Good Technology Submission to National Commission of Audit

Good Technology welcomes this opportunity to provide a submission to the National Commission of Audit. Good Technology's submission primarily addresses Phase 1:

> *Efficiency and effectiveness of government expenditure*: adoption of new technologies in service delivery and within government.

Our position

Good Technology believes that securing handheld devices in an environment where users increasingly opt to use smartphones and tablets to connect to the internet, email and data sources can drive real productivity and efficiencies benefits for government, and hence, offer massive service delivery dividends for governments as well.

About Good Technology

Good Technology is the global innovation leader in secure mobility solutions enabling business and government to work more efficiently. Good's comprehensive solution consists of a secure containerised mobility software platform, a suite of collaborative applications, and a broad third party application construction and partner environment that unlocks mobile potential. Good Technology has been working with Australian and US top-tier departments in national security and across the civilian agencies, as well as a range of industry and political organisations to secure their handheld devices and apps and enable these organisations to take advantage of the efficiency and productivity dividends offered by increased mobility, while maintaining data security.

Introduction

Good Technology recognises that Government is exploring ways for the use of new technologies to reduce costs, lift productivity and develop better services.

The Government has been clear in its pre-election policy for E-Government and the Digital Economy, as well as in the terms of reference for the National Commission of Audit that it is looking to identify and recommend the next generation of government process and operations in order to achieve these objectives.

The identification of solutions that leverage the potential of new technology to achieve productivity and efficiency gains is further targeted to evolving government services to be more citizen-centric and transparent by using technologies that enable secure access to big data and are easily transferable within, between and outside of government. The key focus of digitised interactions must be security and the integrity of the information being transmitted within and between governments as well as with citizens and third parties such as contractors.

Mobility Environment

Mobility has transformed the efficiency of personal and commercial workflows and interaction over the past few decades as governments around the world have recognised the potential opportunities for efficiency gains through mobility.

The first generation of government mobility has already been rolled out with government employees able to access mobile telecommunications, email and calendar functionality securely. Currently, the various methods of mobilising government workforces securely include:

- Mobile device management (MDM) manages the device settings to ensure that mobile data is secured by locking all of the vulnerabilities, including any non-secured applications and functions such as cameras, GPS, etc.
- Secure Portals effectively create a secure window from a mobile device to a secure workstation to enable mobile viewing of a secure system without any data being transferred to, or stored on, the device.
- Containerisation creates a secure container within a mobile device that does not affect the operability of the rest of the applications and functions, but separates and secures the required data on each device. This essentially creates two domains on the device – agency secure and personal unclassified.

The next evolution of mobility sees the use of applications that leverage device functionality to achieve personal and commercial workflow efficiencies in orders of magnitude above mobile telephony and email. Governments are currently grappling with the issues around delivering a secure solution that enables government to deliver these next order efficiencies by creating applications that enable mobile workflows for government employees.

The security frameworks outlined above that are currently available to government approach these issues in different ways:

- While an obvious first step taken by most governments around the world, MDM coupled with hardening guidelines is by definition a superficial mobility solution as it locks down the very functionality of mobile devices such as applications, cameras and GPS that are the key to creating mobile workflows to leverage these next order efficiencies by streamlining paper-based processes to save time and costs.
- Secure portals are capable of delivering some efficiencies as they enable access to traditional workstations where the applications are housed. However, they offer minimal operability as they create a series of secure tunnels where information cannot be shared between applications on the device. In addition, to date it cannot guarantee the prevention of data leakage from other device functions such as cameras and GPS.
- Containerisation secures the data within each application right on the device. Good Technology is the only ASD-evaluated purely containerised solution on

the market today, and using a patented shared services framework, enables data to be securely shared between authenticated applications on a device. In addition to this, the container enables secure use of the device functionality such as camera, microphone, GPS, accelerometer, gyroscope, compass and other functions that may be available on the device. This enables applications to securely leverage the full mobile functionality of these devices and create streamlined and efficient mobile workflows and realise those next order efficiencies. Examples of some secure mobile workflows are outlined later in this document.

Efficiency and productivity gains

Good Technology enables business and government to access productivity and efficiency improvements through mobile device security.

For government, the greatest barrier to harnessing the efficiency opportunities offered by workers' use of mobile devices is the need for security. All government organisations possess, collect and utilise sensitive data, especially in the defence and law enforcement sectors, but also in human services and other customer service areas. Securing this data is an overriding and growing concern for government as information sharing becomes easier and the growing need for flexible working arrangements, even in sensitive areas such as secure access to government data for war fighting capabilities.

Good Technology bridges the gap between security and mobility, allowing government employees secure access to workplace data from mobile devices. The Australian Signals Directorate (ASD) has approved Good Technology's Good for Enterprise (GFE) products for government use. The ASD Cryptographic Evaluation (DCE) certification allows iOS devices secured with GFE to communicate and store classified information up to and including 'Protected' level. GFE has also been certified as Common Criteria Evaluation Assurance Level 4 Augmented (EAL4+). EAL4+ is the highest certification level recognized internationally under the Common Criteria program, and is frequently conducted for products that are deployed in environments handling sensitive government data. With this certification for GFE, organisations can be assured that their mobile data has been certified for the highest levels of protection. GFE is the only cross-platform mobile collaboration solution to achieve EAL4+, and the only solution to meet this level of certification on either iOS or Android.

Good Technology's solution is a containerised security package at the application layer of implementation, which makes it fully customisable and therefore inherently efficient and cost-effective because it is tailored to each organisation's specific needs. By facilitating a mobile government workforce, Good Technology unlocks opportunities for government to improve its efficiency of expenditure and service delivery, as well as improve employee productivity.

Mobility benefits

The benefit afforded by mobile technology is its ‘anywhere’ capability. This unlocks opportunities for government in a number of ways, namely the ability of workers to access information wherever they are, e.g. in transit, at home etc., reducing the amount of potential lost productivity when people are working away from the physical office. It also enables the use of mobile workflows through its shared services framework, using customised applications to improve the capacity of workers whose jobs are mobile in nature, e.g. law enforcement and emergency services personnel, to discharge their duties with better access to vital data and systems in real-time.

The outcomes from the above improvements enable:

- Improved service delivery
- Streamlined workflow
- Increased productivity
- Greater accountability
- A more cost effective interaction within government
- A more cost effective interaction between government and the general public
- A cost effective way to mobilise information from existing technology investments (e.g. SAP, Oracle, MSFT)
- Government to be a more attractive workplace for the best employee talent by providing a flexible workplace environment

Flexible security

The flexibility enabled by using Good Technology to synthesise mobility and security is a game changer for the future of the workforce, including government. Growing Australia’s participation rate will be easier if workers are offered more choices on where and how they work. Mobile technology empowers employees to conduct their work remotely while maintaining access to resources equivalent to office-based employees.

Further opportunities

Good Technology welcomes the opportunity for further consultation with the Commission to discuss the possibilities for even greater efficiencies and productivity gains in government service delivery, and government processes more broadly.

We are able to provide further information on request.

Secure Mobile Workflows in the Public Sector

Good's Secure Mobility Solution has been adopted by public sector agencies globally to increase productivity, speed operations and better serve the public. The following table contains examples of how public sector organizations have leveraged or plan to leverage Good's Secure Mobility Solution to enable secure mobile workflows.

Mobile Activity	Mobilised Capabilities	Benefits
Mobile police officer	▪ Officer uses tablet during an incident investigation ▪ Before arriving to the scene of the incident, officer launches custom app to run background checks. ▪ Connects to HQ and uses Good Dynamics-secured 3rd party app, MobileForce Fonemine for Good, to open document to report incident. Takes photograph and adds to report. ▪ Opens iAnnotate for Good, a Good Dynamics- secured PDF annotator, and adds notes to report. ▪ Uses DocuSign for Good to have witness digitally sign report. ▪ Uses Good Connect to check for supervisor's presence at HQ to discuss incident. ▪ Uses Fonemine for Good to review case with supervisor before leaving scene.	▪ More time in the field for officers. ▪ Save administration time and money. ▪ Increase victim satisfaction through efficiency and accuracy.
Remote training	▪ Before leaving home, military field officer downloads military reference manual from the branch file server to his tablet using Good Share, a secure file synchronization application. ▪ In the field, officer is able to view manual and makes annotations on a specific reference diagram using iAnnotate for Good, a Good Dynamics-secured PDF annotator. ▪ Good Vault provides an additional level of security requiring officer to slide CAC card into device sleeve before launching Good For Enterprise, in order to email the annotated document to other officers for review.	▪ Shifting away from paper saves staff hours needed to build and maintain manuals. ▪ Field officer is more productive by being able to quickly find and share information. ▪ Sensitive information is protected.

Disaster recovery	▪ In the field, disaster recovery agent launches a custom app, Disaster Assessment Reporting System. ▪ Collects victim’s critical, sensitive information including Social Security and insurance information and enters into disaster reporting app. ▪ Agent accesses disaster report file stored on tablet using GoodReader for Good1, a Good Dynamics- secured 3rd party Office doc editing app, and captures specific information related to event. ▪ Launches Good for Enterprise to email and send the report to her supervisor.	▪ Reduction in time needed to provide victim assistance, service restoration. ▪ Protection of PII post data collection.
Military officer on the go	▪ In the field, officer uses tablet and launches Good Share to access Mission Critical Operations Report. ▪ Launches Office Pro for Good, a Good Dynamics-secured 3rd party Office doc editor to view and edit the report. ▪ Launches custom mapping app secured by Good Dynamics, and copies the information into the document. ▪ Uses Good for Enterprise to email the document to commanding officer.	▪ Improved productivity while enabling faster decision to achieve successful mission. ▪ Mission information protected.
Real-time inspection reporting	▪ In the field, inspector uses Good Share to access inventory checklists, regulation, compliance and licensing on agency databases and SharePoint servers. ▪ Launches Office Pro for Good, a Good Dynamics-secured Office document editor, and writes the report, noting areas of non-compliance. ▪ Launches custom photo app secured by Good Dynamics and embeds the photo into the report. ▪ Uses Good for Enterprise to email the report to their supervisor, and a copy to the customer.	▪ Improved inspection operations. ▪ Paperless process and automatic updating to data- bases.