COMMONWEALTH OMBUDSMAN

# A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

**For the period 1 July 2016 to 30 June 2017**

**Report by the Commonwealth Ombudsman**
**under s 186J of the *Telecommunications (Interception and Access) Act 1979***

**November 2018**

COMMONWEALTH OMBUDSMAN

# A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

**For the period 1 July 2016 to 30 June 2017**

**Report by the Commonwealth Ombudsman**
**under s 186J of the *Telecommunications (Interception and Access) Act 1979***

**November 2018**

ISSN 2207-4678 (Print)
ISSN 2207-4686 (Online)





Contact us
Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: **1300 362 072**
Email: **ombudsman@ombudsman.gov.au**

# Contents

# Executive Summary

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) from 1 July 2016 to 30 June 2017. These inspections examined agency records relating to telecommunications data for the period 13 October 2015 to 30 June 2016, and records relating to stored communications for the period 1 July 2015 to 30 June 2016.

Under the Act, 20 specified law enforcement agencies are able to lawfully access individuals' telecommunications data and/or stored communications when investigating certain offences.

Telecommunications data, also known as metadata, is information about a communication, but does not include the contents or substance of that communication. Agencies have the power to internally authorise access to this information, however, if an agency wishes to access telecommunications data that will identify a journalist's information source, the agency must apply to an external issuing authority for a warrant.

Stored communications are communications that have already occurred and are stored on a carrier's systems—they contain the content of the communication. An agency must apply to an external issuing authority for a warrant to access stored communications. Before a warrant is issued an agency may authorise the 'preservation' of a stored communication, to prevent a carrier from destroying the communication before it can be accessed under a warrant.

These are covert and intrusive powers, given to agencies for the purposes of law enforcement. A person who has been subject to the use of these powers will not be aware of their use, and therefore, will not be in a position to make a complaint. Instead, the Office provides independent oversight by conducting inspections of each agency that has exercised these powers during the relevant period. At these inspections, we assess whether agencies' use of the powers complies with the legislation.

In addition to assessing compliance, we enhance transparency and public accountability by reporting our findings to the Minister for Home Affairs (the Minister) who must then make the report public.

As a result of our 2016–17 inspections we formed the view that agencies were generally exercising their powers to access stored communications and telecommunications data appropriately. Agencies had frameworks in place to ensure appropriate access to intrusive powers and these frameworks appeared to be working as intended. Agencies also demonstrated a commitment to compliance and responded appropriately to compliance issues.

An inspection may identify a range of issues including minor administrative errors, instances of serious non-compliance and systemic issues. In reports the Ombudsman may make suggestions for improvement or make formal recommendations if an issue has not been addressed by the agency and/or is sufficiently serious.

From the 37 inspections we conducted under the Act during 2016–17, we made three recommendations.

## Summary of Telecommunications Data Findings

Overseeing access to telecommunications data is a relatively new function for our Office, having commenced in late 2015. Prior to our oversight, agencies had accessed telecommunications data for a number of years, and already had policies and procedures in place.

During the 2016–17 inspections, agencies demonstrated a high level of compliance with the Act. We noted good levels of transparency and accountability and strong compliance cultures, which are important in mitigating the risk of relying on individual staff's diligence to achieve compliance. However, we identified non-compliance in a number of key areas including:

- adherence to the Journalist Information Warrant provisions
- inability to sufficiently demonstrate required privacy considerations
- access to unauthorised telecommunications data
- statistical issues
- record keeping.

All agencies were receptive to our findings, recommendations and suggestions.

## Summary of Stored Communication Findings

Our Office has had an oversight role for certain agencies' access to stored communications since 2006.

Our 2016–17 inspections assessed agencies as generally compliant with the Act. During our stored communications inspections we noted good levels of transparency and accountability and strong compliance cultures. We also noted agencies' willingness to disclose compliance issues they had identified.

Notwithstanding these positive observations, we also identified non-compliance in a number of key areas, including:

- mandatory revocation requirements for preservation notices
- agencies' actions in response to receiving unlawfully accessed stored communications from carriers
- destruction requirements
- proper delegation of stored communications powers.

All agencies were receptive to our findings and suggestions.

# Introduction

Amendments to the *Telecommunications (Interception and Access) Act 1978 (the Act)* commenced on 13 October 2015, giving the Office an over-arching role in assessing agencies' compliance with Chapter 3 (preserving and accessing stored communications) and Chapter 4 (accessing telecommunications data) of the Act.

The Office inspects agencies' records to assess the extent of compliance with the Act when their officers use these powers. The Ombudsman is also required to report to the Minister on the results of those inspections. The Minister must then table the report in Parliament.

Access to stored communications and telecommunications data are intrusive powers afforded to agencies. Our role is to independently assess compliance with legislation to enhance transparency and public accountability.

Prior to the amendments to the Act, agencies could lawfully obtain telecommunications data from telecommunications carriers (carriers) and there was no independent oversight of the use of this power.

The Office has performed an oversight role in relation to stored communications since 2006. Prior to the amendments to the Act, however, this role was limited to assessing compliance with the record keeping and destruction provisions of Chapter 3. The amendments expanded our role to encompass the whole of Chapter 3, consistent with the oversight of telecommunications data.

In performing this role the Office does not oversee carriers; however, we do liaise with carriers to understand how their practices may impact agencies' compliance.

***How we oversee agencies***

We have developed a set of inspection methodologies we apply consistently across all agencies. These methodologies are based on the legislative requirements of the Act and are regularly updated in response to legislative amendments and changes to agency processes. This ensures we can comprehensively assess compliance.

During inspections we focus on areas of high risk and consider the impact of non-compliance; for example, where there is unnecessary privacy intrusion.

Assessments are based on the records made available at the inspection, interviews with relevant agency staff, processes we observe and information agency staff provide in response to any identified issues. To ensure agencies understand what we will be assessing, our Office provides a broad outline of its criteria prior to each inspection. This assists

agencies to identify sources of information to demonstrate compliance. We also have coercive powers to obtain any information relevant to the inspection.

We encourage agencies to disclose any instances of non-compliance and inform us of any remedial action they have implemented. Our Office also provides assistance to agencies to achieve compliance through assessing policies and procedures, communicating better practices in compliance, facilitating communication across agencies and generally engaging with agencies outside of the inspection process.

Due to the sensitive nature of the information inspected, part of our risk mitigation strategy is to limit inspections to records relating to authorisations or warrants that are no longer in force.

The criteria for our telecommunications data inspections can be found at Appendix A, and for our stored communications inspections at Appendix B.

***Inspection limitations***

Due to the significant volume of records that fall within the scope of our oversight, a representative sample is chosen to inspect. Selection of a sample is guided by the Auditing Standard ASA 530 *Audit Sampling*. Prior to an inspection our Office requests agencies provide details of the total number of records subject to the inspection. This information is used to prepare a sample, which focuses on areas of high risk and is representative of the total number of records.

At inspections we assess written records, electronic records and the policies and procedures used by the agency. We supplement this with interviews with relevant officers involved in the use of these powers. Our Office is not present during the application of these covert powers and we assess the use of powers retrospectively, through records based inspections.

***How we report***

To ensure procedural fairness, agencies are provided with our preliminary inspection findings following an inspection and given the opportunity to provide comments prior to finalisation. The finalised inspection findings are used to prepare this report to the Minister.

In this report our Office may comment on issues beyond instances of non-compliance, such as the adequacy of an agency's policies and procedures or any risks to compliance. We do not generally include administrative issues or instances of non-compliance where the consequences are negligible, for example where the actions of an agency did not result in unnecessary privacy intrusion.

In reporting the results of our inspections, we are constrained by the secrecy provisions in sections 133, 181B and 182 of the Act. These provisions prohibit the disclosure of certain information.

***Agencies we oversee***

There are currently 20 agencies that have access to telecommunications data and stored communications under the Act. The Minister may declare additional agencies in prescribed circumstances, however this did not occur in 2016–17. These agencies are:

| Agency | Acronym |
|---|---|
| Australian Criminal Intelligence Commission | ACIC |
| Australian Competition and Consumer Commission | ACCC |
| Australian Commission for Law Enforcement Integrity | ACLEI |
| Australian Federal Police | AFP |
| Australian Securities and Investments Commission | ASIC |
| Corruption and Crime Commission Western Australia | CCC (WA) |
| Crime and Corruption Commission Queensland | CCC (QLD) |
| Former Department of Immigration and Border Protection (including the Australian Customs and Border Protection Service) [1] | DIBP |
| Independent Broad-based Anti-corruption Commission | IBAC |
| Former Police Integrity Commission[2] | PIC |
| New South Wales Crime Commission | NSW CC |
| Independent Commission Against Corruption (New South Wales) | ICAC (NSW) |
| New South Wales Police Force | NSW Police |
| Northern Territory Police | NT Police |
| Queensland Police Service | QLD Police |
| Independent Commissioner Against Corruption (South Australia) | ICAC (SA) |
| South Australia Police | SA Police |
| Tasmania Police | TAS Police |
| Victoria Police | VIC Police |
| Western Australia Police | WA Police |

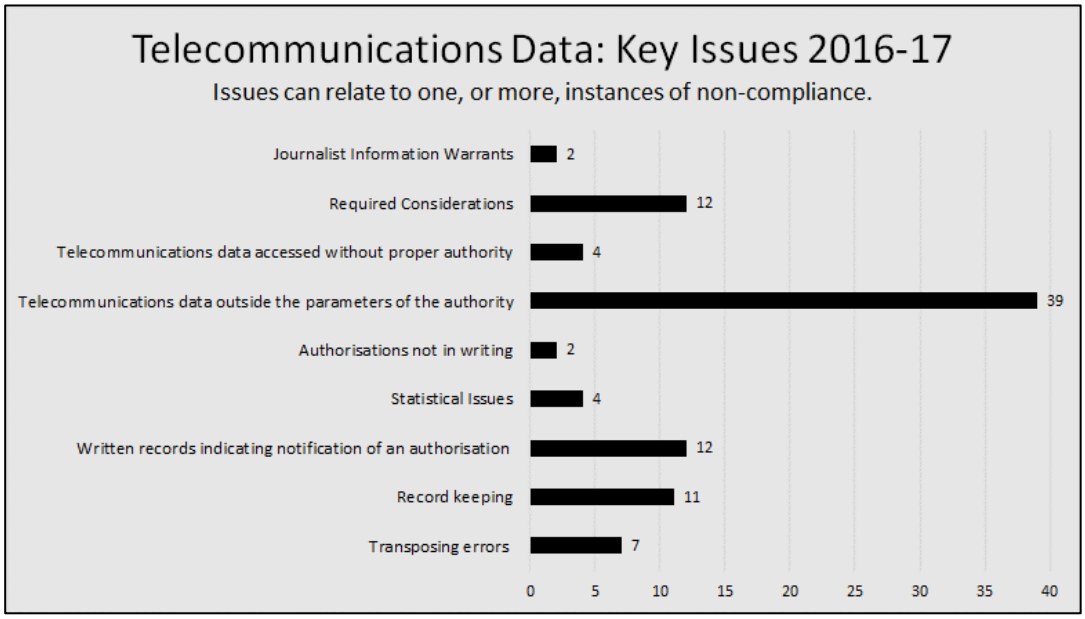
[1] On 20 December 2017, the Department of Home Affairs (Home Affairs) was formally established and comprises the former DIBP. As the DIBP was still an entity during the inspection period it is referred to as such for the purposes of this report; however any suggestions or recommendations have been directed to Home Affairs.

[2] On 1 July 2017, the PIC was abolished and the Law Enforcement Conduct Commission (LECC) commenced operations. As the PIC was still an entity during the inspection period it is referred to as such for the purposes of this report; however any suggestions or recommendations have been directed to LECC.

# Inspection Findings

## Results of telecommunications data inspections conducted in 2016–17

During 2016–17 our Office conducted 21 inspections of agencies' access to telecommunications data; these inspections covered records made from 13 October 2015 to 30 June 2016.[3]




**Telecommunications Data: Key Issues**

As the 2015–16 inspections were the first time agencies had been scrutinised on how they access telecommunications data, our Office focused on understanding the policies, procedures and controls already in place at each agency. During 2016–17 our Office relied on this understanding and continued to assess, and monitor the effectiveness of these policies, procedures and controls.

During our 2015–16 inspections we found that agencies generally had sound policies and processes in place for accessing telecommunications data. We identified common areas of risk for all agencies including:

- the level of involvement and support from senior leadership

[3] An exception to this is the records covered by our non-routine inspection conducted on 5 May 2017.

- the timeliness and comprehensiveness of training given to staff exercising telecommunications data powers

- the effectiveness of agencies' internal communications in raising awareness of relevant changes and sharing better practices.

With these common areas of risk in mind, the following key issues were identified in our 2016–17 inspections.

**Journalist Information Warrants**

On 13 October 2015, the Act was amended to introduce a higher threshold for instances where agencies wished to access telecommunications data in relation to a journalist for the purpose of identifying that journalist's source. The Journalist Information Warrant provisions were introduced in recognition of the public interest in protecting journalists' sources, while ensuring agencies have the investigative tools necessary to protect the community. These provisions require an application to be made to an issuing authority, such as an eligible Judge or Administrative Appeals Tribunal Member. Applications for a warrant are also subject to scrutiny by a Public Interest Advocate, who is appointed by the Prime Minister under the Act. These oversight mechanisms aim to ensure that access to such information is only permitted where it is reasonably necessary and where the public interest in the issuing of the warrant outweighs the public interest in maintaining the confidentiality of the journalist's source.

Section 180H of the Act states that an authorised officer of an enforcement agency must not make an authorisation that would authorise the disclosure of information or documents relating to a particular person if:

- the authorised officer reasonably believes that person to be a journalist or journalist's employer, and

- the purpose of making the authorisation would be to identify a person whom the authorised officer reasonably believes to be a source of the journalist or journalist's employer.

If the above conditions are met, a Journalist Information Warrant must be sought before the authorised officer grants an authorisation in relation to the journalist or journalist's employer. Section 180Q(1) of the Act states that an enforcement agency may apply to a Part 4–1 issuing authority for a Journalist Information Warrant.

In determining compliance with the Journalist Information Warrant provisions we take into account agencies' processes and procedures, as well as records provided during the inspection. Most agencies had strong controls in place to mitigate non-compliance with

these provisions; for example, system prompts to remind officers of the requirements of the Act, mandatory training for relevant officers and comprehensive guidance material.

On 26 April 2017 the AFP disclosed to our Office that it had accessed the telecommunications data of a journalist without obtaining a Journalist Information Warrant, contrary to the requirements of the Act. In response to this disclosure our Office conducted an inspection of the AFP on 5 May 2017, which focused on understanding how the breach occurred and assisting the AFP to minimise the chances of future breaches. The results of that inspection were tabled in Parliament in November 2017 and can be accessed on our Office's website.[4] Through our routine annual inspections of the AFP we continue to monitor the AFP's compliance, including the progress made by the AFP in addressing previous inspection findings. Our Office assessed how the AFP was addressing this issue during our routine inspection in 2017–18 and again during a non-routine inspection conducted in 2018–19.

In addition to the breach disclosed by the AFP, during 2016–17 we identified two instances where WA Police made an application for a Journalist Information Warrant to a person who was not a Part 4–1 issuing authority. This occurred due to a lack of awareness by WA Police regarding to whom an application for a Journalist Information Warrant could be made. In response to this issue, WA Police took steps to quarantine all information obtained under the invalid warrants.

**Required Considerations**

Under s 180F of the Act, before making an authorisation for telecommunications data, an authorised officer must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of the telecommunications data is justifiable and proportionate.

An authorised officer may only make an authorisation under Chapter 4 if they are satisfied, on reasonable grounds, that any interference with privacy is justifiable and proportionate. Section 186A(1)(a)(i) of the Act requires the chief officer to ensure documents or other materials are kept that indicate whether an authorisation was properly made, including whether all relevant considerations have been taken into account. In considering 'other materials', we may rely on an agency's policies and processes, systems checks, and interviews with relevant officers of the agency to inform our understanding of an agency's processes, which are then used to assess an agency's compliance with s 186A(1)(a)(i).

Our Office does not assess the merits of internally approved authorisations unless they are clearly contrary to the legislative thresholds. Our assessment focuses on whether

[4] The report can be accessed at: http://www.ombudsman.gov.au/__data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf

authorised officers were provided enough information to appropriately consider the requirements under s 180F and all other relevant considerations.

During 2016–17 our Office conducted interviews with authorised officers, requesting officers and other relevant staff to ascertain the effectiveness of processes and procedures agencies had in place to ensure authorised officers were considering the required matters. Generally, privacy was being appropriately considered by authorised officers within agencies, however we did identify a number of instances where agencies were unable to demonstrate authorised officers had been satisfied of the required considerations. When we raised these instances, agencies were receptive to our findings, and showed commitment to addressing the issue.

Our Office also identified a number of instances where authorisations specified an offence which was inconsistent with the offence specified in the application for the authorisation.[5] Such inconsistencies cause ambiguity in demonstrating the grounds for making an authorisation. It also indicates that agencies' quality assurance mechanisms may not always be effective in identifying such errors.

**Telecommunications data accessed without proper authority**

Section 5AB(1A) of the Act states that the Commissioner of Police (of the AFP) may authorise in writing a senior executive employee within the AFP to be an 'authorised officer'. Under the Act, only an authorised officer may authorise the disclosure of telecommunications data.

During 2015–16 the AFP disclosed to our Office that, between 13 and 26 October 2015, all authorisations within ACT Policing were made by an officer not authorised under s 5AB(1A) of the Act. This issue affected 116 authorisations during the period. This issue also affected a large number of authorisations dating back to March 2015, which precede the commencement of our Office's oversight on 13 October 2015.

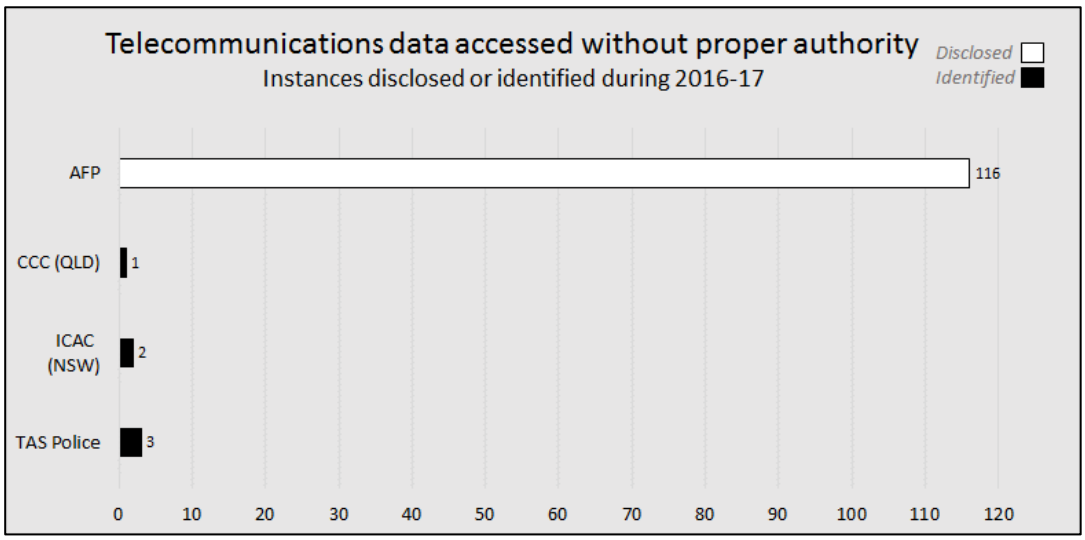
The AFP advised this non-compliance occurred due to the Commissioner's written authorisation under s 5AB(1A) failing to authorise any officers within ACT Policing. The AFP advised this omission on the written authorisation was due to an administrative oversight. Upon identifying the error, the AFP updated the Commissioner's written authorisation on 26 October 2015 to appoint the relevant position within ACT Policing as an authorised officer.

In response to this disclosure, our Office suggested the AFP quarantine all telecommunications data obtained under the 116 authorisations made by the unauthorised ACT Policing officer between 13–26 October 2015 from further use and

[5] This issue was identified at TAS Police and AFP. IBAC also disclosed one instance.

communication. Following the inspection, the AFP accepted this suggestion; however it did not act to quarantine the affected data at that time, which resulted in additional use and communication of the data. Partial quarantining of the affected data was initiated in February 2018, after our Office contacted the AFP to ask whether remedial action had been finalised. In April 2018 the AFP advised the affected telecommunications data had not yet been fully quarantined and it was seeking legal advice regarding the use of the affected telecommunications data. Due to the scale of this non-compliance, we will continue to monitor this issue closely with the AFP.

In addition to the AFP's disclosure, we identified a small number of instances at other agencies where telecommunications data was obtained either prior to, or without a valid authorisation.[6] This occurred as a result of processes and procedures being incorrectly applied. We were satisfied by the prompt remedial action these agencies took in response to identified instances.




**Telecommunications data outside parameters of the authority**

Under the Act an authorised officer may authorise the disclosure of specified telecommunications data that *came into existence before the carrier received notification of the authorisation*. We refer to this as an 'historic authorisation'. As historic authorisations only permit access to existing telecommunications data, any telecommunications data dated after the authorisation comes into force is outside the parameters of the authority.

The Act also establishes that an authorised officer may authorise the disclosure of specified telecommunications data that *comes into existence during the period the authorisation is*

[6] TAS Police, CCC (QLD) and ICAC (NSW).

*in force (subsection 180(3))*. This is a 'prospective authorisation'. A prospective authorisation comes into force at the time the carrier receives notification of the authorisation and, unless the authority is revoked, ends at the time specified in the authorisation. Any telecommunications data dated before the authorisation comes into force, after its expiry, or after it was revoked is outside the parameters of the authority.

An agency may further limit the scope of the telecommunications data it authorises by restricting the request to a particular date range or search terms.

When conducting our compliance assessments under these sections, we take into consideration what telecommunications data the agency has specified on the authorisation and whether the telecommunications data provided by the carrier complies with those parameters.

Broadly speaking, for these types of authorisations, telecommunications data received outside the parameters of the authority can be divided into four distinct categories:

**I.** variations or omissions of names for searches conducted on the Integrated Public Number Database

**II.** telecommunications data provided to agencies outside the authorised period

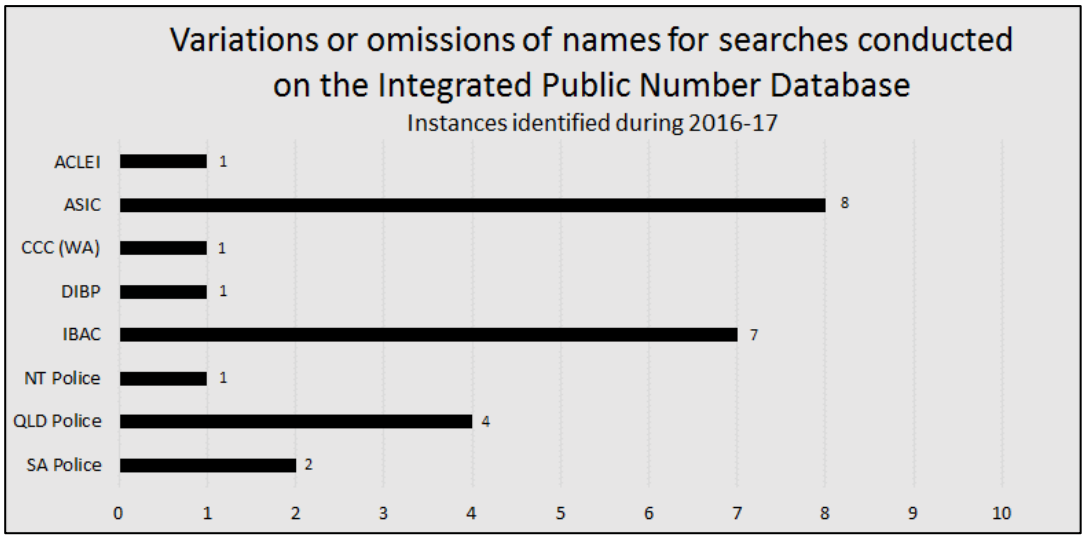
**III.** telecommunications data received after revocation took effect

**IV.** obtained telecommunications data not specified on authority.

### *I. Variations or omissions of names for searches conducted on the Integrated Public Number Database*

One of the most prevalent issues we identified across our inspections was searches of the Integrated Public Number Database (IPND) that were outside the parameters of the authority. The IPND is an industry-wide database which contains all listed and unlisted public telephone numbers. Information contained in the IPND may include the name and address of the customer and the type of service registered to that customer.

In several instances, IPND searches did not match the criteria specified on the authorisations. Generally these searches either included names or versions of names not included on the authorisation (thereby increasing the privacy intrusion). In our view authorised officers should be fully aware of the particulars of each search that will be conducted under an authorisation, so they can be satisfied of the required considerations. Permutations of names and additional aliases will invariably impact upon these considerations.

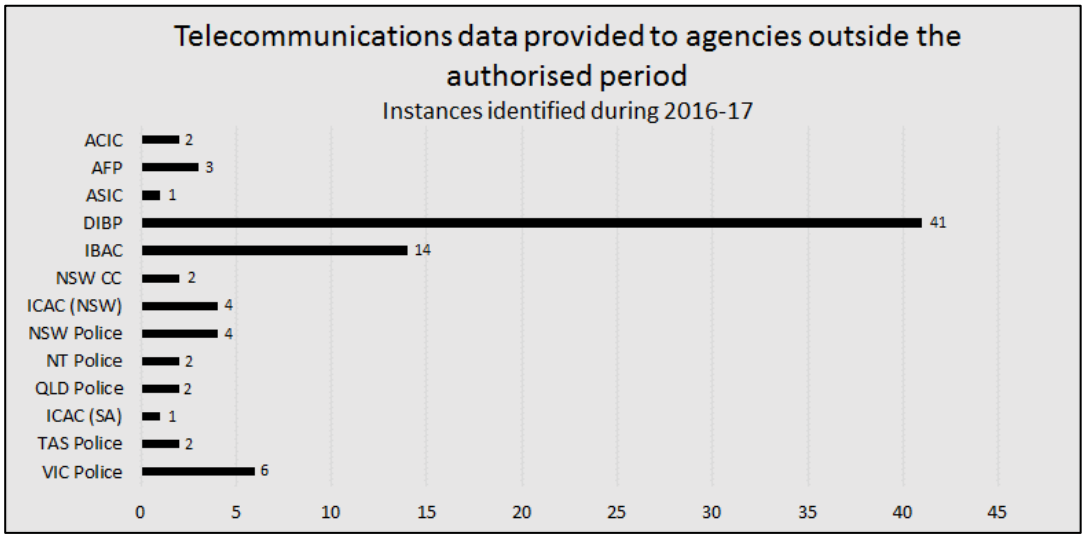



### *II. Telecommunications data provided to agencies outside the authorised period*

For historic authorisations, we encountered a significant number of instances in which telecommunications data obtained by agencies was either outside the date range specified on the authority or was dated after the carrier was notified of the authorisation. Although an agency has limited control over whether the telecommunications data provided by a carrier is in accordance with an authorisation, the onus is on the agency to verify that any telecommunications data received outside the terms of the authorisation is managed appropriately. Any telecommunications data received that is outside the authorised period should be quarantined from use and disclosure. Ideally, initial screening and vetting should be undertaken as a matter of course to mitigate against the risk of accessing telecommunications data that is outside the authorised period.

For prospective authorisations we noted fewer instances where telecommunications data was received outside the authorised period, except for authorisations where a revocation was made which is discussed in the next section.

Initial screening and vetting practices offer agencies additional assurance that they are only dealing with lawfully accessed telecommunications data. We accept such vetting is not feasible in all instances, particularly where an agency accesses a significant volume of telecommunications data. It is particularly important that an agency's processes mitigate such non-compliance by ensuring those who receive, and use, information from carriers are aware of the need to identify and quarantine telecommunications data which is outside the authorised period. Generally, agencies responded appropriately to the instances identified by our Office and quarantined the relevant telecommunications data. Our Office will report on the remedial actions taken by agencies in our next annual report.

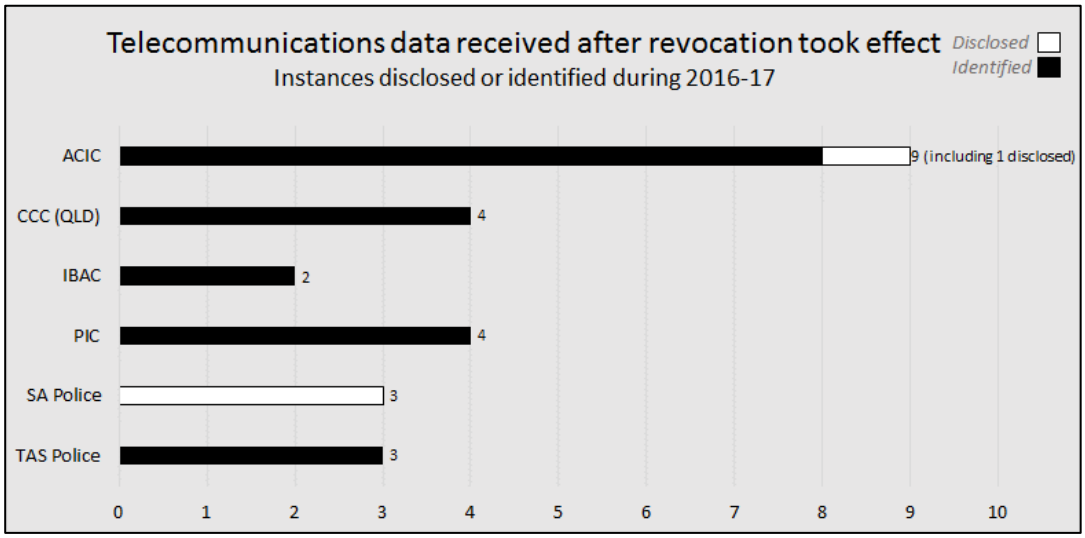



### *III. Telecommunications data received after revocation took effect*

During our inspections, we identified risks related to the revocation of prospective authorisations. Although it appears the legislation is silent on when a revocation takes effect, our interpretation is that a revocation takes effect at the time the carrier was notified of the revocation, unless a date and time for the revocation to take effect is specified on the instrument of revocation.

There is a risk of agencies receiving telecommunications data outside the parameters of an authorisation where their practice is to state, on the revocation instrument, that it comes into effect when it was made or signed. Due to delays in the carrier being notified and actioning the revocation, this practice has the potential to render any telecommunications data received thereafter outside the parameters of the authorisation. We note that, to counter this, some agencies advise the carrier of a proposed revocation and seek a disconnection before the formal revocation is made.

Although this may continue to be a risk identified at our next inspections, we anticipate instances of non-compliance attributed to this issue will decrease as a result of our Office raising awareness in its inspection reports and agencies updating their procedures in response.



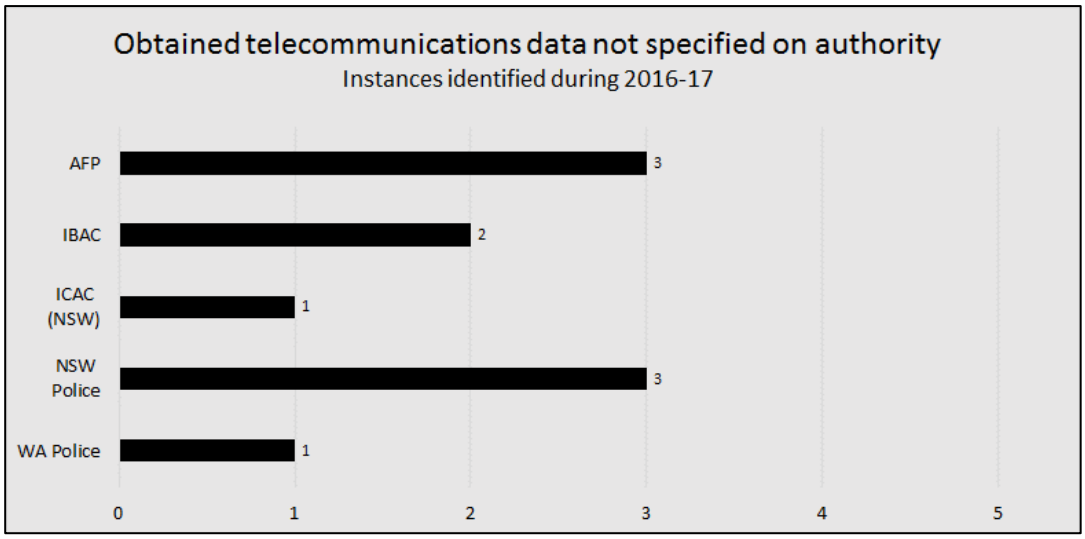

### *IV. Obtained telecommunications data not specified on authority*

At five inspections our Office identified agencies had received telecommunications data that was not specified on the authority. This occurred as a result of agencies:

- accessing telecommunications data which was specified on the supporting information but had been erroneously omitted from the authorisation itself
- carriers providing telecommunications data the agencies had not requested
- transposing errors on the notification of authorisation which resulted in telecommunications data being obtained which was not specified on the authority.

In two instances at NSW Police, there was nothing from the carrier that specified the telecommunications service to which the information related. As a result, our Office was unable to determine whether the telecommunications data received from the carrier was within the parameters of the authority.

Quality assurance mechanisms during the authorisation process and prior to notification enable agencies to mitigate the risk of receiving telecommunications data not specified on the authorisation. It is also important that agencies' processes are geared towards mitigating this type of non-compliance by ensuring that those who receive such telecommunications data are aware of the need to identify and quarantine information not specified on the authorisation.




**Authorisations not in writing**

In certain circumstances, an agency may need to authorise access to telecommunications data urgently. This may mean that, for example, it is operationally impractical for the agency to follow the standard procedures for seeking a written authorisation. Chapter 4 has no framework to govern the use of verbal or urgent authorisations. However, s 183 of the Act requires that an authorisation for telecommunications data must be in written or electronic form, and must be signed by the authorised officer.

The following considerations must be made when an authorised officer decides whether to give an authorisation:

- the interference in a person's privacy is justifiable and proportionate, and
- the disclosure is reasonably necessary for a permitted purpose, such as the enforcement of criminal law.

Additionally, for Journalist Information Warrants, an authorised officer must not authorise the disclosure of the telecommunications data of a journalist or their employer for the purpose of identifying their source, unless a Journalist Information Warrant is in force.

In the absence of any records to demonstrate these considerations, we are unable to determine that an authorising officer took into account the requisite considerations when giving the authorisation.

In the course of our inspections, we noted several instances where agencies had given verbal approval to access telecommunications data, both in an urgent context and as the

agency's standardised process. Under s 183 of the Act, an authorisation for telecommunications data must be in written or electronic form, and must be signed by the authorised officer. Telecommunications data accessed through a verbal approval, outside an agency's formal authorisation process may not demonstrate the core considerations required to access telecommunications data nor does it meet the requirements under s 183 of the Act.

During 2016–17 we identified five instances at NSW Police where telecommunications data had been accessed in urgent circumstances or out-of-hours. In two of these instances, there was no written or electronic authorisation on file, however records indicated that a verbal approval had been provided. In the remaining three instances, the authorised officer prepared a written authorisation after telecommunications data had already been accessed on the basis of verbal approval. We also identified one area of the NSW Police which was routinely exercising its telecommunications data powers without a written or electronic authorisation in place. The area's process at the time of our inspection was for access to telecommunications data to be verbally approved and a written record of the verbal approval to be made in a log. We do not consider this practice is permitted by the Act and suggested to NSW Police that it review its policies and procedures to ensure all authorisations for telecommunications data are in written or electronic form and signed by the relevant authorised officer.

**Statistical Issues**

Section 186 of the Act sets out agencies' reporting obligations to the Minister. Under this section agencies must, as soon as practicable and in any event within three months after the end of the financial year, provide the Minister with a written report that sets out specific details of that agency's access to telecommunications data. This includes the number of authorisations made by an agency during the financial year.

During 2016–17 we identified a small number of agencies that had discrepancies in their statistics. This occurred for a number of reasons including the type of authorisation being recorded inconsistently, agency officers erroneously recording authorisations made, and system limitations which prevented the agency from obtaining accurate reflections of the total number of authorisations made.

As a result of these sorts of issues, we made one recommendation to Home Affairs:

**Recommendation:**

The Department of Home Affairs should implement measures to ensure it can accurately account for the number of telecommunications data authorisations it issues in any given period to enable effective oversight and to comply with the reporting and record keeping requirements of the Act. This should include:

- implementing measures to ensure stored communications requests can be accounted for separately to telecommunications data authorisations, in particular noting the reporting obligations to the Minister under s 186 of the Act
- taking immediate action to manage the risk of inadequate technical support for the Request for Information (RFI) system, as the RFI system is heavily relied upon for reporting purposes and to assist compliance under the Act.

Home Affairs accepted this recommendation and advised it is working to identify and implement measures to ensure accurate accounting of the telecommunications data authorisations made in a given period. Our Office will continue to monitor this issue at future inspections of Home Affairs.

Generally, agencies were receptive to our suggestions and advised their processes and procedures would be updated to ensure statistical information provided to the Minister under s 186 reflects the total number of authorisations made.

**Written records indicating notification of an authorisation**

Under s 186A(1)(a)(iii) of the Act, agencies must retain documents or other materials that indicate when a carrier is notified of an authorisation under s 184(3). In considering 'other materials', we may take into account an agency's policies and procedures.

One of the most common risks we identified during our inspections was agencies not maintaining written records to indicate when notification of authorisation occurred. While it is reasonable to conclude notification would need to have occurred in order to receive telecommunications data from the carrier, the lack of these records poses a risk that agencies may not be able to demonstrate they are accessing authorised telecommunications data.

An example of this is where an agency has made a historic authorisation requesting telecommunications data from the same day the notification of authorisation occurred.

Without a written record of when notification occurred, the agency may not be able to demonstrate the telecommunications data obtained came into existence before the authorisation came into force.

During 2016–17 we identified a small number of agencies that did not routinely keep records indicating when notification occurred. We also identified a number of agencies which had isolated instances where this record could not be located during the inspection. In three instances this resulted in agencies being unable to demonstrate that all telecommunications data obtained had been authorised.

Given the importance of knowing when notification occurred for determining whether the telecommunications data was lawfully obtained, we have suggested agencies adopt processes to keep clear written records of the date and time the carrier received notification of the authorisation.

**Record keeping**

Section 186A(1)(g) of the Act requires the chief officer of an enforcement agency to keep documents or other materials that indicate whether use or disclosure of telecommunications data occurred in certain circumstances. Under s 185, agencies must also retain each authorisation by an authorised officer for a period of three years beginning on the day the authorisation is made.

During our inspections, we made several findings regarding agencies being unable to provide access to, or locate the telecommunications data obtained under authorisations. In conducting our compliance assessment, we review the telecommunications data received under an authorisation to ensure it is within the parameters of the authorisation, including confirming the information is linked to the telecommunications service authorised and otherwise within the parameters of the authorisation.

Although there is no express legislative provision requiring agencies to retain accessed telecommunications data, an inability to account for the whereabouts of obtained telecommunications data may mean agencies are not able to appropriately account for whether, and how that telecommunications data was used and/or disclosed in accordance with s 186A(1)(g).

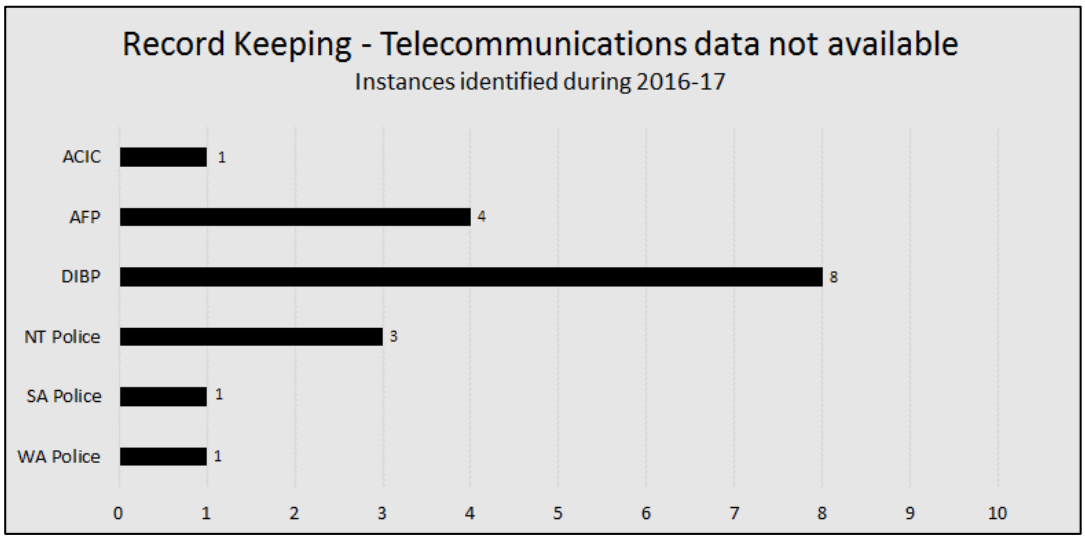
In one instance, the AFP had destroyed the telecommunications data in accordance with their destruction policies and in another, the ACIC was unable to access the telecommunications data obtained because it had been archived. In all other instances where we made findings, agencies were simply unable to locate the telecommunications data accessed through the authorisation.

We made one recommendation to Home Affairs regarding its record keeping:

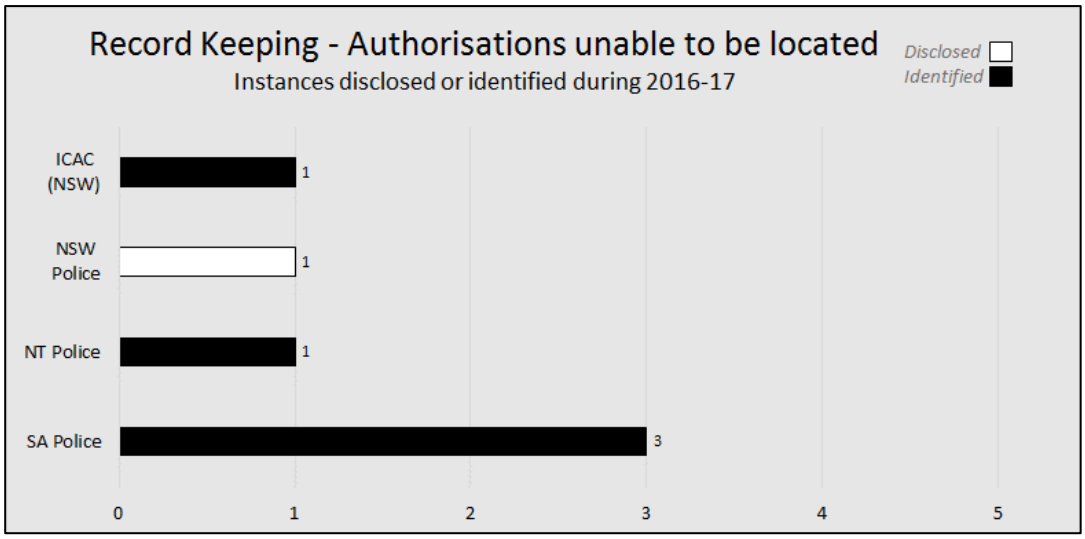
**Recommendation:**

The Department of Home Affairs should implement measures to centrally store, and/or monitor, telecommunications data once it has been provided to investigators. In doing so, the Department of Home Affairs should be mindful of the record keeping requirements regarding use and disclosure of telecommunications data under s 186A(1)(g) of the Act.

Home Affairs accepted this recommendation and advised that, since the inspection, it has developed new practices and processes for storing telecommunications data. Home Affairs also advised it is continuing to review its processes with a view to effectively monitoring telecommunications data and developing an appropriate centralised record management system. Our Office will continue to monitor this issue at future inspections of Home Affairs.




We also identified a small number of instances in which agencies could not locate the authorisation itself. In these circumstances we relied on agencies' processes and procedures to confirm the access to telecommunications data had been properly authorised prior to access.




**Telecommunications Data: Spotlight Issues**

During our 2016–17 inspections, we identified a number of issues with the form of authorisations, revocations or notifications as well as a number of transposition errors. As these were identified at a majority of the agencies inspected, this section emphasises the importance of these issues and the risk to further non-compliance that may result from them.

***Spotlight Issue One: Form of authorisations, revocations and notifications***

Section 183 of the Act states that an authorisation, the notification of an authorisation, the revocation of an authorisation and the notification of a revocation must comply with requirements determined by the Communications Access Co-ordinator under s 183(2). The requirements of the Communications Access Co-ordinator are stipulated in the *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2015* – which we refer to as the 'CAC Determination'.

At almost half of the agencies inspected, we identified issues with the form of authorisations, revocations, or notifications. In some instances, the issues were solely administrative and related to the use of erroneous legislative references or typographical errors in completing templates. In a small number of instances, the forms of authorisations, revocations and notifications used by agencies did not meet the requirements of the CAC Determination.

Issues with forms are not identified often during our inspections of agencies' records under more established oversight regimes; for example, our inspections under Chapter 3 of the Act regarding the preservation of, and access to stored communications. Such issues are common during the implementation of a new and complex legislative framework and we acknowledge each agency's efforts to ensure compliance, including liaising with our Office on issues of uncertainty.

Form issues have the ability to significantly impact upon an agency's compliance, as applicants and authorised officers often rely on the accuracy of these documents to guide them through the authorisation process. Comprehensive and clear templates support an agency's compliance framework, and are one of the key controls in ensuring that applications, revocations and notifications are made in accordance with the Act.

As agencies' familiarity and corporate knowledge regarding the requirements of the Act develop, we anticipate seeing a reduction in the number of issues associated with the form of authorisations, revocations and notifications. Given the flow-on effects of form-related issues, we also anticipate a commensurate decrease in other areas of non-compliance.

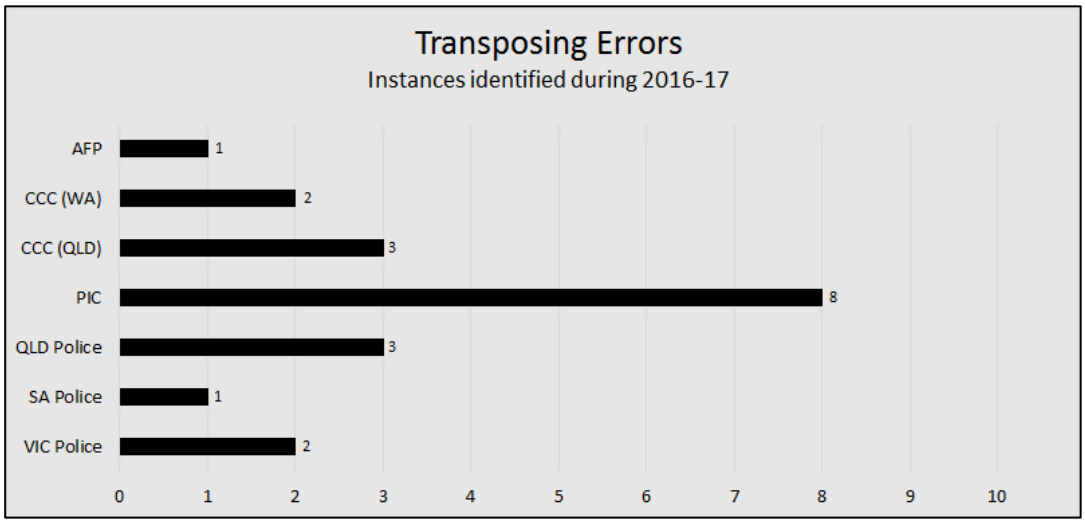
***Spotlight Issue Two: Transposing Errors***

At several agencies, we noted instances of transposing errors and other typographical[7] errors which presented a risk of accessing telecommunications data unrelated to the target of the investigation. When conducting our compliance assessment, we examined the consistency of parameters specified on authorisations with what was specified on the supporting documentation. In some instances, these parameters may be incorrectly transposed across documentation or incorrectly entered into systems, such as the IPND system. Although the majority of these errors did not result in telecommunications data being unlawfully disclosed, two resulted in an assessment of non-compliance because the error caused the agency to access telecommunications data that was outside the parameters of the authority. This highlights the risk that transposing errors may lead to inadvertent privacy intrusions.

Despite measures agencies have in place during the application stage to ensure applications meet the requirements of the Act, such as comprehensive templates and guides, human error always remains a possibility. Currently, most agencies rely on quality assurance measures, such as vetting by compliance officers, as a means to identify these errors.

[7] For the purposes of this report and in the table below, we have included typographical errors as transposing errors.

At a number of agencies, we identified authorisations that included erroneous details, such as incorrect authorisation periods or telecommunications services. These may, in turn, have resulted in telecommunications data being obtained which was inconsistent with what was intended to be authorised. In most instances, these were identified and amended by agencies during their quality assurance process.




**Telecommunications Data: Good Practices**

During our inspections we examine the adequacy of agencies' policies and procedures for ensuring compliance with the Act, based on information provided during inspections. This includes identifying practices that assist agencies in achieving compliance, as well as practices that pose risks to an agency achieving compliance with the Act. Examples of both types of practices, as identified during our inspections for the 2016–17 period, are outlined below.

***Good Practice: Cooperation and Frankness***

We encourage agencies to be proactive in identifying compliance issues and risks, disclosing issues when they are identified, and taking appropriate remedial action. When agencies take these steps, it indicates to our Office the agency is committed to complying with the requirements of the Act. A positive compliance culture is vital in promoting a broader understanding of an agency's obligations when accessing telecommunications data under Chapter 4 of the Act.

In 2016–17 we observed positive compliance cultures in all agencies, with many disclosing issues at or before inspections that may have a bearing on their compliance with the Act. In some instances these disclosures did not result in a finding of non-compliance, but we

consider this openness reflects positively on agencies and indicates a compliance-minded approach to accessing telecommunications data.

We also noted several instances where agencies contemporaneously (outside of an inspection) advised our Office of compliance issues as they were identified and outlined any remedial action taken. Our Office commends this approach to disclosure.

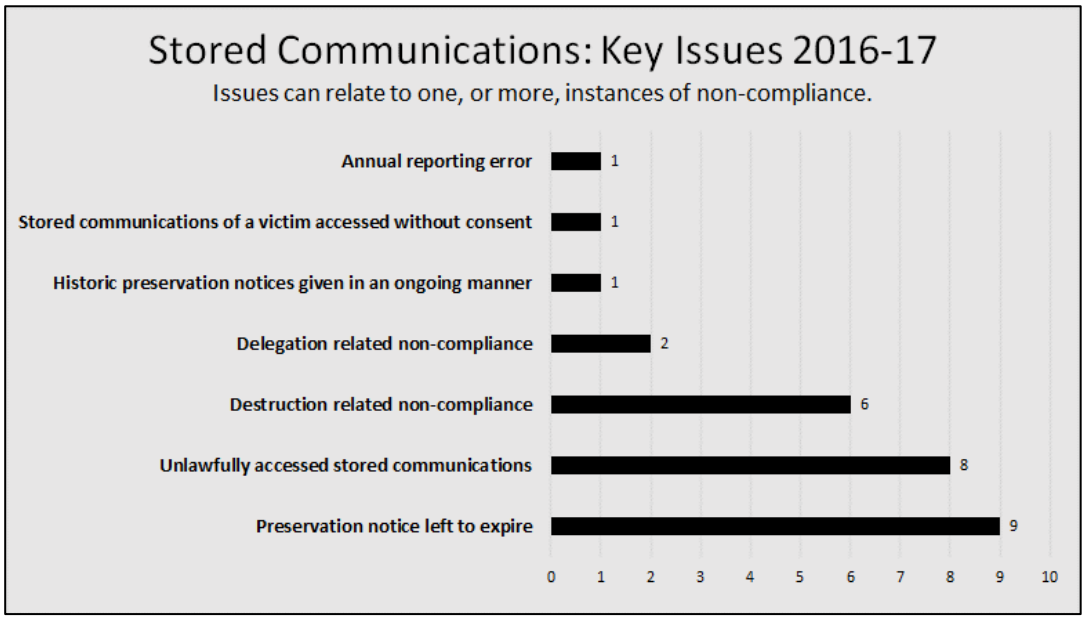
***Good Practice: Demonstration of Authorised Officer Considerations***

During our inspections we identified occasions where authorising officers either requested additional information from applicants or made additional notes to contemporaneously capture their considerations prior to making an authorisation. Clear records of the authorised officer's decision making process demonstrate to our Office the required considerations are being met.

We noted only a small number of applications that were lacking sufficient detail to demonstrate applicants and authorising officers were turning their mind to privacy considerations and the thresholds for satisfying the requirements of the Act.

## Results of stored communications inspections conducted in 2016–17

During 2016–17 our Office conducted 16 inspections of agencies' access to stored communications. These inspections covered records made from 1 July 2015 to 30 June 2016.




### Stored Communications: Key Issues and Trends

During 2016–17, there was a noticeable decrease in overall non-compliance, as well as instances where we were unable to determine compliance, when compared to the 2015–16 inspection period.[8] The most common issues, which were also present during the previous inspection period, related to:

- the application of the mandatory revocation requirements for preservation notices
- instances where stored communications were accessed unlawfully
- mandatory destruction requirements for stored communications records
- proper delegation of stored communications powers.

[8] Records inspected during 2015–16 were in accordance with our Office's 2015–16 inspection methodologies, which pre-dated the commencement of the Data Retention Act. Changes to the Act have informed the development of our 2016–17 inspection methodologies, which have impacted on our inspection results.

**Preservation notice left to expire**

Section 107L(2)(a)(ii) of the Act states that an issuing agency must revoke a preservation notice if the agency decides not to apply for a warrant under Chapter 3 (or Part 2–5) to access stored communications.

In determining compliance with this provision our Office assesses, in instances where a preservation notice has expired, if information is available to indicate whether an agency maintained an intention to apply for a stored communications or Part 2–5 warrant. When available records indicate an agency did not maintain an intention to apply for a warrant at the time the preservation notice expired, our Office reports this as non-compliant with s 107L(2)(a)(ii). When no such record is available, our Office reports it is unable to determine whether an agency complied with s 107L(2)(a)(ii).

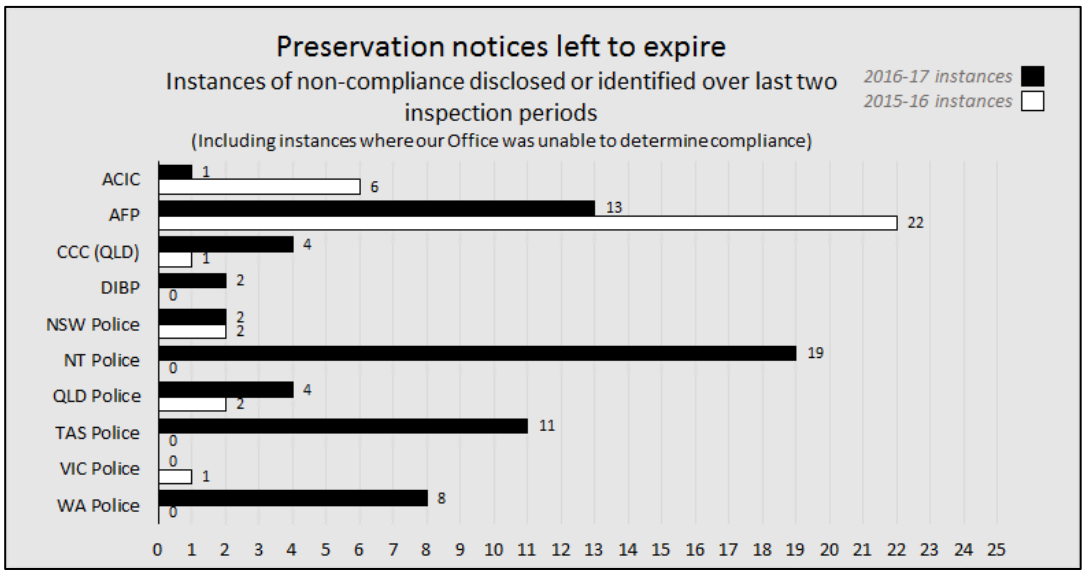
Instances of non-compliance with the mandatory revocation requirements increased in 2016–17 compared with 2015–16. Of the 16 agencies inspected in 2016–17, nine were found to be non-compliant or our Office was unable to determine an agency's compliance with the mandatory revocation requirements. This compares to seven out of the 16 agencies inspected in 2015–16.

After raising this issue in our 2015–16 report, some agencies advised they would implement additional training and procedural updates to address this issue. Given the increase in non-compliance for some agencies during the most recent inspection period, it is not clear these actions were effective. Some agencies that had few, if any, instances of non-compliance with mandatory revocation requirements in 2015–16 presented instances of non-compliance, or instances where we were unable to determine compliance in this period. This indicates there may be a need for agencies to do more to reinforce the requirement to revoke a preservation notice when there is no longer an intention to apply for a stored communications warrant.

All inspected agencies had processes in place to contact investigators to determine whether they still maintained an intention to obtain a warrant. Notwithstanding these processes, in many instances investigators did not respond to this contact.

The number of instances identified during 2016-17 indicates a possible knowledge gap regarding the obligation to revoke a preservation notice when there is no longer an intention to apply for a warrant.

It is clear agencies have attempted to implement solutions to this recurring issue. In our view the person best placed to make a decision on whether a preservation notice should be revoked is usually the investigator. We encourage agencies to continue with awareness raising activities, to remind investigators of the mandatory revocation requirements of the Act.




**Unlawfully accessed stored communications**

Under s 117 of the Act a stored communications warrant authorises, subject to any conditions or restrictions specified, access to stored communications made by, or sent to, the person listed on the warrant. Section 133 sets out a general prohibition on dealing with accessed information or stored communications warrant information, including information obtained by accessing stored communications in contravention of s 108(1), which prevents access to a stored communication without a warrant.

In 2016–17, eight of the 16 agencies inspected had received stored communications which fell into one of the following three categories:

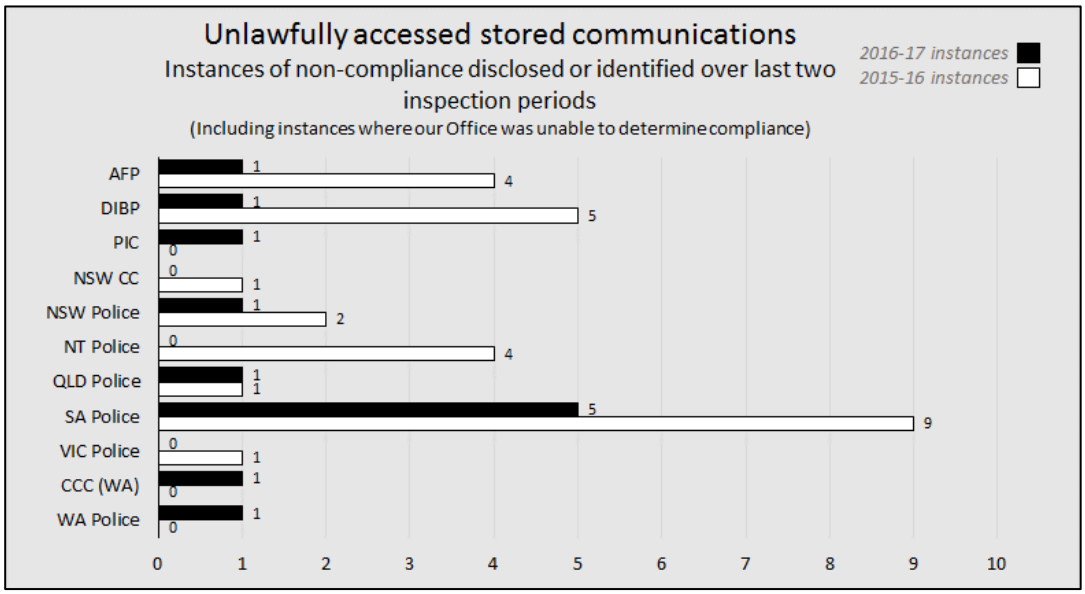
- the accessed stored communications did not relate to the person listed on the warrant
- there was insufficient information provided by the carrier to determine whether the accessed stored communications related to the person listed on the warrant
- a condition or restriction was placed on a warrant, which was not adhered to by the carrier, when it provided stored communications to an agency.

Although all three issues relate to carrier errors, in our view it is agencies' responsibility to ensure they are only dealing with lawfully accessed stored communications. In instances where an agency has received unlawfully accessed stored communications from a carrier, our Office reports on the agency's approach to identifying, and then quarantining the stored communications from investigators.

We note the CCC (WA) and SA Police both disclosed instances in which they had received unlawfully accessed stored communications, but identified and quarantined the stored communications from investigators prior to them being used. This is a positive reflection on the agencies' quality assurance processes.

During the last two reporting periods, we noted a significant decrease in the number of identifications reported at each agency.

We suggest agencies ensure they continue to apply processes to review the lawfulness of stored communications prior to access by investigators. In instances where there is insufficient information to determine the lawfulness of accessed stored communications, we suggest agencies request the information from the carrier again and quarantine the original stored communications until their lawfulness can be verified.




**Destruction related non-compliance**

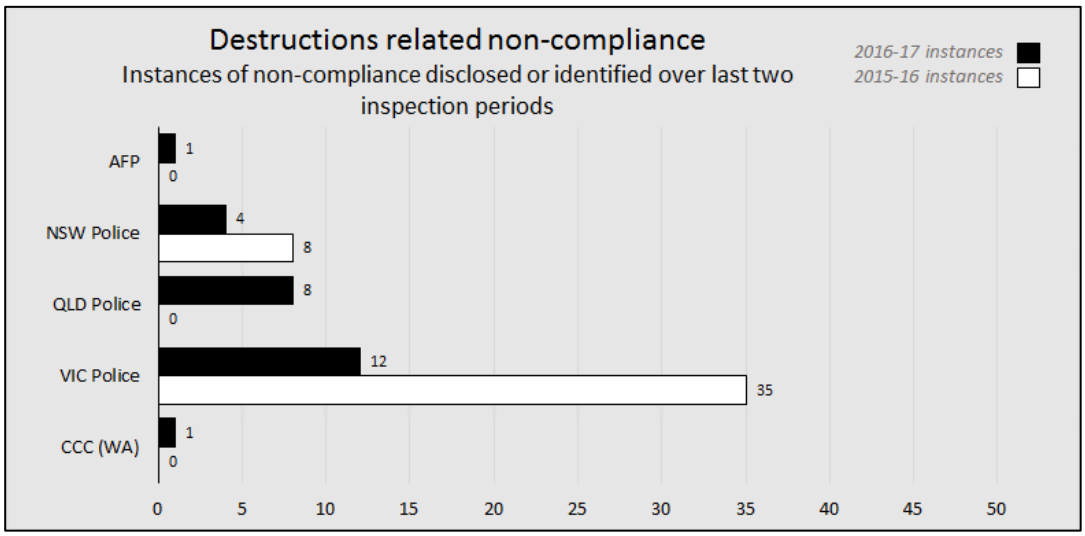
Section 150(1) of the Act states that if the chief officer of an agency is satisfied that a record obtained by accessing stored communications is not likely to be required for a permitted purpose, then the chief officer must cause the record to be destroyed forthwith. As 'forthwith' is not a timeframe defined in the Act or elsewhere, we previously sought advice from the AGD (in its former role as administrator of the Act) on how the term should be applied when assessing an agency's compliance. AGD's view was that, although forthwith should not be applied as a strict timeframe, the term indicates a level of urgency. We assess

compliance based on what we think is reasonable for each agency, given what we know of its processes.

At five of the 16 agencies inspected during 2016–17, we identified instances of non-compliance, or instances where we were unable to determine compliance, relating to the destruction obligations under s 150(1). While the details of each instance differed, all could broadly be grouped under the following categories:

- stored communications records that were destroyed long after being certified for destruction, or records where there was nothing to indicate when destruction had occurred
- copies of stored communications records that had been certified for destruction but were located during an inspection
- stored communications records, including copies, which had been destroyed prior to being certified for destruction.

The number of destruction-related disclosures and findings have decreased at most agencies over the past three reporting periods; however the issue continues to be identified in our inspections. We suggest agencies continue to apply targeted training measures to address these issues. We also suggest agencies consider the effectiveness of their destruction processes, particularly in relation to the timing of destruction of stored communications records. We will continue to monitor these issues at future inspections.



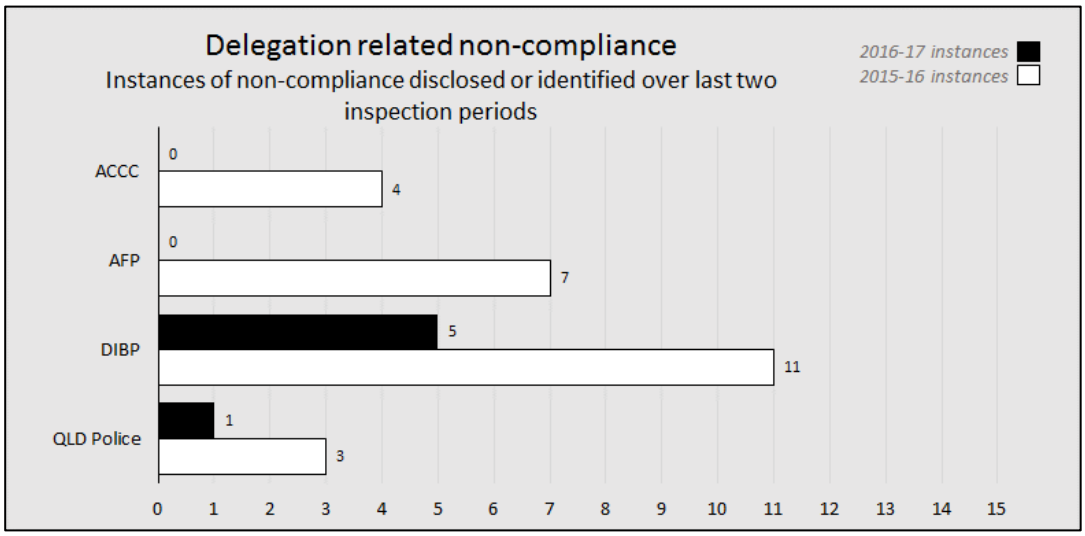
**Delegation related non-compliance**

The Act provides for specific powers of the chief officer of a law-enforcement agency to be delegated to specific individuals or classes of individuals. For example, s 5AB permits the chief officer of an agency to designate authorised officers which, by extension, under s 107M(2), allows that person to give an ongoing domestic preservation notice. Section 110 permits the chief officer to designate an office or position within the agency authority to apply for warrants, and by extension, under s 107M(1), historic domestic preservation notices.

In assessing compliance with delegated responsibilities and powers, our Office requests copies of all delegations relevant to an inspection period. Our Office also assesses an agency's records to determine whether it is able to clearly demonstrate that a specific person is using a delegated responsibility or power.

In 2016–17, there was an overall reduction in delegation-related findings of non-compliance across all agencies.

We suggest agencies continue to remind officers exercising powers under the Act to ensure they are appropriately delegated to do so. At agencies where we identified minimal delegation-related issues, this was achieved through effective stored communications training, application checklists that prompt applicants to check for appropriate delegation and strong quality assurance processes.



**Stored Communications: Spotlight Issues**

***Spotlight Issue One: Stored communications of a victim accessed without consent***

Section 116 sets out the circumstances in which an issuing authority may issue a stored communications warrant to an agency. One of the requirements is that an agency must be investigating a 'serious contravention' in which the person whose stored communications the agency seeks to access is involved (including as a victim of the contravention) (see s 116(1)(d)).

Section 116(1)(da) operates so that if the stored communications warrant applied for is in relation to stored communications of the victim of the contravention, the warrant can only be issued if the victim is unable to consent, or it is impracticable for them to consent to the stored communications being accessed.

We identified two instances where it appeared VIC Police had accessed the stored communications of the victim of a serious contravention without first obtaining the victim's consent. Based on available records, it did not appear that the victim was unable to consent or that it was impracticable for them to consent.

This issue has been identified in previous years at a number of agencies, and continues to be an area of focus for our inspections. We have previously sought AGD's views, (in its former role as administrator of the Act) on the meaning of the terms 'unable' and 'impracticable' under s 116(1)(da). The AGD advised our Office a person would be deemed 'unable to consent' where, for example, they are missing and cannot be located, are incapacitated or deceased. Obtaining consent would be deemed 'impracticable' where a person's particular situation makes contacting them extremely difficult, time-consuming or expensive.

AGD advised that if the victim has an opportunity to consent and they do not wish their stored communications to be accessed, then an agency must not use s 116 to access their stored communications. AGD also advised that the victim's reasons for not providing consent are immaterial.

***Spotlight Issue Two: Historic preservation notices given in an ongoing manner***

Under s 107H of the Act, there are two types of domestic preservation notices; historic and ongoing. Historic notices may be given by a law enforcement agency to require a carrier to preserve stored communications from the time it receives the notice until the end of that day. Ongoing notices may be given by a law enforcement agency that is also an interception agency, to require a carrier to preserve stored communications from the time it receives the notice until the end of the 29$^{th}$ day after that date.

During the inspection period, we identified that ASIC gave a series of 29 historic domestic preservation notices to the same carrier on consecutive days, each relating to the same person. In our view, while this practice is not strictly in breach of any legislative provision, it has a similar effect to giving an ongoing preservation notice. ASIC is not authorised to give an ongoing preservation notice because it is not an interception agency.

This practice was also identified at a different agency during the previous inspection period. We provided advice to the effect that a series of historic preservation notices may be interpreted as being akin to an ongoing notice, which only an interception agency may give.

**Stored Communications: Good Practices and Risks**

During our inspections we comment on the adequacy of policies and procedures that agencies have in place to ensure compliance with the Act, based on information made available to us during the inspection. This includes identifying practices that assist agencies to achieve compliance. Where appropriate, we also comment on practices that pose risks to an agency's ability to achieve compliance with the Act. Examples identified during our 2016–17 inspections are outlined below.

***Good practices: dealing with lawfully accessed stored communications***

Across several agencies, we identified good screening and quarantining processes aimed at ensuring that agencies were only dealing with lawfully accessed stored communications. As discussed in the *unlawfully accessed stored communications* section of this report, these practices allowed agencies such as the CCC (WA) and SA Police to identify instances where carriers had provided stored communications not authorised by the warrant. They also enabled those agencies to take appropriate remedial action, such as quarantining the product from investigators.

During 2016–17 we noted WA Police and DIBP had recently implemented, or were in the process of implementing checklists to screen stored communications prior to dissemination to investigators. We note this has helped in identifying instances where carriers have provided unlawfully accessed information, and suggest all agencies consider a similar approach.

***Good practices: proper management of accessed information***

During our inspections we also assess whether an agency has properly managed accessed stored communications. This involves assessing an agency's compliance with the destruction provision of the Act and our understanding of an agency's usual destruction process as discussed in the *destruction related non-compliance* section of this report.

VIC Police has implemented practices to mitigate compliance issues relating to destructions, whereby the chief investigator of an operation is required to sign a declaration certifying that all copies of stored communications have been returned before a destruction is certified by the chief officer. VIC Police further requires that, upon receipt of stored communications, investigators sign a form stating that they will deal with the information in accordance with relevant policy, procedures and guidelines.

WA Police also applies a good practice, whereby it logs each copy of stored communications created, to keep a record of which areas need to be contacted when destruction of the relevant stored communications has been certified by the chief officer.

These practices serve as a means to remind those dealing with stored communications of their obligations under the Act, as well as ensuring accountability for copies of stored communications prior to destruction.

Identified examples of better practices were not limited to measures put in place to prevent non-compliance, but also included proactive remedial action taken by agencies in response to findings. For example, following an inspection in which our Office identified electronic copies of stored communications that had previously been certified for destruction, WA CCC advised it had undertaken an internal audit that had identified further copies which were, in turn, destroyed. This approach is reflective of a positive compliance culture and a strong understanding of agencies' obligations when accessing stored communications under the Act.

***Risk: satisfying record keeping and reporting obligations***

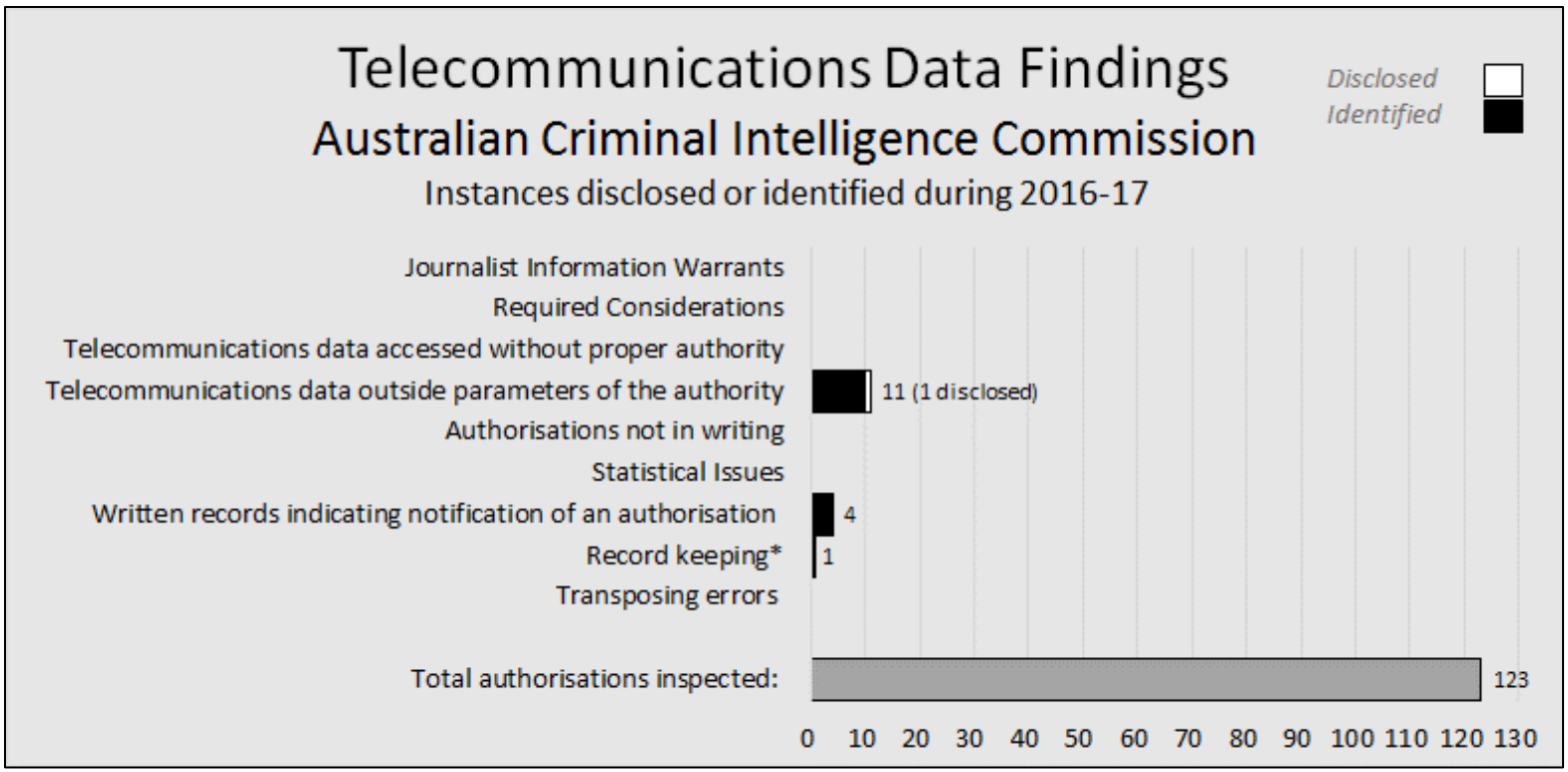
Under the Act, agencies have a number of record keeping obligations against which we assess compliance. Agencies use different methods to satisfy these obligations, including spreadsheets and databases. In some instances the absence of adequate record keeping processes poses a risk for agencies in assuring the accuracy of their record keeping and reporting. It also impacts on the ability of our Office to effectively conduct inspections of stored communications information.

At the time of inspection, the DIBP did not have a comprehensive process in place for keeping track of stored communications information.

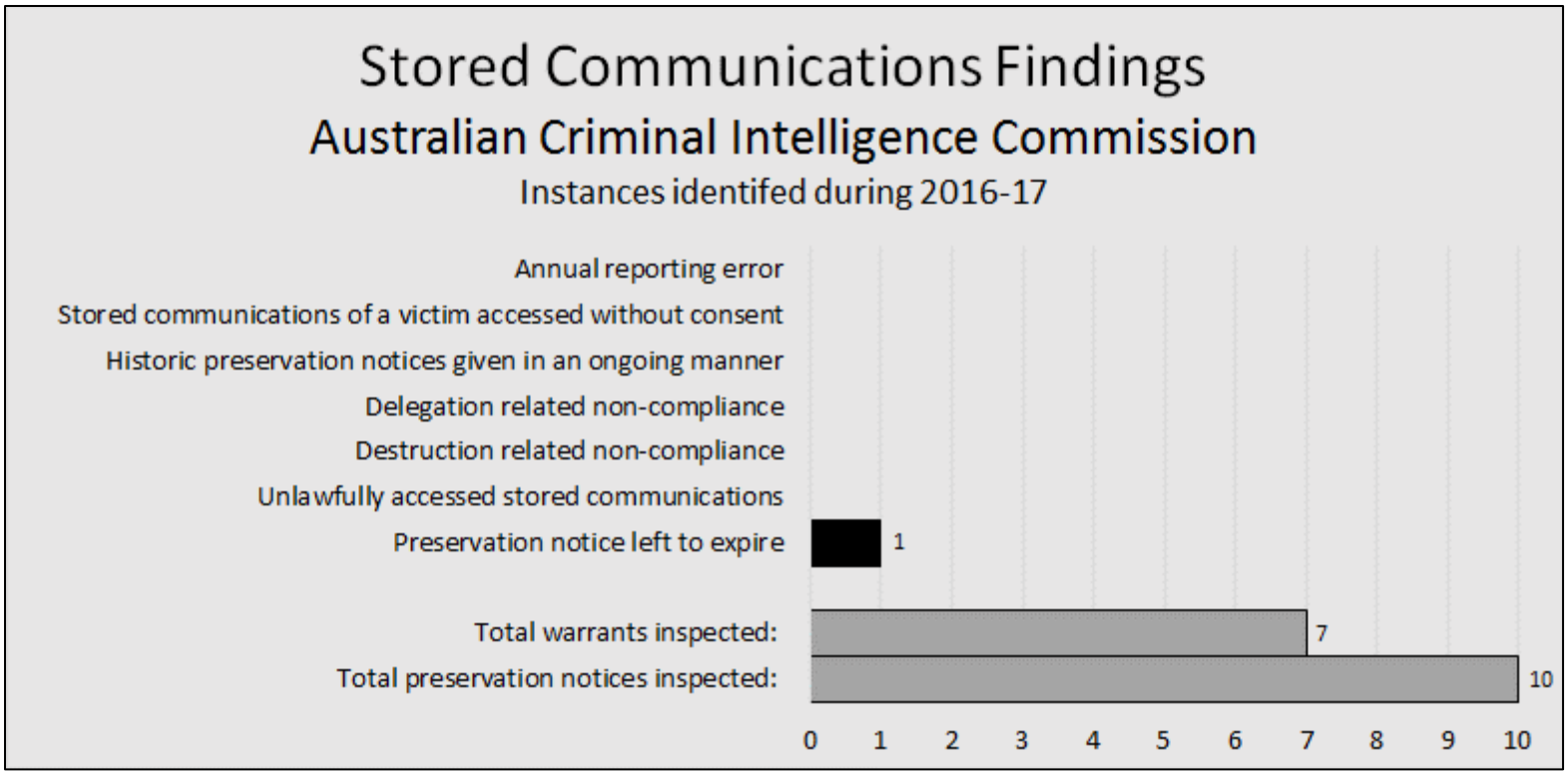
As a result of our 2015–16 inspections we made a recommendation to the DIBP about its record keeping processes. In its response the DIBP advised it had implemented a centralised record keeping system for all stored communications warrants and preservation notices. At the most recent inspection in February 2017, it was apparent the DIBP did not have a centralised record keeping system and therefore the risks previously identified had not been addressed.

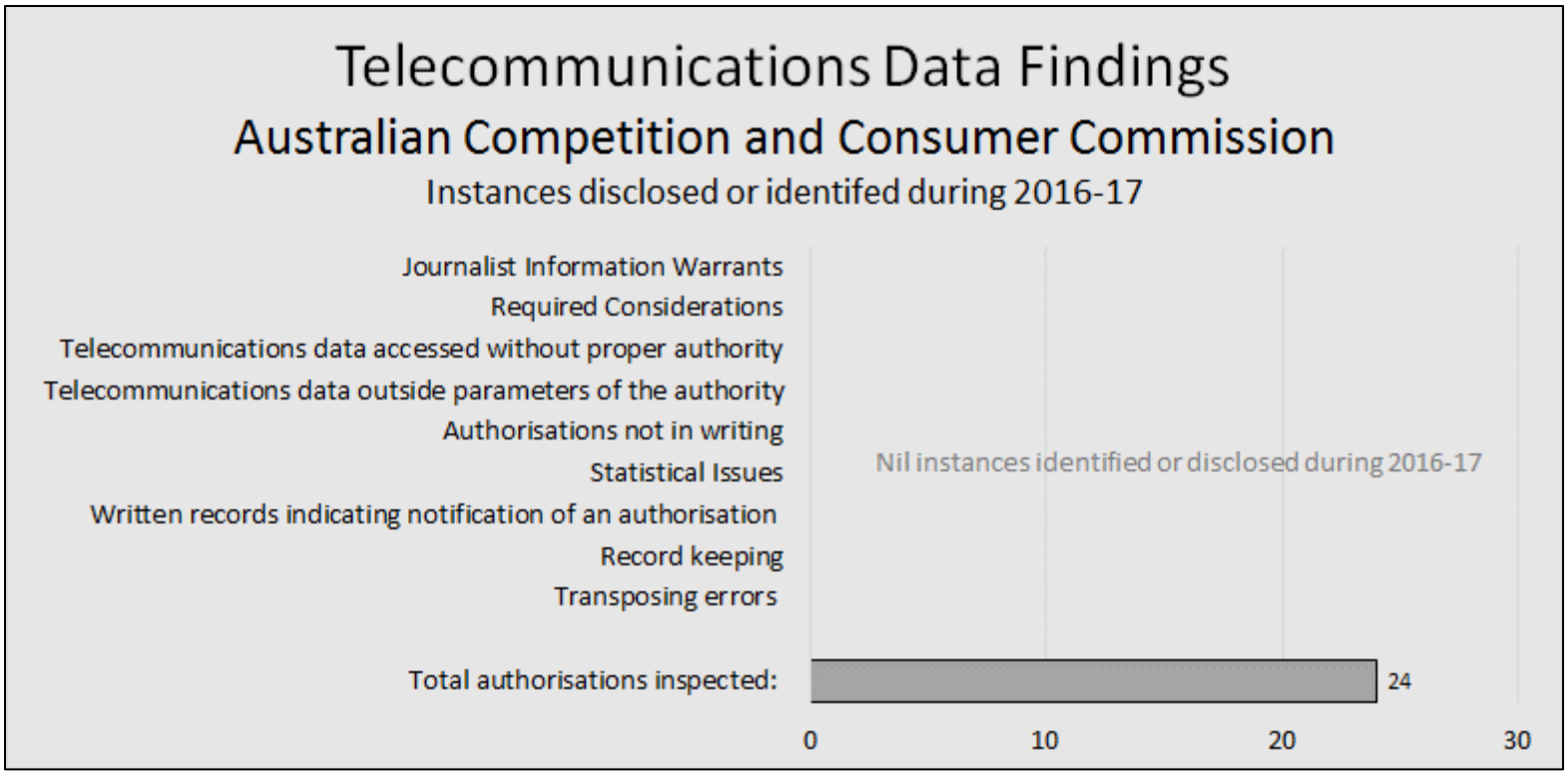
Following the February 2017 inspection, the DIBP advised it would implement a manual process to keep track of stored communications records. We will assess the effectiveness of this process at future inspections of Home Affairs.

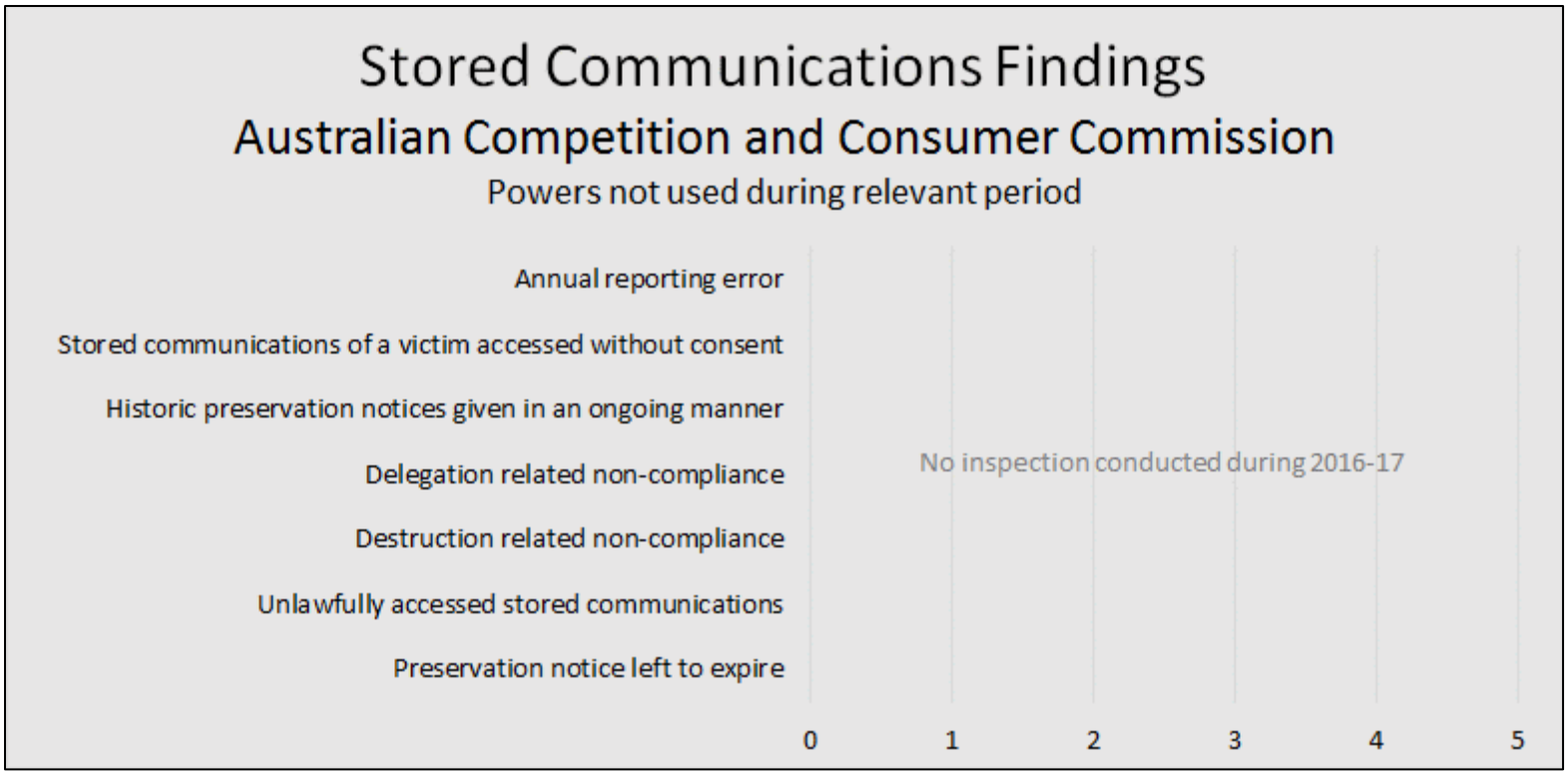
# Agency Findings for 2016–17

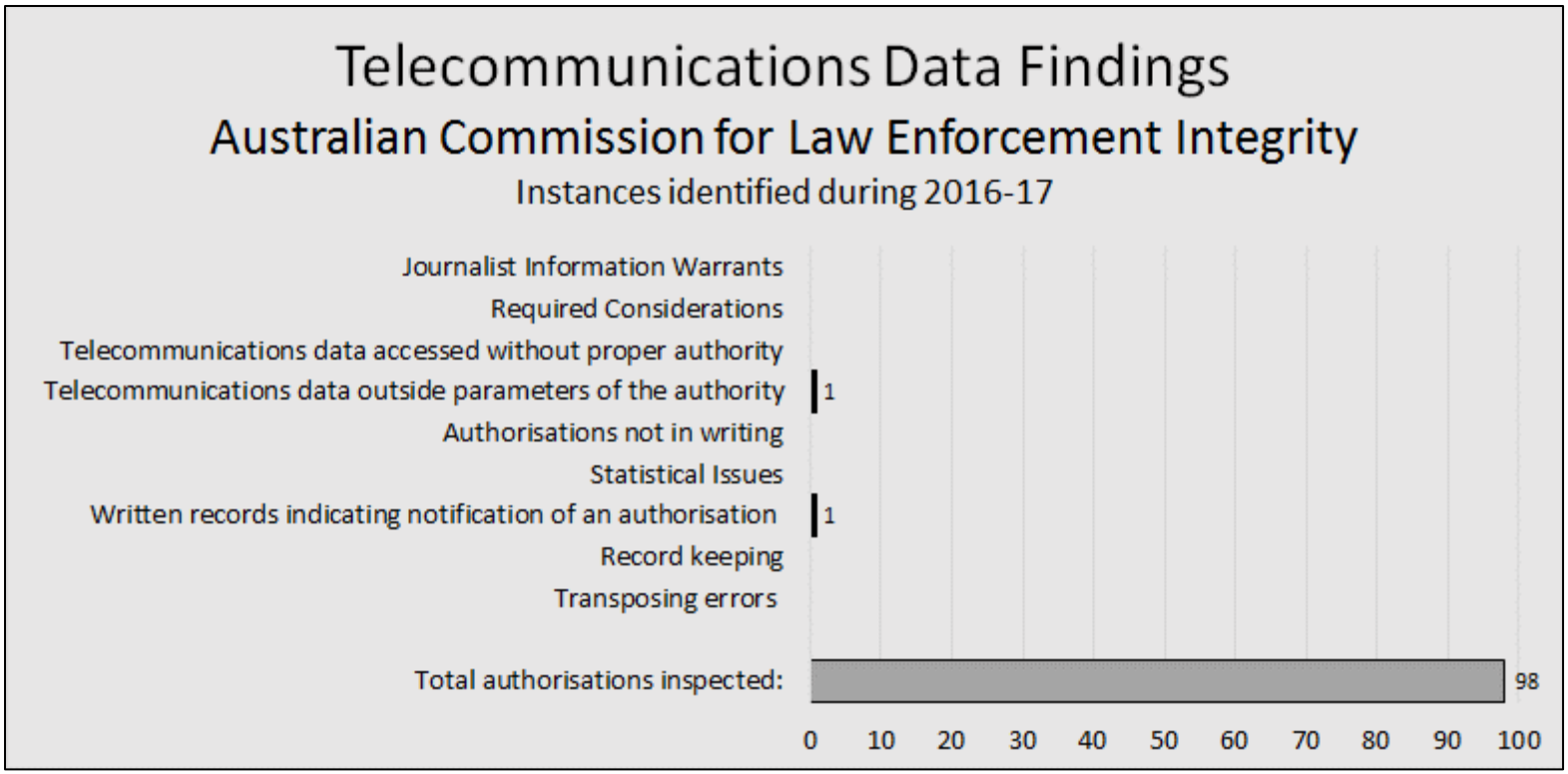


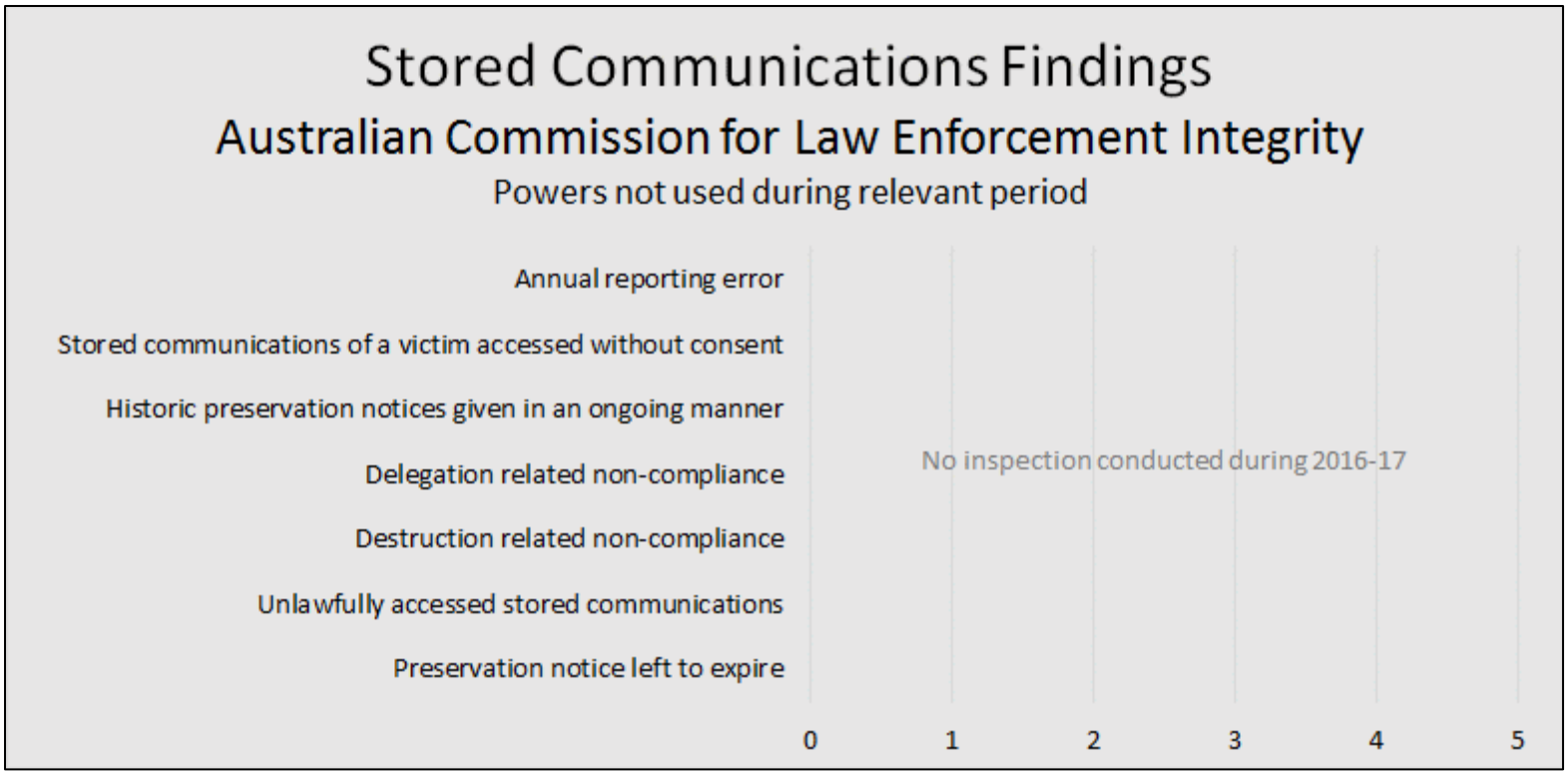

*In one instance, the ACIC was unable to make available the telecommunications data accessed. We acknowledge the efforts of the ACIC to try to retrieve the telecommunications data; however we were unable to assess whether the telecommunications data received from the carrier was within the parameters of the authority.

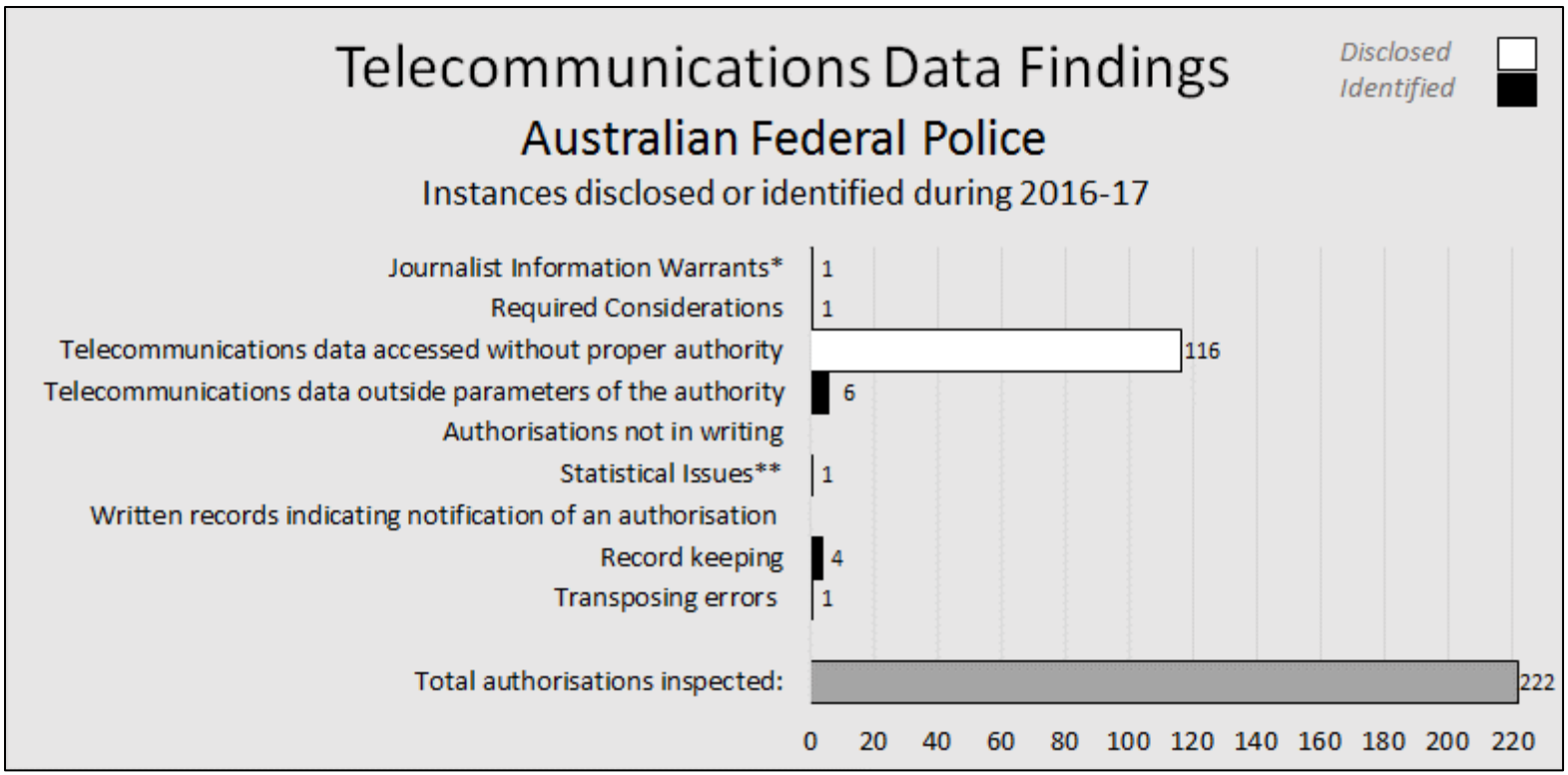

Stored Communications Findings
Australian Criminal Intelligence Commission
Instances identifed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
1
Total warrants inspected:
7
Total preservation notices inspected:
10
0 1 2 3 4 5 6 7 8 9 10


Telecommunications Data Findings
Australian Competition and Consumer Commission
Instances disclosed or identifed during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
Nil instances identified or disclosed during 2016-17
Total authorisations inspected:
24
0
10
20
30


Stored Communications Findings
Australian Competition and Consumer Commission
Powers not used during relevant period
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
No inspection conducted during 2016-17
0
1
2
3
4
5

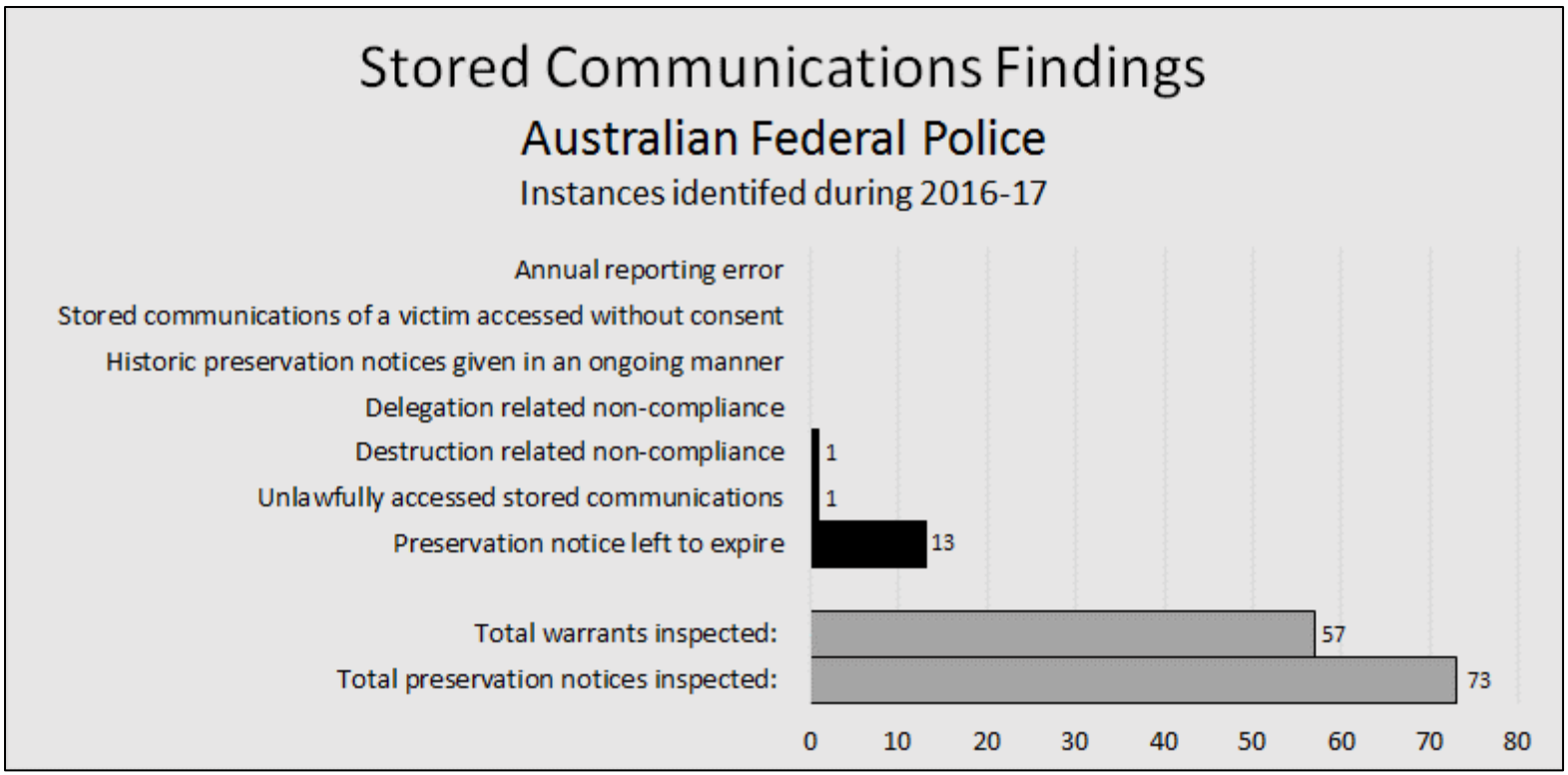

Telecommunications Data Findings
Australian Commission for Law Enforcement Integrity
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
1
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
1
Record keeping
Transposing errors
Total authorisations inspected:
98
0
10
20
30
40
50
60
70
80
90
100

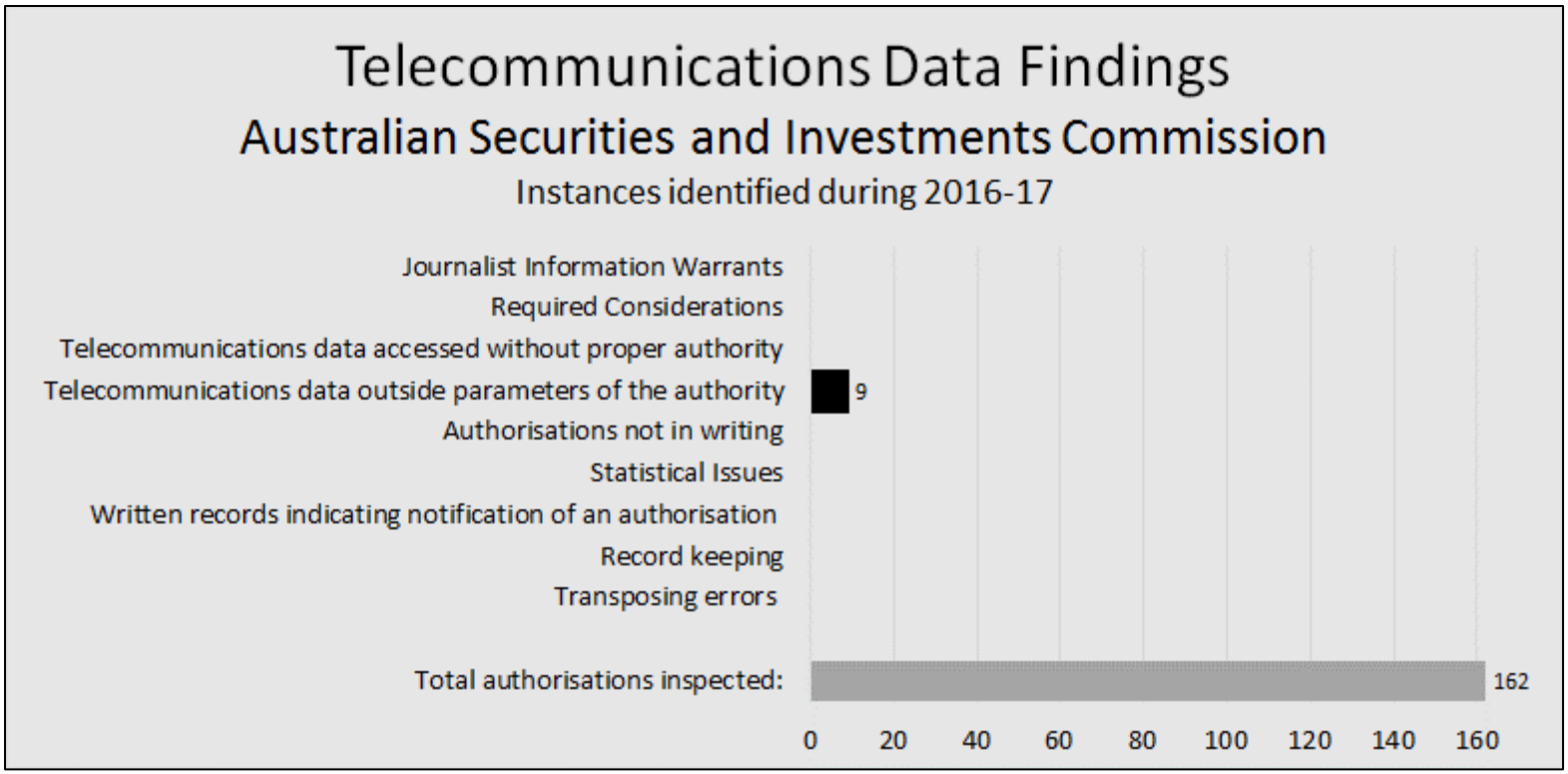

Stored Communications Findings
Australian Commission for Law Enforcement Integrity
Powers not used during relevant period
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
No inspection conducted during 2016-17
0
1
2
3
4
5

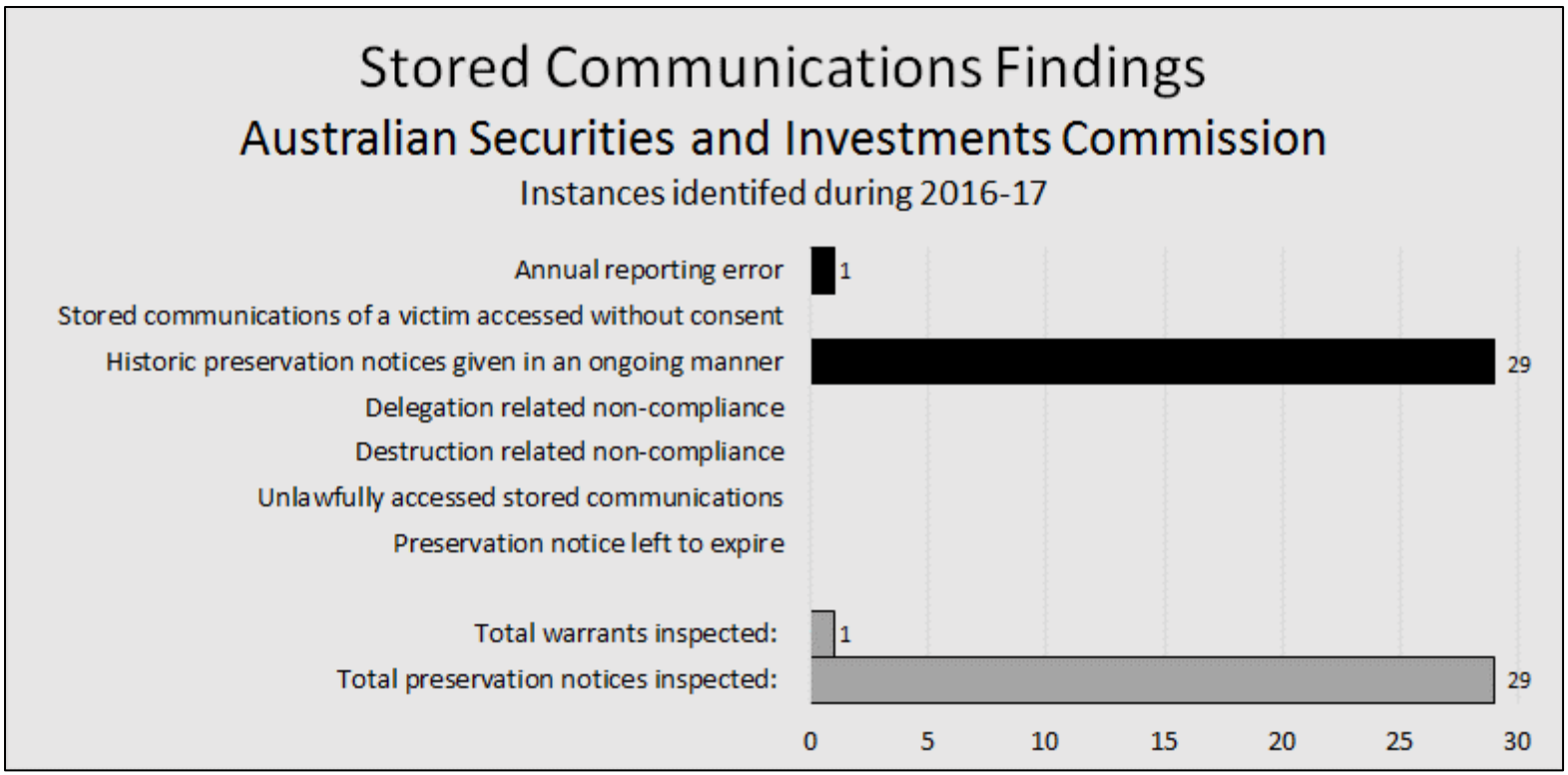


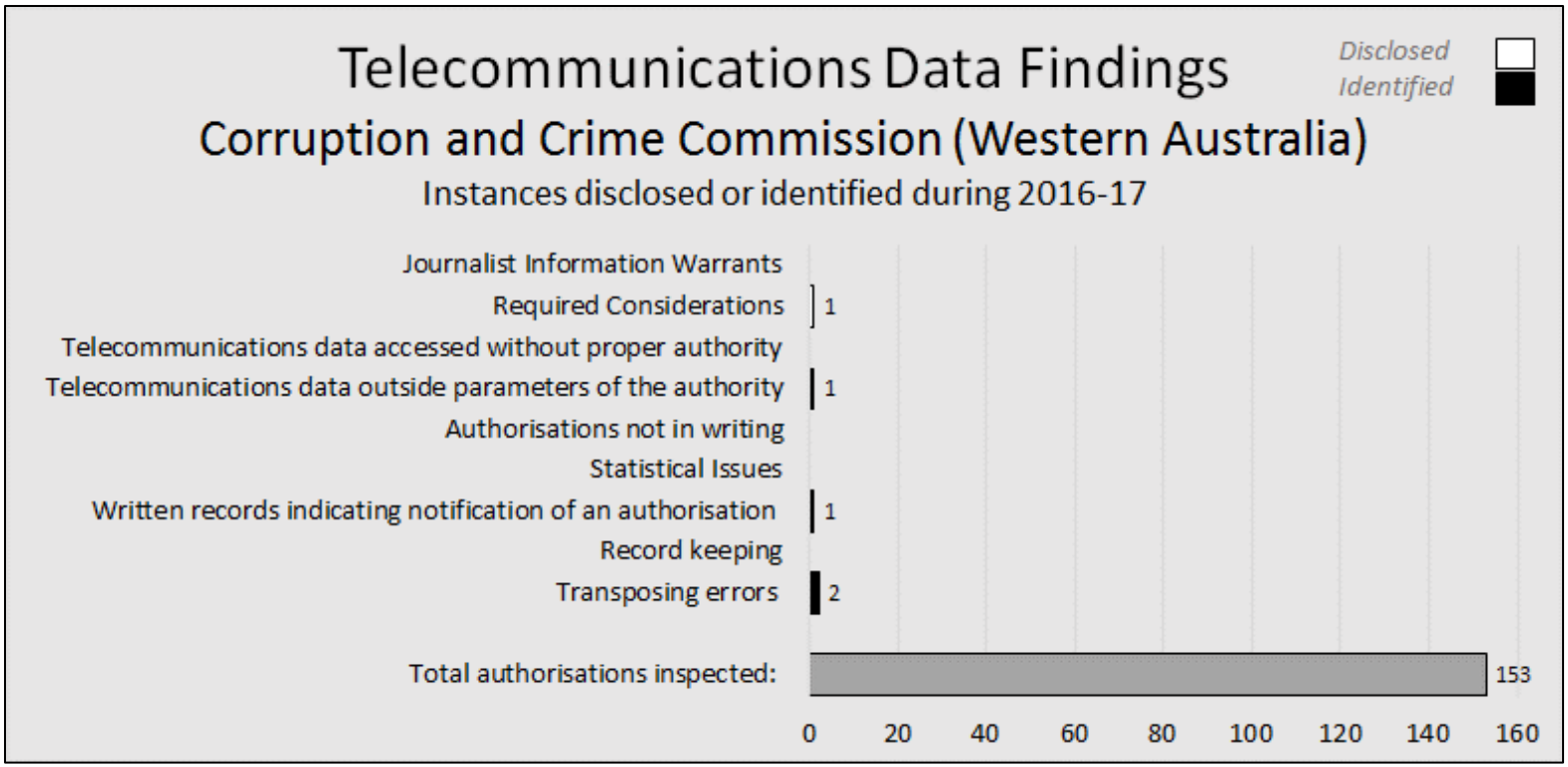

* Details of the AFP's breach of the Journalist Information Warrant provisions are provided in our October 2017 report: http://www.ombudsman.gov.au/__data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf

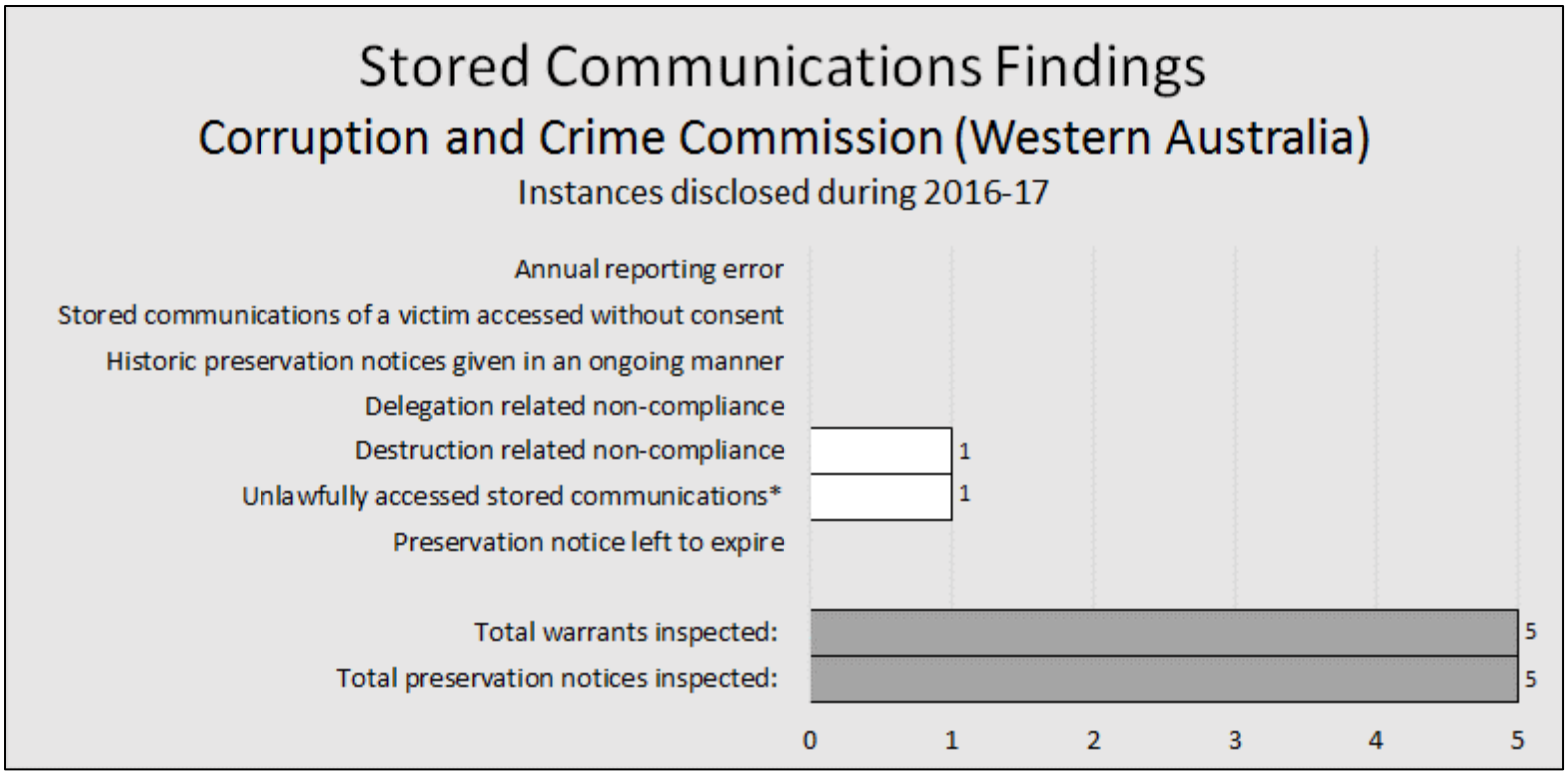
** In providing our Office with statistical information prior to the inspection, the AFP omitted a specific type of authorisation due to incorrect search parameters being used in collating this information. The omitted authorisation type was provided to our Office during the inspection.


Stored Communications Findings
Australian Federal Police
Instances identifed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
1
1
13
57
73
0
10
20
30
40
50
60
70
80


Telecommunications Data Findings
Australian Securities and Investments Commission
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
Total authorisations inspected:
9
162
0
20
40
60
80
100
120
140
160


Stored Communications Findings
Australian Securities and Investments Commission
Instances identifed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
1
29
1
29
0
5
10
15
20
25
30


Telecommunications Data Findings
Disclosed
Identified
Corruption and Crime Commission (Western Australia)
Instances disclosed or identified during 2016-17
Journalist Information Warrants
Required Considerations
1
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
1
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
1
Record keeping
Transposing errors
2
Total authorisations inspected:
153
0
20
40
60
80
100
120
140
160

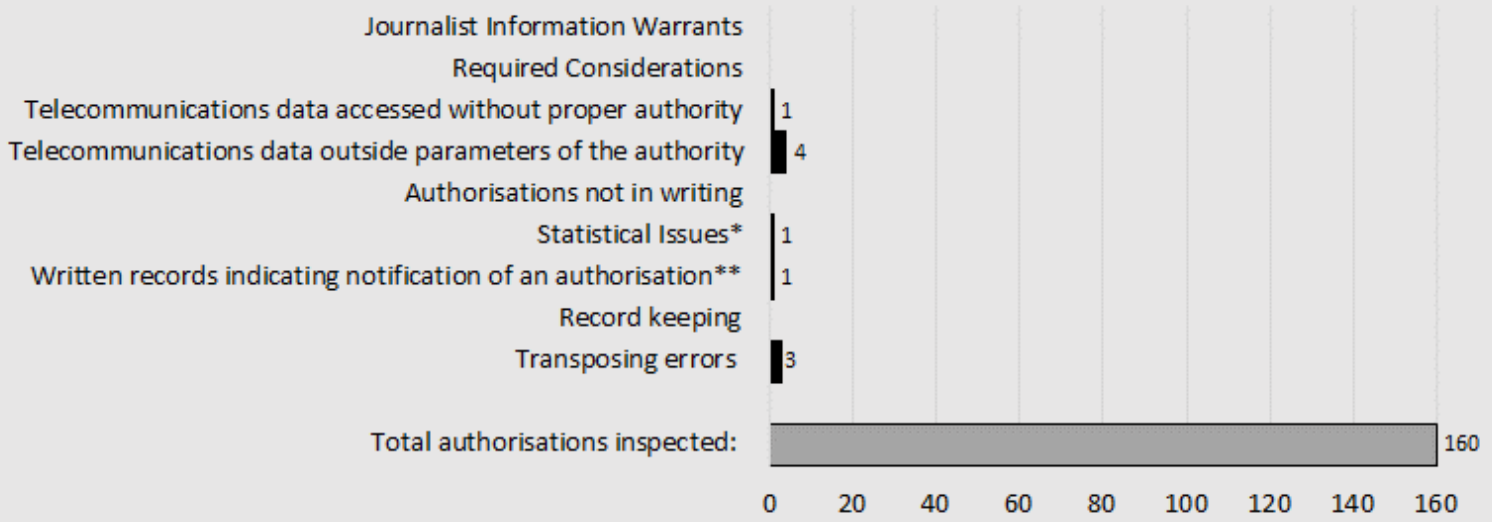



* While CCC (WA) received unlawfully accessed stored communications, we were satisfied the agency's processes worked effectively to screen, identify and quarantine this information prior to it being disseminated to investigators.

# Telecommunications Data Findings

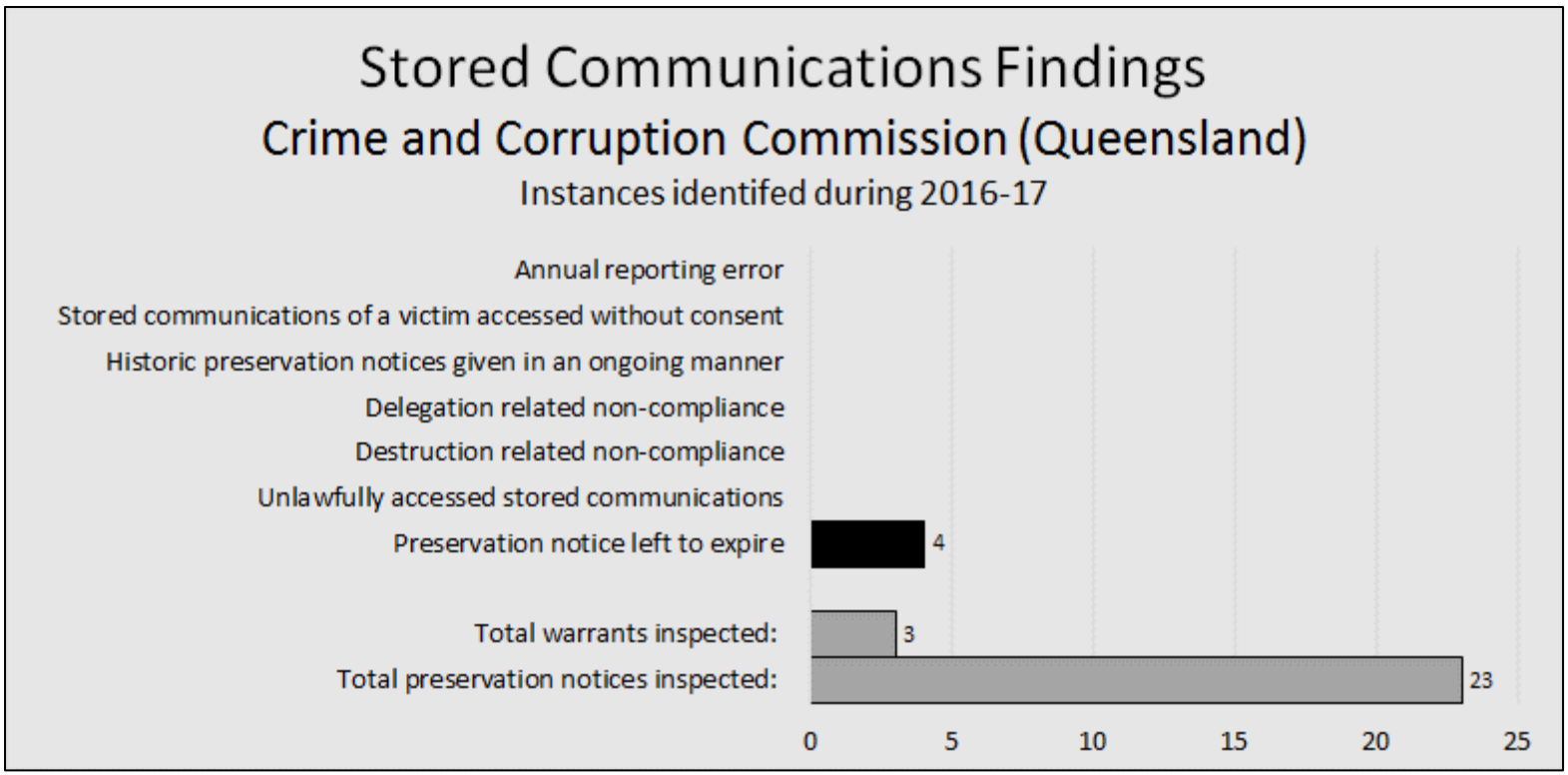
## Crime and Corruption Commission (Queensland)

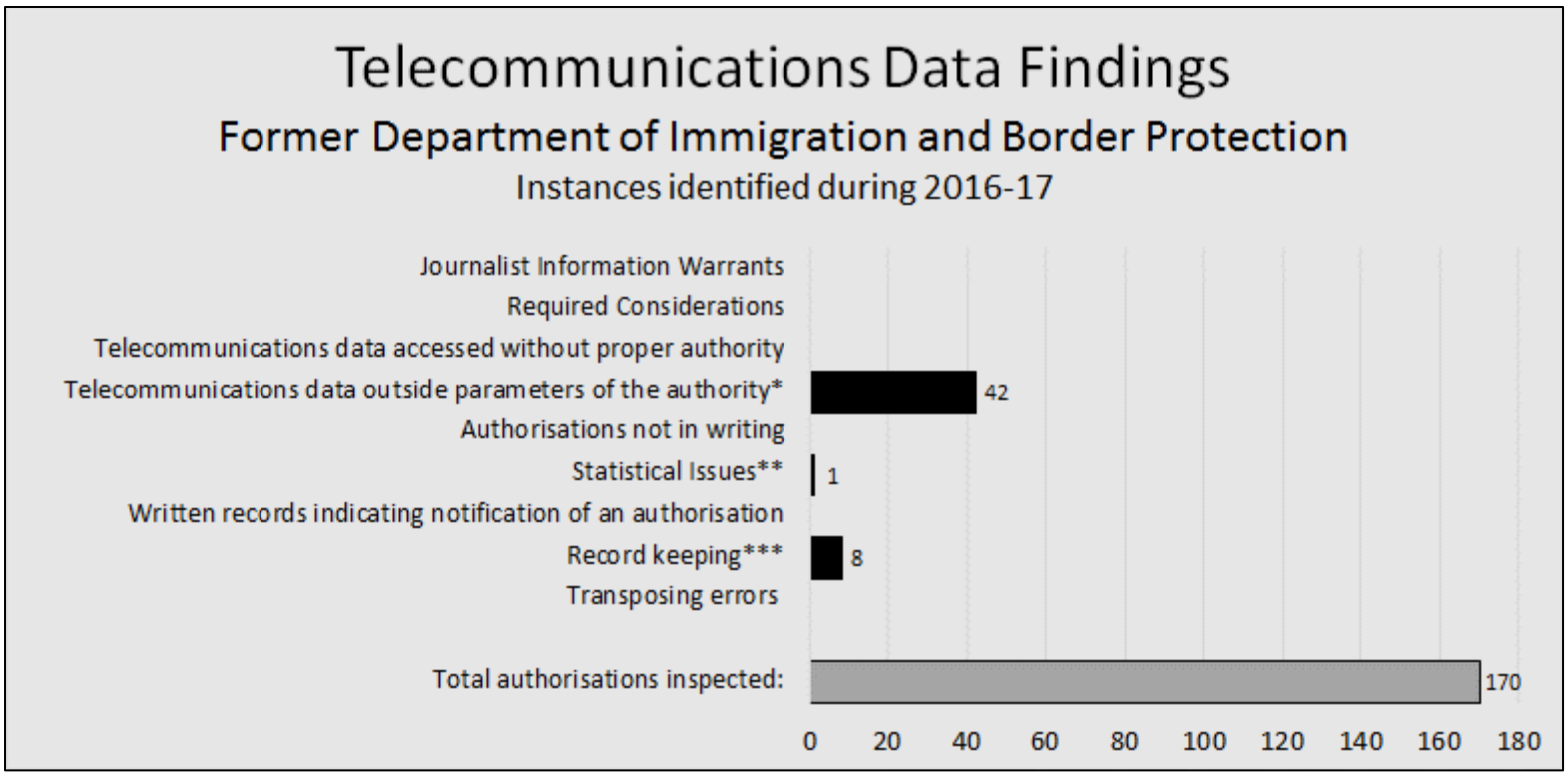
Instances identified during 2016-17



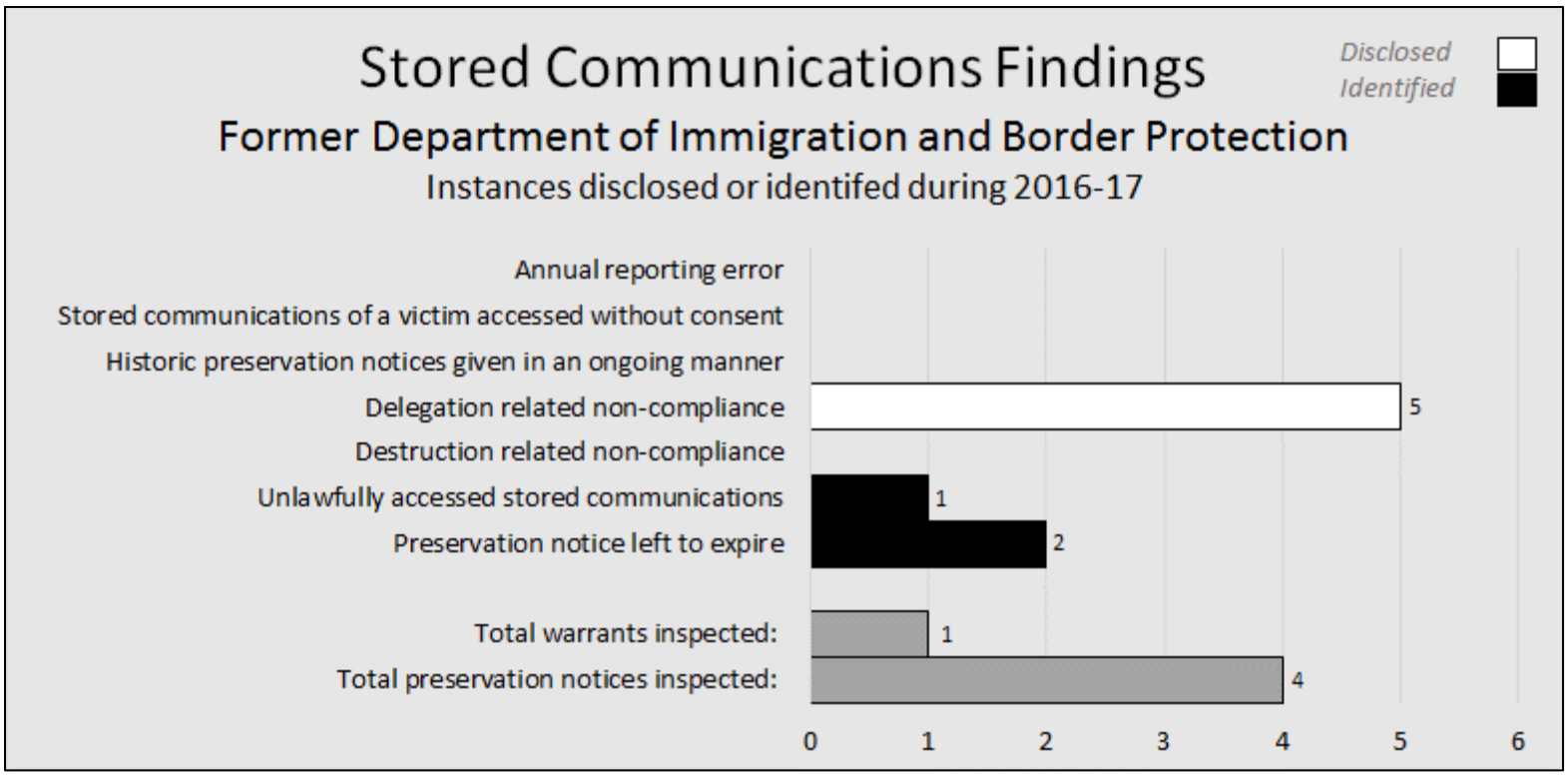

*During our inspection, we noted instances where reports to our Office, and to the Minister about the number of authorisations made were inconsistent with what the inspected records reflected. This was the result of typographical errors, combined with inconsistencies in how authorisations were counted. CCC (QLD) has advised our Office of remedial action it has taken in response to this issue, which we will continue to monitor at future inspections.

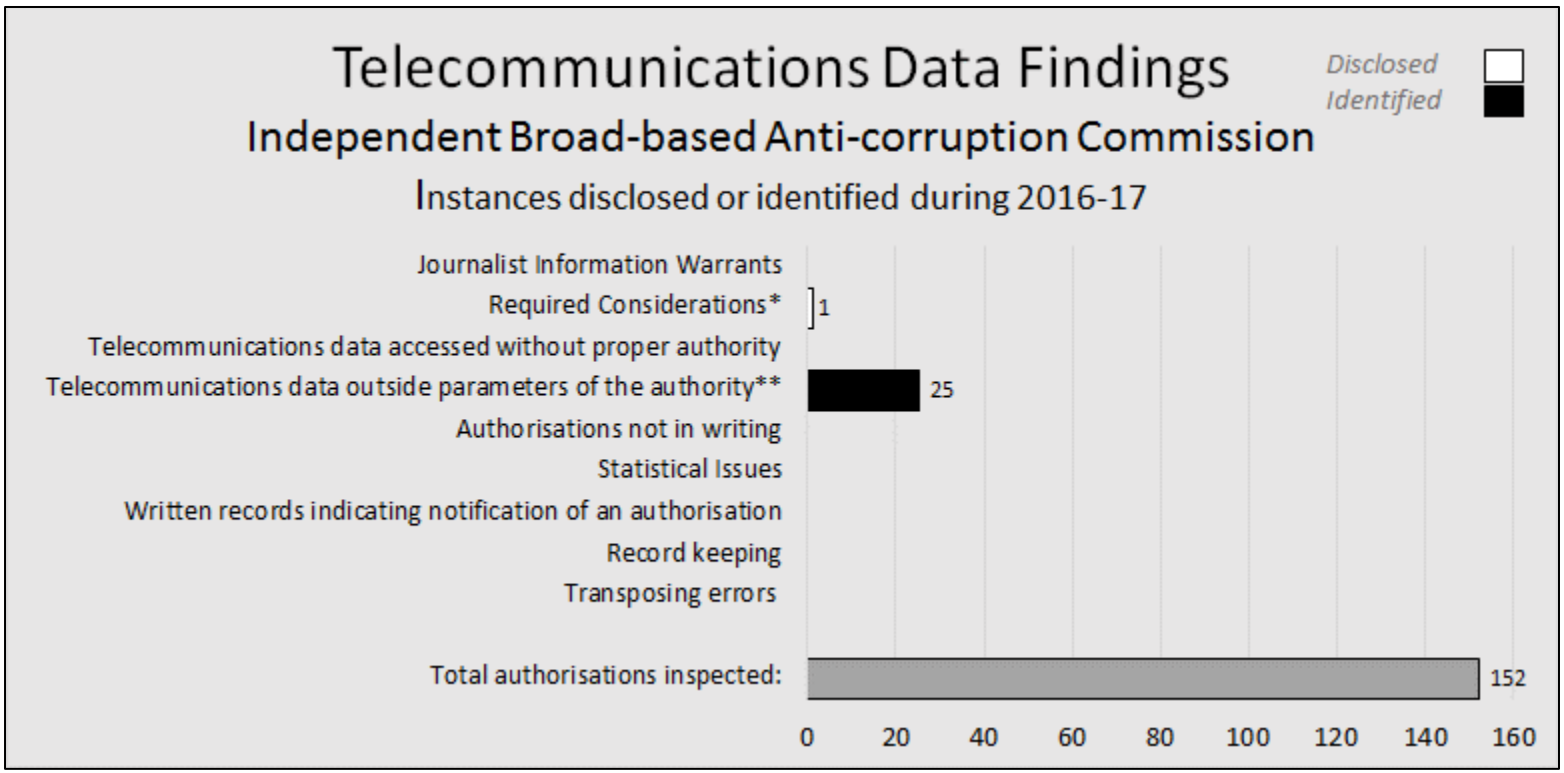
**In each instance where an authorisation was notified to the relevant carrier by fax, there was nothing to indicate the exact moment notification of the authorisation occurred. In these instances, this record keeping issue did not cause ambiguity in determining whether obtained telecommunications data was within the parameters of the authorisation; however CCC (QLD) has amended its processes to ensure a written record of notification is kept.


Stored Communications Findings
Crime and Corruption Commission (Queensland)
Instances identifed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
4
Total warrants inspected:
3
Total preservation notices inspected:
23
0
5
10
15
20
25



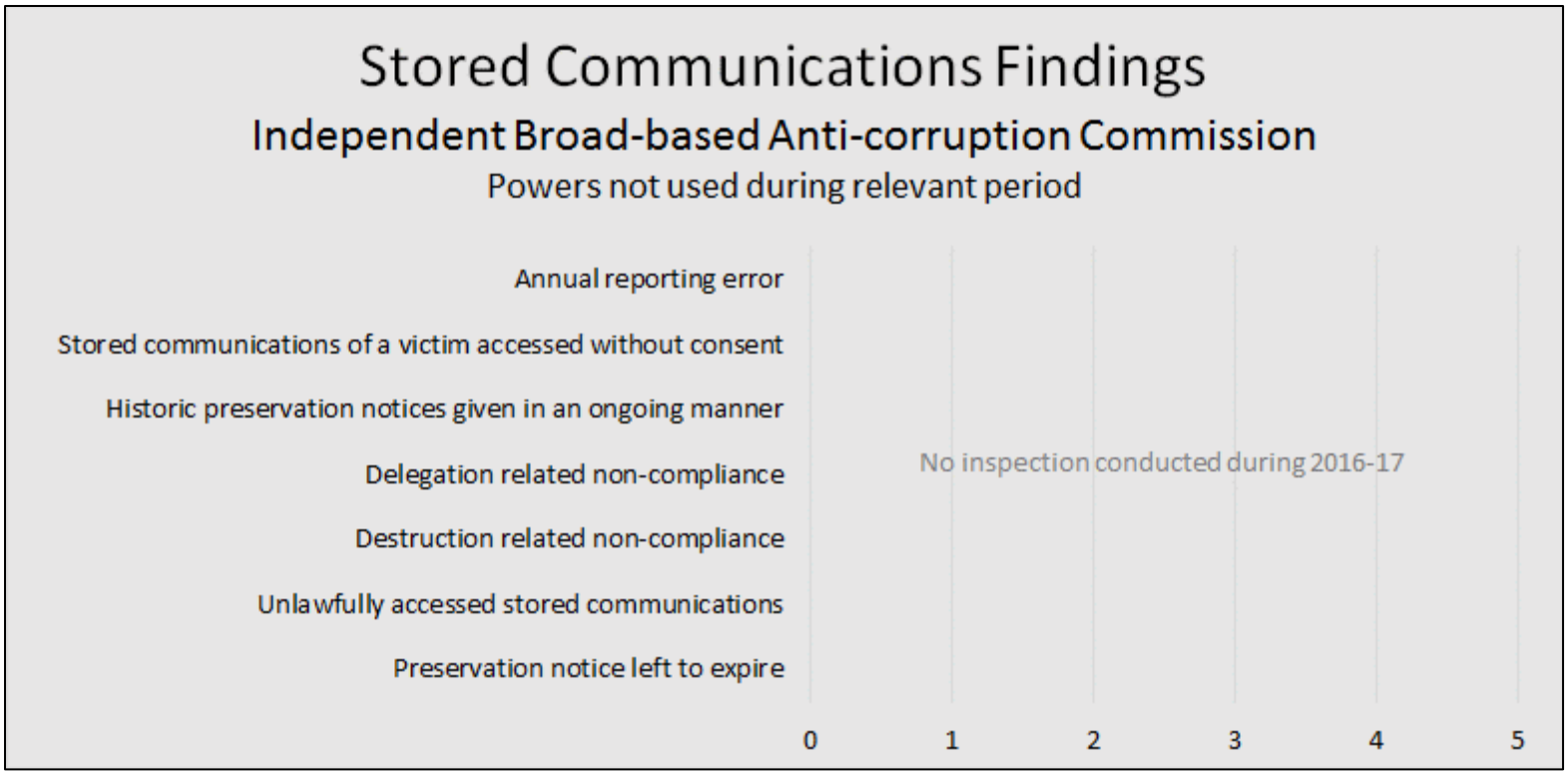

*41 out of these 42 instances were the result of automatic, and unintentional, input from DIBP's electronic database. Home Affairs has since amended its processes to mitigate recurrence of this issue and we will monitor the effectiveness of this measure at future inspections.
**Recommendation made to Home Affairs as detailed on page 18.
***Recommendation made to Home Affairs as detailed on page 20.

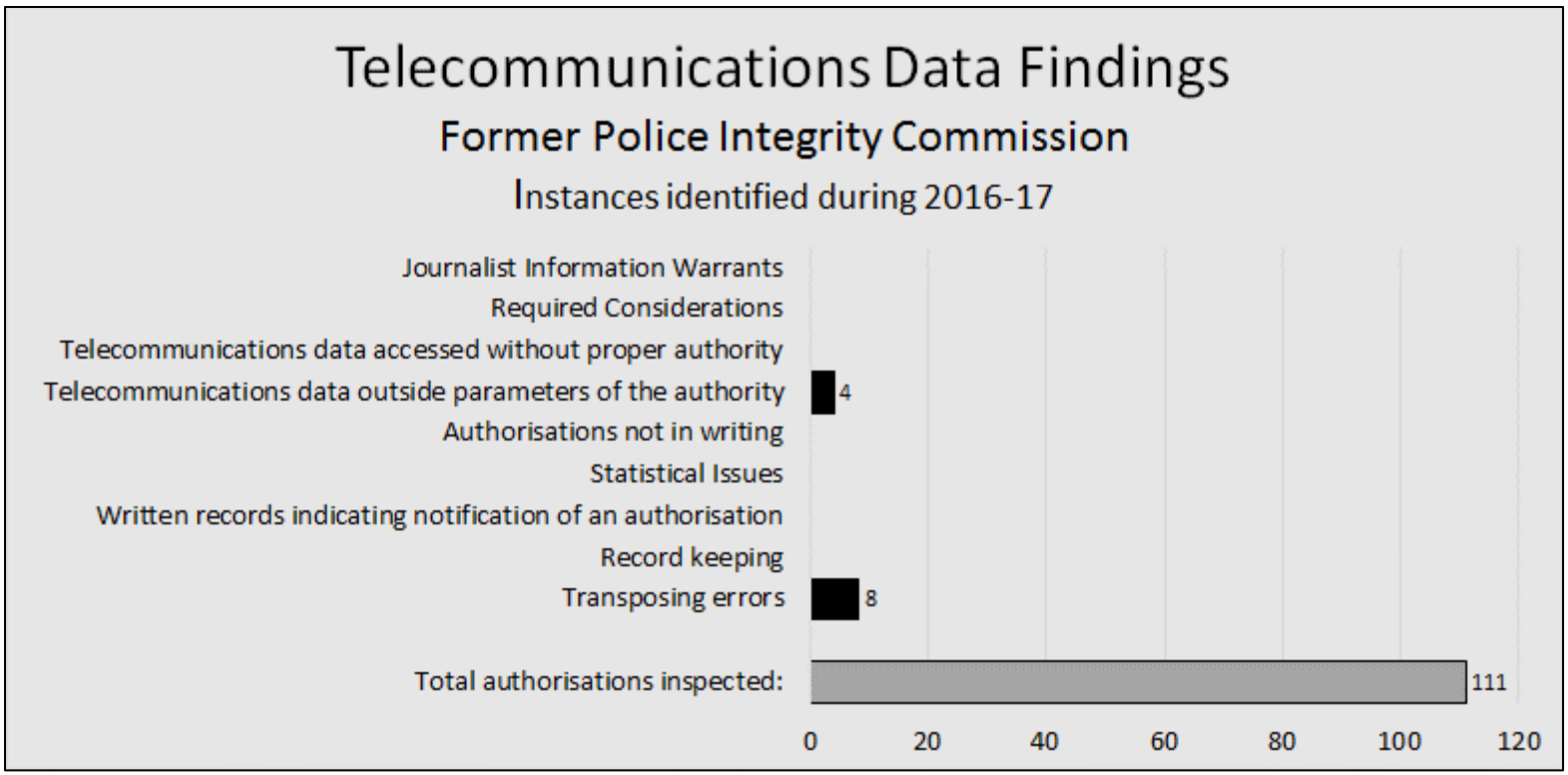

Stored Communications Findings
Disclosed
Identified
Former Department of Immigration and Border Protection
Instances disclosed or identifed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
5
1
2
1
4
0
1
2
3
4
5
6

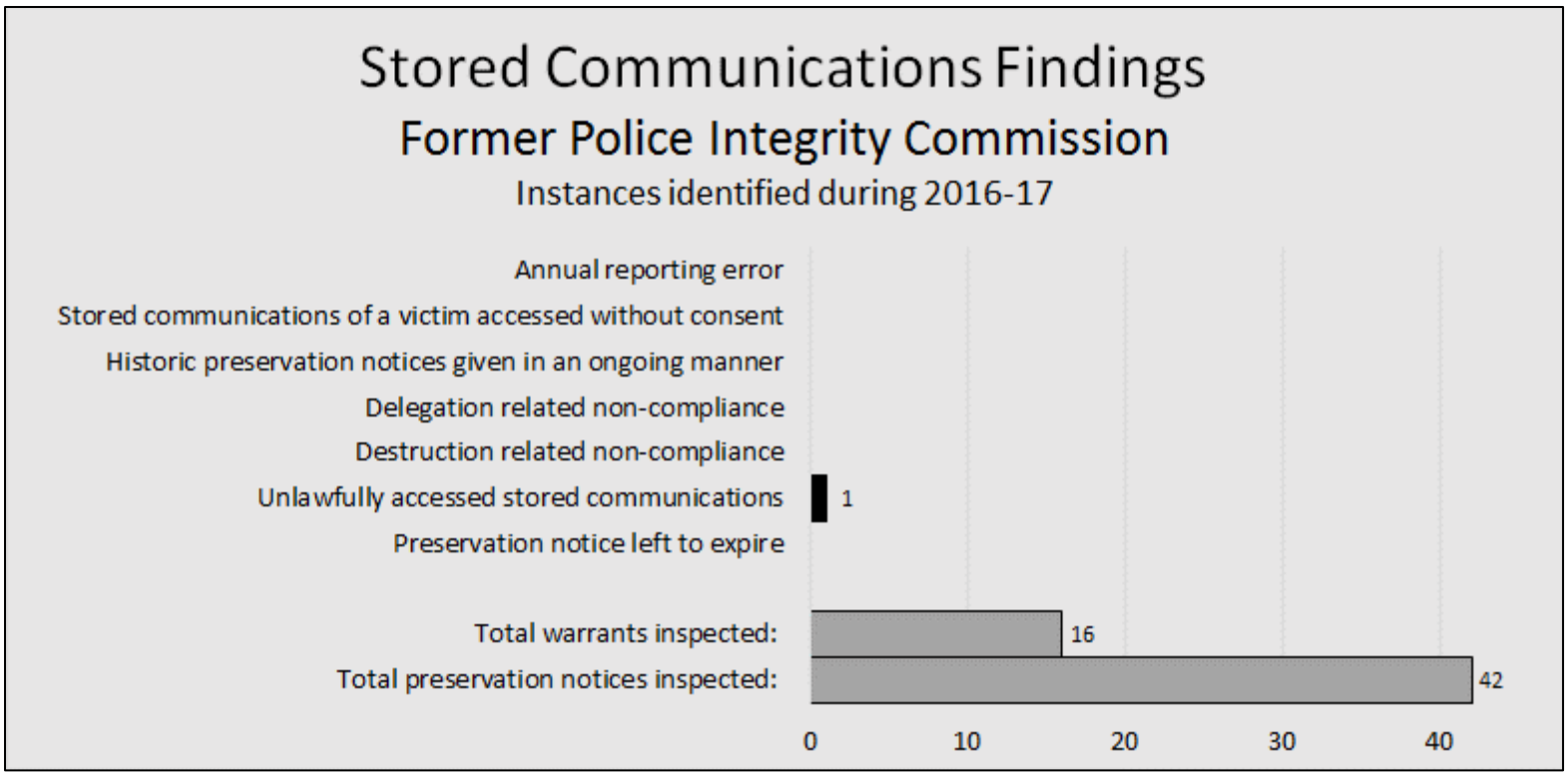


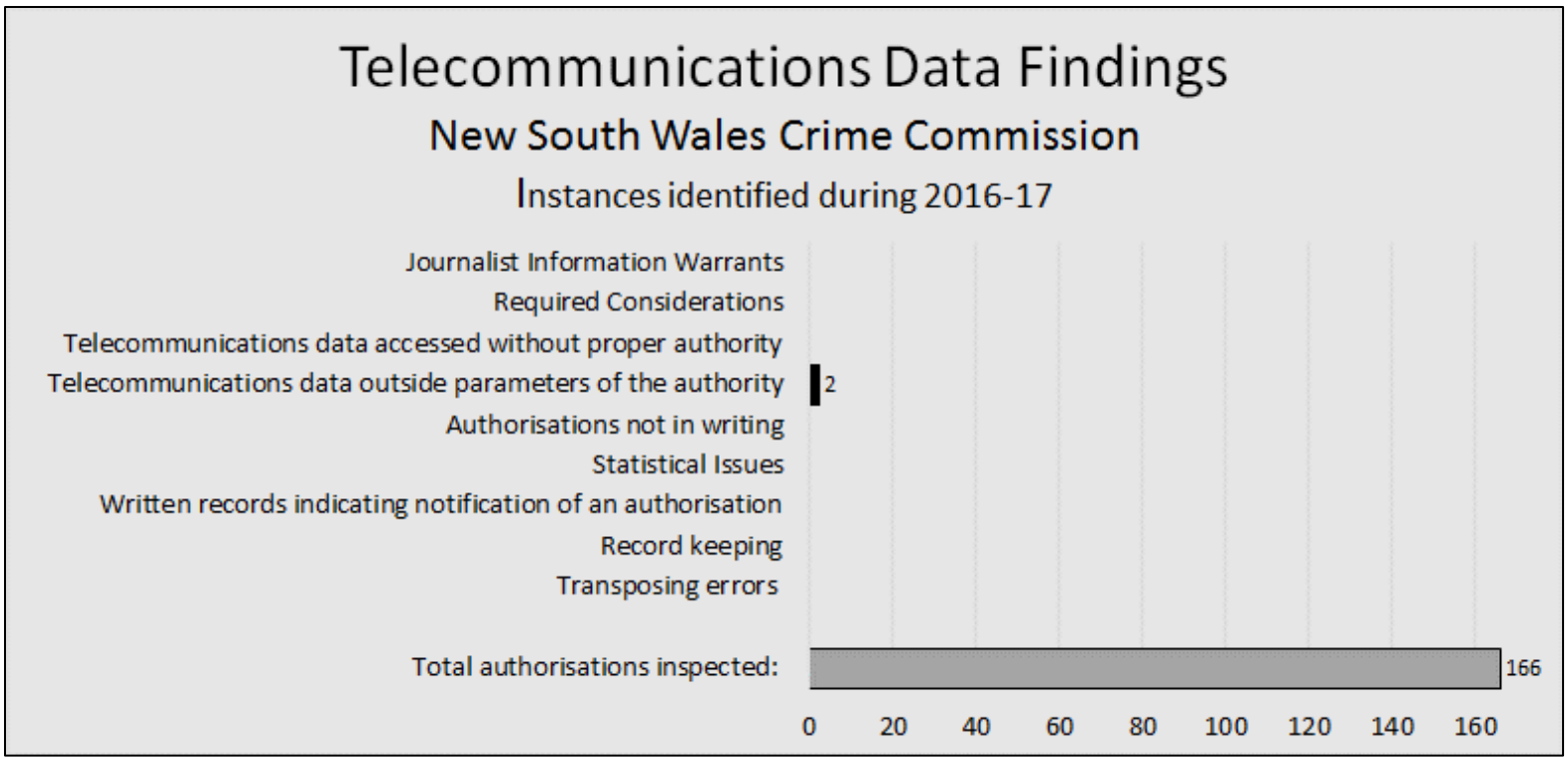

*In this instance, IBAC disclosed that an authorisation had been made under the incorrect provision. Upon identifying the error, IBAC quarantined the telecommunications data received under the authorisation.

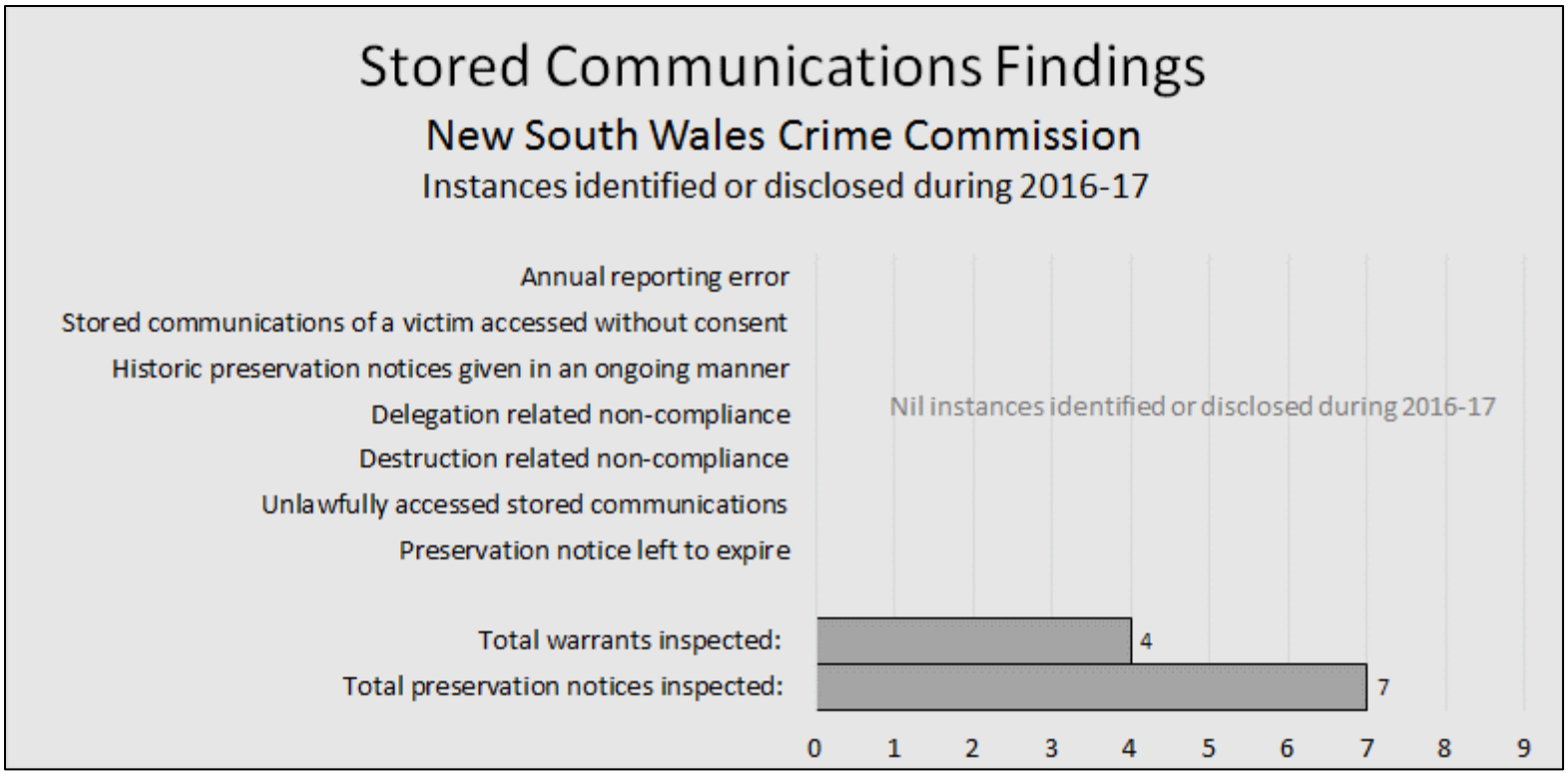
**In two of these 25 instances, on the basis of incomplete advice from our Office, IBAC only partially quarantined the relevant telecommunications data. We acknowledge the remedial action taken by IBAC and have suggested the remaining telecommunications data be quarantined. In 13 of these instances, telecommunications data was received outside the parameters of the authority as a result of automatic, and unintentional, input from IBAC's systems. IBAC has since amended its systems to mitigate recurrence.

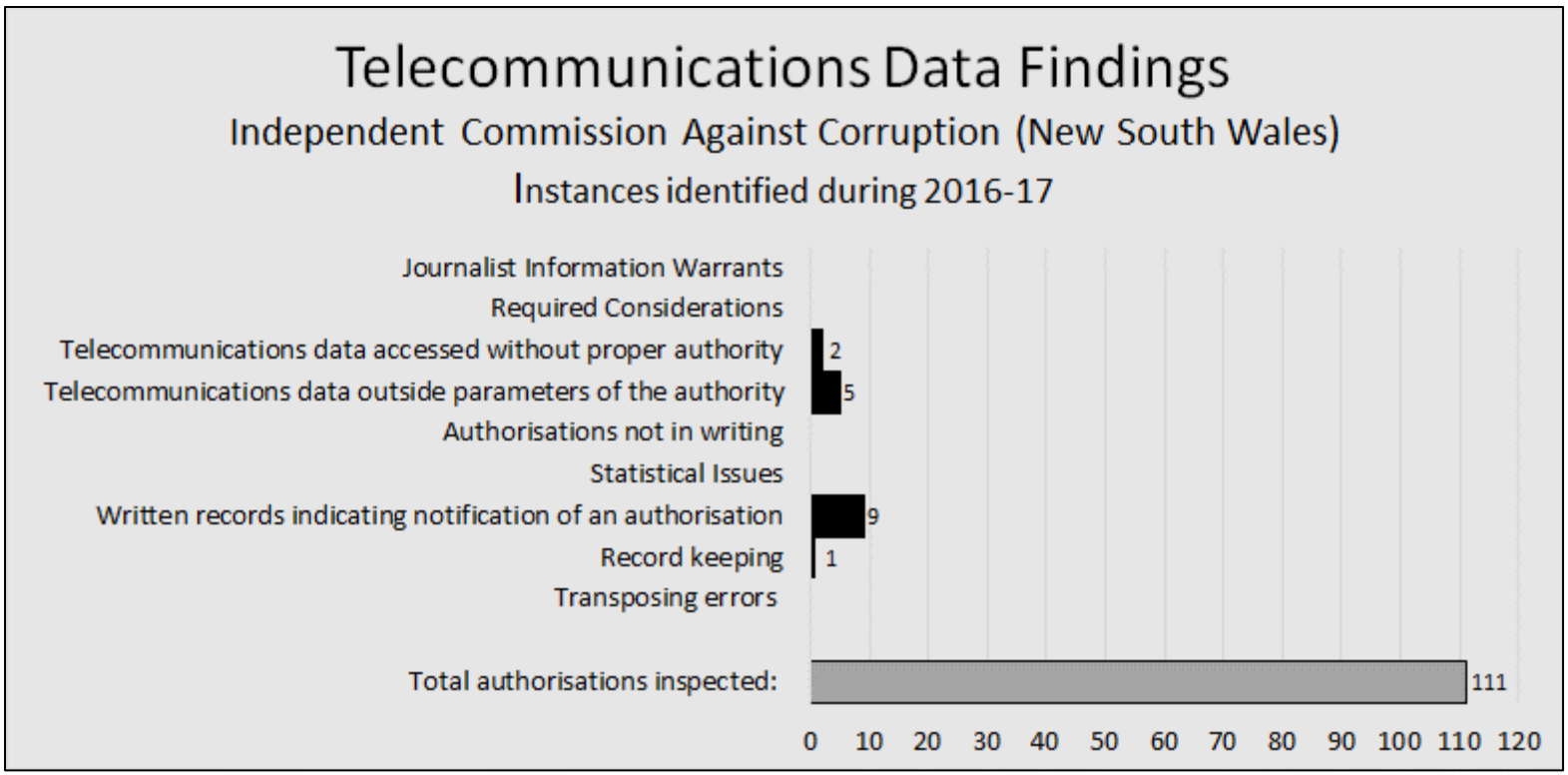

Stored Communications Findings
Independent Broad-based Anti-corruption Commission
Powers not used during relevant period
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
No inspection conducted during 2016-17
0
1
2
3
4
5

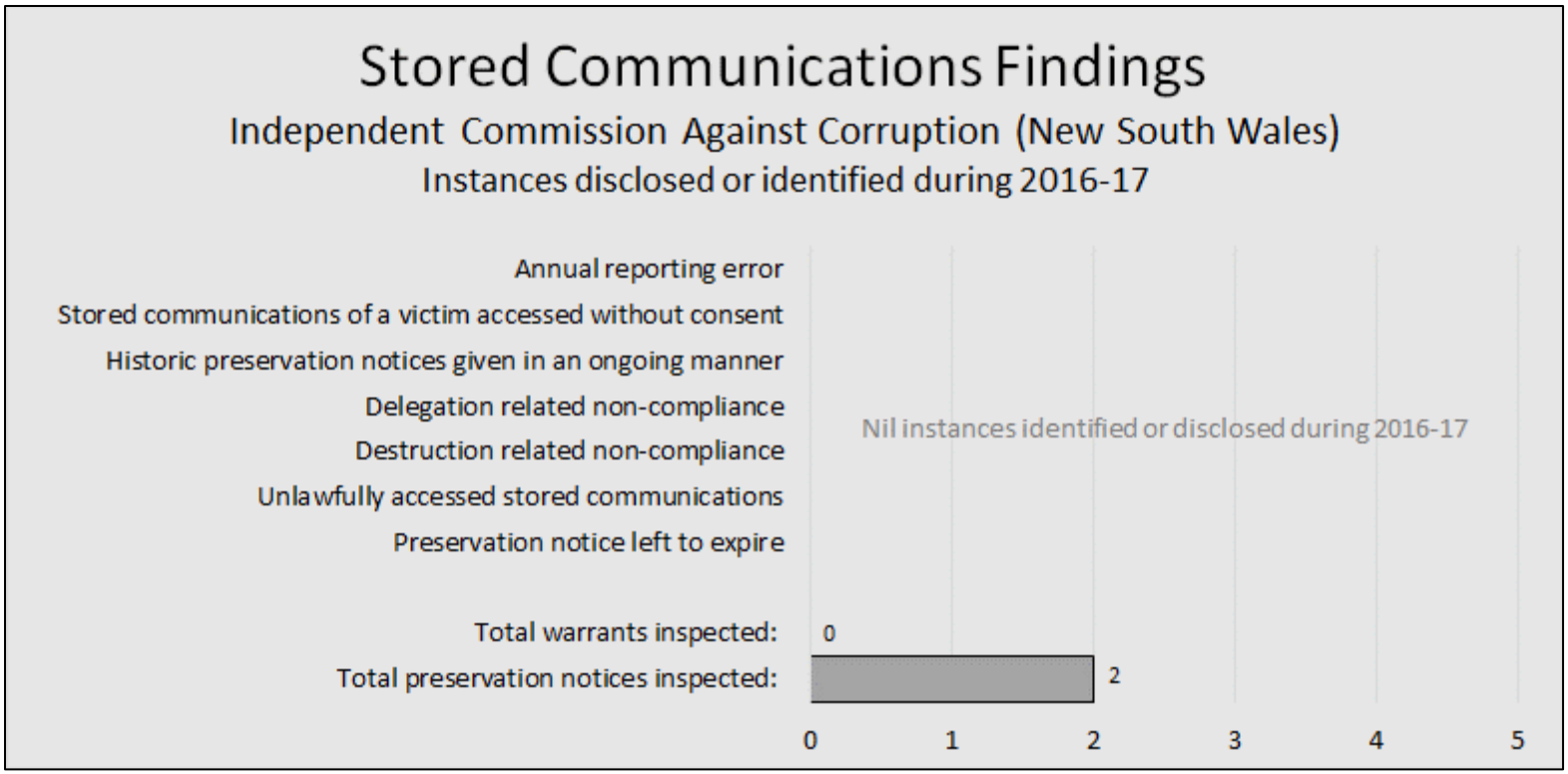

Telecommunications Data Findings
Former Police Integrity Commission
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
4
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
8
Total authorisations inspected:
111
0
20
40
60
80
100
120

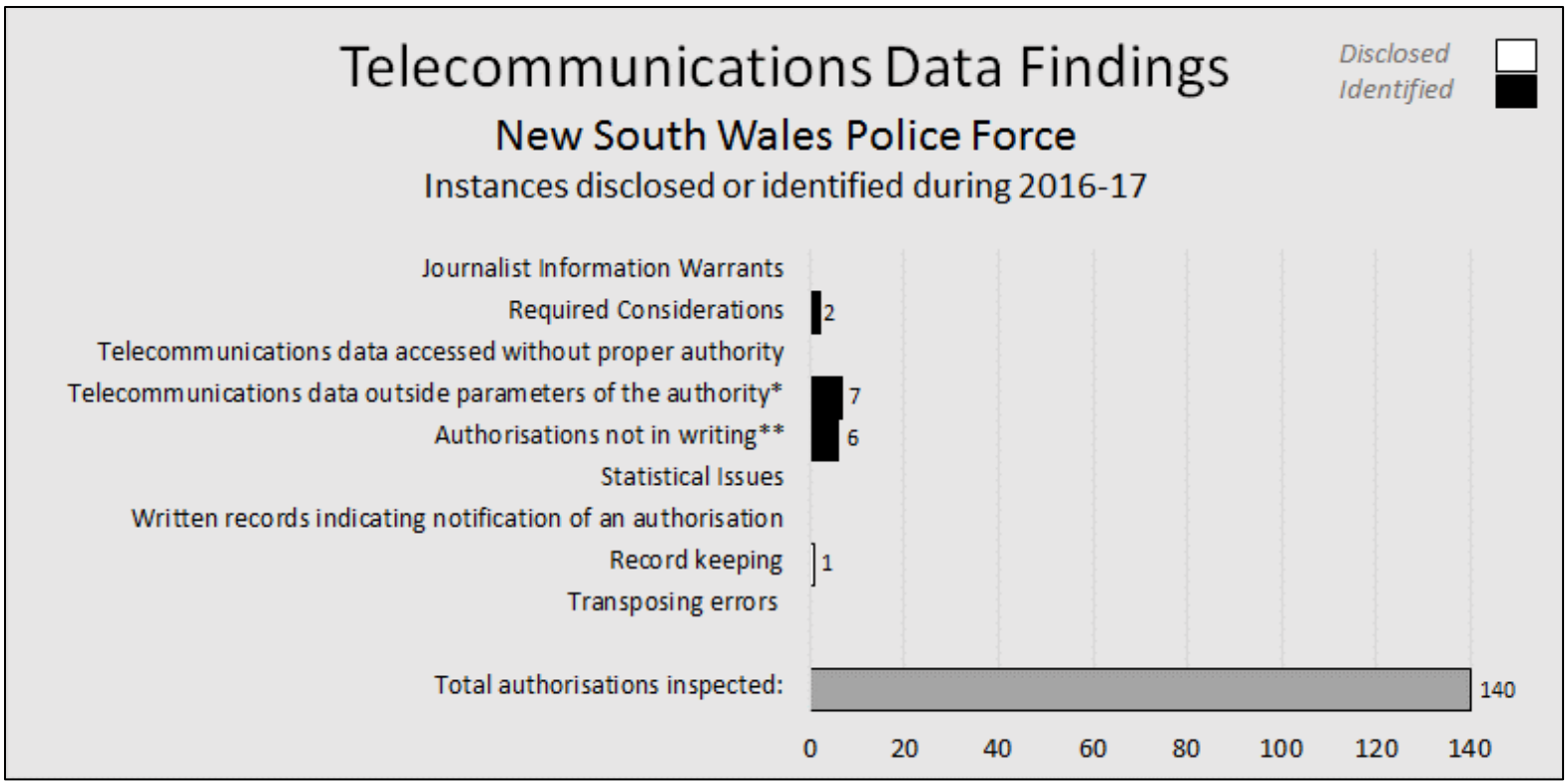

Stored Communications Findings
Former Police Integrity Commission
Instances identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
1
16
42
0
10
20
30
40


Telecommunications Data Findings
New South Wales Crime Commission
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
2
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
Total authorisations inspected:
166
0
20
40
60
80
100
120
140
160


Stored Communications Findings
New South Wales Crime Commission
Instances identified or disclosed during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Nil instances identified or disclosed during 2016-17
Total warrants inspected:
Total preservation notices inspected:
4
7
0 1 2 3 4 5 6 7 8 9

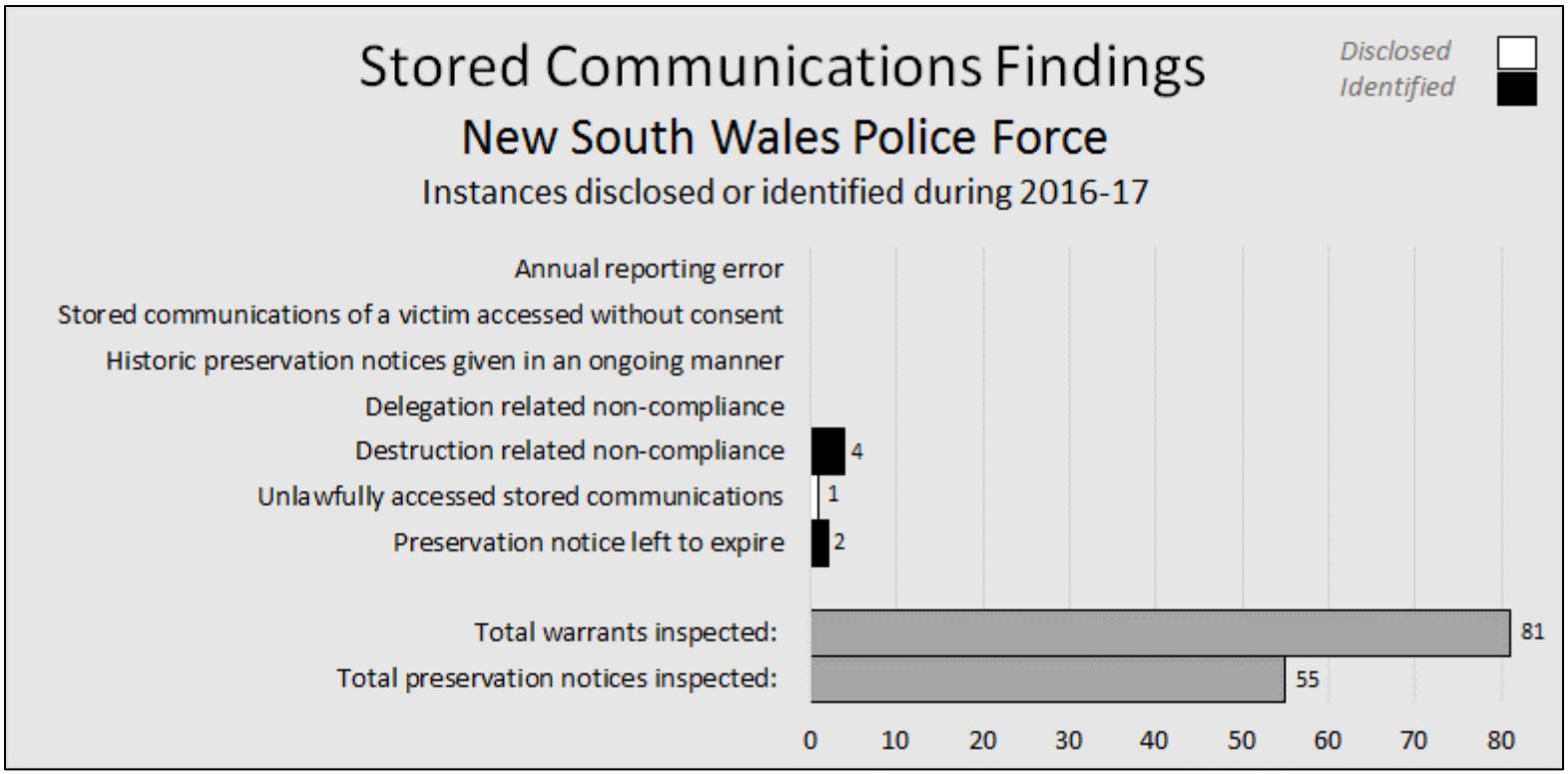

Telecommunications Data Findings
Independent Commission Against Corruption (New South Wales)
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
2
Telecommunications data outside parameters of the authority
5
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
9
Record keeping
1
Transposing errors
Total authorisations inspected:
111
0 10 20 30 40 50 60 70 80 90 100 110 120

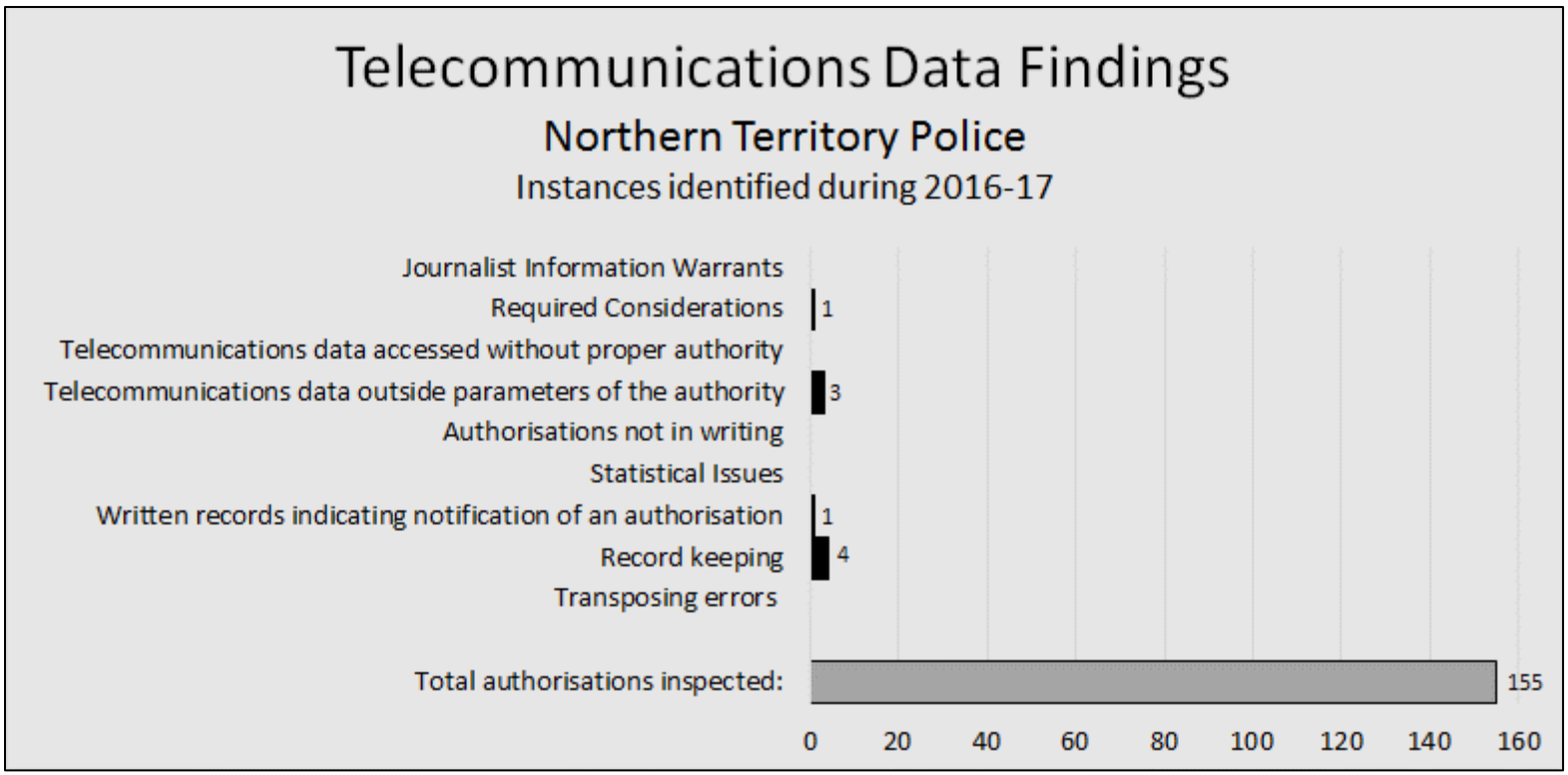

Stored Communications Findings
Independent Commission Against Corruption (New South Wales)
Instances disclosed or identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Nil instances identified or disclosed during 2016-17
Total warrants inspected:
Total preservation notices inspected:
0
2
0
1
2
3
4
5

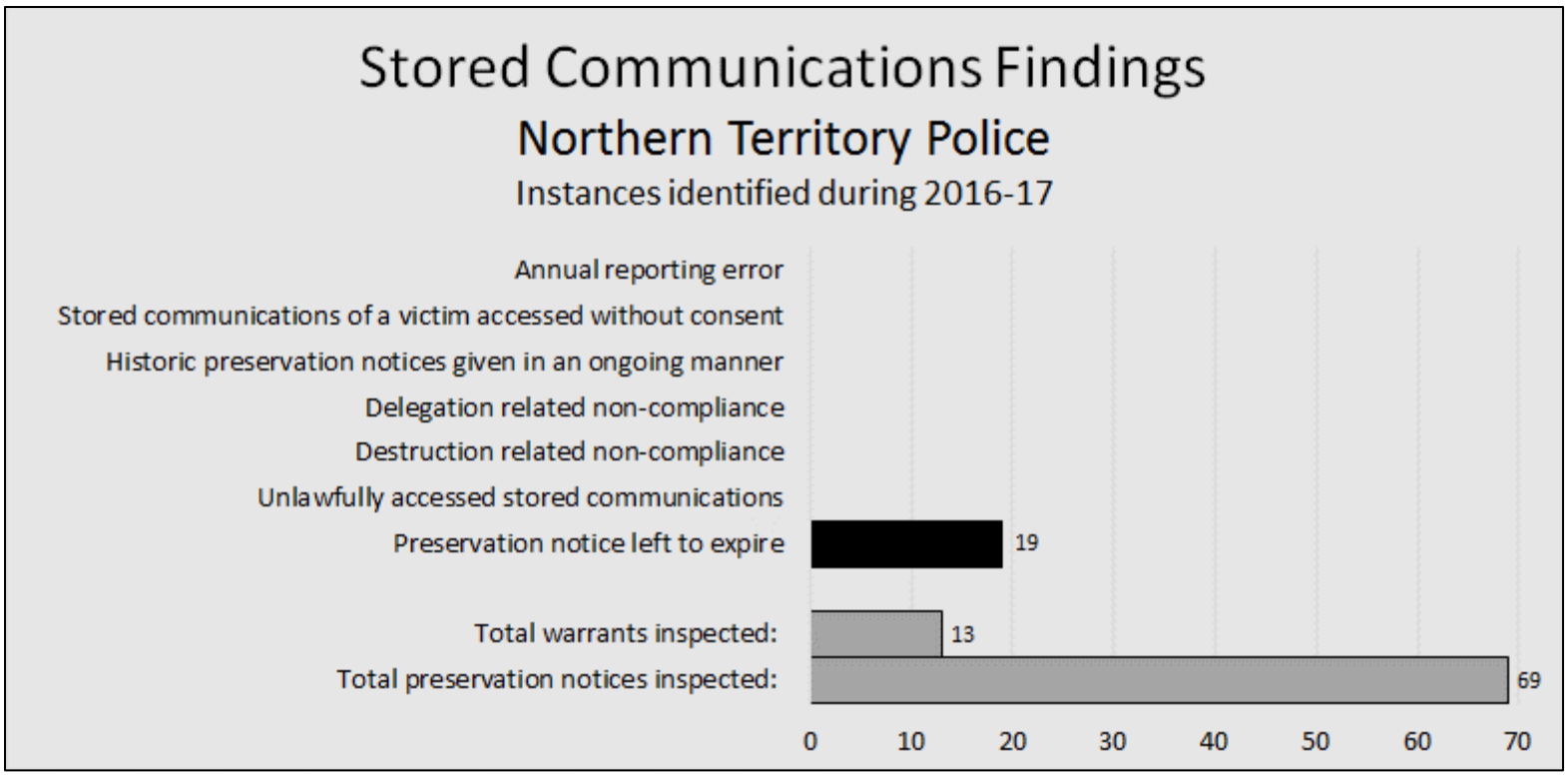


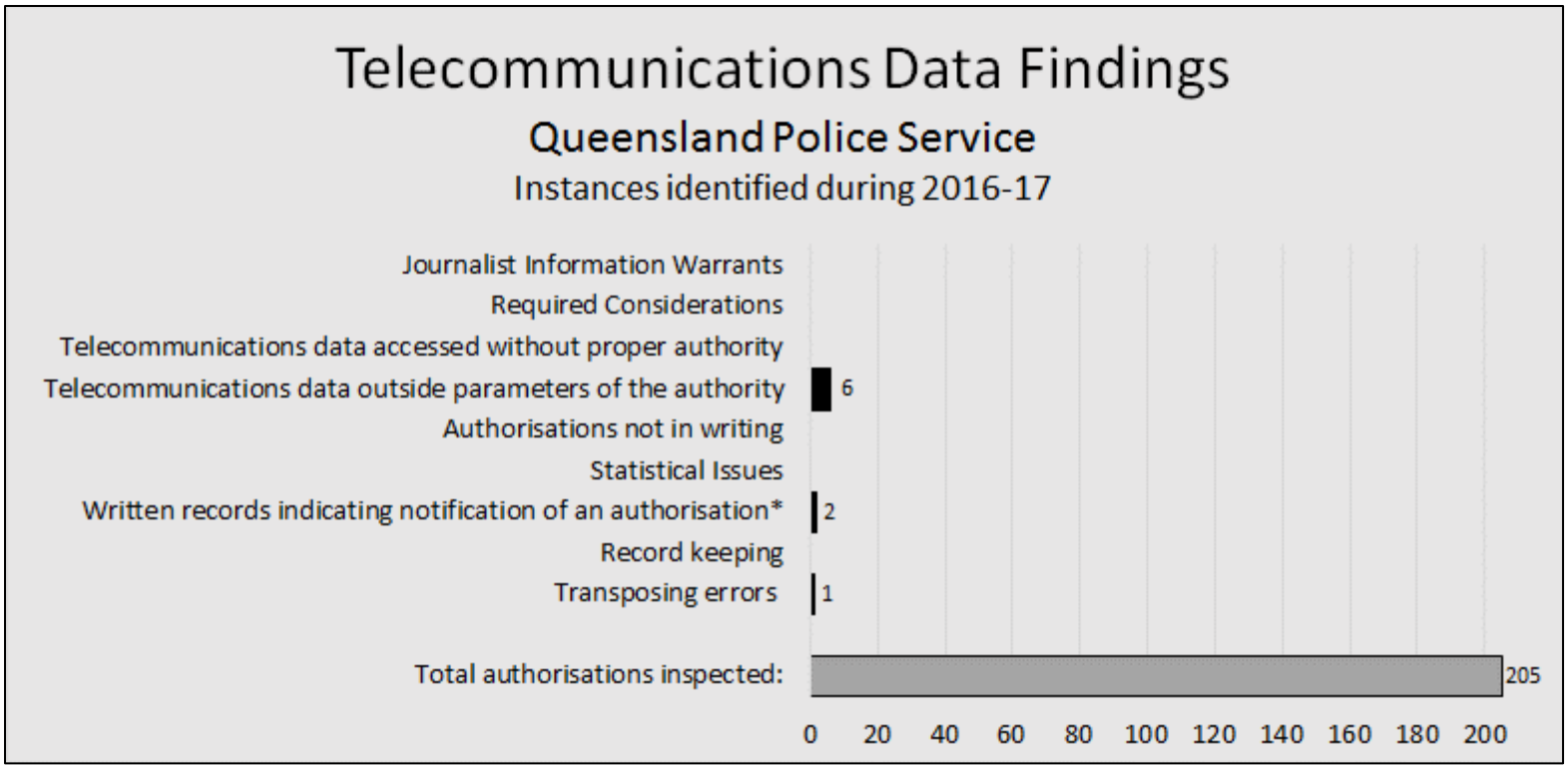

*In two of these instances, our Office was unable to determine whether the telecommunications data received from the carrier was within the parameters of the authority because the carrier had not specified the telecommunications service to which the information related.

**This includes one area of NSW Police that was routinely exercising its telecommunications data powers without a written or electronic authorisation in place.

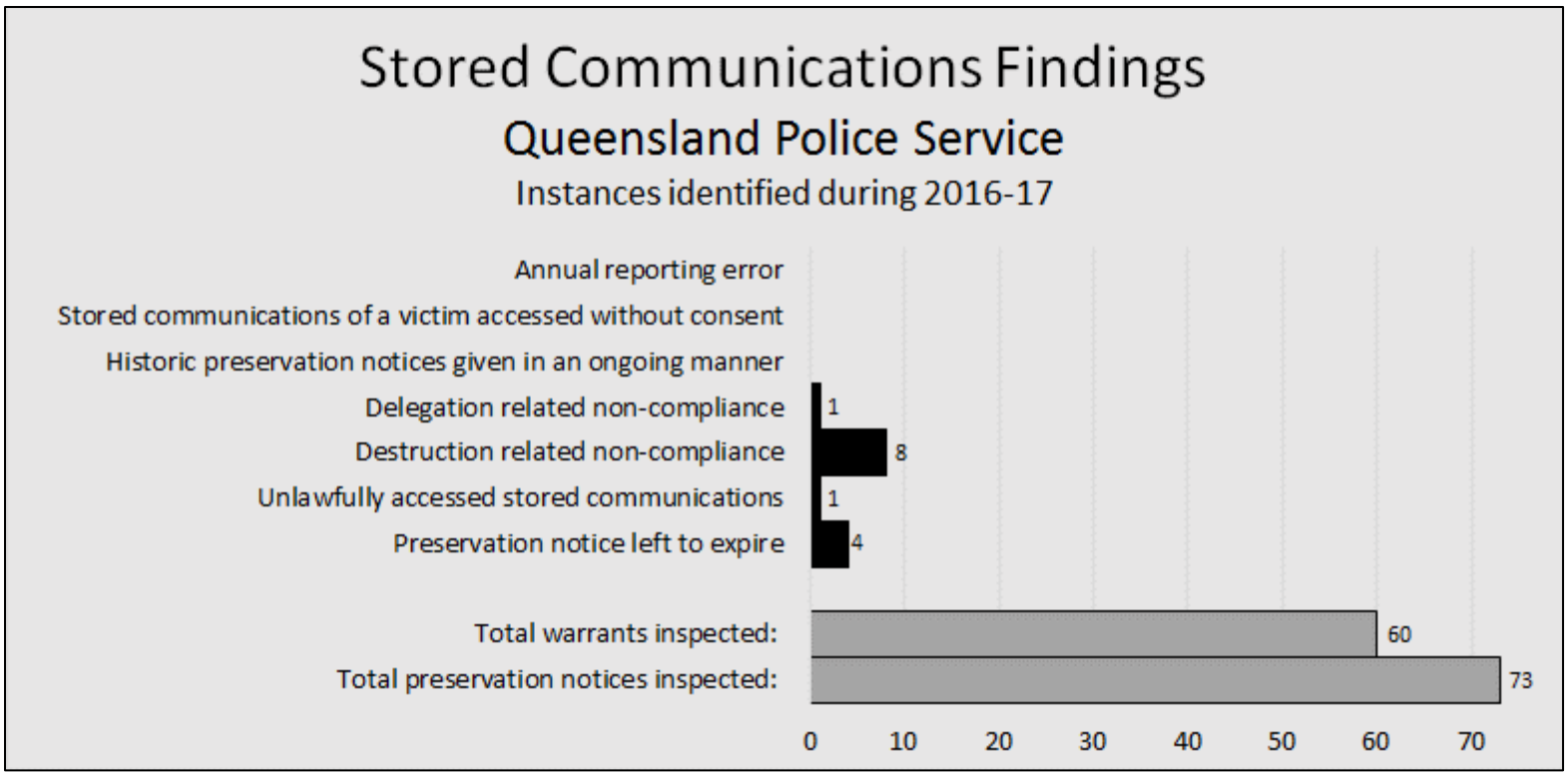

Stored Communications Findings
New South Wales Police Force
Instances disclosed or identified during 2016-17
Disclosed
Identified
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
4
Unlawfully accessed stored communications
1
Preservation notice left to expire
2
Total warrants inspected:
81
Total preservation notices inspected:
55
0
10
20
30
40
50
60
70
80

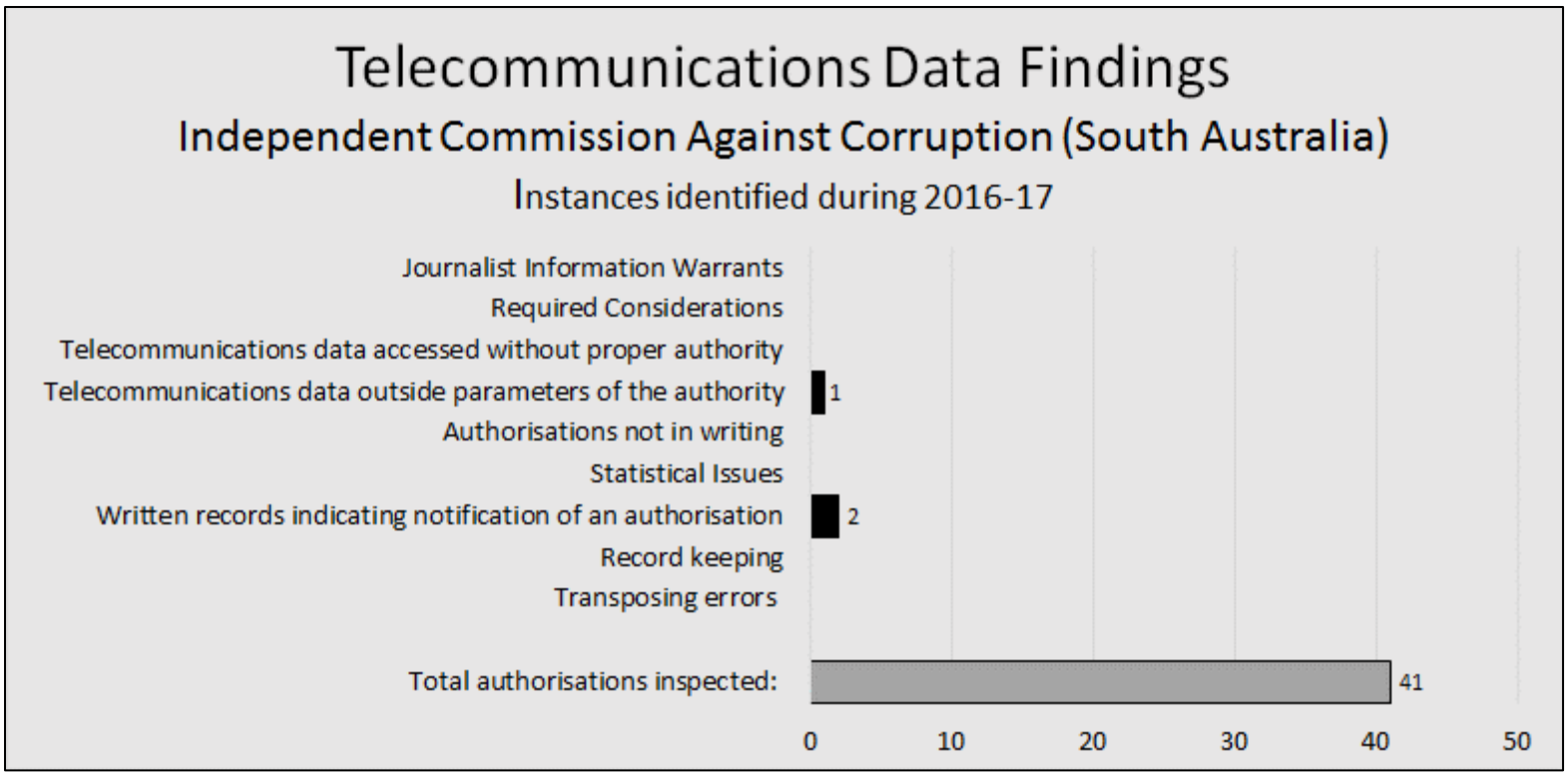

Telecommunications Data Findings
Northern Territory Police
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
Total authorisations inspected:
1
3
1
4
155
0
20
40
60
80
100
120
140
160

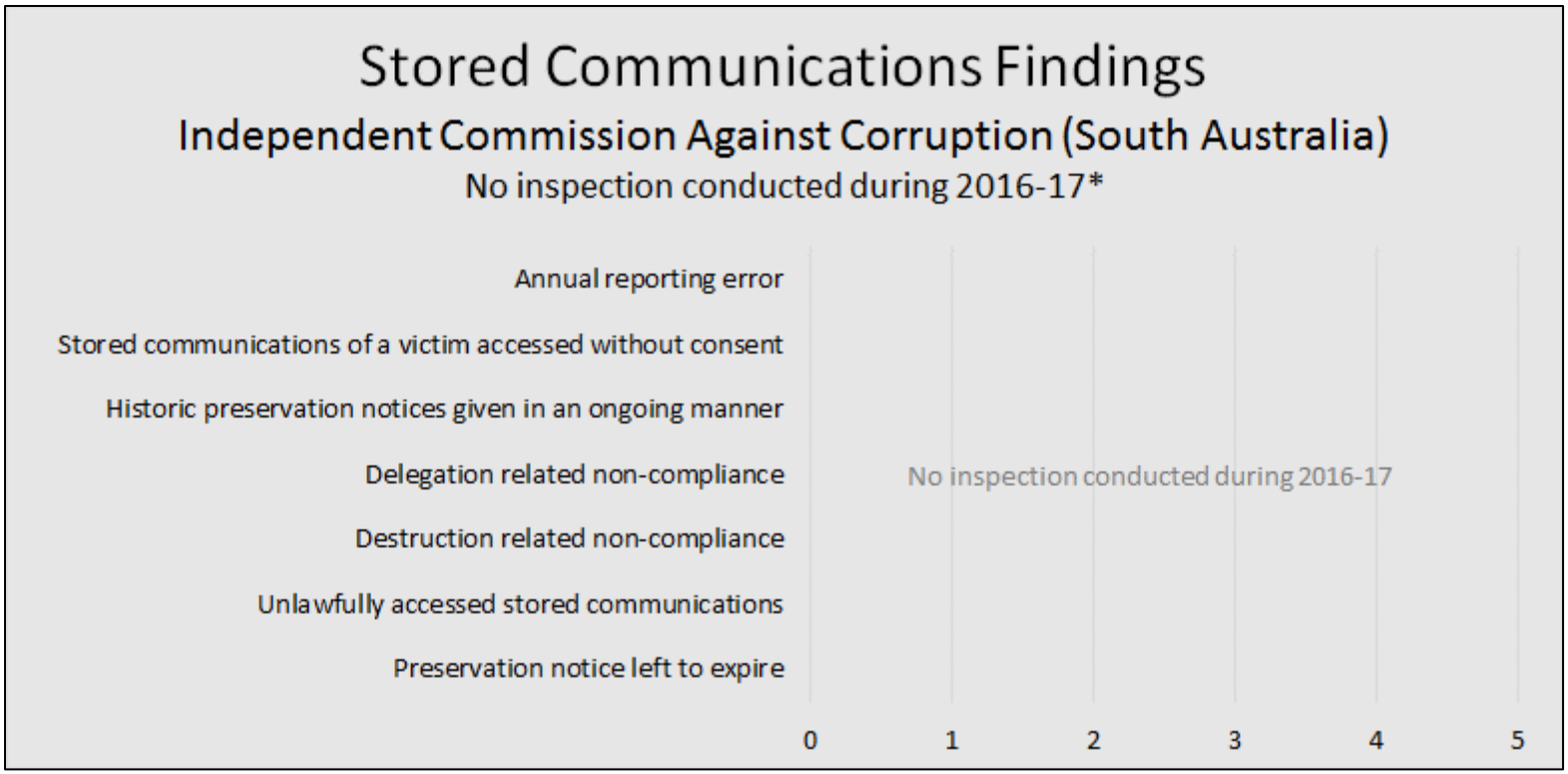

Stored Communications Findings
Northern Territory Police
Instances identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
19
Total warrants inspected:
13
Total preservation notices inspected:
69
0
10
20
30
40
50
60
70



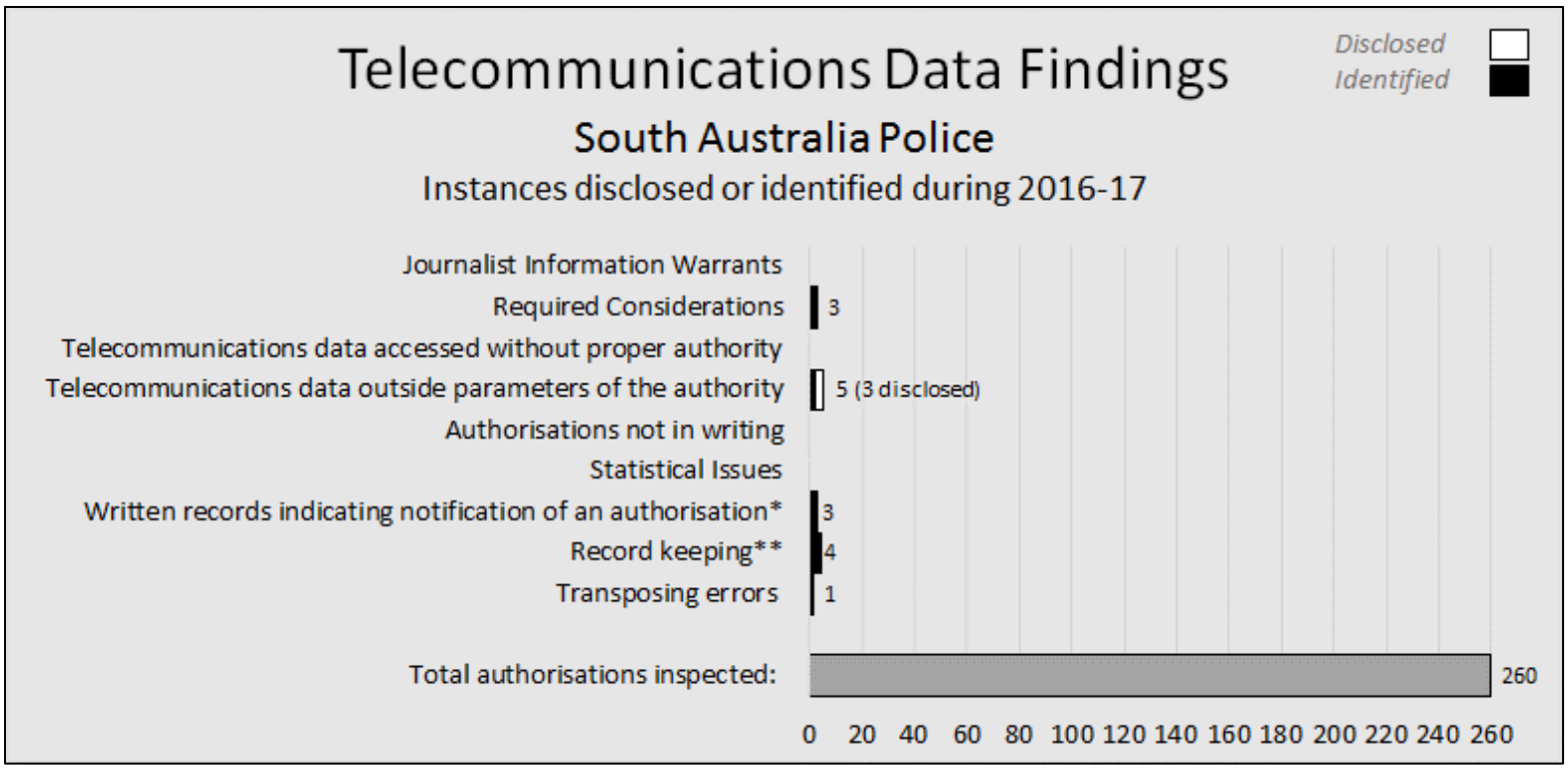

*In each instance where an authorisation was notified to the relevant carrier by fax, there was nothing to indicate the exact moment notification of the authorisation occurred. In these instances, this record keeping issue did not cause any ambiguity in determining whether obtained telecommunications data was within the parameters of the authorisation; however QLD Police has since amended its processes to ensure a written record of notification is kept.


Stored Communications Findings
Queensland Police Service
Instances identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
1
8
1
4
60
73
0
10
20
30
40
50
60
70


Telecommunications Data Findings
Independent Commission Against Corruption (South Australia)
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
1
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
2
Record keeping
Transposing errors
Total authorisations inspected:
41
0
10
20
30
40
50

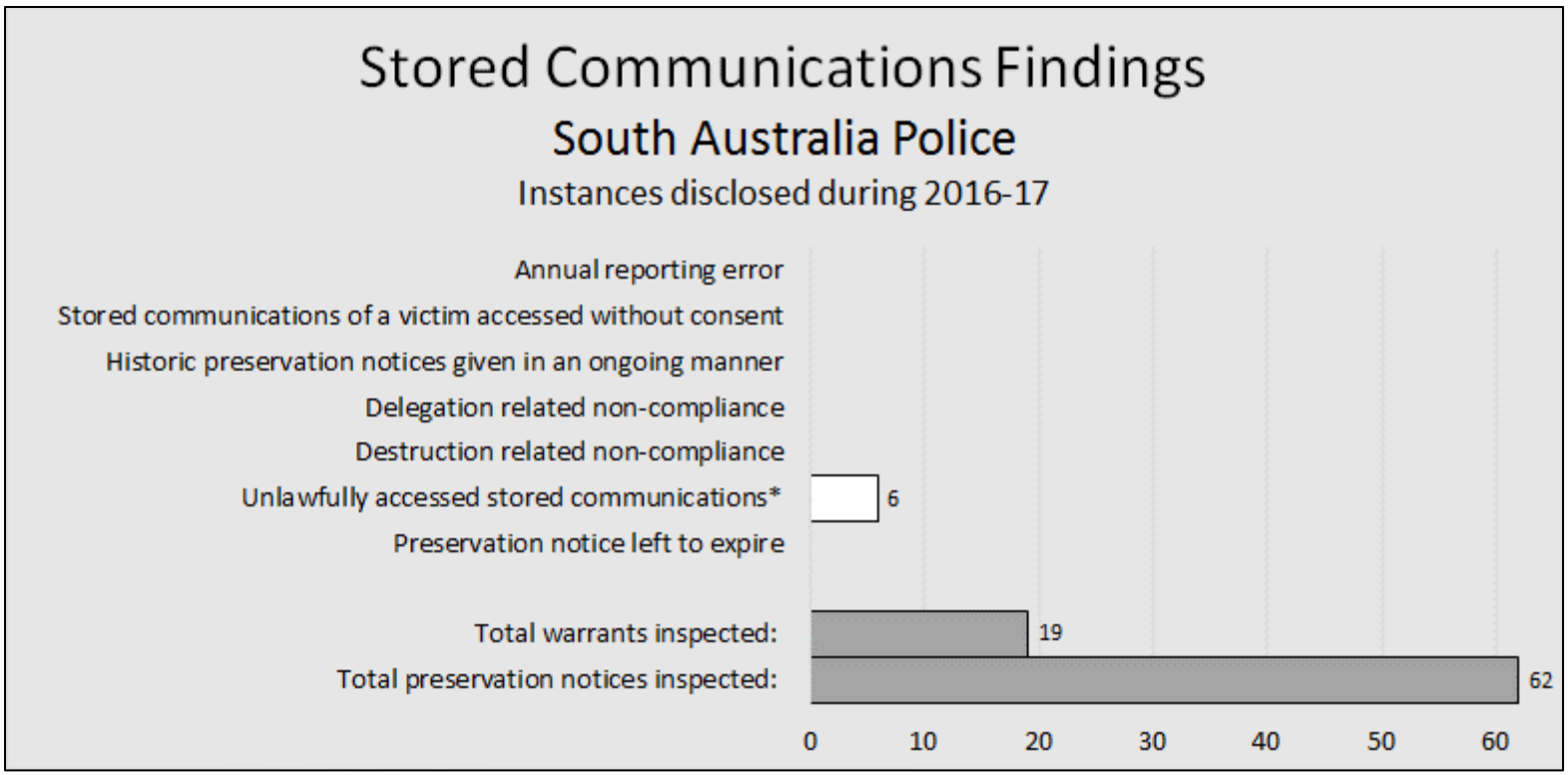



* Our Office did not conduct a stored communications inspection of ICAC (SA) during 2016-17, due to ICAC (SA) erroneously advising it had not given any preservation notices in the relevant period. When ICAC (SA) identified this error it advised our Office of these preservation notices and they were subsequently inspected during our 2017-18 inspection. Therefore, the results of our assessment of these records will be reported in our annual report covering inspections conducted during 2017-18.

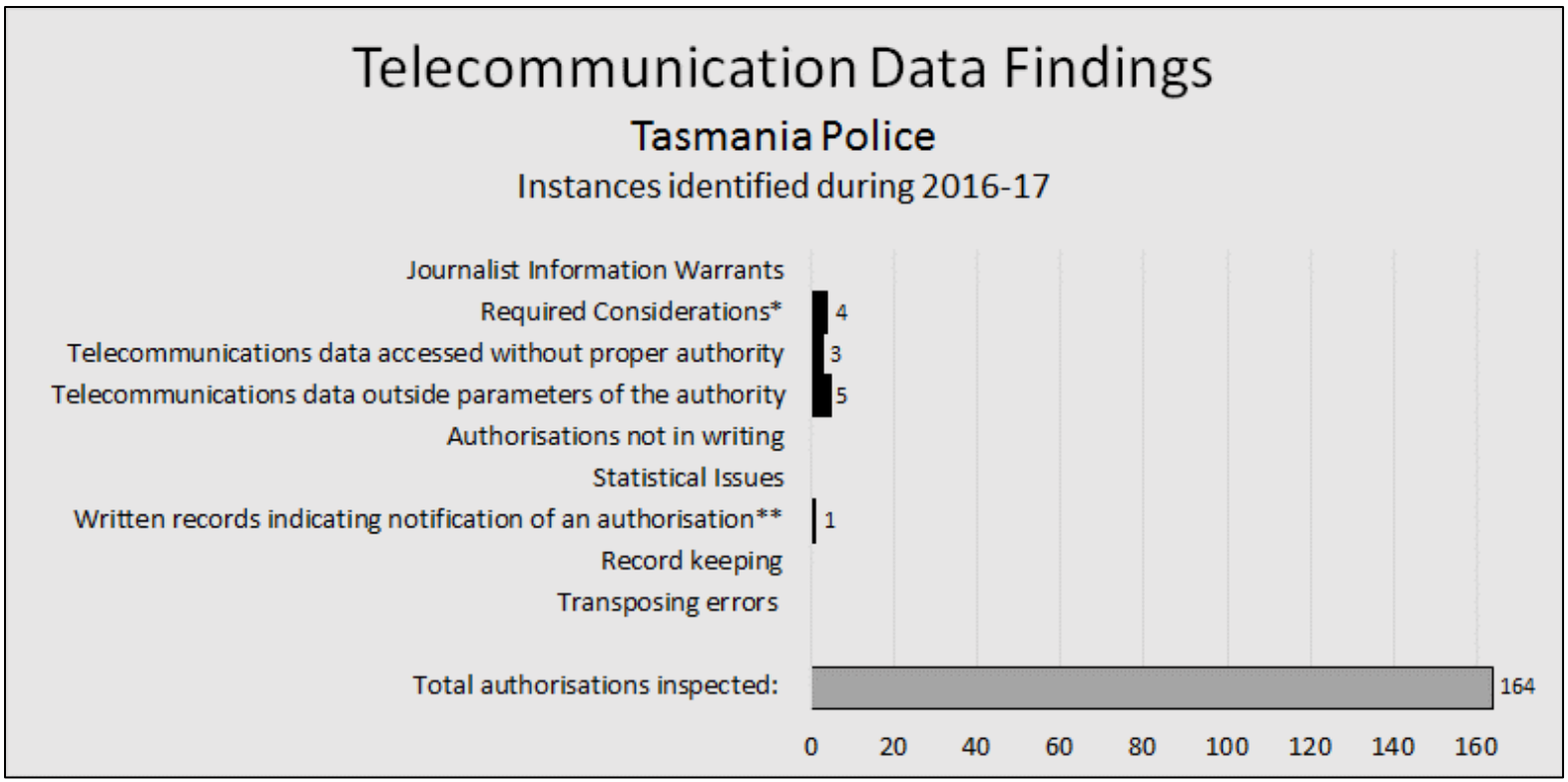



*This included all notifications, except one, in a specific area of SA Police. None of these instances resulted in ambiguity in determining whether the obtained telecommunications data was within the parameters of the authorisations; however SA Police has since amended its processes to ensure a written record of notification is kept.

**At the time of inspection, one specific area of SA Police was not retaining the telecommunications data obtained from the IPND as a matter of course. As a result, we were unable to assess this telecommunications data to ensure it was within the parameters of the authorisation. That being said, based on our understanding of the processes and procedures of this area, we were satisfied it was able to account for whether, and how telecommunications data was used and/or disclosed in accordance with s 186A(1)(g).

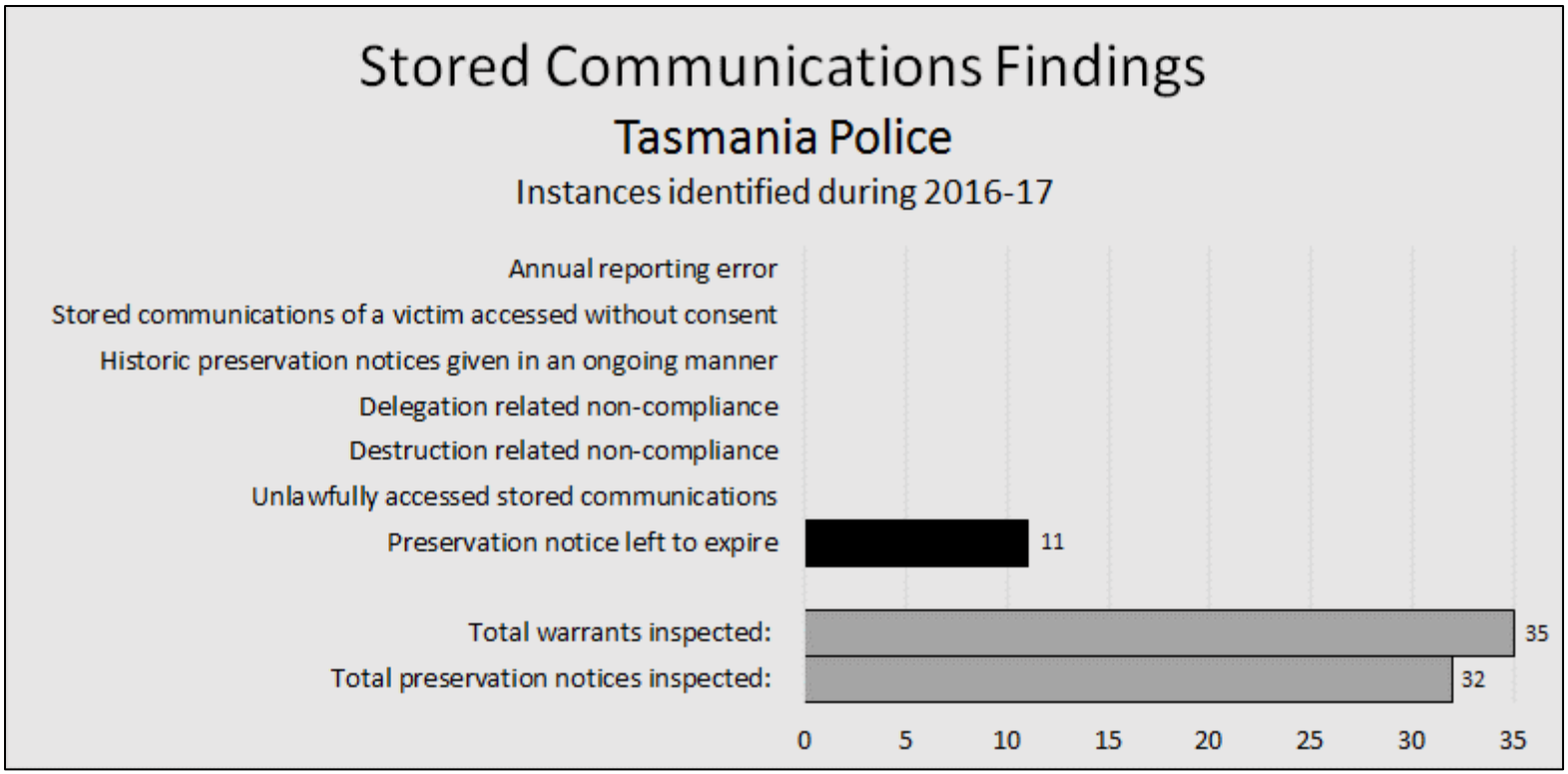


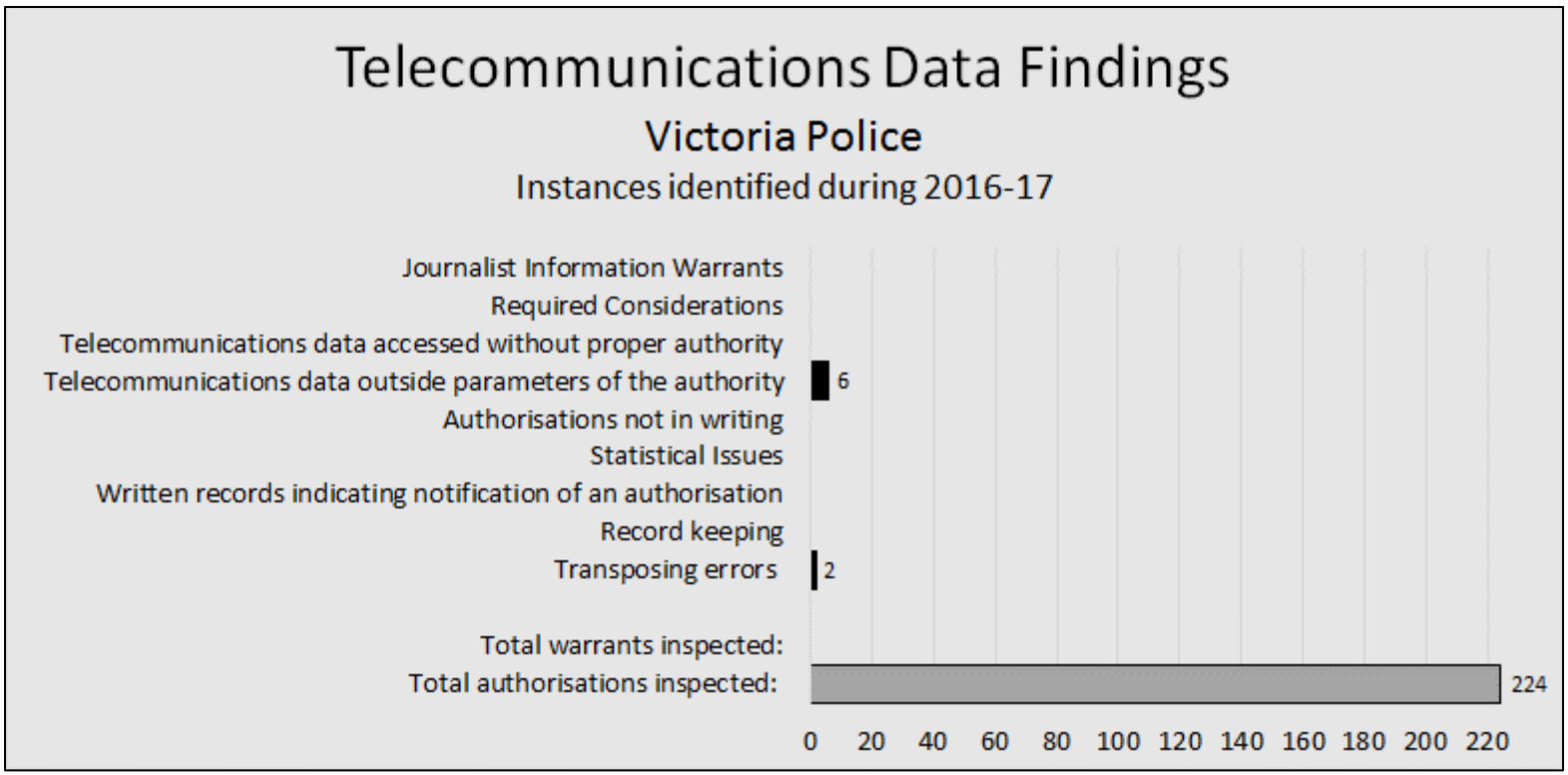

*In three of these instances, we were satisfied the agency's processes worked effectively to screen, identify and quarantine the unlawfully accessed stored communications received, prior to it being disseminated to investigators.

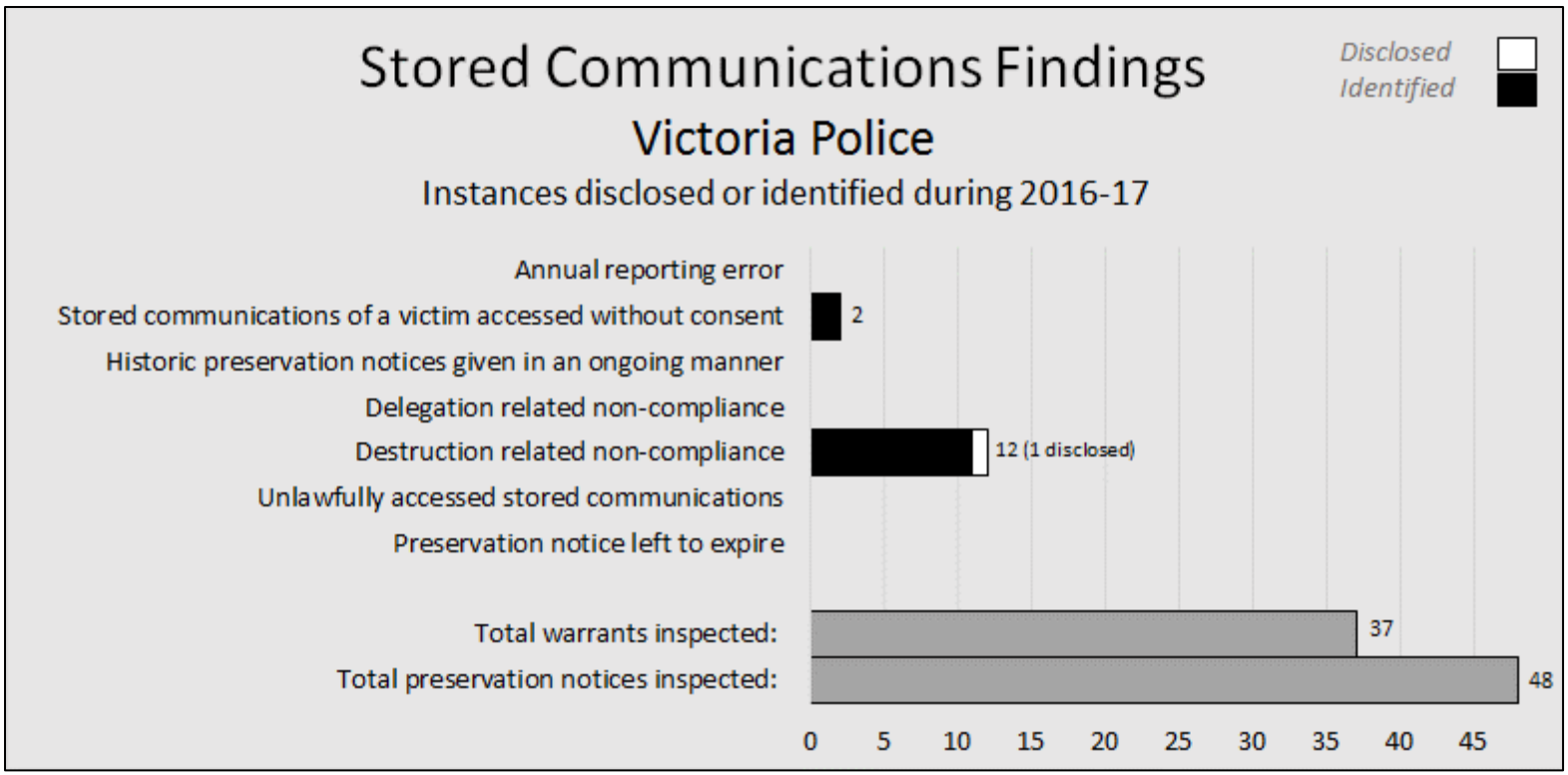


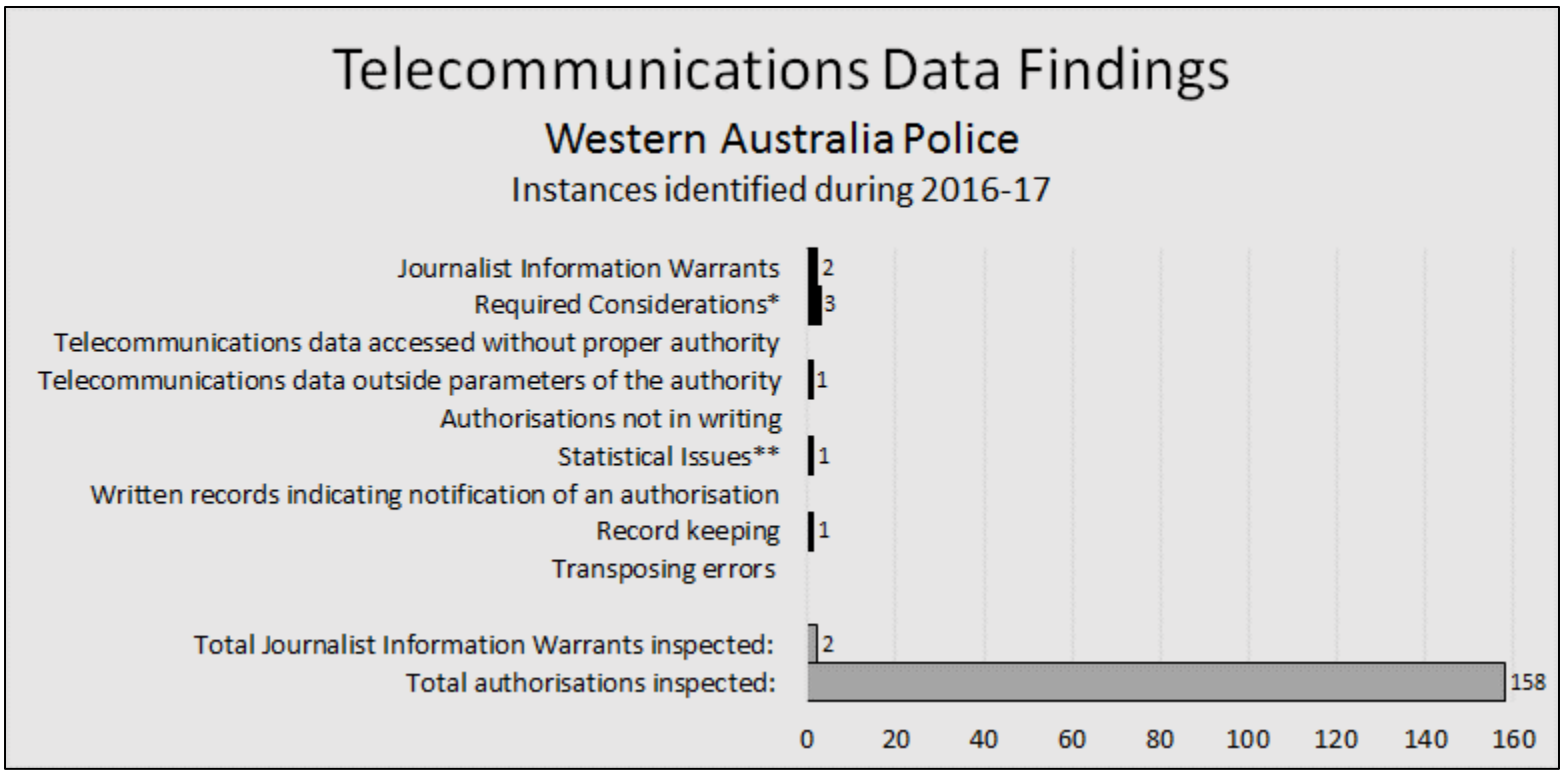

*In relation to authorisations for access to the IPND, TAS Police was unable to demonstrate that authorised officers had been satisfied of the required considerations. Following the inspection, TAS Police advised it had reinforced to authorised officers the requirement to make the necessary privacy considerations prior to authorisation.

**In each instance where an authorisation was notified to the relevant carrier by fax, there was nothing to indicate the exact moment notification of the authorisation occurred. These instances did not cause any ambiguity in determining whether the obtained telecommunications data was within the parameters of the authorisation; however TAS Police has since amended its processes to ensure a written record of notification is kept.


Stored Communications Findings
Tasmania Police
Instances identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
11
Total warrants inspected:
35
Total preservation notices inspected:
32
0
5
10
15
20
25
30
35

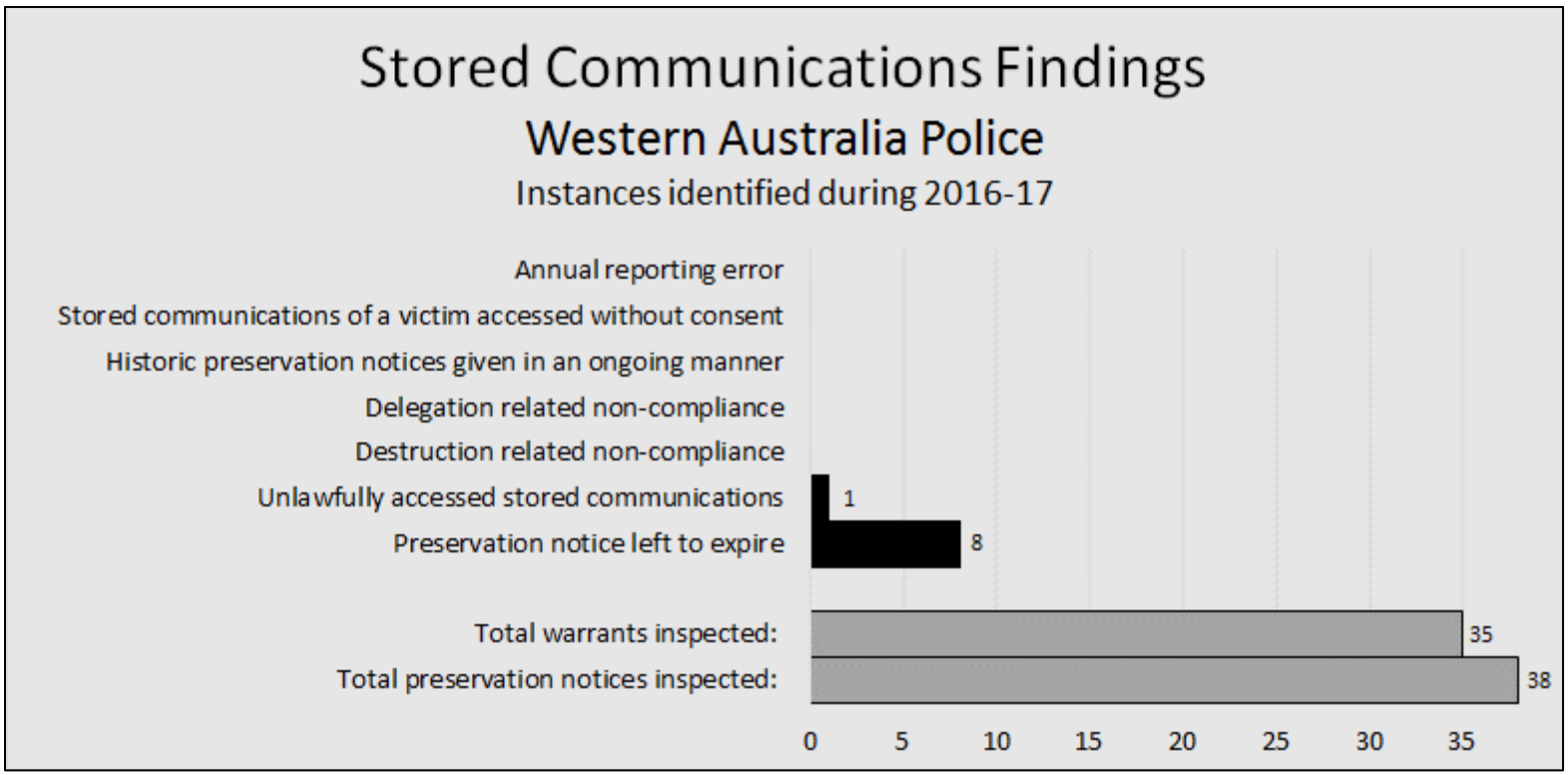

Telecommunications Data Findings
Victoria Police
Instances identified during 2016-17
Journalist Information Warrants
Required Considerations
Telecommunications data accessed without proper authority
Telecommunications data outside parameters of the authority
Authorisations not in writing
Statistical Issues
Written records indicating notification of an authorisation
Record keeping
Transposing errors
Total warrants inspected:
Total authorisations inspected:
6
2
224
0 20 40 60 80 100 120 140 160 180 200 220


Stored Communications Findings
Victoria Police
Instances disclosed or identified during 2016-17
Disclosed
Identified
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
2
12 (1 disclosed)
37
48
0
5
10
15
20
25
30
35
40
45




*Based on our understanding of its processes at the time of the inspection, a specific area of WA Police was unable to demonstrate that authorised officers had been satisfied of the required considerations. WA Police has since amended its processes and addressed this issue.

**Due to the limitations of its existing systems, the statistics provided to our Office in respect of one specific area of WA Police accurately reflected the number of historic authorisation made by WA Police during the inspection period. WA Police has since amended its processes and addressed this issue.


Stored Communications Findings
Western Australia Police
Instances identified during 2016-17
Annual reporting error
Stored communications of a victim accessed without consent
Historic preservation notices given in an ongoing manner
Delegation related non-compliance
Destruction related non-compliance
Unlawfully accessed stored communications
Preservation notice left to expire
Total warrants inspected:
Total preservation notices inspected:
1
8
35
38
0
5
10
15
20
25
30
35

# Appendix A—Telecommunications Data Inspection Criteria: 2016–17

**Inspection Objective:** To determine the extent of compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* by the agency and its officers

## 1. Is the agency only dealing with lawfully obtained telecommunications data?

### 1.1 Were authorisations for telecommunications data properly applied for, given and revoked?

*Process checks:*

- Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient?
- Does the agency have effective controls, guidance and/or training in place for authorised officers to ensure that authorisations are properly given?
- Does the agency have effective procedures in place to revoke prospective authorisations when required and notify carriers of any revocations?

*Record checks in the following areas:*

- Whether authorisations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f))
- Whether authorisations were made by officers authorised under s 5AB
- Whether authorisations were made in relation to specified information or documents (ss 178 to 180)
- Whether authorised officers have considered privacy in accordance with s 180F

*Specific to prospective authorisations*

- Whether prospective authorisations are in force only for a period permitted by s 180(6)
- Whether prospective authorisations were revoked in relevant circumstances (s 180(7))

**1.2 Did the agency identify any telecommunications data that was not within the parameters of the authorisation?**

*Process checks:*

- Does the agency have effective procedures in place to screen and quarantine telecommunications data obtained?

*Record checks in the following areas:*

- Whether telecommunications data obtained by the agency was within the parameters of the authorisation
- Whether the agency identified any telecommunications data (including content) that did not appear to have been lawfully disclosed, and if appropriate, sought clarification from the carrier and quarantined the data from use

**1.3 Were foreign authorisations properly applied for, given, extended and revoked? [AFP only]**

*Process checks:*

- Does the agency have effective procedures in place to ensure that foreign authorisations are properly applied for, given, extended and revoked, and are they sufficient?

*Record checks in the following areas:*

- Whether authorisations for telecommunications data on behalf of a foreign law enforcement agency were properly given and disclosed (ss 180A to 180E)
- Whether foreign prospective authorisations were properly revoked in accordance with s 180B(4)
- Whether extensions of foreign prospective authorisations were properly made in accordance with ss 180B(6) and (7)

## 2. Has the agency properly managed telecommunications data?

*Process checks:*

- Does the agency have secure storage facilities for telecommunications data and associated information?
- Does the agency have processes in place to account for the use and disclosure of telecommunications data?

*Record checks in the following areas:*

- **Spot Check:** Whether the use and disclosure of telecommunications data can be accounted for in accordance with s186A(1)(g)

## 3. Has the agency complied with Journalist Information Warrant provisions?

### 3.1 Did the agency properly apply for Journalist Information Warrants?

*Process checks:*

- Does the agency have effective procedures and controls in place to ensure that a Journalist Information Warrant is sought in every instance where one is required (s 180H)?
- Does the agency have effective procedures in place to ensure that Journalist Information Warrants are properly applied for and issued in the prescribed form?

*Record checks in the following areas:*

- Whether the application was made to a Part 4-1 issuing authority (s 180Q(1))
- Whether the application related to a particular person (s 180Q(1))
- Whether the application was made by a person listed under s 180Q(2)
- Whether the warrant was applied for a period permitted by s 180U(3) noting that no warrant extensions are permitted (s 180U(4))
- Whether the warrant was in the prescribed form and signed by the issuing authority (s 180U(1))

### 3.2 Did the agency notify the Ombudsman of any Journalist Information Warrants?

*Record checks in the following areas:*

- Whether the Ombudsman was given a copy of each warrant issued to the agency as soon as practicable (s 185D(5))
- Whether the Ombudsman was given a copy of each authorisation given under the authority of a Journalist Information Warrant, as soon as practicable after the expiry of that warrant (s 185D(6))

### 3.3 Did the agency revoke Journalist Information Warrants when required?

*Process checks:*

- Does the agency have effective procedures in place to review the continuous need for a Journalist Information Warrant?

*Record checks in the following areas:*

- Whether the warrant was revoked in the relevant circumstances (s 180W)
- Whether the revocation was in writing and signed by the chief officer or their delegate (s 180W)

## 4. Has the agency satisfied certain record keeping obligations?

*Process checks:*

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of authorisations made and journalist information warrants issued (s 186)?
- Does the agency have effective record keeping practices in place?

*Record checks in the following areas:*

- Whether the agency sent an annual report to the Minister on time, in accordance with s 186
- Whether the agency has kept records in accordance with s 186A

## 5. Was the agency cooperative and frank?

- Is there a culture of compliance?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose issues?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Ombudsman's Office, as necessary?

# Appendix B—Stored Communications Inspection Criteria: 2016–17

**Inspection Objective:** To determine the extent of compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* by the agency and its officers

## 1. Is the agency only dealing with lawfully accessed stored communications?

### 1.1 Were stored communications properly applied for?

*Process checks:*

- Does the agency have effective procedures in place to ensure that warrants are properly applied for and issued in the prescribed form (s 118(1))?

*Record checks in the following areas:*

- Whether applications for stored communications warrants were made in accordance with ss 110 to 113, or ss 111, 114 and 120(2) for telephone applications
- Whether the warrant was only in relation to one person (s 117)
- If the application relates to the same telecommunications service as a previous warrant – whether the application was made in accordance with s 119(5)
- Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service (s 117)

### 1.2 Was the authority of the warrant properly exercised?

*Process checks:*

- Does the agency have effective procedures and authorisations in place to ensure the authority of the warrant is properly exercised?

*Record checks in the following areas:*

- Whether the authority of the warrant was exercised in accordance with s 127

### 1.3 Did the agency screen stored communications and quarantine any that were unlawfully accessed?

*Process checks:*

- Does the agency have effective procedures in place to identify and quarantine accessed stored communications that are not authorised by the warrant?

*Record checks in the following areas:*

- Whether accessed stored communications were within the parameters of the warrant, including any conditions and restrictions (s 117)
- Whether stored communications provided to the agency had been accessed by the carrier(s) while the warrant was in force (s 119)
- Whether the agency identified stored communications that did not appear to have been lawfully accessed, and if appropriate, sought clarification from the carrier(s) and quarantined them from use (s 108)

## 2. Has the agency properly managed accessed stored communications?

### 2.1 Were stored communications properly received by the agency?

*Process checks:*

- Does the agency have effective procedures and authorisations in place to properly receive accessed stored communications in the first instance?
- Does the agency have secure storage facilities for accessed information?

*Record checks in the following areas:*

- Whether stored communications were received in accordance with s 135

### 2.2 Were stored communications properly dealt with and destroyed?

*Process checks:*

- Does the agency have procedures in place for the destruction of stored communications and the reporting of destruction activities?
- Does the agency have controls, guidance and/or training in place to ensure that stored communications are only dealt with for a permitted purpose (s 133)?
- Can the agency account for its use and communication of lawfully accessed information?

*Record checks in the following areas:*

- **Spot-check**: Whether the use, communication or recording of lawfully accessed information can be accounted for in accordance with ss 139 to 142A
- Whether accessed stored communications were destroyed in accordance with s 150

## 3. Has the agency properly applied the preservation notice provisions?

### 3.1 Did the agency properly apply for and give preservation notices?

*Process checks:*

- Does the agency have effective procedures in place for applying for and giving preservation notices?

*Record checks in the following areas:*

- Whether the agency was authorised to give the preservation notice (s 107J(1) or 107N(1))
- Whether the preservation notice only requested preservation for a permitted period (s 107H(1) or s 107N(1))
- Whether the preservation notice only related to one person and/or one or more services (s 107H(3) or s 107N(2))
- Whether the preservation notice was only issued after the relevant conditions had been met (s 107J(1))
- Whether the preservation notice was given by an authorised officer (s 107M or s 107S)

### 3.2 Did the agency revoke preservation notices when required?

*Process checks:*

- Does the agency have effective procedures in place for revoking preservation notices?

*Records checks in the following areas:*

- Whether the preservation notice was revoked in the relevant circumstances (s 107L or s 107R)
- Whether the preservation notice was revoked by an authorised officer (s 107M or s 107S)

## 4. Has the agency satisfied certain record keeping obligations?

*Process checks:*

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of preservation notices given and warrants issued (s 159)?
- Does the agency have effective record keeping practices in place?

*Record checks in the following areas:*

- Whether the agency has kept records in accordance with s 151

## 5. Was the agency cooperative and frank?

- Is there a culture of compliance?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose issues?
- Were issues identified at previous inspections addressed?