REPORT TO THE AUSTRALIAN BUREAU OF STATISTICS

REVIEW OF ABS SENSITIVE INFORMATION CONTROLS

BELINDA GIBSON

23 July 2014

1. BACKGROUND

1.1 The Australian Bureau of Statistics (ABS) has commissioned this review of the scheme of controls relating to unauthorised disclosure by ABS staff of market sensitive information held by ABS. The Review follows the ABS announcement of 9 May 2014 that a staff member had been arrested for a range of offences under the Criminal Code Act and Corporations Act relating to the alleged disclosure of sensitive statistics to a private individual whilst under embargo. It is the first time in the 109-year history of the ABS that an employee has been charged with offences in these circumstances.

1.2 The operative parts of the terms of the reference for the Review state:

> "The ABS holds a range of information that is potentially market sensitive. This includes information about particular companies that is not publically available and aggregate statistical information that has not been publicly released. A number of ABS employees have access to this information to enable them to perform legitimate business activities. However there is a risk that there may be unauthorised disclosure by individuals for financial or other personal gain.
>
> The review will assess the ABS system of controls relating to the unauthorised disclosure of market sensitive information. It will make recommendations on practical and proportionate means of enhancing the system of controls to improve the management of unauthorised disclosure risk that could be implemented by ABS.
>
> The review will assess all aspects of the system of controls, including policies, processes, education and awareness, culture and IT systems. However the review will not undertake detailed technical assessment of IT security systems, possible avenues of leakage of information held in the ABS, or a forensic review of data access by specific staff members.
>
> The review will consider Australian government best practices for handling sensitive financial information as well as the practices of national statistical offices in comparable countries."

1.3 In preparing this Review the author has been provided with copies of the ABS policies and materials that set out the restrictions on disclosure and misuse of information held by ABS. She has had the benefit of interviews with executives and ABS staff, and also confidential discussions with representatives of other Australian federal government agencies who might hold market sensitive information from time to time, and of national statistical offices in other countries. The author has also reviewed the published practices of companies in the private sector that must protect against the unauthorised release of their own market sensitive information.

1.4 The Review does not deal with the events leading to the charging of the ABS staff member. Those matters are in the hands of the Federal Police.

2. EXECUTIVE OVERVIEW

2.1 The ABS compiles a number of national economic reports (called Main Economic Indicator or MEIs) for release to the public at 11.30am. The currency, securities and some commodities markets commonly react to the information in some of the reports. It is fundamental to ABS's business reputation that information it holds will be kept confidential unless and until release is authorised, and that all staff who have access to it will act with the utmost integrity, and specifically not use it for personal gain.

2.2 ABS operates with a coherent scheme of controls to protect against the unauthorised public release of information by staff within ABS, and the misuse of that information by staff. The scheme of controls includes legislation proscribing certain conduct and imposing significant imprisonment terms, a strong culture and training program to protect information that the ABS holds, an extensive policy infrastructure designed to manage access, IT controls on access and a governance framework that considers threats to security such as a rogue trusted insider.

2.3 The Review looked at the schemes of control operating at a selection of comparable Australian government departments and agencies. The ABS scheme of controls is broadly in line with that of the other reviewed Australian government departments and agencies that produce market sensitive statements. It is also consistent with the practices of the national statistical agencies reviewed. Some of the Australian agencies apply more stringent rules to staff with access to highly sensitive data. A small number of overseas agencies also have specific values and ethics programs focused on misuse of information for personal gain.

2.4 The APS Code of Conduct requires public servants not to misuse information for personal gain. Insider trading would be an example of that, but the term would also encompass actions such as selling corporate information and personal information protected by privacy laws. For this reason the Review makes recommendations that focus on misuse of position for personal gain rather than just insider trading.

2.5 It is not possible to absolutely prevent any misuse of information by a trusted insider. A person intent on breaching those laws can usually find a way to do so and the key objective of an organization such as ABS is to do what is practicable and proportionate to minimize the access of individuals to the information, and also to deter misuse, to monitor for that and to punish the conduct if it is discovered.

2.6 The Review assesses the quality of the ABS scheme of controls at 2 levels.

- the first is the organisation's ability to confine the access to information of ABS staff to those who must have it to perform their work.
- the second is the activities taken to deter the misuse of information by trusted insiders who do have access. This is analysed under the headings of:
  - culture and training
  - disclosure of financial assets and dealings
  - monitoring and surveillance of IT access
  - staff vetting procedures.

2.7 The foundation of every ABS information access control is 'need to know'. Access is only granted to those who would be hindered in the performance of their duties without that access. The Review makes recommendations to enhance the access limitations, in terms of elevating the importance of applying the policies designed to restrict access as a priority of management and developing strategies to assist

management to do that. There should be an immediate review of all lists and the processes that are applied to maintain and audit those lists (see paragraph 4.1).

2.8 Every person the author interviewed spoke of the strong culture of ABS. ABS has a set of values for its staff that are set out in the Corporate Plan under the headings of professionalism, integrity, trust, access for all, relevance and service. It is however difficult to identify the current corporate activities that reinforce to ABS staff the values of integrity, in the sense of not misusing information. The Review makes recommendations on some organisation-wide activities to reinforce to staff the importance of not misusing confidential information, including the rules against insider trading and tipping (see paragraph 4.2).

2.9 The ABS has limited information from its staff about their financial assets and dealings, and does not impose any restrictions on trading, other than the obligation of all federal public servants to disclose potential conflicts and not misuse information for personal gain. The Review makes recommendations for ABS to consider requiring regular financial interest declarations from staff, or at least those with access to market sensitive data, restricting short term trading and introducing standard guidelines for disclosing and dealing with conflicts (see paragraph 4.3).

2.10 The ABS IT system has capacity to monitor specific databases for unathorised access and to audit the access by authorised persons to ensure usage is consistent with their job responsibilities. The Review makes recommendations for ABS to institute regular surveillance programs that utilize that capacity (see paragraph 4.4).

3. REPORT

Confidential market sensitive information

3.1 The ABS compiles a number of national economic reports (called Main Economic Indicators or MEIs) for release to the public at 11.30am. The currency, securities and some commodities markets commonly react to the information in some of the reports. The most significant reports in this regard are the Australian National Accounts, the Consumer Price Index and Labour Force Australia.

3.2 The MEIs are mainly prepared in separate divisions of ABS, called Subject Matter Areas (SMAs), supported by specialist units that provide specific statistical analyses and manage distribution of the final reports. All those team members will have access to some MEI data. A significant number of ABS employed IT administrators also have access to facilitate the statisticians' access. Approximately 230 people of the ABS staff of 2,600 are in the SMA divisions generating MEIs and there are a further 110 in the specialist service areas.

3.3 In compiling data to prepare the MEIs ABS will receive confidential information from survey respondents, including listed companies with continuous disclosure obligations to the Australian Securities Exchange. Legislation requires that it is provided to the ABS, and held confidential by it, though it is not yet published to the ASX. It is possible that on occasion this information will be market price sensitive though that seems to be rare. Accordingly this Review is primarily concerned with MEI data access.

Review methodology

3.4 It is not possible to absolutely prevent insider trading or tipping by a trusted insider. A person intent on breaching that law can usually find a way to do so and the key objective of an organization such as ABS is to do what is practicable and proportionate to minimize the access of individuals to the information, and also to deter misuse, to monitor for that and to punish the conduct if it is discovered.

3.5 The Review assesses the quality of the scheme of controls at 2 levels.

- the first is the organisation's ability to confine the access to information of ABS staff to those who must have it to perform their work.
- the second is the activities taken to deter the misuse of information by trusted insiders who do have access. This is analysed under the headings of:
  - culture and training
  - disclosure of financial assets and dealings
  - monitoring and surveillance of IT access
  - staff vetting procedures.

3.6 The APS Code of Conduct requires public servants not to misuse information for personal gain. That is repeated in the recent Public Governance and Performance Accountability legislation. Insider trading is an example of that, but the term would also encompass actions such as selling corporate information and personal information protected by privacy laws. For this reason the Review makes recommendations that refer to misuse of position rather than just insider trading.

ABS' scheme of controls

3.7 It is fundamental to ABS's business reputation that information it holds will be kept confidential unless and until release is authorised, and that all staff who have access to it will act with the utmost integrity, and not use it for personal gain. Confidentiality is a commitment to its data providers, to ensure their trust and continued willingness to be open. Releasing the market sensitive MEIs to everyone in the market at exactly the same time is a commitment to market integrity and a statement of professionalism to ABS' users.

3.8 ABS operates with a coherent scheme of controls to protect against the unauthorised public release of information, and the misuse of that information, by staff within ABS. The controls include:

- Legislation that imposes significant penalties, including imprisonment, for unlawful disclosure or misuse for personal gain of information provided to the ABS.
  - The Census and Statistics Act makes it an offence to divulge any information given to ABS under the Act, punishable by up to 2 years imprisonment.
  - The Public Service Act requires all Commonwealth public servants to abide by the APS Code of Conduct, one requirement of which is that an employee must not make improper use of inside information in order to gain or seek to gain a benefit or advantage for the employee or any other person. Breach is punishable by termination, job reassignment or financial penalty. The Public Governance Performance and Accountability Act makes the same stipulation.
  - The Crimes Act makes it an offence for a Commonwealth officer to communicate a fact which comes to his knowledge by virtue of his office to any person except one to whom he is authorised to communicate it, punishable by up to 2 years imprisonment.

- Legislation that imposes significant penalties, including imprisonment for up to 10 years, for insider trading, including tipping of material price sensitive information.

- An organisation-wide culture that places high value on being a professional organization that can be trusted by its information providers to maintain confidentiality. The desired culture is described in the ABS Corporate Plan.

- Policies and guidance to support the confidentiality obligations, including policies on the processing and release from embargo of MEIs and maintaining a clear desk and clear screen. Policies are founded on the principle of only giving access to those who need to know.

- Controls built into the various IT operating systems to restrict individuals' access to particular confidential data to those persons that are designated by the Subject Matter Area as needing access to the information for ABS' business.

- IT system capability to monitor specific databases for unathorised access and to audit the access by authorised persons to ensure usage is consistent with their job responsibilities. The system also records emails that issue from ABS.

- Induction training programs that introduce new employees to their responsibilities to maintain confidentiality of information, supported by e-training modules for ongoing employees. Employees are required to also sign secrecy and fidelity undertakings and acknowledgments when they first join ABS.

- A protective security policy and governance framework that monitors areas of threat to the security of the organisation, and oversees the introduction of controls to mitigate the threats to security, including technology-based solutions.

The scheme of controls also applies to contractors in ABS. ABS engages few contractors and has a policy that they are not allowed to have access to sentitive data. Nontheless ABS should formally check that the controls are operating at the point of engagement of contractors.

Benchmarks

3.9 The Review looked at the schemes of controls operating at a selection of comparable Australian government departments and agencies. The ABS scheme of controls to protect information is broadly in line with that of other Australian government departments and agencies issuing market sensitive statements, though some agencies apply more stringent rules to staff who have access to highly sensitive data.

3.10 The ABS scheme of controls is also consistent with its overseas national statistical agencies reviewed, though a small number of them also have specific values and ethics programs focused on misuse of information for personal gain.

Access restrictions

3.11 The foundation of every ABS information access control is 'need to know'. Access is only granted to those who would be hindered in the performance of their duties without that access. This principle is a constant theme in relevant policy documents, and underpins the rules relating to both electronic and on-site access.

3.12 The control of the number of people who have access to any set of numbers is made more complex with the centralising of common parts of the work program to specialised ABS units, such as Web Publishing and Dissemination. Methodology and Time Series Analysis are also specialist units. A significant number of IT administration managers also have access to administer facilities and databases, including enabling IT access for the statisticians. These units are managed separately from the Subject Matter Areas, and are in physically diverse locations. This feature complicates oversight, though is more efficient in terms of preparation of reports.

3.13 There has been a trend to expand access rights to ensure backup support for completing a task. The ABS' culture of building knowledge capability has also meant involvement of more people in particular sets of confidential information. Access entitlements for staff who move out of an SMA to another unit must be manually changed, as a separate process from adjusting the human resources records. There has been varying rigour in effecting these changes as people move about the organisation, exacerbated by system complexities.

3.14 A number of the ABS staff interviewed for the Review commented that they see scope to update and refine their access control lists. ABS does periodically initiate organization-wide access audit exercises but there has not been one run for some time. The author understands that some ABS MEI units have recently started a review exercise.

3.15 In keeping with modern office design principles ABS has moved away from allocated offices to an open plan environment. There are no physical barriers to entry, such as password protected doors, to an area handling a particular MEI release. This is consistent with other agencies. In some respects an open-plan environment hinders a passerby stealing information on a desk or screen, so long as those authorised to be in the restricted area are aware of who is authorised to see information and are prepared, and tasked, to challenge outsiders.

3.16 The ABS' IT environment is aged in an infrastructure sense, and a composite of a number of data warehouses and work environments. There are plans to modernize the various platforms, but these require significant new funding grants. The Technology Services Division has management of external access and intrusion into the ABS system, and that is not the subject of this Review. Within the ABS environment the relevant Subject Matter Area director is accountable for managing all ABS' staff access when compiling their particular MEI. He or she is not able to readily determine at any single point of time which ABS staff have access through the IT system portals to the sensitive information, and therefore determine with confidence that the need to know principle is fully observed at all places in ABS up to the point of formal release. The complexity of the system has probably discouraged directors from monitoring access regularly, and challenging the access granted to the specialist teams.

3.17 The Review **recommends** enhancing the access limitations. ABS should:

- conduct a close review of all IT access lists to ensure only necessary persons are included and make regular review of those lists an office-wide priority for management. ABS should also review the processes that are applied to maintain need to know (for example appointing data custodians in all divisions with standardized role responsibilities).

- reinforce the importance of enforcing the clear desks and clear screen policy and preventing unauthorised staff from physically entering specialist areas when there are information access restrictions in place.

- establish systems and procedures to enable ready determination by the relevant officers of all persons who have authority to view specified sensitive information at any point in time.

Deter misuse of information – culture and training

3.18 Every person the author interviewed spoke of the strong culture of ABS, generally in terms of protecting providers' confidential information. ABS has a set of values for its staff that are set out in the Corporate Plan under the headings professionalism, integrity, trust, access for all, relevance and service. All staff are also bound by the Australian Public Service values which include acting with integrity. The use of ABS' confidential information to trade for personal profit in the financial markets is unlawful and also inconsistent with those values and the Australian Public Service Code of Conduct, which is binding on all ABS employees by the Public Service Act and now the Public Governance Performance and Accountability Act.

3.19 It is however difficult to identify the current specific corporate activities that actively reinforce to ABS staff the values of integrity, in the sense of not misusing confidential information. ABS is a large organization of approximately 2600 staff spread over all capital cities of Australia. The need for confidentiality in an operational sense is included in relevant policies, and promoted in that context, however the corporate values are not prominent in current corporate messaging activities. A number of people volunteered that ABS perhaps takes the strong culture as a given, and that the events in May have come as a shock to the organisation's belief in the strength of its culture. None of those persons identified any practices that are inconsistent with the ABS values.

3.20 The staff training program is primarily an electronic offering and once a person has completed the induction program there is little mandatory training, which many organisations use as a vehicle to promote wider organizational values. Confidentiality is a part of a number of policy training programs, but a distinct confidentiality module has not been run across the whole organisation for some time.

3.21 On joining ABS staff must sign undertakings of secrecy and fidelity and acknowledge they are aware of the relevant laws requiring secrecy. Each year they must confirm electronically that they (relevantly) will adhere to the APS Code of Conduct in accessing the IT system. The statements are legalisitic in their terms, in the sense that they refer to legislation rather than prohibited conduct. There are no specific standards as to the nature of the explanations given to staff when the signatures are required. Securing the signature is part of the administrative process when joining into the ABS system, rather than part of a discussion with the person's manager about culture, values and ethics.

3.22 The importance of confidentiality is generally tied to provider information. The market sensitivity of information, whether generated internally in the production of MEIs or collected from providers, is not addressed in any corporate wide policy materials, though is implicit in the documents surrounding the release of MEIs. There is no specific ABS-wide training about the laws against insider trading, though some MEI business units have conducted that training in past years, and that has recently been reinstated. There is no specific ABS-wide training about the laws against misuse of information for personal gain.

3.23 Only one of ABS' peers in Australia and overseas that the author interviewed specifically focus on market sensitive information and the insider trading rules. Only a few have specific programs targeted at misuse of information for personal gain.

3.24 The Review **recommends** ABS undertake some corporate wide activities to deter insider trading based on ABS' confidential information:

- introduce training programs on misuse of information for personal gain, including illegal insider training and the onerous penalties that it attracts, available on-line and required to be repeated as part of the mandatory program of e-learning.

- revisit the secrecy and fidelity undertakings signed on joining ABS, and associated induction materials, to make clearer the prohibited conduct which staff undertake not to engage in, and include insider trading and tipping. Revisit the annual IT access electronic affirmation in the same manner.

- integrate the message that ABS may have market sensitive information and it is illegal to trade on that, or provide it to others, in ABS policies and other materials that address confidentiality.

3.25 The author suggest that ABS consider using the May event as a catalyst for an organization-wide awareness campaign about the importance of information retention and of not using it for personal gain, including trading in the financial markets.

Disclosure of personal financial assets and dealings

3.26 In recent years it has become easier for all people to access the financial markets for trading, and it is more likely that staff have both opportunity and interest in trading. It is also more likely that staff have direct ownership of financial assets.

3.27 The ABS has limited information about the personal financial situations of its staff. The most senior ABS staff provide the Australian Statistician with an annual declaration of their financial assets, but it is not a general requirement of all staff. There is no formal ABS policy regarding securities, commodities or currency trading, either in terms of prohibition or trading only with consent. There is no formal ABS policy stipulating declarations of conflicts of interest, beyond the general requirement to do so in the APS Code of Conduct.

3.28 Private financial organisations will (and in some cases are obliged to) require regular declarations of assets and trading from all staff, and place trading restrictions on staff who have access to market sensitive information. Some of ABS' peer organisations in Australia require annual asset disclosure statements from staff in areas where market sensitive information is held, irrespective of the seniority of the staff member, and restrict trading at certain times. It is not common practice for the overseas agencies the author interviewed to be so restrictive.

3.29 The main benefit of disclosure, accompanied by a trading prohibition, is to remove any perception of improper personal gain by staff. These types of requirements support the APS obligation to disclose conflicts, and enable a uniform approach to the requirement across all units in the organisation. It may well be that the fact staff are obliged to disclose financial assets and trading activities will act as a deterrent from illegal conduct. It will remind them that ABS is aware of the issue and monitoring for it. The availability to managers of information about which staff are active in the financial markets would act as a catalyst for discussions about the policies and may assist the managers in monitoring for illegal conduct in their business units.

3.30 The Review **recommends** that the ABS consider introducing some or all of:

- a requirement for staff (or at least those with access to market sensitive information) to provide declarations to their director about their financial assets when they join ABS and then annually to declare their financial assets and also dealings in them in the past year.

- a prohibition on all staff (or at least those with access to market sensitive information) from engaging in short-term trading in the financial markets. Short term trading needs to be defined, but the intent is to remove any perception that a person could benefit from any information gained at ABS.

- rules or guidance to deal with staff disclosing potential conflicts of interest and not trading at a time when they may have confidential information which may be market sensitive. This would apply in the MEI groups but could also apply in groups where survey information contains company specific confidential information. Those rules might include requiring a consent to trade for specific stocks in limited circumstances. The author does not believe an ABS-wide consent requirement is practicable or proportionate.

3.31 ABS may wish to consider refreshing the undertakings of fidelity and secrecy annually as part of the declaration of financial assets and dealings.

Monitoring and surveillance of IT access

3.32 The ABS IT infrastructure is complex, and data can be located in a number of warehouses at one time as it is processed. In recent years ABS has initiated a number of projects to improve access restrictions to the various databases, to consolidate the logging and monitoring information across all databases, and to control the exit of information from ABS through the IT system. Those projects are at various stages of implementation, and some require significant funding before they can be completed. The author is not briefed to review these programs.

3.33 Even without these enhancements ABS has the capacity to monitor access to specific databases. It also has the capacity to audit the trail of individuals through the databases during the course of a day, whether they have authority to be viewing that data or not. The system capacity has not been applied to test unauthorised access as part of standard operating procedure, though will be used when an event occurs that prompts inquiry.

3.34 ABS retains all emails sent out of the business, and can identify sender and content. The information collected from email records and the data loss protection system can be used for post-incident analysis and investigations.

3.35 The Review **recommends** that ABS implement surveillance programs to:

- monitor for and also audit retrospectively the access of unauthorised ABS staff to market sensitive data.

- audit the access to market sensitive information by authorised staff, to ensure that the access is consistent with their job responsibilities and not for some other purpose.

Staff vetting procedures

3.36 The ABS conducts security checks for some senior staff in accordance with Australian government requirements. Those checks will include criminal history and financial background information. ABS also researches the backgrounds of less senior recruits beyond their academic achievements, to assess capability and aptitude for the position.

3.37 There is no single test that can detect likely insider traders in advance. There is no standard profile for an insider trader. The formal security reviews conducted for senior staff are not designed specifically to identify in advance persons who might have a propensity to misuse confidential information for trading. In the author's opinion extending the formal security vetting to cover all potential recruits for the purpose of identifying potential insider traders would not be a cost effective step for ABS.

3.38 Nevertheless recruiters should be reminded to bear in mind that a candidate will have a trusted position of access to market data when assessing capability and aptitude for the position and there may be scope to obtain more targeted information that would assist in the assessment process.

4 RECOMMENDATIONS

4.1 Access to information

ABS should:

- conduct a close review of all IT access lists to ensure only necessary persons are included and make regular review of those lists an office-wide priority for management. ABS should also review the processes that are applied to maintain need to know (for example appointing data custodians in all divisions with standardized role responsibilities).
- reinforce the importance of enforcing the clear desks and clear screen policy and preventing unauthorised staff from physically entering specialist areas when there are information access restrictions in place.
- establish systems and procedures to enable ready determination by the relevant officers of all persons who have authority to view specified sensitive information at any point in time.

4.2 Culture and training

ABS should undertake some corporate wide activities to deter insider trading based on ABS' confidential information:

- introduce training programs on misuse of information for personal gain, including illegal insider training and the onerous penalties that it attracts, available on-line and required to be repeated as part of the mandatory program of e-learning.
- revisit the secrecy and fidelity undertakings signed on joining ABS, and associated induction materials, to make clearer the prohibited conduct which staff undertake not to engage in, and include insider trading and tipping. Revisit the annual IT access electronic affirmation in the same manner.
- integrate the message that ABS may have market sensitive information and it is illegal to trade on that, or provide it to others, in ABS policies and other materials that address confidentiality.

4.3 Financial declarations

ABS should consider introducing some or all of:

- a requirement for staff (or at least those with access to market sensitive information) to provide declarations about their financial assets before they join ABS and then annually to declare their financial assets and also dealings in them in the past year.
- a prohibition on all staff (or at least those with access to market sensitive information) from engaging in short-term trading in the financial markets.
- rules or guidance to deal with staff disclosing potential conflicts of interest and not trading at a time when they may have confidential information which may be market sensitive.

4.4 IT monitoring and surveillance

ABS implement surveillance programs to:

- monitor for and also audit retrospectively the access of unauthorised ABS staff to market sensitive data.
- audit the access to material sensitive information by authorised staff, to ensure that the access is consistent with their job responsibilities and not for some other purpose.

5 ASSUMPTIONS AND LIMITATIONS

The author assumes that all information provided to her by ABS staff is accurate and complete, and that the persons she interviewed in preparing the report were the most appropriate.

The author has not tested the operation of the controls on access to information within ABS and relies on the advice from ABS staff interviews in that regard.

The author has not reviewed the various IT strategies that ABS is developing to enhance the controls on access to information. These are the subject of separate review by the Protective Security Management Committee.

The author has not tested the application of the need to know principle to specific situations and makes no comment on whether more persons have access to information than is necessary under that principle.

The question of access by outsiders to ABS systems is outside the terms of reference for this Report.

6. QUALIFICATIONS

Belinda Gibson is a company director, business adviser and solicitor.

She was a partner of the international law firm Mallesons Stephen Jaques for 20 years to 2007, specialising in corporate law, securities transactions and corporate governance issues, including staff share trading policies.

From 2007 to 2013 she was a commissioner and then deputy chairman of the Australian Securities and Investments Commission, with primary responsibility for the capital markets. She led ASIC's initiatives to prosecute insider trading, and to promote the actions companies should take to control their own information.