From: Media
Sent: Monday, 29 January 2018 7:45 PM
To: Laube, Wade MR 1
Cc: Kelton, Alexandra MS; Hawkins, Amy MS; Fraser, Katherine MRS 1; Media
Subject: FOR OMINDEF CLEARANCE: UPDATED STRAVA RESPONSE [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Wade

As discussed, please see below update to STRAVA response.

DSVS confirmed they are happy to use these words (highlighted in blue below) and also confirmed neither the use of the application by Defence personnel or the release of the data is a security breach.

Below response for your clearance.

Response:

Defence is aware of the possible risks of the collection of location data through personal electronic devices and applications. The circumstances of this application does not constitute a security breach.

All Defence personnel are required to complete annual mandatory security training which includes information on the risks posed by internet-connected devices and online activities. Defence personnel are advised to actively use and manage privacy controls to limit the amount of information they make publicly available and report any suspicious online activities or contacts. Defence also provides regular personal security awareness information to personnel.

On operations, the online presence of ADF personnel and their use of electronic devices is managed in accordance with operational security requirements developed for each activity. Personnel are advised of pertinent restrictions as part of their force preparation and arrival in theatre.

Strava is one of many applications and devices, which collects user information. Many of these devices and activities are important to the quality of life of Defence staff. Defence manages the risks associated with the collection of such information by having layered physical and information security protections for Defence personnel and facilities.

Jessica Skorupa
Assistant Director | Corporate Communication
Ministerial Executive Co-ordination & Communication (MECC) Division

Department of Defence | R1-5-A060 Russell Offices | PO Box 7909 Canberra BC ACT 2610
Phone: (02) 6127 1957 Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

STRAVA APPLICATION USED BY US SOLDIERS

ISSUE: The Australian Defence Force may have to ban fitness app watches during deployments due to applications potentially revealing locations and movements of Defence personnel.

Current media:

KEY POINTS:

- The release of Strava-related information does not constitute a security breach.
- Strava is one of many applications and devices which collect user information. Many of these devices and activities are important to the quality of life of Defence staff.
- While the use of electronic devices is controlled in some sensitive locations, Defence primarily manages the risks associated with the collection of such information by having layered physical and information security protections for Defence personnel and facilities, and by educating staff about the risks.
- All Defence personnel are required to complete annual mandatory security training which includes information on the risks posed by internet-connected devices and online activities.
  - Defence personnel are advised to actively use and manage privacy controls to limit the amount of information they make publicly available and report any suspicious online activities or contacts.
  - Defence also provides regular personal security awareness information to personnel.
- In light of the Strava information release, Defence is reviewing policies and training materials related to the use of personal devices.
- On operations, the online presence of ADF personnel and their use of electronic devices is managed in accordance with operational security requirements appropriate to the degree of risk for each activity.

BACKGROUND TALKING POINTS

- Defence is continuing to review the Strava information, but Defence has not identified any classified or sensitive Australian information being made available through the Strava heat map.

Recent media::
30 January 2018, the Australian, "Fitness app poses a risk to soldiers". Article outlines how sensitive security information on the location of soldiers can be uploaded from fitness watches, such as Fitbits when synced with a smartphone or device.

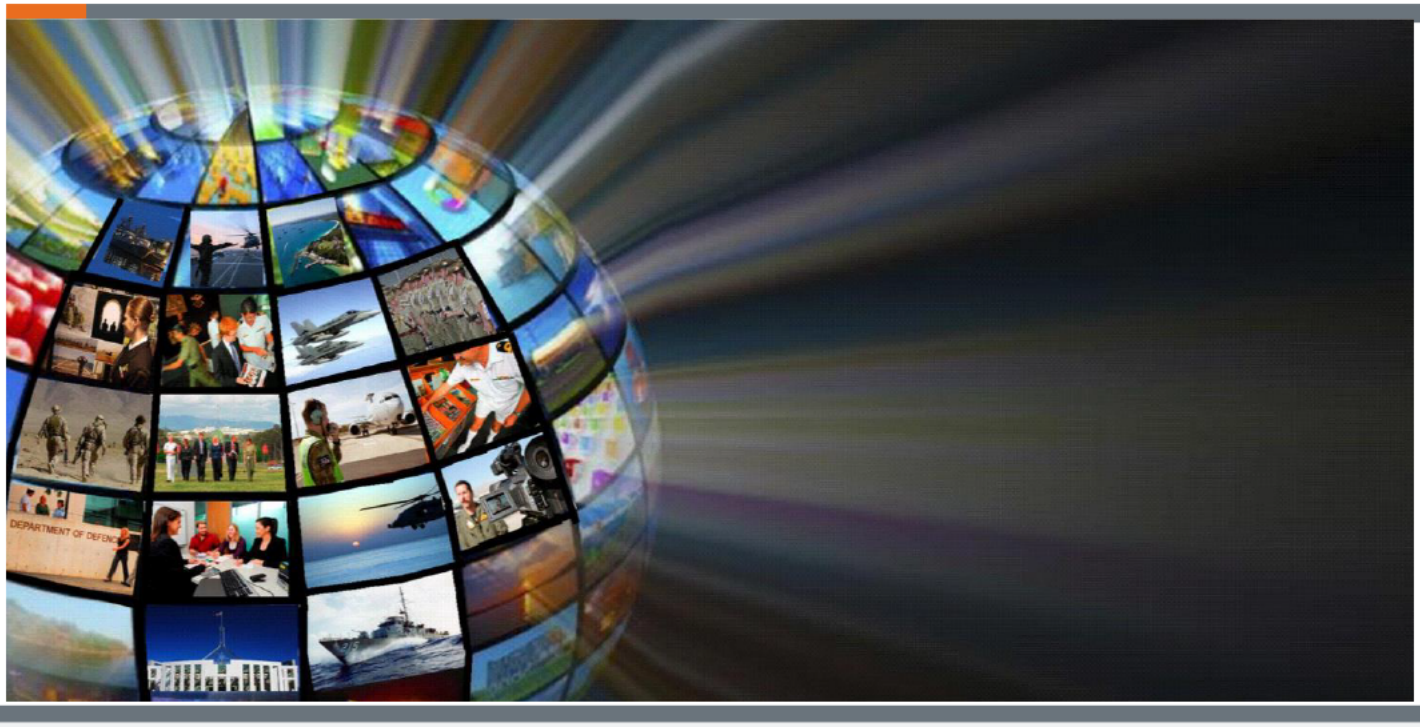
A broad range of media organisations have put questions to Defence concerning the global 'heat map' of user fitness data release by the company Strava over the weekend, and the potential security risks created by the release of this information to Defence personnel.

Contact:	Peter West, ASSPP, 6266 3638	**Min ID:**	QB18-000048
		Division:	Security and Vetting Service
Cleared by:	Celia Perkins, FASS&VS, 6266 2634	**Created:**	30 January 2018
		Updated:	31 January 2018 09:41 AM

Australian Government
Department of Defence

Daily Issues Brief

Wednesday, 31 January 2018



Compiled by the Ministerial and Parliamentary Branch
(02) 6127 1955

While the Daily Issues Brief is unclassified, the information it contains is sensitive in nature and is to be used For Official Use Only. The Daily Issues Brief should be treated as a **Limited Distribution** document and not forwarded to any other party without the authority of Ministerial and Executive Coordination and Communication Division.

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

STRAVA APPLICATION USED BY US SOLDIERS (*NEW*)

ISSUE: The Australian Defence Force may have to ban fitness app watches during deployments due to applications potentially revealing locations and movements of Defence personnel.

KEY POINTS:

- The release of this information does not constitute a security breach.
- Strava is one of many applications and devices which collect user information. Many of these devices and activities are important to the quality of life of Defence staff.
- While the use of electronic devices is controlled in some sensitive locations, Defence primarily manages the risks associated with the collection of such information by having layered physical and information security protections for Defence personnel and facilities, and by educating staff about the risks.
- All Defence personnel are required to complete annual mandatory security training which includes information on the risks posed by internet-connected devices and online activities.
  - Defence personnel are advised to actively use and manage privacy controls to limit the amount of information they make publicly available and report any suspicious online activities or contacts.
  - Defence also provides regular personal security awareness information to personnel.
- In light of the Strava information release Defence is reviewing policies and training materials related to the use of personal devices.
- On operations, the online presence of ADF personnel and their use of electronic devices is managed in accordance with operational security requirements developed for each activity.

BACKGROUND TALKING POINTS

- Defence is continuing to review the Strava information, but Defence has not identified any classified or sensitive Australian information being made available through the Strava heat map.

Recent media::
30 January 2018, the Australian, "Fitness app poses a risk to soldiers". Article outlines how sensitive security information on the location of soldiers can be uploaded from fitness watches, such as Fitbits when synced with a smartphone or device.

A broad range of media organisations have put questions to Defence concerning the global 'heat map' of user fitness data release by the company Strava over the weekend, and the potential security risks created by the release of this information to Defence personnel.

Contact: Peter West, ASSPP, P 6266 3638

Cleared by: Celia Perkins, FASS&VS, P 6266 2634

Min ID: QB18-000048
Division: Security and Vetting Service

Created: 30 January 2018
Updated: 31 January 2018 09:41 AM

From: Media
Sent: Monday, 29 January 2018 5:30 PM
To: s22 [redacted]
Cc: Hawkins, Amy MS; Kelton, Alexandra MS; Fraser, Katherine MRS 1; Media
Subject: For OMINDEF clearance: STRAVA - draft statement to media enquiries [SEC=UNCLASSIFIED]

Good afternoon

Defence media has received six enquiries today off the back of media reporting about Strava, a fitness app that has a 'global heat map' application within it. Copied below are sites for reference.

https://labs.strava.com/heatmap/#7.00/-120.90000/38.36000/hot/all
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Defence Security Vetting Service has prepared the below statement to provide to the following journalists:

- Luke Henriques-Gomes, News Daily
s47F [redacted]

The statement has been by OSEC and OCDF.

For OMINDEF clearance.

Regards
Jess

Jessica Skorupa
Assistant Director | Corporate Communication
Ministerial Executive Co-ordination & Communication (MECC) Division
Department of Defence | R1-5-A060 Russell Offices | PO Box 7909 Canberra BC ACT 2610
Phone: (02) 6127 1957 Email: media@defence.gov.au | Follow us on Twitter: @DeptDefence

Response:

Defence is aware of the possible risks of the collection of location data through personal electronic devices and applications.

All Defence personnel are required to complete annual mandatory security training which includes information on the risks posed by internet-connected devices and online activities. Defence personnel are advised to actively use and manage privacy controls to limit the amount of information they make publicly available and report any suspicious online activities or contacts. Defence also provides regular personal security awareness information to personnel.

On operations, the online presence of ADF personnel and their use of electronic devices is managed in accordance with operational security requirements developed for each activity. Personnel are advised of pertinent restrictions as part of their force preparation and arrival in theatre.

Strava is one of many applications and devices, which collects user information. Many of these devices and activities are important to the quality of life of Defence staff. Defence manages the risks associated with the collection of such information by having layered physical and information security protections for Defence personnel and facilities.