Review report

Vessel tracking data security

1. Background

This report is prepared in response to item 8.1 and 8.3 in the Queensland Ombudsman's preliminary observations and proposed actions.

Table 1 Extract from Ombudsman's preliminary observations and proposed actions, 8.1 and 8.3

No.	Observations	Proposed actions
8.1	The department has acknowledged the significance, sensitivity and commercial value of the industry's fishing data. The current framework for vessel tracking, involves numerous private companies and government agencies, each with varying access to vessel tracking information (the industry's fishing data). These parties include satellite operators, airtime service providers, suppliers, data management companies and various government agencies. The department's internal audit[1] made a number of recommendations to improve the security of this sensitive information.	• Review the action taken on the recommendations made by the department's Internal Audit report. • Publish the outcomes of the review and any further actions the department has taken to strengthen privacy controls.
8.3	The complainants have raised concerns about the information privacy controls around their vessel tracking information. The department's internal audit report[1] addressed this issue and was further considered in PricewaterhouseCoopers (PWC) Assurance Report[2]. Both of these reviews have made recommendations for action. The department has also confirmed it is working towards achieving the requirements of ISO27001 – Information Security Management standard.	• Provide advice to the industry about the data access availability and security controls that exist to each of the entities (i.e. satellite service providers, airtime service providers, suppliers, the department, compliance agencies, Trackwell etc.) involved in the vessel tracking framework. This advice is to address the actions taken by the department to implement the audit recommendations and the department's progress to achieve the implementation of ISO27001.

[1] Readiness review of vessel tracking system, internal audit report, July 2018
[2] Assurance report on confidentiality security controls in relation to the vessel tracking system – for the period 1 October 2018 through 31 March 2019, PwC, 19 July 2019
Source: Ombudsman's Preliminary Observations and Proposed Actions - https://daf.engagementhub.com.au/projects/download/8309/ProjectDocument

This report provides an overview of the vessel tracking data flow from the point of collection through to its use and disclosure. It includes the parties involved in each step and the controls in place to manage data security including those identified in the internal audit conducted in July 2018.

2. Overview of vessel tracking system and data flow

The overview of the vessel tracking system and the vessel tracking data flow is depicted in Figure 1 below.

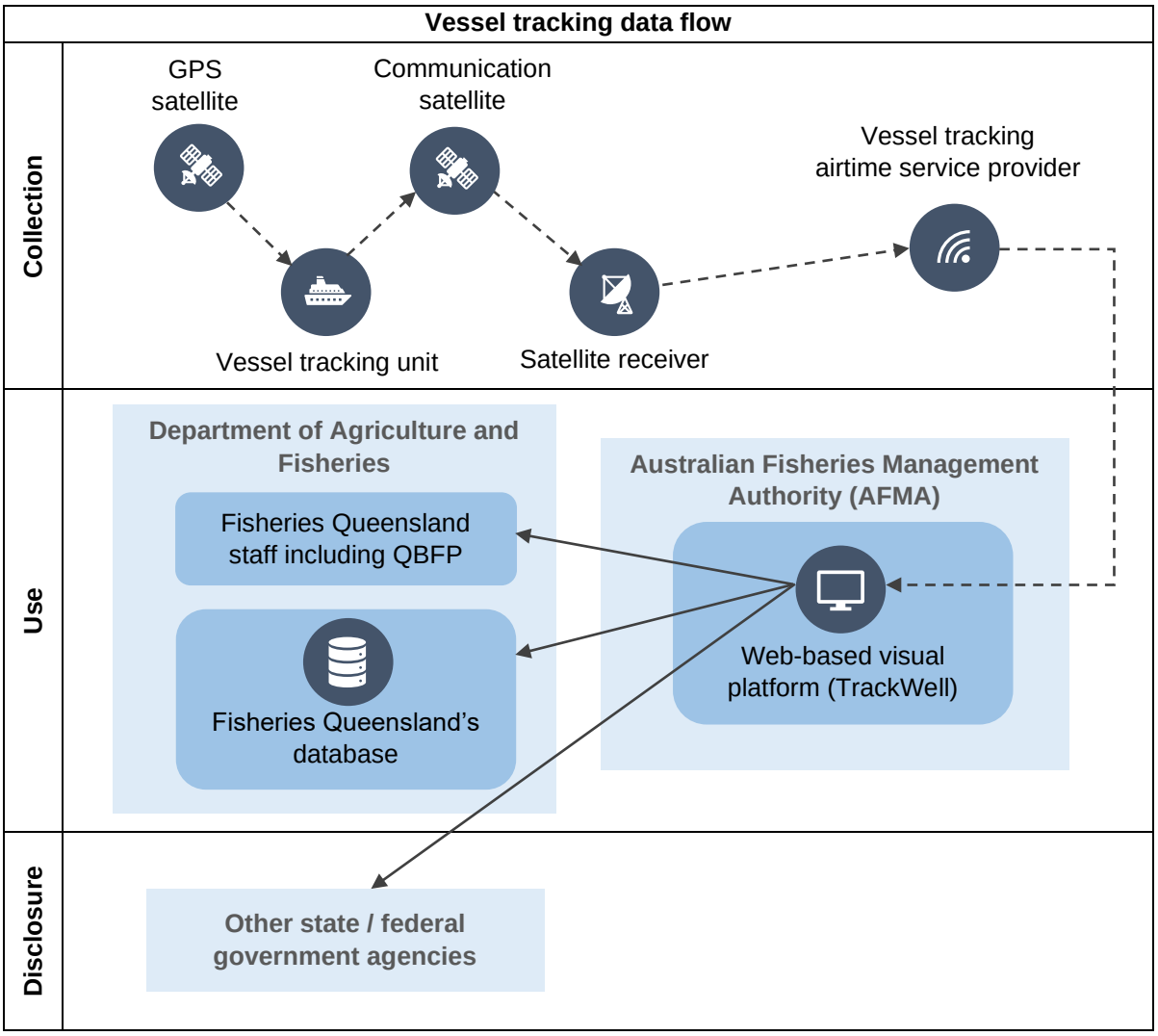

Figure 1: Vessel tracking system and data environment

2.1 Collection of vessel tracking data

The Department of Agriculture and Fisheries (DAF) collects vessel tracking data from commercial fishers under section 80 of the *Fisheries Act 1994*. Under this section, commercial fishers have the obligations to install approved vessel tracking units, and to send vessel tracking data to DAF via the approved vessel tracking airtime service provider. The current approved airtime service providers are Pivotel, Pole Star and CLS Oceania.

The information of a vessel's location is sent from the vessel tracking unit directly to a communications satellite. This information is then received by a land based receiver station and forwarded to a web-based visual platform and to DAF's database.

2.2 Use of vessel tracking data

The web-based visual platform is accessible by relevant DAF staff members including Queensland Boating and Fisheries Patrol officers to help monitor compliance. The web-based visual platform is managed by the Australian Fisheries Management Authority (AFMA), the Australian Government fisheries agency.

Vessel tracking data collected by DAF is used to:

- monitor quota in near real time (e.g. deducting fishing days from individual's quota)
- monitor compliance with area and seasonal closures (including marine park zones)
- provide intelligence and evidence for investigations
- help validate logbook data on where and when fishing occurred
- provide fishing effort data that is used in stock assessments to estimate the biomass of a fish stock
- help inform fishery management changes that may be needed.

2.3 Disclosure of vessel tracking data

Under section 217A of the *Fisheries Act 1994*, DAF may enter into information sharing arrangements with other state or federal government entities to share vessel tracking data if it helps that entity to perform functions under a law of the relevant state or federal government. These external state / federal agencies only have access to the web-based visual platform, not the database, which is kept by DAF.

Separate to any information sharing arrangements under section 217A of the *Fisheries Act 1994*, section 217B of the *Fisheries Act 1994* allows DAF to disclose vessel tracking data in certain circumstances. These include if DAF has the consent of the person to whom the information relates or in certain situations where the disclosure is required or permitted by law.

3. Data security controls

3.1 Vessel tracking providers

DAF has established a deed of confidentiality and privacy with the vessel tracking unit and airtime service providers to safeguard vessel tracking data collected from commercial fishers. The deed of confidentiality and privacy outlines the providers' obligations to keep data secure and confidential and ensure it is not used for personal gain.

Separate to this, vessel tracking contracts between commercial fishers and the providers have standard terms and conditions that limits liability of the company. This is like mobile telephone plans. As is the case with most commercial contracts, liability is limited and based on proven negligence. These contracts are still subject to federal and state consumer and privacy legislation that protects the rights of individuals.

Vessel tracking providers have their own internal processes and security controls to ensure safe handling of personal information. Further details on management of private information by vessel tracking providers can be found in the contract held between fishers and the providers, as well as their privacy policy that are available online.

- Pivotel's privacy policy (https://www.pivotel.com.au/privacy_policy/)
- Pole Star's privacy policy (https://www.polestarglobal.com/privacy-cookie-policy)

In addition, Pole Star Space Applications Ltd is certified to ISO 27001 Information Security Management Standard.

3.2 Web-based visual platform (TrackWell)

The web-based visual platform, called TrackWell, is currently governed and used by the Australian Fisheries Management Authority (AFMA) to manage the Australian Government fisheries. In terms of the management of private and confidential information, the level of security meets the federal data security requirement. AFMA is required to comply with the Australian Government Information Security Manual. All the contractual requirements with Trackwell, including security and privacy provisions, are in accordance with Australian Signals Directorate specifications and Australian Government procurement, security, data and privacy regulations, guidelines and rules.

Access to TrackWell is restricted to authorised and appropriate personnel in DAF to perform functions under the *Fisheries Act 1994*. TrackWell is currently accessible to the Vessel Tracking team members to provide vessel tracking administrative support and to Queensland Boating and Fisheries Patrol officers to assist with compliance. Access to TrackWell is also provided to personnel in other state and federal government entities, which DAF has an information sharing agreement with to share vessel tracking data under section 217A of the *Fisheries Act 1994*.

The following controls were implemented within the TrackWell applications and configuration:

- Role-based permissions that enable limit of use or access by each user
    - These permissions include a read-only access, access limited to jurisdiction, administrative access to update vessel tracking unit details and high-level administrative access to add new users.
- Automatic locking of accounts after a period of inactivity
- Password setting
- Ability to audit search parameters that an individual undertakes in the application.

In addition to the configured controls above, the following form part of current operational procedure to maintain logical access to TrackWell:

- Access requests require review and approval.
    - All DAF staff must complete the Code of Conduct.
    - Requests from other government entities that have an information sharing arrangement under section 217A of the *Fisheries Act 1994* must be accompanied by their Director approval.
- Access levels are reviewed quarterly.
- Monthly QBFP user audit is conducted to ensure up-to-date user list.
- Access provided to other agencies is periodically confirmed for appropriateness.
- Audit logs in TrackWell that enable identification of user activity.

3.3 DAF's database

Vessel tracking data stored in DAF's database is used by DAF to conduct fishing effort analysis and data validation. Access to the database is restricted to relevant DAF staff members and reviewed periodically.

The following physical access controls are applicable to servers that store the vessel tracking data:

- Servers are housed in locked buildings.
- Access to servers is restricted to issued swipe cards.

3.4 External service providers

External service providers contracted to maintain the operation of DAF's systems are required to undergo annual Code of Conduct training. Additionally, the contract held with service providers includes a Deed of Confidentiality to safeguard private and confidential information that the service providers may access while performing their work.

3.5 Other state / federal government agencies

DAF has established information sharing agreements under section 217A of the *Fisheries Act 1994* with other state and federal government entities to share vessel tracking data. The information sharing agreement outlines the requirement to keep data secure and confidential and ensure it is not used for personal gain. It includes a reporting obligation on the agencies to provide DAF an annual report detailing data usage including compliance outcomes from the agencies' use of the data.

Additionally, all state and federal government agencies are required to comply with their relevant Code of Conduct and all relevant laws applicable to the handling of private and confidential information. This includes the *Privacy Act 1988 (Commonwealth)* relevant to federal agencies and the equivalent legislation or guidelines applicable to government agencies in each state.

3.6 Queensland legislations

Section 217B of the *Fisheries Act 1994* establishes an offence for the inappropriate use or dissemination of information. Any inspector, public service employee, Local Government employee or delegate who inappropriately uses or disseminates such information could face a maximum penalty of up to 50 penalty units ($6 892)[3].

Further, there are additional protections against the use of personal information provided for in the *Information Privacy Act 2009* (Qld).

4. Data security assurance

DAF engaged PricewaterhouseCoopers (PwC) to conduct an external audit to review procedures and control measures put in place for the vessel tracking system, throughout the period 1 October 2018 to 31 March 2019. PwC finalised audit found that the controls put in place by DAF, were suitably designed to achieve the control objectives throughout the audit period and the controls that could be tested, operated effectively throughout the audit period. A copy of the assurance report is available upon request.

5. DAF Information Security Management System

DAF has implemented and actively maintains an Information Security Management System (ISMS) based on the international security standard ISO 27001. This is in accordance with the requirements outlined in the *Queensland Government Information Security Policy IS18:2018*.

The ISMS includes all information, system and technology assets identified in the department's information asset register and application asset register. The ISMS takes a systematic and repeatable risk-based approach to managing information, ensuring that steps are taken to minimise threats outside of the department's established risk appetite. This includes managing information security risks related to the confidentiality, integrity and availability of information entrusted to us.

In line with the ISMS, DAF conducts six-monthly risk assessment and monitoring of existing data security controls in the vessel tracking system as part of the Whole of Government Information and Communication Technology planning process administered by the Queensland Government Customer and Digital Group. This enables risk mitigation activities to be identified and implemented. DAF also undertakes other regular ongoing improvement activities and assessments as part of its ISMS.

---

[3] Based on penalty unit value in Queensland of $137.85 current from 1 July 2021.