Document 3

[redacted]

From: [redacted]
Sent: Thursday, 17 November 2011 4:17 PM
To: [redacted]

Subject: s33(a)(i) + s47E(d) → [redacted] Security Discussion minutes [SEC=UNCLASSIFIED]
Attachments: [redacted].doc; [redacted].jpg; [redacted].JPG

Security Classification: UNCLASSIFIED

s 33(a)(i) + 47E(d)

Hi [redacted],

Attached are the meeting minutes of the [redacted] Security discussion that was held yesterday, so that we are all on the same page.

In the meeting minutes I have also included emailed responses to selected dot points for those invitees which could not attend.

Regards,

[redacted]

Position details removed
s. 33(a)(i) + 47E(d)

Australian Government
Bureau of Meteorology

[redacted]
Information Technologies Branch,
Bureau of Meteorology,
Melbourne, Australia.

Email: [redacted]
Phone: [redacted]
Fax: [redacted]
Web: www.bom.gov.au

s33(a)(i)+s.47E(d)

s33(a)(i)+ s.47E(d)

Document 3A

[redacted] Security Discussion/Meeting - Integrity of [redacted] – Meeting Minutes:

Date: 15-11-11

Bureau Attendees: [redacted]

Apologies: [redacted]

Where are we at with security on [redacted]?

S33(a)(i) & S47E(d)

- All [redacted] for all of the [redacted] have been checked for [redacted] **S33(a)(i) & S47E(d)** **S33(a)(i) & S47E(d)** **S33(a)(i) & S47E(d)** **S33(a)(i) & S47E(d)** have also been checked. No further evidence of a compromise to the [redacted] has so far been uncovered.

s33(a)(i) + s47E(d)

S33(a)(i) & S47E(d)

- **S33(a)(i) & S47E(d)** no evidence of unusual activity has been detected on the [redacted] have been similarly audited and do not appear to have been compromised. All media [redacted] used to provision and maintain systems on [redacted] have been audited and no exceptions have been detected.

2.
3. **Out of Scope - Remediation S22**
4.
5.

s33(a)(i)+ s47E(d)

6. The Bureau's [redacted] have been checked for security breaches; none were found.
7. **S33(a)(i) & S47E(d)** systems have been checked for intrusions, with none found.
8.
9. **Out of Scope - Remediation - S22**

Out of Scope - Remediation S22

Pages 2&3 - S22 - Out of Scope - Remediation

[redacted]

From: [redacted]
Sent: Tuesday, 8 November 2011 12:20 PM
To: [redacted]
Cc: [redacted]
Subject: Re: [redacted] Security checks [SEC=UNCLASSIFIED]

Security Classification: UNCLASSIFIED

↑ s47E(d); s33(a)(i).

Hi [redacted]
To best answer your queries:

Can we ascertain when [redacted S33(a)(i) & S47E(d)]
We have [redacted S33(a)(i) & S47E(d)]
[redacted S33(a)(i) & S47E(d)]
[redacted] has completed an audit of the [redacted S33(a)(i) & S47E(d)]
[redacted] and has not found any other instances of [redacted S33(a)(i) & S47E(d)]
[redacted S33(a)(i) & S47E(d)] A first audit of the [redacted S33(a)(i) & S47E(d)] has also been completed for the same purpose and has so far uncovered nothing else untoward.

s33(a)(i) + s47E(d)

Have we found any sign of how we were compromised yet?
It would appear that the users accessed [redacted S33(a)(i) & S47E(d)]
[redacted S33(a)(i) & S47E(d)] This is yet to be 100% verified but [redacted]
[redacted S33(a)(i) & S47E(d)] strongly suggest this as the method of access. [redacted] is still working to confirm this and to identify whether or not any other access method was used.
Note: [redacted S33(a)(i) & S47E(d)]
[redacted S33(a)(i) & S47E(d)]

Additional:

All Remaining Content - S22 - Out of Scope - Remediation

[redacted]

Document 9

From: [redacted]
Sent: Wednesday, 16 November 2011 08:54 AM
To: [redacted]
Cc: [redacted]

Subject: Re: Updated: [redacted] Security Discussion [SEC=UNCLASSIFIED]

↑ s47E(d) ; s33(a)(i)

s33(a)(i) + s47E(d)

've compiled some additional notes to supplement the information already distributed by [redacted]:

All [redacted] for all of the [redacted] have been checked for [redacted] S33(a)(i) & S47E(d) [redacted]. The [redacted] have also been checked. No further evidence of a compromise to the [redacted] has so far been uncovered.

[redacted] S33(a)(i) & S47E(d) [redacted], no evidence of unusual activity has been detected on the [redacted]

The [redacted] have been similarly audited and do not appear to have been compromised. All media (e.g. [redacted] used to provision and maintain systems on [redacted] have been audited and no exceptions have been detected.

s47E(d) s33(a)(i)

S22 - Out of Scope - Remediation

The intrusion is most likely to have originated over [redacted] S33(a)(i) & S47E(d) [redacted]

All Remaining Content - S22 - Out of Scope - Remediation

[redacted]

From: [redacted]
Sent: Friday, 4 November 2011 02:13 PM
To: [redacted]
Cc: [redacted]
Subject: Security: Things to Look For

[redacted],

We have found specific S33(a)(i) & S47E(d) . They were discovered by running a S33(a)(i) & S47E(d) [redacted]

S33(a)(i) & S47E(d) [redacted]

S22 - Out of Scope - Remediation

-

e

S33(a)(i) & S47E(d) [redacted]