CIO
COUNCIL

Adoption of Commercial Mobile Applications within the Federal Government

Digital Government Strategy Milestone 5.4

May 23, 2013

Contents

I. Executive Summary

Milestone #5.4 of the Digital Government Strategy tasks the Federal CIO Council and Digital Services Advisory Group with developing models for the secure, yet rapid, delivery of commercial mobile applications ("apps") into the Federal environment. This document highlights the current status of adopting commercial mobile applications into agency operations based on discussions with agency representatives in March and April 2013. In addition, it details key findings and recommendations to accelerate secure delivery of mobile applications into the Federal Government. The analysis is focused on deployment of commercial apps to government furnished equipment (GFE). It does not cover deployment of commercial apps to employee owned devices (i.e., Bring your own device [BYOD]).

Among the key findings are:

- Agencies are already progressing and deploying commercial mobile apps across subsets of their employee base, with many agencies already using anywhere from 5 to 20 apps;
- Most agencies are in the early stages of deploying mobile device management (MDM) solutions to support a variety of platforms;
- While there are similarities in the process for reviewing and approving commercial apps across agencies, there is not a standardized process government-wide; and
- Agencies are taking a policy/paper-based approach to managing user behavior with commercial apps.

Throughout the discussions with agencies, there were several consistent challenges. The list below highlights the major challenges identified by agencies, but is not comprehensive of all challenges outlined later in this document.

- It is difficult to control and regulate access to mobile applications on government furnished mobile handheld devices;
- There is significant fragmentation of mobile operating systems, handheld device models, and mobile applications, which all require additional security reviews;
- It is not clear how to handle storage of information in non-government clouds; and
- Unique terms of use for each commercial application can require a high level of government review and negotiation.

To assist agencies in developing an approach for integrating commercial applications into their operations, Section V includes an analysis which outlines common agency activities during the commercial mobile application lifecycle. These activities are plotted in relation to the level of organizational control vs. user flexibility that can be employed by agencies. Typically, a higher risk tolerance corresponds to greater user flexibility, while a lower risk tolerance corresponds to greater organizational control. Agencies must determine their own risk tolerances based on the types of users they have and the information they are processing.

Based on the challenges identified in agency discussions, several recommendations were developed to help rapidly and securely deliver commercial mobile applications into the Federal environment. They are:

- Establish a government-wide catalog for commercial mobile applications that highlights key functionality and characteristics relevant for government use;
- Document best practices regarding commercial mobile application review processes;
- Develop standard government-wide terms of service for commercial mobile applications; and
- Initiate a government-wide cloud storage service.

For each recommendation, a set of notional implementation steps is included in the analysis. Implementation of these recommendations will require sizeable resources and effort. However, leveraging existing commercial mobile applications for government use can yield significant dividends as mobile productivity becomes the "new normal" for government employees.

II. The Mobile Opportunity

Mobile applications (apps) are changing how we work. Federal employees now have access to mobile handheld devices (smartphones and tablets) with extensive functionality and can be productive anytime, anywhere. Mobile apps can be less expensive and easier to review, download, install, and test compared to desktop applications. As of May 2013, there are well over one million commercial mobile apps available, with thousands of software updates happening every day, across all the major mobile platforms (Apple, Android, Windows, Blackberry).

The commercial mobile app marketplace provides a wealth of opportunities that the Federal Government can take advantage of by leveraging existing commercial mobile applications. Similar to the trend in using Commercial Off-the-Shelf Software (COTS) on the desktop, by utilizing existing mobile software that is free or inexpensive, the government and its employees are able to do more with less.

Over the past several years, IT experts have debated whether or not we are coming to the end of the Personal Computer (PC) era. As of the second quarter of 2012, PCs no longer consume the majority of the world's memory chip supply.[1] This is the first time since the invention of the PC in the 1980s that PCs' demand for memory chips is less than 50 percent of the overall market. Much of the new demand for memory chips is coming from mobile and tablet devices. According to market research (Figure 1), growth in smartphones (+46%) and tablets (+78%) has far outpaced laptops (-3%) and desktop PCs (-4%).[2]

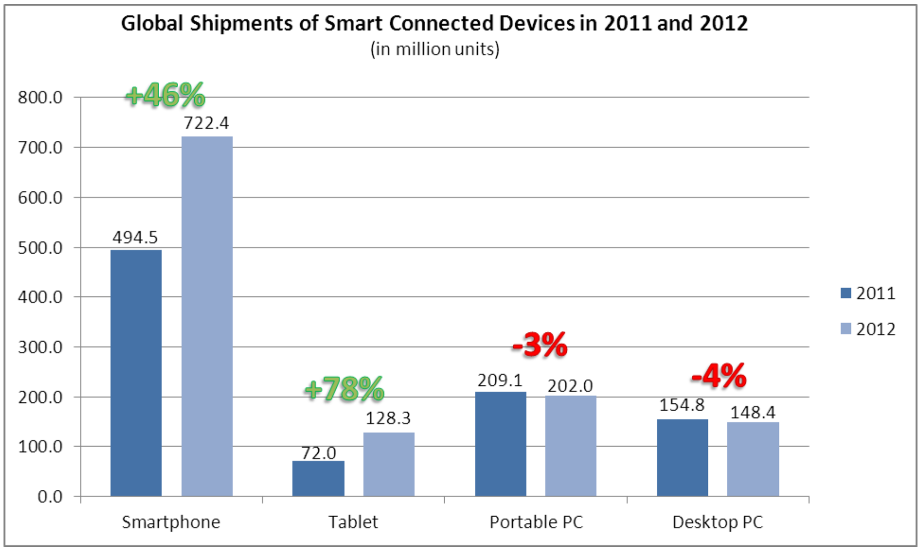


Figure 1: Global Shipments of Smart Connected Devices

As mobile functionality and productivity become the new normal for Federal workers, it is important that government agencies share best practices and adopt unified approaches to discover, approve, procure, install, and manage commercial applications for government furnished equipment in order to truly take advantage of this opportunity.

Just as mobile functionality is sweeping across the consumer and corporate landscape; it is likely that it will come to dominate the public sector as well. Ultimately, it is possible to envision a "screen agnostic" future where the computer/processor is a small device that connects to any sized screen that users can access (e.g., pocket, laptop, desktop, theater). This will be made possible due to exponential increases in

[1] IHS Isuppli Market Research. (2012). *Sign of the Times: PC Share of DRAM Market Dips Below 50 Percent for First Time.* [Press Release]. Retrieved from http://www.isuppli.com/Memory-and-Storage/News/Pages/Sign-of-the-Times-PC-Share-of-DRAM-Market-Dips-Below-50-Percent-for-First-Time.aspx.

[2] International Data Corporation. (2011). *Worldwide Smart Connected Device Market Crossed 1 Billion Shipments in 2012.* [Press Release]. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS24037713.

Source: IDC

processing power, the ubiquity of high-speed wireless networks, and the rise of cloud computing models. There is a unique opportunity for the Federal Government to embrace mobile technologies at an early stage, thereby accelerating adoption, reducing risk, and realizing benefits as soon as possible.

III. The Mobile Difference

While there are many similarities between mobile and desktop applications, it is important to distinguish their differences. Many government agencies already have long-standing and established processes for incorporating commercial desktop software into their operations. Therefore, it is possible that as agencies adopt new lifecycle processes for mobile apps, there may be existing IT infrastructure, business processes, and procedures that can be leveraged government-wide. Enterprise mobile solutions, however, are distinctly different from other enterprise IT strategies and, thus, agencies must approach mobile applications with a fresh perspective.

Table 1 is an overview of the primary differences between mobile and desktop applications, with a particular focus on commercial applications:

	Mobile Experience	Traditional Desktop Experience
User expectations	• Enhanced personalization features make mobile services more useful to consumers (e.g., location based searches) • Consumer mindset is that users want instantaneous software capabilities on mobile handheld devices • Enterprise configuration management is less prevalent in mobile handheld devices, there is a lack of control	• Some personalization features typically not available (e.g., GPS) • Consumers sparingly download new applications to desktops due to price, access constraints, etc. • Enterprise Configuration management is standard, providing strong controls on the users
Ease of installation during discovery of apps	• Easily installed on devices through existing centralized app stores • Harder to control which apps are installed on devices, even with Mobile Device Management (MDM) or Mobile Application Management (MAM)	• No centralized store for all apps across all platforms • Controls on desktop/laptop downloads are well established and mature
Pace of innovation and change	• New uses for mobile apps are being discovered on a daily basis, which is a larger opportunity for mobile developers	• Most applications are offered by large COTS vendors and meet well-established needs
Diversity of Ecosystem (Platforms, devices, OS)	• Significant fragmentation and diversity of handheld devices and operating systems mean there is no standard platform • Android open source operating system has garnered a large share of the market with little standardization	• Relative homogeneity within corporate and government communities
Connectivity to the public cloud and other apps	• More data is stored in the cloud and less data is stored on the device, making data security more of a challenge • Apps frequently integrate and share data with other apps to increase their utility among users	• Most data is typically stored on the device, network drives, and/or on internal collaboration platforms
Procurement	• App store model is prevalent across many platforms. In most cases, billing information (e.g., credit card) is already on file and users can purchase commercial mobile apps with a single click • Mobile apps are typically less expensive • Centralized app stores reduce piracy and protect proprietary content • There is limited enterprise licensing • There are numerous high quality free apps	• Desktop apps licenses are more expensive particularly for professional enterprise applications • There is no dominant centralized desktop app store, and software is procured via the web or hardcopy media • Enterprise licensing is standard practice • Freeware can contain malware

Table 1: Mobile and Desktop Applications Differences

IV. The Federal Mobile Landscape

This section provides an overview of the current Federal mobile landscape, outlines the methodology use to develop this paper, and present key findings and major challenges from the agencies interviewed.

A. Methodology

Interviews with agencies were conducted over a two week period in March 2013 in order to develop an understanding of the current state of efforts to integrate commercial apps into agency operations. There were over 20 interviewees across nine departments and agencies of the Federal Government. Participants included key subject matter experts (SME) and other key stakeholders in offices of the Chief Information Officer, Information Technology, and Mobile Infrastructure.

Agencies interviewed included:

- Alcohol, Tobacco, and Firearms (ATF) (component of DOJ);
- Department of Homeland Security (DHS);
- Department of Defense (DOD);
- Department of Justice U.S. Attorney's Office (component of DOJ);
- Department of Transportation (DOT);
- General Services Administration (GSA);
- U.S. Agency for International Development (USAID);
- Department of Agriculture (USDA);
- Department of Veterans' Affairs (VA).

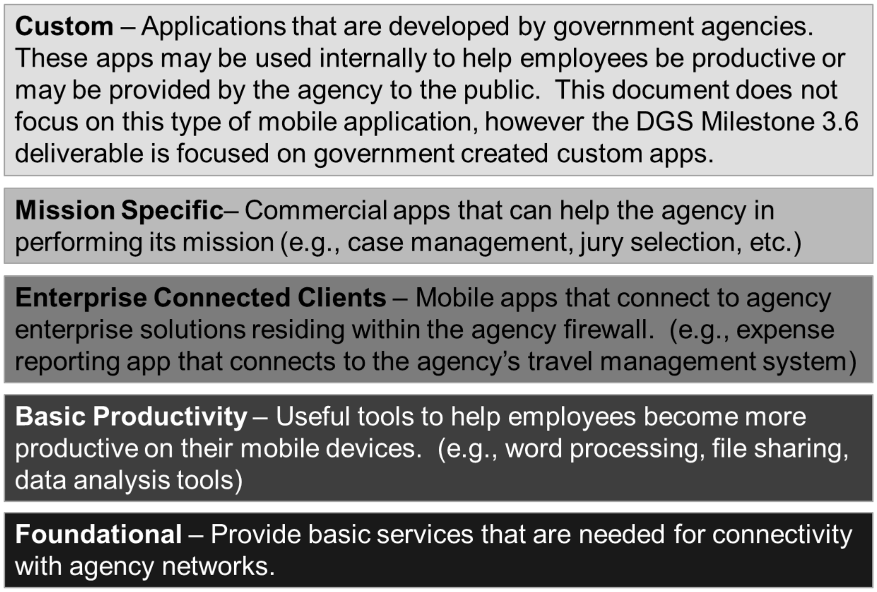
All agencies' interview results were compiled and the data was analyzed to develop composite themes and recommendations.

B. Current State

This section summarizes similarities between Federal agencies' activities to adopt commercial applications into the Federal mobile environment on government furnished equipment (GFE). These findings are based off agency interviews.

1. **Many agencies are already deploying commercial mobile applications:** The majority of agencies interviewed have approved and deployed commercial mobile applications onto GFEs. While there are differences in how apps were deployed and managed, particularly among agencies with different risk profiles, agencies agreed that it is necessary and valuable to leverage commercial apps for government operations. Of the nine agencies interviewed, eight expressed a focus on integrating commercial mobile apps into their operations.
2. **Agencies are working on or have implemented MDM/MAM solutions:** Most agencies are in the early stages of deploying infrastructure for managing mobile handheld devices and applications, including mobile device management (MDM) and mobile application management (MAM) solutions. Many agencies are using 'container' solutions to create a trusted environment by segmenting agency approved apps and data. Containerized solutions allow users to download apps and use them freely outside the container without jeopardizing the integrity of the government apps and data within the trusted environment. Some agencies used common MDM or MAM products; however, there is still significant diversity in the specific products and solutions being employed by the Federal Government in this area.

3. **Applications being deployed fall into several basic categories:** Agencies distinguished among several types of mobile applications (Figure 2) that have been integrated into their environments. The vast majority of commercial apps (up to 90%) that have been integrated into the Federal environment are foundational and basic productivity apps. Mission apps have been integrated to a much lesser extent. Most agencies envisioned integrating as many as 20 to 100 commercial applications into their operations, while one outlying agency saw the need for more.



Custom – Applications that are developed by government agencies. These apps may be used internally to help employees be productive or may be provided by the agency to the public. This document does not focus on this type of mobile application, however the DGS Milestone 3.6 deliverable is focused on government created custom apps.

Mission Specific– Commercial apps that can help the agency in performing its mission (e.g., case management, jury selection, etc.)

Enterprise Connected Clients – Mobile apps that connect to agency enterprise solutions residing within the agency firewall. (e.g., expense reporting app that connects to the agency's travel management system)

Basic Productivity – Useful tools to help employees become more productive on their mobile devices. (e.g., word processing, file sharing, data analysis tools)

Foundational – Provide basic services that are needed for connectivity with agency networks.

Figure 2: Types of Commercial Mobile Apps

4. **While specific processes vary, agencies are taking similar approaches to app approval and review:** Many agencies have set up 'app review committees' with varying levels of formality. While specific criteria differ, these committees are typically made up of a group of agency SMEs who are qualified to make determinations on whether the app should be approved. For example, one agency set up an App Services Council to drive policies and procedures for mobile apps. Another agency has a Technology Control Board that meets on a regular basis and serves as a voting body that accepts new tools once they go through the agency's testing and evaluation processes. In some cases, there are multiple review committees that address different aspects of the review process, such as business requirements, security, and infrastructure. Agencies may take as short as several days to review an app, or as long as several months, depending on the complexity of the analysis conducted. The major questions these committees address include:
   - Is there a legitimate business need for the app?
   - Are there security or privacy risks inherent to the code or the operations of the app itself?
   - Does the app pose threats to existing infrastructure? (e.g. excessive use of bandwidth)
   - Does the app meet 508 accessibility requirements?

5. **Most agencies are taking a policy/paper-based approach to managing user behavior:** While not all agencies have developed methods to review, approve, and manage commercial mobile apps, almost all have existing policies in place to guide user behavior. Policies typically request that users not use any sensitive or classified information on commercial mobile applications. Some agency policies go as far as to request that users not download certain commercial applications on mobile GFE, although in many cases there is no way to enforce this directive unless specific MDM/MAM capabilities have been procured. These capabilities restrict the downloading and/or usage of certain apps and do not exist in all MDM/MAM solutions. As a result, most agency policies are paper based, rather than technical solutions.

C. Common Challenges

The interviews revealed that agencies face a number of common challenges as they work to integrate commercial applications into their operations:

1. **Control and Access - It is difficult to control and regulate access to mobile applications:** The technology to control app distribution and usage across an enterprise is not yet mature enough for use across the Federal Government, and many agencies have not yet adopted a comprehensive solution that balances flexibility and security. Most app stores do not currently allow the capability for an enterprise level “whitelist” or “blacklist”. This leads to problems, such as:
   - **Fraudulent apps:** With hundreds of thousands of commercial apps on the market, there is great opportunity for fraudulent apps to make their way onto GFE. Examples include apps that pose as official government applications, or apps that pose as other, widely used applications.
   - **Malware:** Due to the relative ease with which government users can download mobile apps onto GFE, the risk of malware greatly increases, especially on app stores that have fewer or no built-in checkpoints. This can lead to information compromise, data leakage, and identity theft, among other risks.
   - **Inappropriate apps:** The relative ease of downloading mobile apps on GFE inevitably leads to the installation of apps that are not appropriate for government use.
   - **Excessive usage of network resources:** Some mobile apps require a great deal of bandwidth to operate, especially those that stream media (e.g., video, music). In addition to consuming network resources, use of these apps can significantly increase service costs where the GFE data plan is limited and subject to overage charges.

2. **Frequent Updates - Mobile applications, operating systems, and devices are more frequently updated and fragmented, which requires additional security review:** Commercial mobile developers frequently update their applications and distribute updates through official app stores, allowing users the ability to update those apps at any time. With the number of mobile apps in the marketplace, these updates can happen at more frequent intervals than many desktop apps, and may require additional security reviews by government IT managers.

   To complicate it further, mobile handheld device operating systems are more fragmented than desktop operating systems. The numerous combinations of mobile hardware, operating systems, and applications, make the security implications more time consuming and costly to assess. Additionally, most commercial app stores do not currently have the capability for an enterprise level ‘whitelist’ or blacklist’. With thousands of apps being updated every day, monitoring mobile apps and operating system updates on government devices is a significant challenge.

3. **Public Cloud - Agencies are not clear on how to handle storage of information in non-government clouds:** Many agencies see public cloud data storage as one of the preeminent challenges for commercial applications on government furnished mobile handheld devices. Many of the most highly sought after commercial applications use public cloud data storage to enhance worker productivity and data accessibility. Agencies, however, have concerns with the public cloud on several fronts, including security, privacy, and records management. Agencies all have different requirements, policies, and levels of risk tolerance with regard to the public cloud, so while there are opportunities for common government-wide policies, there are also major agency specific considerations. To date, no agency interviewed has conquered this challenge, other than to issue policy restricting use of sensitive data in the public cloud.

4. **App Integration - Agencies are not clear on how to control sharing of data across applications and access to services on the device:** Many leading commercial apps, particularly social media apps, promote their use by integrating and sharing data with other apps. This creates additional security risks. When approving commercial apps for agency-wide use, including social media apps, government IT managers must assess and control the interactions between apps in order to protect private data and to limit the sharing of data.

5. **Licensing - There is a lack of enterprise licensing/volume-purchasing options:** Enterprise licensing and volume purchasing practices are not prevalent in the mobile application space. Mobile apps are inherently less expensive than desktop applications and app stores and app vendors have not been prone to negotiating volume discounts or enterprise licenses for government customers. Agencies may have a difficult time tracking procurement activity for commercial apps because the market is fragmented and almost all app purchases are considered micro-purchases. Additionally, the population of commercial mobile apps being developed solely for the Federal government is tiny. It is likely that the cost of achieving a volume discount, even government-wide, would not be recouped.

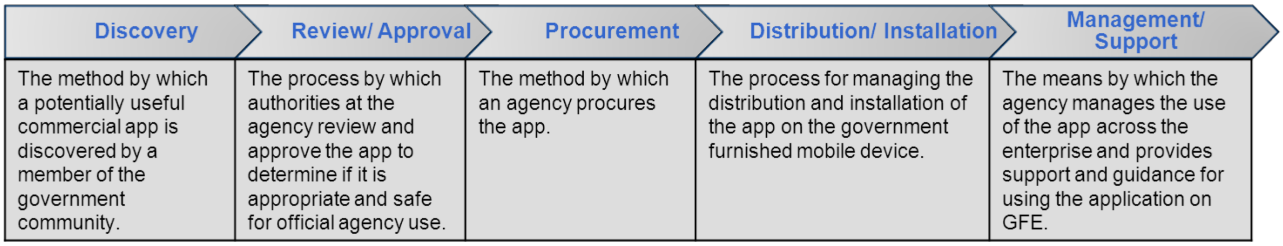
6. **Terms of Use - Unique terms of use between each commercial application require government review and negotiation:** Each commercial application typically has its own terms of use and/or license agreement the user must accept in order to download the app. For the government to adopt a commercial app, the terms of use must be acceptable to the government. In many cases, the terms require negotiation to make changes acceptable to the government, which require a high level of resources. It would be prohibitively costly for the government to review, negotiate, and agree to terms of service for tens of thousands of commercial mobile applications. Additionally, it is unclear what happens to licenses upon the departure/termination of the employee, especially if the user used personal credentials to procure the app.

V. Approaches to Adopting Commercial Applications

This section defines the typical commercial mobile application lifecycle for government agencies and provides examples of the potential approaches for agency adoption of commercial mobile applications. The aspects of the potential approaches are oriented towards the activities taking place during the lifecycle.

A. Commercial Mobile Application Lifecycle Framework

The commercial mobile application lifecycle is defined in five phases (Figure 3). Depending on the level of control and flexibility that agencies need in adopting commercial apps, activities during these phases can vary.   These phases pertain to the current state of the lifecycle as it exists for each agency. If there are government-wide standard policies and procedures implemented in the future, some of these phases may be completed through government-wide activities, rather than activities at the agency level.



Discovery	Review/ Approval	Procurement	Distribution/ Installation	Management/ Support
The method by which a potentially useful commercial app is discovered by a member of the government community.	The process by which authorities at the agency review and approve the app to determine if it is appropriate and safe for official agency use.	The method by which an agency procures the app.	The process for managing the distribution and installation of the app on the government furnished mobile device.	The means by which the agency manages the use of the app across the enterprise and provides support and guidance for using the application on GFE.

Figure 3: Commercial Mobile Application Lifecycle Framework

B. Flexibility vs. Control Methodology

Agency activities during the commercial mobile application lifecycle could have differing levels of organizational control and user flexibility (Figure 4). This analysis has been defined in terms of a 'Flexibility vs. Control' spectrum as outlined below. Each agency may have a differing level of flexibility in adapting commercial mobile applications for government use versus the level of control that is exerted. The relationship between flexibility and control will vary, based on the decisions of the agency. The optimal mix of user flexibility vs. organizational control will depend on each agency's risk tolerance.

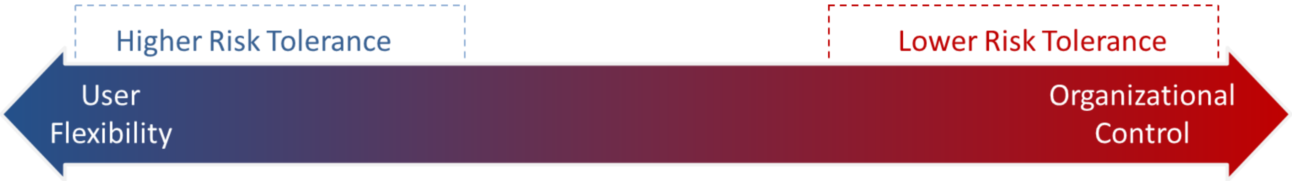
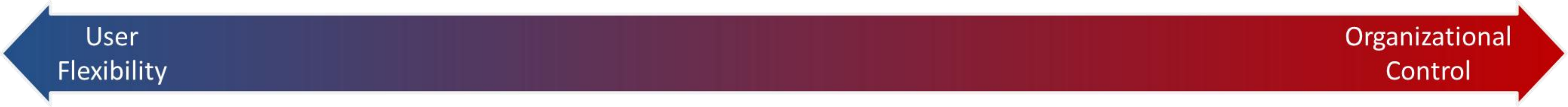


Figure 4: Levels of Organizational Control and User Flexibility

Given the relative immaturity of the overall mobile space, the correlation between organizational control and user flexibility is not yet fully understood. The tables in the following sections describe the approaches that agencies may take in relation to the flexibility and control spectrum as they progress through the Commercial Mobile Application Lifecycle Framework.

1. Discovery

This table highlights the possible approaches and decisions that agencies must make as they determine their preferred method to discover new commercial mobile applications for official agency use on government furnished equipment.



Approaches	• Apps are discovered by anyone at the agency at any time, and may be discovered on personal devices or GFE.	• The process for discovering apps is collaborative and creative, with a focus on 'bottom up' discovery of apps. • Commercial apps are discovered by mission-focused staff that would like to download the app to increase productivity or collaboration. • There can be "dual personas" on the device, including the "personalized" persona where users experiment with and discover new apps, and the "containerized" persona that holds government enterprise apps and other approved apps and data.	• Process for discovering apps is highly restricted, very few outside apps are considered. • Apps are identified by IT managers at the agency for a specific use or to meet specific requirements. • Input from mission focused end-users is limited as to the commercial apps that are discovered and adopted. • The focus is the development of native, mission-based apps to meet a specific need.
Considerations	• Employees freely discover apps that will enhance their productivity and mobile capabilities. • May result in security challenges including fraudulent apps and malware, among others.	• The 'bottom up' approach to discovery encourages creativity and exploration by mission focused staff to find the most useful apps. • Results in many apps (potentially overlapping and/or duplicative) being discovered and requested.	• By limiting the discovery of apps that are considered for review and approval, the agency limits the risks that are inherent to using commercial mobile apps on government furnished devices. • Does not leverage the creativity of mission-focused end users. • Development of native apps is expensive and time-consuming in relation to adopting pre-existing commercial apps. • Perception that the utility of the device has been limited or constrained.

2. Review and Approval

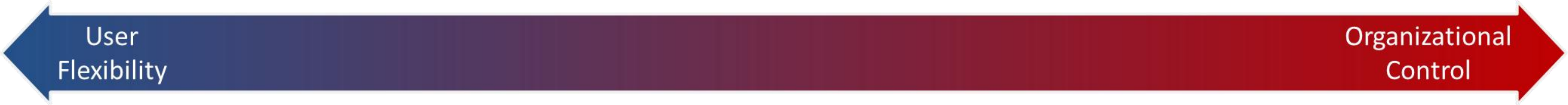
This table highlights the possible approaches and decisions that agencies must make as they determine their preferred method to review and approve new commercial mobile applications for official agency use on government furnished equipment.

User Flexibility
Organizational Control

Approaches	• Limited review and approval process for apps, only focusing on those apps who pose a significant and immediate risk. (e.g., cloud apps). • The agency IT department makes determinations on which apps are restricted and uses policy to support those determinations. • The agency may maintain a whitelist and/or blacklist with no enforcement mechanisms.	• Flexible review process that can be customized based on agency needs. • Upon discovery of the app, a request for review is filed with an IT Manager at the agency. • The review and approval is conducted by a formal committee or panel of experts at the agency, focusing on the business need for the app, the security risks, and any infrastructure challenges the app may pose. • Apps are reviewed and approved based on minimum security baselines. • The agency may maintain a whitelist and/or blacklist. • Apps that have not been approved are not permitted to be downloaded onto the government enterprise's "trusted environment" on the device.	• Highly structured and formal review process for externally developed commercial apps. • Apps are discovered by a centralized group at the agency (e.g., IT Managers) • The review and approval is conducted by a formal committee or panel of experts at the agency, focusing on the business need for the app, the security risks in accordance with the NIST Risk Management Framework (as identified in NIST Special Publications 800-30, 37, and 39), and any infrastructure challenges the app may pose. • Upon approval, the app is added to a list of verified commercial apps. • If an app is not approved, the MDM or MAM directly restricts its use.
Considerations	• With little review/approval needed, the number of apps that are discovered and tried is very high, leading to a greater level of flexibility in meeting user needs. • Maintaining a whitelist and blacklist is difficult without constant review of app updates. • The lead time for review/approval is negligible or non-existent. Users can download apps when they want them.	• The volume of apps to review is very high due to the collaborative nature of the discovery phase. • Due to the volume of apps to review, the process for reviewing mobile apps must be faster than the process to review desktop apps • App reviewers set a target timeframe (e.g., one to two weeks) to make a decision on approval.	• Identifies the majority of risks and threats inherent to commercial mobile apps. • Agencies may set up systems to perform automated scanning of source code to speed up review and approval of app updates.

3. Procurement

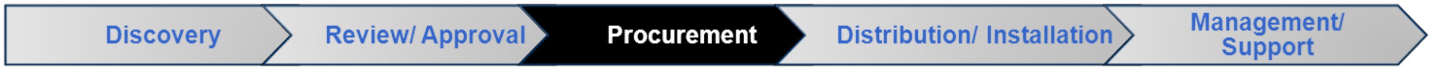
This table highlights the possible approaches and decisions that agencies must make as they determine their preferred method to procure new commercial mobile applications for official agency use on government furnished equipment.



User Flexibility

Organizational Control

Approaches	• Apps are procured by users through their personal app store accounts. Users are reimbursed through standard agency reimbursement practices. • Agencies may provide an official agency app store account to employees for procurement of mobile handheld devices.	• If the procurement is a reimbursable expense and the app is on the "whitelist", a personal app store account or wireless account can be used to procure the app. • Bulk or enterprise licensing are an option for apps that are enterprise focused. • An MDM/MAM solution helps manage procurement by providing a key number for every license. Key numbers are then distributed to users to enable use of the app on specific devices. • MDM/MAM can meter number of downloads of the pre-paid volume purchased apps.	• Procurement of commercial app licenses is managed through the MDM/MAM solution. Apps licenses are procured centrally and downloads are metered. • The MDM/MAM solution provides a key number for every license, and the key numbers are distributed to users to enable use of the app on specific devices. Without the key, the application will not run on the device.
Considerations	• Without a more formalized procurement process, the number of reimbursement requests can be overwhelming for agency procurement departments. • Agency app store accounts require active management to ensure that funds are not misused on inappropriate apps or app store products.	• The procurement phase is flexible based on agency requirements. Licenses can be purchased by individuals, using their own accounts, as long as the app is not prohibited. Likewise, licenses for approved, enterprise apps can be volume purchased and metered by the MDM/MAM solution. • App store gift cards can be deployed to employees with the necessary value to get the apps that are sanctioned by the organization.	• Most MDM or MAM solutions cannot restrict government users from procuring and downloading the app itself, but can restrict the app from being used. • Strict user policies must still be enforced to restrict unauthorized procurement and download of unauthorized apps.



Discovery

Review/ Approval

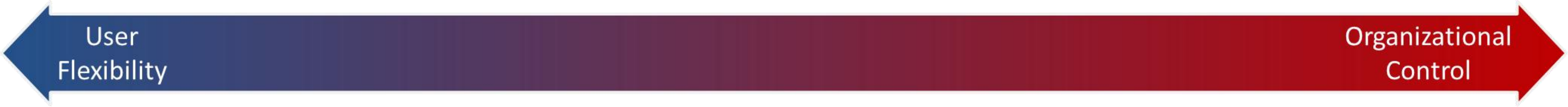
Procurement

Distribution/ Installation

Management/ Support

4. Distribution and Installation

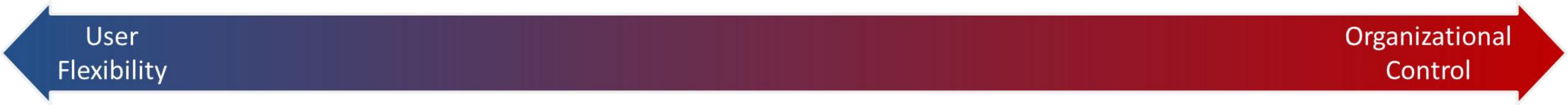
This table highlights the possible approaches and decisions that agencies must make as they determine their preferred method to distribute and install new commercial mobile applications for official agency use on government furnished equipment.



Approaches	• Apps are downloaded by the users themselves, or can be pre-installed by the agency if the agency develops a list of approved apps. • If the agency has an MDM or MAM solution, it can monitor what users are downloading in accordance with policy, but does not physically restrict downloads, and does not typically enforce violations of policy.	• Allows use of other apps outside the container, but not with sensitive data. • Apps may come 'pre-loaded' on the device when the user receives it. • Similar to the procurement phase in Model 1, approved apps can be installed by users using a personal or government app store account, or they can be installed on the device by IT managers.	• Distribution and installation of commercial apps is managed through the MDM or MAM solution by the agency IT department. • Apps may come 'pre-loaded' on the device when the user receives it. • The user account for downloading apps from apps stores to specific mobile handheld devices is an official government account. Personal accounts cannot be used for downloading apps.
Consideration	• Without active monitoring, agencies have no control or perspective on which apps users are downloading onto their mobile handheld device. This poses a major risk.	• There is enhanced control of distribution/installation through the MDM container solution, while users can still experiment with new apps outside the container.	• A MDM/MAM solution is needed to ensure the secure distribution and installation of mobile apps on government devices Prohibiting installation of apps is an all or nothing function. • The MDM/MAM solution can provide notice of infractions by users.

5. Management and Support

This table highlights the possible approaches and decisions that agencies must make as they determine their preferred method to manage and support new commercial mobile applications for official agency use on government furnished equipment.



Approaches	• Policy directs users not to enter sensitive data into apps, but the policy cannot be fully enforced. • The agency can negotiate terms of service with vendors to set forth management and support procedures. • The MDM/MAM solution provides insight into app usage.	• Some commercial apps can be managed through the MDM solution. This “container solution” creates a trusted environment whereby activity on the device is managed through enterprise connectivity and/or a mobile VPN. • Policy is used as ‘behavior management.’ Enforcement can take a tiered response, whereby punishment is progressively worse if the user has multiple infractions. • If there is an MDM solution in place, it has the capability to wipe the device or container at any time.	• Commercial apps are managed through the MDM solution. This “container solution” creates a trusted environment whereby all activity on the device is managed through enterprise connectivity and/or a mobile VPN. • App use and data transmission/download are monitored • All app developer updates are pre-screened by the agency IT department. • MDM has the capability to wipe the device at any time.
Considerations	• IT managers must be aware of trends in app usage in order to make informed decisions if there are emerging apps that pose a risk. • Typically, fewer apps are approved as ‘official’ agency apps, requiring less management and IT support.	• The higher number of supported apps requires greater IT support resources.	• Requires the highest level of control during the management and support phase of the lifecycle. • Some “container” solutions can be configured to restrict functionality of commercial apps.

Discovery
Review/ Approval
Procurement
Distribution/ Installation
Management/ Support

C. Key Decision Factors

This section provides key decision factors as agencies determine their preferred approach to adopting commercial mobile apps into their operations. Agencies should tailor these factors based on their own specific requirements and needs.

- **Agency Risk Posture -** Some agencies will require a much higher level of control and security as they work to meet NIST Risk Management Framework (RMF) requirements and protect highly sensitive government datasets. For those agencies, greater organizational control is the best choice. However, many agencies can utilize restrictive policies to ensure that employees do not compromise sensitive information on their mobile handheld devices, while still allowing some flexibility in the apps that users choose. Where the capability exists, the use of a "containerized" solution and/or a "user persona" on the mobile handheld device further reduces risk for these agencies.

- **MDM Solution -** Most agencies will find that an MDM solution is a good first step, regardless of the preferred levels of control and flexibility. Currently, the objective of DGS Milestone 5.5 is for the General Services Administration to set up a government-wide mobile device management program. The outcomes of Milestone 5.5 can be leveraged by agencies who have not yet implemented a MDM solution. The DGS 5.5 team, comprised of a cross-governmental group of CIOs, CISOs, and IT Program and Mobility offices, developed a set of functional requirements capturing the critical capabilities required to meet at 80%-100% of an agency's need, and identifies potential solution sources whose responses were assessed against these requirements.

- **Business Need for Existing Mobile Apps -** When looking at its own operations, it is important for agency IT managers to determine if there is a business need for a high number of officially sanctioned commercial mobile apps within its operations. Many agencies have business operations that are similar to commercial firms. For these agencies, business needs are easily met by existing commercial apps that have been developed for their specific line of business (e.g., lawyers). Many agencies, however, have specialized business needs that are not easily served by existing commercial applications; therefore, it may not be practical to expend resources to vet a large number of commercial apps.

- **Policy Around Cloud Data Storage -** As the cloud becomes increasingly prevalent for both personal and professional use, agencies will be forced to make policy decisions on cloud data storage, if they have not already. Many agencies, in the interest of security, have disallowed their employees from storing any government data in the cloud. Others have taken the pragmatic approach to allow their users to utilize the cloud, as long as there is no sensitive data stored there. Any decision will have major implications for how an agency approaches security and collaboration for its datasets.

- **Mobile Handheld Device User Population -** An agency with a larger population of smartphone users will have a greater need to implement a stricter model.

VI. Recommendations & Considerations

This section provides a number of recommendations related to government-wide policies and services that could be developed to facilitate and aid agencies that are working to adopt commercial mobile applications. This section also provides considerations for the development of government-wide policies and guidance that align with these recommendations.

A. Government-wide Commercial Application Catalog

Challenges Addressed: Control and Access, Frequent Updates, Public Cloud, App Integration, Licensing, and Terms of Use

Many agencies recognize that there is a need for a government-wide commercial application catalog (the "App Catalog"). At the core, the App Catalog is a repository of information that agencies can contribute to and draw from to help them make decisions on which apps should be allowed on their own government furnished devices. If an agency performs an independent review of an app, the information coming out of that review can be shared with other agencies who are interested in the app, thus reducing the time and effort required to review the app in the future.

Some of the features of the App Catalog could be integrated with functionality of the government-wide MDM solution being developed under Milestone 5.5 of the Digital Government Strategy. Key attributes of the catalog might include:

- Capability to search, rate, and comment on commercial apps;
- Direct links to the app store site for each app;
- Ability to complete a standardized app review form (including a standard set of metadata and characteristics) that tags directly to the catalog's app profile;
- Checklist of app functionality and behavior to assist IT managers in making quick decisions on whether the app is appropriate for their agency. For example, the checklist might specify whether an app utilizes certain elements of the phone, including the microphone, camera, or contacts database;
- Customizable dashboard views for each agency to track what is approved (whitelist), what is not approved (blacklist), what is pending review, and a list of similar apps; and
- "App request" capability to help aggregate future demand for an app among agencies, thereby increasing purchasing power.

To the extent possible, work being done by NIST to support the vetting of mobile apps should be leveraged to help define the metadata characteristics of apps.[3]

To ensure the utility of the App Catalog, the Federal Government could require that all agencies provide input to the App Catalog for all commercial apps that they have been reviewed.

Implementation Steps (Notional)

1) **Develop Draft Characteristics** – Assemble team of subject matter experts from across agencies and leverage work already being done across the Federal Government (in particular at organizations such as NIST) to develop draft set of application characteristics to help agencies in assessing particular apps. Characteristics to include items such as: "Access to Mobile Device Camera", "Access to Your Location", "Access to Contact List", etc.

2) **Review Draft Characteristics with Agencies** – Review draft set of characteristics with agencies to determine relevance and fit. Incorporate agency feedback and update characteristics as

[3] NIST is currently developing Special Publication 800-163 which will provide a framework for vetting mobile applications across a number of areas, including security and privacy, and will provide insights into characteristics to describe common mobile application behavior.

appropriate. Agencies should determine which characteristics are appropriate or acceptable to them.

3) **Develop Process to Add and Update Content** – Work with agencies to determine how apps and app characteristics are submitted, how the submissions are reviewed, and finally added to the catalog. Processes should also include how existing content in the catalog is updated.
4) **Standup App Catalog** – Develop online searchable catalog, with appropriate access controls (i.e., should this be viewable by the public, government-only?), to allow entry and review of application characteristics.
5) **Populate Content** - Using process determined in prior steps, populate catalog with information for apps already adopted by agencies.
6) **Scale & Rollout**

B. Best Practices Regarding Application Review Processes

Challenges Addressed: Control and Access, Public Cloud, App Integration, Terms of Use

In order to develop a standardized App Catalog as described in Recommendation A, it is essential to compile a set of best practices based on existing app review processes at agencies and the associated requirements for those reviews. Standardized review requirements and government-wide best practices will ensure that the App Catalog is successful by creating a common language with which to assess commercial apps. This review process should align with the Digital Government Strategy Milestone 9.1: Develop Government-wide Mobile and Wireless Security Baseline.

The Federal Government can also look to use commercially available tools to test commercial apps. The government could look to develop a contract with one or more tool vendors to provide these testing capabilities as a government-wide shared service. The Government could also provide a centralized service using these tools to test mobile applications, at which point results could then be published and shared among agencies using the App Catalog. While these tools typically do not take long to run, they do produce detailed reports which can require significant analysis. The government could provide technical experts to assist agencies in reviewing these reports to determine suitability of apps based on agencies' risk profiles.[4] Lastly, the government could provide guidance on terminology and nomenclature that these tools should leverage in reporting their findings so that the results from the various tools can be used consistently across the community.

The government should conduct outreach to collect best practices and review requirements, and then develop the standardized app review form based on the findings. The Federal Government can issue a data call for this information and issue guidance on how commercial apps should be reviewed government-wide.

<u>Implementation Steps (notional)</u>

1) **Work with Agencies to Develop Application Review Guidelines –** Leverage NIST research and industry and government best practices to develop a framework for testing and reviewing mobile apps. The framework can include descriptions and behaviors of apps, how each characteristic impacts the government agency, and how each should be reviewed in the context of an agency's policies. In particular, ensure alignment of framework with Digital Government Strategy Milestone 9.1 to incorporate government-wide mobile and wireless security baselines.
2) **Identify Potential Automated Solutions –** Conduct market research to identify possible automated testing solutions to address application security, functionality and other areas of concern as necessary. Market research efforts should factor in technical capabilities, business

[4] DARPA and NSA have done work in conjunction with NIST to review several of these tools and develop testing frameworks.

models, ease of implementation within the federal government, and pricing considerations. If relevant, look to establish a contracting vehicle with one or more testing tool vendors to provide test services on a government-wide basis.

3) **Develop Process For App Review** – Develop and document processes for agencies to use in reviewing applications. Include approaches for the use of automated testing tools (where relevant), the use of government-wide services (where relevant), and methods for publishing review outcomes to the App Catalog.
4) **Develop Process for Updating Guidance –** Establish a process for how the guidance can be updated as agency needs and the mobile app marketplace change.

C. Government-wide Terms of Service

Challenge Addressed: Terms of Use

Evaluating, and agreeing to the terms of service (ToS) of commercially produced applications can significantly delay the adoption of new technologies. When the number of ToS documents is few, the current approach is manageable but as the number of candidate apps grows, the existing process does not easily scale. As mobile app usage proliferates, this can grow into a time consuming and labor intensive process tying up precious and scarce government resources.

Typically, the vendor originates the process – providing their terms of service to the government for review and acceptance. Given the wide range of potential vendors, especially in the mobile application space, the government is forced to review a different Terms of Service document for each application. The number of reviews can become backlogged, further delaying the procurement process. An alternative would be for the government to publish a set of common clauses, or an entire ToS document that vendors were required to review and incorporate into their terms of service. The vendor could adopt the government ToS in its entirety or use the government ToS as an initial framework or basis for their ToS. The government would still need to review the ToS but the review process could be shortened because only potential modifications need to be reviewed.

By making these terms of service publically available, developers and vendors can voluntarily choose to meet the requirements. When vendors or developers agree to these terms, they are increasing their customer base to all government users. Apps that meet the terms of service can thereby be included in the government app catalog. Over time, this solution may significantly reduce the burden on the government to review and approve, deny, or negotiate terms of service for thousands of commercial apps.

Additionally, this same effort could include open source licenses to encourage faster adoption of commercial mobile apps. There are a multitude of open source licenses in the marketplace today. Pre-emptive review and approval of open source licenses can speed up the adoption of open sourced software.

<u>**Implementation Steps (Notional)**</u>

1) **Collect & Review Commonly Used Terms of Service Agreements –** Collect and review commonly used terms of service agreements based on discussion with agencies and surveys.
2) **Develop Government-Standard Terms of Service Agreement –** Work with Agencies and Subject Matter Experts (e.g., technical experts, legal resources, business analysts) to develop Government-Standard Terms of Services for distribution to commercial mobile application developers.
3) **Conduct Review of Government-Standard Terms of Service –** Conduct review with key stakeholders across Government and industry, with particular focus on the mobile application development community. Incorporate feedback and update Government-Standard Terms of Service as appropriate.

4) **Conduct Outreach & Awareness Activities –** Conduct campaign to raise industry awareness of Government-Standard Terms of Services in effort to increase usage and accelerate adoption of commercial mobile applications across the Federal Government.

D. Government-wide Cloud Storage Service

Challenges Addressed: Control and Access, Public Cloud, Terms of Use

Many commonly used mobile applications access, process, and store data using the public cloud or hosting facilities provided by the app vendor. As these applications have been developed for the broader commercial market, the storage solutions utilized typically do not conform to Federal Government requirements around areas such as security, privacy, and records management. This challenge is broader, encompassing desktop apps as well. The non-conformity with government requirements leads many agencies to look to restrict access to these applications, despite their potential value to Federal employees. Despite these restrictions, employees in many cases currently use mobile applications that leverage cloud-based storage (e.g., note-taking apps, file sharing apps).

While in certain instances mobile application developers are willing to modify their applications to meet Government requirements, in most cases this is not practical given the costs and effort required – especially for small businesses and individual entrepreneurs who are predominantly focused on the broader commercial market.

To reduce the burden on mobile applications developers in doing business with the Federal Government and consequently accelerate adoption of commercial applications, the Government could develop a “storage-as-a-service” solution that meets all baseline Federal requirements (e.g., security, privacy, records management) and is accessible in an API-based manner. For instance, mobile application developers interested in accessing the Government-provided storage could register, using a lightweight application process, to receive API keys and would then be able to “re-point” existing applications to make use of the Government-provided storage as well as develop new applications consistent with Government requirements. By using government-provided storage and APIs, mobile application developers can access and use of storage solutions meeting Government requirements at a fraction of the cost of developing them independently. As developers realize that they can grow their customer base by becoming approved app developers for the government cloud, they will focus more attention on government facing commercial applications and solutions.

Alternatively, the government could agree to purchase a copy of a commercially available app and make it available solely for government use. The data could be stored on the “storage-as-a-service” solution and the app could be made available solely on government issued devices. Ultimately, this will support expanded use and adoption of commercial mobile applications within the Government.

Additionally, the “storage-as-a-service” solution would be available to all Federal agencies for use in government-developed applications, mobile or otherwise – leading to potential cost savings and operational efficiencies as agencies move to paying for the storage they need, when they need it.

Implementation Steps (Notional)

1) **Stand-up Storage-as-a-Service Core Implementation Team & Program Management Office (PMO) –** Establish core team responsible for management and day-to-day execution for Storage-as-a-Service setup and pilot activities. Activities should include assignment of a program manager, business analysts, contracting officials, key subject matter experts, etc.
2) **Develop Baseline Government-wide Requirements –** Works with agency stakeholder and policy SMEs to develop a baseline set of requirements in areas such as security, privacy, and records management. The baseline is intended to represent common requirements relevant to a broad

range of agencies. Individual agencies may have specific requirements that go beyond the baseline.

3) **Develop Concept of Operations** – Develop operating model for Storage-as-a-Service including operational processes, chargeback models, agency customer terms of service, new app onboarding procedures, etc.

4) **Develop Storage-as-a-Service Pilot Solutions**
    a. Identify initial pilot use case
    b. Develop Storage environment & related solutions
    c. Obtain FISMA certification for pilot solution
    d. Develop API for access
    e. Apply "Best Practices for Application Review Process"

5) **Identify Pilot Agencies –** Determine subset of agencies and users (components, offices, or otherwise) for piloting Storage-as-a-Service solution

6) **Conduct Pilots –** Execute pilots and collect feedback on pilot activities.
    a. Storage only
    b. Mobile Application Enhancement

7) **Scale Storage-as-a-Service Solution**
    a. **Scale Environment & Incorporate Lessons Learned from Pilots**
    b. **Develop Mobile Application Developer Certification Program –** Develop program for reviewing and certifying mobile application developers interested in directly accessing the Government Storage-as-a-Service solution for use in commercially developed applications
    c. **Promote & Roll-Out to Broader Set of Agencies**