership, staff, and/or IT department.

Allow Only Authorized Users

Many apps rely on the device for user authentication, so devices should employ a personal identification number (PIN) or password to unlock the device, automatically lock after a period of inactivity, and (if available) have authorized security software installed to allow for device tracking and the remote deletion of data.

Download From a Trusted Source

Many sources exist for downloading apps, but only trusted sources should be used. Ideally, apps should be acquired from sources that have performed public safety-specific security and/or performance vetting. At a minimum, do not download apps that require "sideloading" to be turned on in the device settings, or require the device to be jailbroken or rooted unless authorized by the department/agency.

Read and Understand Permissions

When downloading an app, the app must request permission to access specific capabilities or information (known as "permissions"). Before clicking "I agree", be sure to review all permissions to be granted for legitimacy and necessity. Many permissions allow access to personal and location information. In some instances, the permissions may not be necessary for the core functionality desired and can be turned off using the privacy and permission settings of the device operating system.

Maintain Performance

Test the Application

Check the availability, reliability, responsiveness, resiliency, scalability, and accuracy of the app before using in a response and operations environment. Testing the app may include reviewing documentation, assessing operation under various circumstances (e.g., roaming, no network connectivity, large scale events, group use), and evaluating results against known values.

Update Regularly

Updating the app regularly is important, as many apps update not only for convenience but to avoid known performance and security issues. However, before accepting an update, be sure to determine if any permissions have been changed, such as access to location information or PII. Also, when upgrading to a new device, ensure the app is updated correctly during transition.

Reduce Clutter & Distractions

Adding an app to a device uses valuable, limited resources–the screen, battery life, storage, and processing power–even wireless bandwidth availability. Regular evaluation of the number/types of apps on a device is recommended. Deleting an app can reduce clutter and save resources dedicated to its maintenance. In some instances, the use of folders or other organizational systems can limit clutter on the interface. In other instances, app attributes, such as permission to run updates in the background or providing home screen notifications, could be limited.

Report Unexpected Behavior

Apps that have been compromised can respond in unexpected ways. Suddenly closing (crashing), freezing the screen, draining battery and/or processing power, disappearing after installation, appearing without user-specified installation, or failing to launch are some examples of suspicious behaviors. In the case of a suspect app, reporting those suspicions to the source of the app and department/agency network administrator is important.

* For more information on mobile device adoption, please visit dhs.gov/maps for the "Mobile Device Adoption Best Practices Guide"

Homeland Security

Office of Emergency Communications

MOBILE APPLICATION ADOPTION BEST PRACTICES: APPENDIX A – SAMPLE QUESTIONS

App evaluation can be challenging. These sample questions can assist with app selection, but a comprehensive mobile application management strategy is recommended for mission-critical use of apps. Some of the more advanced questions may require technical assistance or more advanced testing to answer, but are provided as part of the sample questions as considerations during research of an app.

Define Benefits and Seek Approval

Determine if Desired Function and Operation Will be Achieved	▪ Does the app provide timely, actionable information in an intuitive fashion? ▪ Does the app provide information using familiar data types and terminology? ▪ Will the app be easy to install, launch, operate, and maintain? ▪ Does the app support universally familiar actions (e.g., swipe, "trash can" = delete)? ▪ Does the app provide technical support and/or support documentation if needed? ▪ Will the app require extensive training for use? ▪ Does the app require changes in current operations/procedures in order to be adopted? ▪ [Advanced] Is the app Section 508 compliant (http://www.section508.gov/)? ▪ [Advanced] Does the app have the necessary logging/auditing features and automatic tamper-resistant relevant tagging to support non-repudiation?
Determine if the Application Will Meet Operational Demands	▪ Are the majority of reviews favorable? ▪ Has the app had regular maintenance and updates? ▪ Is the developer legitimate and reputable? ▪ [Advanced] Does the app's data come from trusted, reliable, regularly updated sources?
Seek Leadership Approval	▪ Does leadership agree with the use of the app? ▪ Does the app violate any stated information security policies? ▪ Are there limitations on when or how the app can be used? ▪ Is there formal guidance or other requirements available that must be followed?

Avoid Security Threats

Limit Data Input and Output	▪ If the device was lost, stolen or shared – what information would be vulnerable? ▪ Does the app allow users to inadvertently send data to non-authorized places? ▪ Does app data handling meet local and/or State guidelines on data transmission? ▪ Can the device or network impede unauthorized access or allow for the disablement of the app if corrupted? ▪ [Advanced] Does that app use industry-recognized, sufficient cryptography?

Allow Only Authorized Users	▪ Are device protections sufficient for data protection (e.g., PIN/password/gesture to unlock the device, automatically locking after a period of inactivity, mobile security software installed that allows for device tracking and the remote deletion of data)? ▪ Is a PIN or password required by the app? ▪ If roles change during the course of an event, can the app adapt accordingly? ▪ [Advanced] Is the app providing information only to authorized users?
Download from a Trusted Source	▪ Does the app come from a trusted source? ▪ [Advanced] Has the app been vetted or certified for security and/or performance?
Read and Understand Permissions	▪ What permissions are requested by the application? ▪ What permissions are necessary? ▪ Will the permissions put the user or data at risk if compromised?

Maintain Performance

Test the Application	▪ Is the app reliably responsive? ▪ Can a call or other data session be made or received during app operation? ▪ Does the app work well with existing operating procedures? ▪ Does the app retain the data necessary and in a way that can be easily used? ▪ Does the app need to be exited at any point to use other functions or access information? ▪ Will the app be available when needed (e.g., roaming, no network connectivity)? ▪ Does the information accuracy meet the need (e.g., are GPS coordinates correct? is the data coming from regularly updated, accurate databases?) ▪ [Advanced] Does the data meet any necessary evidentiary standards? ▪ [Advanced] Does the app have any known vulnerabilities or weaknesses? ▪ [Advanced] Does the app perform well under all circumstances (e.g., poor lighting, large scale event)?
Update Regularly	▪ Is there notification of an app update being available? ▪ When updates are required, what kind of connectivity is necessary? ▪ [Advanced] Does the app have any known vulnerabilities or weaknesses? ▪ [Advanced] Are updates mandated to continue use of application? If so, how quickly?
Reduce Clutter	▪ Are the number of apps on the device cluttering the interface, draining battery power, or limiting storage and processing power? ▪ Which apps are most valuable – are they placed prominently for easy access? ▪ Which apps are least valuable – should they be removed to conserve resources? ▪ [Advanced] Does the app interfere with or limit the availability of another app or service?
Report Unexpected Behavior	▪ Is there a feedback mechanism to report unexpected behaviors? ▪ Is there technical support available if unexpected behaviors occur? ▪ [Advanced] Can network administrators limit the app if unexpected behaviors occur?