Australian Government
Department of Defence

Minute

Associate Secretary
CIO
CIOG Executive
ASICTA

WHATSAPP – AUTHORISATION FOR MOBILE ICT PROOF OF CONCEPT

References:

A. TN4279-009 - AA Brief - PMICT Configuration
B. TN4279-009 - Certification Report - PMICT Configuration of Prod to new design

1. Mobile ICT (MOBICT) was provided a Provisional ICT Accreditation (PICTA) on 08 June 2018 for 6 months. The provisions of the PICTA allow WhatsApp with the following conditions.

    (1) WhatsApp is limited for Defence Senior Leadership Team (SLT) on the upgraded MOBICT POC infrastructure only;

    (2) WhatsApp must only be provisioned on MOBICT devices that are managed via the MDM through the UNCLASSIFIED application path;

    (3) WhatsApp is compliant with ASD approved encryption algorithms therefore it is suitable to handle up to and including UNCLASSIFIED DLM information; and

    (4) Requests to access WhatsApp are approved through the existing Defence CIR and application approval process and only on the MOBICT POC infrastructure at this time.

2. Defence ICT Security policy and the acceptable user guide articulate the security risks and users acknowledgement and acceptance of the risk of utilising MOBILE ICT. This is inclusive of the risk of applications allowing Defence Data up to UNCLASSIFIED DLM being exposed to internet facing systems and user's responsibility to ensure the data is protected at that level.

3. CIOG MOBICT are updating Standing Operating Procedures to reflect the use of encrypted applications such as WhatsApp.

4. This minute is authorisation for the use of WhatsApp within the conditions of the PICTA and MOBICT POC and SOP's.

[redacted]

Aiyaswami Mohan
Chief Information Security Officer

27 August 2018

[redacted]

Australian Government
Department of Defence
Chief Information Officer Group

Certification Report

Accreditation

Certification Management
ICT Security Branch

Objective ID: BO493247

TN 4676-003

APW-3-261

CERTIFICATION REPORT – MOBILE ICT CLOUD OPERATIONS NETWORK CHANGE – THE ADDITION OF WHATSAPP – UNCLASSIFIED - STANDALONE

PURPOSE

1. This document reports on the process and outcome of the security assessment conducted by Certification Management, ICT Security Branch (ICTSB) on the Mobile ICT Cloud Operations Network (MCON) System.

2. The report provides the IT Security Advisor (ITSA) with mitigation strategies and residual risk statements to assist in providing a suitable recommendation to the Accreditation Authority (AA) on whether to provisionally accredit the system.

3. Referenced residual risk levels have been defined in Annex A.

BACKGROUND

4. ICTSB performed an assessment of the MCON System at the request of Project Support Officer.

5. The MCON system is a temporary mobile ICT standalone UNCLASSIFIED system, based on commercial cloud computing and telecommunications solutions. The aim is that MCON will be used for future ADF operations where a temporary UNCLASSIFIED standalone mobile solution is required, in either Australia or overseas, using Telstra or local carriers as required. It was approved under TN4676-002 on 16/07/18. A change to the MCON solution is proposed by adding WhatsApp to the applications used by iOS devices.

7. HICTO has been identified as the Accreditation Authority (AA) for the MCON system as CIOG are building and managing the system, and is therefore responsible for authorising its use. Authorisation requires either the acceptance of identified risks or advice towards their further mitigation.

8. The certification process included an ICTSB review of the capabilities and architecture of the system. The assessment noted that the following capabilities exist for the MCON system:

a. The sharing of data, such as text, voice, video and imagery between the Deployed Mobile Units (DMU) and the Joint Headquarters Units (JHQ), which are Semi-Static teams in various locations;

b. The communications of orders to the DMU from the JHQ;

c. The transfer of the DMU's Geo location (via the Russian Federation manufactured Traccar Application (AP)) to the JHQ;

d. The JHQ can:

   (1) Manage the structure of the information repositories stored in the cloud;

   (2) Manage the location data reported by the DMU; and

   (3) Manage the infrastructure supporting the system.

e. The transfer of situational awareness information from JHQ to HQJOC; and

f. The secure sharing of situational awareness and threat updates between Defence and DFAT staff via WhatsApp.

SECURITY ASSESSMENT

9. ICTSB has assessed that the current system implementation does not addresses security concerns for a system of its type and data sensitivity. Due to this, ICTSB has some additional security proposals, which have already been adopted by the project.

Current Security Implementation

10. In addition to the existing MCON system, WhatsApp has had the following controls implemented to reduce risk:

a. ASD approved cryptographic algorithms that are compliant with Information Security Manual (ISM) 2017 for protecting UNCLASSIFIED information. Specifically:

   (1) The General Initialisation Protocol (GIP) is as follows:

      i. A shared secret is established using the cryptographic key scheme Elliptic Curve Diffie Helman (EDCH). This is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public private key pair to establish a shared secret over an insecure channel; then

      ii. The shared secret key produced by the EDCH is used as an Advanced Encryption Standard (AES) key to encrypt all the data.

   (2) The User to User Messaging Protocol (UtUMP):

      i. After establishing sessions with the GIP, users can securely send messages to each other using the shared secret key; then

ii. After each use, the shared secret key is changed using a process call double-ratcheting. This means that the shared secret key is a onetime key for every individual message.

(3) Group Messaging Protocol (GMP) is as follows:

i. A group is created using the creator's user ID and a timestamp. Members are added via a group modification message. The WhatsApp server is responsible for the distribution of group modification messages and group messages based on the group management information;

ii. The group modification message is encrypted with AES using the dedicated group key. The dedicated group key is generated using the GIP. Once generated it is not changed; and

iii. The content of the group messages are protected by the GIP and the process call double-ratcheting. Each group message key is unique.

b. The WhatsApp application has been reviewed and tested by the Mobile ICT team and ICTSB. The initial analysis of its communications indications that the product behaves as described in the literature.

Key Security Risk and Vulnerabilities Analysis

11. The following key security risks and vulnerabilities have been noted:

a. While the cryptographic algorithms are ASD approved, the cryptographic protocols used by WhatsApp are not ASD approved, and academic analysis of these protocols have indicated a number of possible security issues, the main one noted below;

b. With respect to the MCON architecture, WhatsApp will increase the attack surface of the mobile devices as it will communicate directly from the mobile device with WhatsApp server (like the phone's voice system, but unlike all the other apps in MCON), and it would be harder for the monitoring and logging to track its usage; and

c. A search of the academic literature and the vulnerability databases indicates that WhatsApp could have some security issues. The most plausible, due to the high threat environment of APEC 18, being a protocol design weakness. This weakness allows an attacker with control over the communications with the WhatsApp Server to spoof a group modification message, because of its fixed key, and become a member of the group and/or add other users to the group without any interaction of the other users.

12. Based on its capabilities, inherent risk, overseas deployment, the high-risk environment of APEC 2018, the implemented controls and the complexity of working with overseas partners in joint operations, ICTSB has assessed the residual risk of the current system security implementation to be **SIGNIFICANT**. Please note that this risk can be reduced with relatively little effort.

13. ICTSB consequently assesses that the addition of WhatsApp to MCON system while overseas in APEC 2018 presents an unacceptable additional risk to Defence and Defence information and recommends the following security implementation to reduce the risks to a minimum.

Additional Security Implementation

14. The following additional controls have been proposed and implemented to reduce assessed risk:

a. That the users of the group function of WhatsApp, while in a high threat environment implement a pre-shared list of members of the group either with a user-to-user message or via an out of band communication channel.

15. Based on its capabilities, inherent risk and proposed controls, ICTSB has assessed that the residual risk of the proposed system implementation would be MODERATE.

16. On advice to Project Support Officer has produced the list implement the new control immediately, this reduces the risk from SIGNIFICANT to MODERATE and hence ICTSB recommends the re-issuance of an Accreditation.

SUMMARY

17. ICTSB recommends the reissuance of an accreditation for one year for the MCON system. Furthermore, as the proposed additional controls to reduce the risk have been agreed to, can be implemented immediately and are being implemented, the residual risk is assessed as **MODERATE.**

18. Should you wish to discuss this report further, the ICTSB contact is

25 October 2018

Annex:

A. Residual Risk Descriptors

ANNEX A TO
CERTIFICATION REPORT

RESIDUAL RISK DESCRIPTORS

1. LOW:

   a. The risk is acceptable given the mitigation strategies in place; and

   b. No additional controls or resources are required.

2. MODERATE:

   a. The risk is acceptable given the mitigation strategies in place; and

   b. Additional controls could be considered and additional resources may be required.

3. SIGNIFICANT:

   a. The risk should be managed by mitigation strategies as resources allow; and

   b. Additional controls could be considered and additional resources may be required.

4. HIGH:

   a. The risk is probably too high and should be promptly managed by mitigation strategies; and

   b. Additional controls and resources are required.

5. EXTREME:

   a. The risk is too high and must be immediately managed by mitigation strategies; and

   b. Additional control and resources are urgently required.

Department of Defence

CHIEF INFORMATION OFFICER GROUP INSTRUCTION 01/2015

January 2015

This Instruction is issued with the authority of the Chief Information Officer pursuant to section 9A of the Defence Act 1903 for members of the ADF; and section 20 of the Public Service Act 1999 for Department of Defence APS employees, in accordance with The System of Defence Instructions Manual.

Note: These instructions are of a permanent nature and remain in force until cancelled. They should be reviewed by the sponsor every three years and repromulgated only where a significant change of content is necessary. Publications can be accessed on the Defence Intranet at http://intranet.defence.gov.au/home/documents/departme.htm.

MOBILE INFORMATION AND COMMUNICATIONS TECHNOLOGY DEVICE MANAGEMENT

Introduction

1. Mobile information and communications technology (ICT) devices provide a range of computing functions that allow users to access certain corporate and Defence networks or the Internet, either from a Defence site or remotely in the course of a Defence person's business activities.

2. All Defence personnel are required to comply with the following policies related to the use of Defence ICT Resources:

a. DI(G) CIS 6-1-001 *Appropriate and inappropriate use of ICT Resources*

b. DI(G) CIS 6-7-002 *Mobile telephones and related services*

c. *Accountable Authority Instruction* 2.3.2 on ICT software purchases

d. *Accountable Authority Instruction* 2.3.2 2.3.3 on ICT hardware purchases

e. *Defence Security Manual* (DSM) Part 2.52—Portable Electronic Devices and Laptops

Policy Statement

3. All CIOG personnel involved in the distribution, use or management of Defence supplied mobile ICT devices must adhere to this Instruction.

Scope

4. This Instruction establishes the basis of provisioning, funding and support of the following Defence mobile ICT devices:

a. Defence unclassified mobile phone (non-smart phone) and pager.

b. Defence BlackBerry device, which has been accredited and approved by ICT Security Branch (ICTSB) to access the DRN for data up to Protected level, and to access the Defence Voice network (DVN) for voice, SMS or MMS at Unclassified level only.

c. Defence Protected iPhone, which has been accredited and approved by ICTSB to access the Defence Restricted Network (DRN) for data up to Protected level, and to access the DVN for voice, SMS or MMS at unclassified level only.

d. Defence Protected iPad accredited and approved by ICTSB to access the DRN for data up to Protected level.

e. Defence unclassified smart phone and tablet devices that have not been accredited or approved by ICTSB to access any classified or sensitive Defence network, except as detailed in paragraph 33.

f. A token to access the Defence Remote Electronic Access and Mobility Service (DREAMS).

g. Wireless data card.

h. USB data transfer device for storage of official data up to Protected by access to the DRN.

i. USB data transfer device for storage of official data up to Secret by access to the Defence Secret Network.

j. Defence Secret mobile phone, eg Sectéra® Wireless GSM® or Secure Mobile Environment – Portable Electronic Device (SME-PED).

5. The list of approved devices and their respective procedures for use will be available on CIOG's ICT services website at http://ciogintranet/Pages/Default.aspx. These will be amended as additional devices become available, accredited and approved to use.

Roles and responsibilities

6. Assistant Secretary Enterprise Technology Operations is the Service Owner for mobile ICT.

7. Director-General Business Relationship Management Office (BRMO) and Director-General ICT Strategy, Planning and Policy, in collaboration with the Director of Fleet Operations, are responsible for ensuring that this policy is being observed by taking appropriate action to correct non-compliance.

8. BRMO managers will encourage their Group Point of Contacts (GPOCs) to follow the intent of this Instruction and implement the relevant Security Standard Operating Procedures and usage procedures provided on the CIOG website, and for ensuring Group allocations are appropriately recorded and managed.

9. All Defence personnel, as a condition of their use of a Defence mobile ICT device, will be advised that they are responsible for:

a. notifying their issuing authority of any change of circumstances, including changes to the cost centre code provided when issued with a device

b. notifying the Defence ICT Service Desk if their mobile ICT device is lost, stolen or damaged

c. raising an SD016—Loss or Damage Report if a device is lost or damage, to initiate an investigation of the cause

d. raising an XP188—Security Incident Report to report if classified data may have been compromised, eg through loss or theft of a classified device,

Basis of provisioning and funding

10. Categories of provisioning. The three categories of mobile ICT users for provisioning are as follows:

a. **Category A.** Very Important Persons (VIP) and Senior Leadership Group (SLG) members.

b. **Category B.** Military unit commanders at the Officer-5/6 rank levels appointed by a formal instrument of command, Defence Military Attachés and the SLG member's immediate office staff , ie Military Assistant, Executive or Principle Staff Officer.

c. **Category C.** Other staff with a justified business need that is authorised by the user's financial delegate and GPOC.

11. The basis for provisioning and funding for each mobile ICT device by user category is at Annex A. The priority for provisioning of mobile ICT devices will normally be in the order: Category A, then B, then C users. The provision of a Defence Protected iPhone or Defence unclassified smart phone will preclude the individual from also having a Defence unclassified mobile phone or BlackBerry device. The provision of a Defence Protected iPad will preclude the individual from also having a Defence unclassified tablet or BlackBerry device.

Level of service support

12. The level of service support provided for users of mobile ICT devices will be advised to users at the time of issue, using the Defence ICT Service Desk and associated service delivery support.

SIM Cards

13. Defence personnel will be advised that they must not use personally funded SIM cards in Defence mobile ICT devices, or use Defence funded SIM cards in personally owned mobile ICT devices. All SIM cards are to be procured from CIOG via the Service Request Catalogue, except where a user is overseas, when paragraphs 38 to 42 apply.

Defence unclassified mobile phone

14. The provisioning and responsibility for costs associated with a Defence unclassified mobile phone are at Annex A.

Defence BlackBerry device

15. Defence BlackBerry devices will be progressively replaced by a Defence Protected iPhone device as availability allows. This will be completed by 30 Jun 15, coordinated by Enterprise Technology Operations Branch, in consultation with BRMO managers and their GPOCs.

16. Until then, as Defence BlackBerry devices are assigned to an appointment position number, if the custodian is transferred to another unit or location, the device is to be transferred to the new incumbent as part of the departure/march-out procedure.

17. Damaged devices must be returned to the Defence ICT Service Desk for replacement and the GPOC advised. If access to the damaged device is possible, the device is to be sanitised in accordance with Australian Signals Directorate (ASD) BlackBerry Hardening Guide. If access is not possible, it is to be packaged and labeled for transport as a Protected item in accordance with the DSM.

18. If the device is no longer required or justified, it must be sanitised by the custodian prior to being returned to the GPOC for either reallocation or be returned to the Defence ICT Service Desk.

Defence Protected iPhone or iPad – DRN Access

19. The provisioning and responsibility for costs associated with a Defence Protected iPhone or iPad are at Annex A. Costs comprise an initial amount for the device and accessories, and a monthly data/voice charge. Costs will be detailed when placing a service request on the Defence ICT SRC.

20. Defence Protected iPhones and iPads must be requested through the SRC, which will require approval by the user’s supervisor or commanding officer, GPOC and financial delegate. These devices are assigned to an appointment position number, so if the custodian is transferred to another unit or location, the device is to be transferred to the new incumbent as part of the departure/march-out procedure.

21. If the custodian of a Defence Protected iPhone or iPad is transferred to another unit or location and is given approval by their supervisor/commanding officer and GPOC to move the device to their new position number, a ‘Change of Circumstances’ form must be completed through the SRC, so that it can be asset managed by the losing and gaining GPOCs.

22. A Defence person may be approved to be a custodian of a number of pool devices at unit level. The issue and return of pool devices must be asset managed to ensure a traceable record of who had responsibility for each device. These devices will be configured so that they do not provide access to DRN email, calendar, contacts or tasks/reminders. Internet and Intranet access will be possible and will require the temporary user of a pool device to authenticate with their personal DRN credentials. Access to the Defence Enterprise App Store will be allowed. When the temporary user has finished using the device, they must close all applications, turn off the device and return it to the manager of the pool devices.

Defence Protected iPhone or iPad – Support

23. Only Defence owned and asset-labelled Defence Protected iPhones and iPads will be supported by CIOG. After necessary unit action, damaged devices must be returned to the ICT Service Desk for repair or replacement. If access to the damaged device is possible, the device must be sanitised in accordance with the ASD iOS Hardening Guide by the user prior to transport for repair or replacement. If access is not possible, it is to be packaged and labelled for transport in accordance with the DSM. The ICT Service Desk must not return devices to the supplier, unless they have been sanitised. If the device cannot be sanitised it must be destroyed in accordance with the DSM.

24. Some Defence unclassified and asset labelled smart phones or tablet devices may be deemed suitable to become a Defence Protected iPhone or iPad device. These devices must first be inspected to ensure compliance and compatibility to meet the CIOG's required minimum state. When this policy is published, the minimum requirements, which may change to later versions without notice, are as follows:

a. It is an Apple iPad 2 or later, Apple iPad Mini or later, or iPhone 4S or later.

b. It has not been 'jail-broken', which is the removing of Apple's built-in limitations on the device to provide root access.

c. It is running iOS v6.1.6 or later.

d. It has been sanitised of classified or sensitive data and has no access protection enabled.

25. If a device is not compliant or compatible, it must not be used to access the DRN. If the device is deemed suitable for access to the DRN, any data on the device must be deleted prior to approval to connect to the DRN.

26. CIOG will only provide support to relevant Defence aspects of Defence Protected iPhones and iPads, eg access to DRN email, calendar, contacts, Intranet, Internet and the Defence Enterprise App Store. Further support details will be provided when a device request is approved.

27. If the device is no longer required or justified, prior to it being returned to the Defence ICT Service Desk, it must be sanitised in accordance with the ASD Hardening Guide, and hygienically cleaned.

28. Defence Protected iPad and iPhone users must comply with requirements detailed in the Defence Protected iOS Service Usage Acceptance Certificate provided for their acceptance prior to device dispatch.

Defence Enterprise App Store and software updates

29. A Defence Protected iPad or iPhone provides access to the Defence Enterprise App Store, which provides a list of pre-approved apps that can be installed on the device. Apps not provided through the Defence Enterprise App Store must not be installed on these devices.

30. Defence Protected iPad and iPhone users with a justified business case may request an additional app to be added to the Defence Enterprise App Store via the Defence ICT Service Request Catalogue. Approval of the app request should not be assumed. App requests will be assigned to the Mobile ICT Program of ICT Delivery Division, who will work with the CIOG BRMO to evaluate the request prior to testing and security vetting of the app.

31. The Apple iOS for Defence Protected iPads and iPhones may be updated over a secure Wi-Fi connection, details of which are provided in the device User Guide. Users must not update the software until they have been informed to do so by the Defence ICT Service Desk.

Defence unclassified smart phone or tablet

32. The responsibility for costs associated with Defence unclassified smart phones or tablets is at Annex A.

33. Defence supplied unclassified smart phones or tablets must not be connected to, or access any classified or sensitive network. The exception is for data access to the DRN by using a DREAMS token via a virtual private network (VPN) through the Citrix Receiver application approved for that device. CIOG will support these unclassified devices to the point of ensuring DREAMS connection to the DRN through the Citrix Receiver. Other technical support is the responsibility of the issuing Group or Service.

Personal smart phone or tablet

34. Personal smart phone or tablets are unclassified/unofficial and must not be connected to, or access any classified or sensitive network. Secure access to the DRN can only be achieved by using a DREAMS token via a VPN through the Citrix Receiver application. CIOG support is not provided for these devices, except to the point of ensuring DREAMS connection to the DRN through the Citrix Receiver. Other technical support is the person's responsibility. Such access may be terminated without warning if the DRN security is threatened.

35. Any use that results in a data spill of classified or sensitive data onto a personal device or printer is to be reported, so that corrective actions can be taken, which will be at the user's expense.

DREAMS token

36. The responsibility for costs associated with a DREAMS token is at Annex A. Defence staff requiring a new or replacement DREAMS token are to contact their GPOC for a token and then complete a request via the SRC to have the token activated.

Wireless data card

37. The responsibility for costs associated with a wireless data card is at Annex A, and as detailed in the SRC.

Overseas use

38. Prior to going overseas, users of mobile ICT devices are to liaise with the Defence Mobile Phone Service Desk to determine the most appropriate and cost-efficient option for using their device overseas. This should include a comparison of a local SIM card for postings against a Casual Global Roaming Data Pack for short visits.

39. Australian Defence personnel posted to overseas positions/posts, including Defence Attaches and their staff, Royal Malaysian Air Force (RMAF) Butterworth staff and Defence Materiel Organisation (DMO) Resident Project Team (RPT) staff, generally use unclassified mobile phones, smart phones, tablets and wireless data cards that they procure locally overseas due to the:

a. high costs inherent in using SIM cards of Australia-based telecommunications providers while overseas, and

b. availability of local service providers to negotiate more efficient support to the device, SIM card, usage/charging plan and technical support, that minimises costs while maximising coverage.

40. As a consequence of the sourcing, use and billing for these mobile ICT devices occurring in overseas countries, CIOG funds the Heads of Defence Staff, Defence Attaches and RMAF Butterworth to locally manage the mobile ICT devices used by them and their staff. DMO funds their RPT staff.

41. However, Defence owned BlackBerry devices (with access to either the DRN or Department of Foreign Affairs and Trade's Satin Low), or Defence Protected iPads/iPhones provided from Australia are not procured locally overseas, while the SIM card used in them may be sourced locally.

42. Irrespective of this local, in-country management at overseas posts, all Defence personnel are required to comply with the Defence policies and regulations for appropriate, secure, safe and economic use of Defence mobile ICT resources (devices and services) that they use.

Further information

43. For further information, first refer to the CIOG website. Suggested improvements to this CIOGI may be sent to the Director of ICT Policy and Doctrine by emailing ICT Policy at ict.policy@defence.gov.au.

Annex:
A. Basis of provisioning, repair or replacement by category

Dr Peter Lawrence
Chief Information Officer
Chief Information Officer Group

Annex:
A. Basis of provisioning, repair or replacement by category

Contact Officer:

Earlier CIOG Instruction Cancelled: 03/2010

ANNEX A

BASIS OF PROVISIONING, REPAIR AND REPLACEMENT BY CATEGORY

Table 1: Basis of provisioning

Category of ICT User	Category A	Category B	Category C
• **Defence Unclassified mobile phone** (non-smart phone)	Pre-approved and device/accessories and call/data costs funded by CIOG.		If approved by the user's supervisor. CIOG funded, supported and fleet managed. Call costs may be recovered from the user's Group/Service.
• **DREAMS token**	Token cost is funded by CIOG if approved by the user's supervisor and their GPOC confirms availability within the Group/Service's allocation.		
• **Defence BlackBerry device** (until 1 Jul 15) • **Defence Protected iPhone – DRN access**	Pre-approved by CIOG if agreed by the user's supervisor and GPOC. Device/accessories and call/data costs funded by CIOG (For SES Band 3/3-star officers - two support staff. For other SLG officers - one support staff).		If approved by the user's supervisor, GPOC and financial delegate. Annual fee for device/accessories, call/data and support costs will be recovered from the user's Group/Service.
• **Defence Protected iPad – DRN access** • **Wireless Data Card** • **Defence Unclassified smart phone or tablet**	If approved by the user's supervisor, GPOC and financial delegate. Device/accessories and call/data costs will be recovered from the user's Group/Service.		
• **USB data transfer device – DRN access** • **USB data transfer device – DSN access (when available)**	If approved by the user's supervisor, GPOC and financial delegate.		
• **Defence Secret phone** (SME-PED or Sectéra® GSM®)	If approved by the user's Communication Security Custodian Officer. CIOG fleet managed. Call/data costs may be recovered from the user's Group/Service.		

[redacted]

From:
Sent: 9 8:36 AM
To:
Cc: CIOG CTOD ICTSB ICT Security Governance; Hunt, Karen MRS 3
Subject: RE: 190923 - Email - Application enquiry - JMCO MEL - Closed group communication applications - UNCLAS [DLM=FOR-OFFICIAL-USE-ONLY]

Please find ICTSB guidelines on using WhatsApp application on **Defence Mobiles (Unclassified Only).**

1. Mobile ICT (MOBICT) was provided a Provisional ICT Accreditation (PICTA) on 08 June 2018 for 12 months. The provisions of the PICTA allow WhatsApp with the following conditions.

   (1) WhatsApp is limited for Defence Senior Leadership Team (SLT) on the upgraded MOBICT POC infrastructure only;

   (2) WhatsApp must only be provisioned on MOBICT devices that are managed via the MDM through the UNCLASSIFIED application path;

   (3) WhatsApp is compliant with ASD approved encryption algorithms therefore it is suitable to handle up to and including UNCLASSIFIED DLM information; and

   (4) Requests to access WhatsApp are approved through the existing Defence CIR and application approval process and only on the MOBICT POC infrastructure at this time.

2. Defence ICT Security policy and the acceptable user guide articulate the security risks and users acknowledgement and acceptance of the risk of utilising MOBILE ICT. This is inclusive of the risk of applications allowing Defence Data up to UNCLASSIFIED DLM being exposed to internet facing systems and user's responsibility to ensure the data is protected at that level.

3. CIOG MOBICT are updating Standing Operating Procedures to reflect the use of encrypted applications such as WhatsApp.

4. WhatsApp only authorised within the conditions of the PICTA and MOBICT POC and SOP's.

For further policy guidelines, please refer to DSPF Principles and Control 22.1 Mobility Device Security.
http://intranet.defence.gov.au/home/documents/data/DEFPUBS/DEPTMAN/DSPF/DSPF.pdf

Regards

ICT Security Specialist
Cyber Security Strategy
ICT Security Branch | ICT Operations Division | CIOG | Department of Defence

I acknowledge the Traditional Custodians of the Canberra Region the Ngunnawal and Ngambri people. And pay my respects to their Elders both past and present.

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

[redacted]

From [redacted]
Sen [redacted]
To: [redacted]
Cc: CIOG CTOD ICTSB ICT Security Governance <ictsecurity.governance@defence.gov.au>
Subject: FW: 190923 - Email - Application enquiry - JMCO MEL - Closed group communication applications - UNCLAS [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi

Can you please provide a response to this query? I know there is policy on it and I know BJ's team may be able to assist.

With thanks

[redacted]

[redacted] ɒer Security Performance
ICT Security Management
ICT Security Branch | ICT Operations Division
Chief Information Officer Group | Department of Defence

[redacted]

"High Performance, Teamwork and Respect"

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

[redacted] **On Behalf Of** CIOG Communications

[redacted]

Subject: FW: 190923 - Email - Application enquiry - JMCO MEL - Closed group communication applications - UNCLAS [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good afternoon

We've just received the below enquiry, I believe this one is best answered by you/your team?

Thanks,

Communication Officer

|

Defending Australia and its National Interests
www.defence.gov.au

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.

From:
Sent:
To: CIOG Communications <ciog.communications@defence.gov.au>
Subject: 190923 - Email - Application enquiry - JMCO MEL - Closed group communication applications - UNCLAS [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good Afternoon Sir, Ma'am, All,

I would like to enquire which third party applications such as WhatsApp, Signal and other closed group communication applications are approved / recommended for use on personnel electronic devices by the ADF?

Further to that, where I would find the document, policy or manual that outlines the approved above mentioned and the associated terms and conditions?

Any assistance or pointing in the general direction would be greatly appreciated,

Thank you

IMPORTANT: This email remains the property of the Department of Defence. Unauthorised communication and dealing with the information in the email may be a serious criminal offence. If you have received this email in error, you are requested to contact the sender and delete the email immediately.