Matt Cahill

From: Matt Cahill
Sent: Friday, 25 October 2019 3:22 PM
To: Tim Roy
Cc: Rob Heferen; Paula Goodwin
Subject: RE: Request [SEC=OFFICIAL:Sensitive]

Tim

I do not currently have definitive answers to all of the below.

I can confirm that after analysis of our security logs and that of our Internet Gateway provider, an individual in the minster's office accessed the City of Sydney website between 17:06 and 17:16 on Monday, 9 September

Regards
Matt

Matt Cahill
Deputy Secretary
Strategy and Operations Group
Department of the Environment and Energy
GPO Box 787 Canberra ACT 2601
Tel: 02 6274 1114

From: Matt Cahill
Sent: Friday, 25 October 2019 9:08 AM
To: Tim Roy <tim.roy@energy.gov.au>
Cc: Rob Heferen <Rob.Heferen@environment.gov.au>
Subject: RE: Request [SEC=OFFICIAL:Sensitive]

Tim

As discussed, I have tasked the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to action this immediately. I will also keep the Chief Operating Officer, who fulfils the role of Chief Security Officer, informed.

The CIO, CISO and the key experts will need to access the accounts of all those concerned. I assure you that they all hold NV1 clearance. Appreciate that the search engine will access areas containing material normally considered as parliamentary privileged. We will take all efforts to avoid any individual access to unrelated documents.

We will advise you on timeframes shortly.

Regards
Matt

Matt Cahill
Deputy Secretary
Strategy and Operations Group
Department of the Environment and Energy
GPO Box 787 Canberra ACT 2601
Tel: 02 6274 1114

From: Tim Roy
Sent: Friday, 25 October 2019 8:14 AM

To: Matt Cahill <Matt.Cahill@environment.gov.au>
Subject: Request [SEC=OFFICIAL:Sensitive]

Hi Matt,

Grateful for your assistance in providing confirmation of activity conducted on departmental IT systems within the Minister's office as per the below.

Time period: likely activity between 5–9 September (inclusive); full window 22 August – 29 September (inclusive)
Relevant website: https://www.cityofsydney.nsw.gov.au
Relevant documents: Statutory Returns Annual Report 2017/18 (pdf and word versions)

The purpose of this request is to confirm the following matters:

- the exact time/s and date/s of any documents accessed by the MO on the cityofsydney website
- any available information for any accessed or downloaded documents from the cityofsydney website during this time, including metadata and content
- any available records relating to printing of documents (or pages of documents) by the MO from the cityofsydney website during this time

Consistent with usual practice, if information becomes available to the Department in the course of these checks that identifies activity that contravenes any relevant Codes of Conduct or IT User Agreements, I would obviously expect the Department to fully comply with its reporting obligations.

Many thanks in advance,
Tim

Tim Roy | Chief of Staff

Office of the Hon Angus Taylor MP
Minister for Energy and Emissions Reduction | Member for Hume
Parliament House CANBERRA ACT 2600

T. +61 2 6277 7120 | M. s. 47F(1)

s. 47F(1)

From: Matt Cahill
Sent: Wednesday, 30 October 2019 5:17 PM
To: Tim Roy
Cc: Rob Heferen; Paula Goodwin
Subject: RE: Request [SEC=OFFICIAL:Sensitive]

Tim

Please find below the answers to three questions you asked the Department on Friday 25 October at 8:14am for the period specified.

Q1 The exact time/s and date/s of any documents accessed by the MO on the cityofsydney website

- What we have established is that www.cityofsydney.nsw.gov.au was accessed by a single IT account in Minister Taylor's office, 9 September between 17:06 and 17:16. The account is assigned to s. 47F(1) .
- We are not able to confirm what individual pages or files were accessed.

Background: The searches conducted were based on information from all IT accounts associated with Minister Taylor's office, the web access logs provided by Splunk, our security incident and event management (SIEM) and our internet provider. The review was conducted from three perspectives, including a review of internet history to determine who accessed the site, a review of browser history and a review of the relevant user account.

- The account logs from our security incident and event management (SIEM) and our internet gateway provider do not provide the information about what individual files were accessed, as the connections are encrypted.
- No meaningful information could be identified through the workstation history due to gaps. The gaps could be as a result of cache automatically being cleared after 30 days.
- Further, the browser history for 6 to 28 September 2019 is absent. There is also an absence of print log history for the local printer that aligns with this period. The correlation of the dates where both browser history and local print log history is unavailable is consistent with the user's desktop having performance issues. A combination of outages which occurred across that period and the user's computer shutdown practices may have contributed.
- While it is possible for a browser history to be cleared by an individual, print log can only be cleared by an administrator. Logs of such administrator actions would be retained and there is no log of activity occurring.

Q2: Any available information for any accessed or downloaded documents from the cityofsydney website during this time, including metadata and content.

- The review has not identified any documents from the website within the parameters you provided.
- We are unable to establish any documents being downloaded from www.cityofsydney.nsw.gov.au website or locate any documents or metadata matching the parameters specified.

Background: The searches conducted were based on information from all home drives, the ministerial share drive folders, emails, Microsoft Office365 OneDrive and related file back-ups associated with the IT accounts for minister Taylor's office for the period specified.

***Q3:* Any available records relating to printing of documents (or pages of documents) by the MO from the *cityofsydney* website during this time.**

- The corporate and local printer logs do not contain any document that clearly identify title words that correlate to the City of Sydney website or the annual report.

Background: The departmental systems only record the title of the document printed and general information such as pages printed. Copies of printed or scanned documents are not automatically retained so it is not possible to determine if a document was printed under a temporary or different name. Note there is an absence of printer log history for the local printer (refer background to question 1).

Tim, any option to explore further would require a more comprehensive review, and would require a different approach including the engagement of specialist expertise.

Happy to discuss

Regards
Matt

Matt Cahill
Deputy Secretary
Strategy and Operations Group
Department of the Environment and Energy
GPO Box 787 Canberra ACT 2601
Tel: 02 6274 1114

From: Matt Cahill
Sent: Friday, 25 October 2019 9:08 AM
To: Tim Roy <tim.roy@energy.gov.au>
Cc: Rob Heferen <Rob.Heferen@environment.gov.au>
Subject: RE: Request [SEC=OFFICIAL:Sensitive]

Tim

As discussed, I have tasked the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to action this immediately. I will also keep the Chief Operating Officer, who fulfils the role of Chief Security Officer, informed.

The CIO, CISO and the key experts will need to access the accounts of all those concerned. I assure you that they all hold NV1 clearance. Appreciate that the search engine will access areas containing material normally considered as parliamentary privileged. We will take all efforts to avoid any individual access to unrelated documents.

We will advise you on timeframes shortly.

Regards
Matt

Matt Cahill
Deputy Secretary
Strategy and Operations Group
Department of the Environment and Energy
GPO Box 787 Canberra ACT 2601
Tel: 02 6274 1114

From: Tim Roy
Sent: Friday, 25 October 2019 8:14 AM
To: Matt Cahill <Matt.Cahill@environment.gov.au>
Subject: Request [SEC=OFFICIAL:Sensitive]

Hi Matt,

Grateful for your assistance in providing confirmation of activity conducted on departmental IT systems within the Minister's office as per the below.

Time period: likely activity between 5–9 September (inclusive); full window 22 August – 29 September (inclusive)
Relevant website: https://www.cityofsydney.nsw.gov.au
Relevant documents: Statutory Returns Annual Report 2017/18 (pdf and word versions)

The purpose of this request is to confirm the following matters:

- the exact time/s and date/s of any documents accessed by the MO on the cityofsydney website
- any available information for any accessed or downloaded documents from the cityofsydney website during this time, including metadata and content
- any available records relating to printing of documents (or pages of documents) by the MO from the cityofsydney website during this time

Consistent with usual practice, if information becomes available to the Department in the course of these checks that identifies activity that contravenes any relevant Codes of Conduct or IT User Agreements, I would obviously expect the Department to fully comply with its reporting obligations.

Many thanks in advance,
Tim

Tim Roy | Chief of Staff

Office of the Hon Angus Taylor MP
Minister for Energy and Emissions Reduction | Member for Hume
Parliament House CANBERRA ACT 2600

T. +61 2 6277 7120 | M. s. 47F(1)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

8.29am Mobile ≒ 15mins 25/10

- Rang Tim Roy and placed on speaker with Sebastian and Blake
- Discussed our approach and had a few clarifying questions from Sebastian/Blake
- We asked for the document they relied on and Tim said he would send it through
- Also discussion of power outage at APH around the time
- Advised Tim I would respond to his email that

we were actioning his request

s. 22(1)(a)(ii)

12.46pm mobile 25/10

- Rang and left message for Tim ~~Ray~~ to call me.

s. 22(1)(a)(ii)

12.51pm mobile. ÷ 5min 25/10

- Tim returned my call.
- Advised him that it was taking time.
- Appreciate that Tim Neal had provided more info to Setonstorm to conduct the search.
- Agreed that it was important now for the team to focus

on their work and I would update him on any facts if we learnt but was mindful that it was important to get them all

- Tim asked is there anything we could advise early stand alone that would be helpful as they would like to respond/ascertain what has happened

3.06pm - Rang Tim Roy and advised it = 1 min 25/10 mobile was taking time and it was Itd what we could tell him definitely.

3.10pm - 1 mobile = 1 min. 25/10

- Tim rang and requested could we/have we ascertained that the web-site had been accessed on certain dates
- I said I would confirm being mindful that we may not ~~Aoke~~ not established all the facts.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

5.15pm mobile. ≒ 1 hr 8 mins 26/10

s. 22(1)(a)(ii)

- Tim came on line.
- Rob outlined where we are at and the high level overview
- I advised Tim of preliminary facts, as no walk through, checking of underpinning evidence by myself in particular, had occurred so there is potential for change.
- Took him through what we had established (prelim)
- Tim asked a couple of clarifications and I put the two on mute and left room and went and asked Team. Focus was on minutiae/ naming of docs so to understand,
- Tim and Rob asked that the focus on the response be on the questions asked.
- I advised that still ~~[illegible]~~ consolidating material so that I would walk through and that would take time
- Agreed (Tim/Rob) that make sure all correct and take the time needed,
- I reiterated that my focus was on facts and not going beyond this.
- Tim thanked Rob and I for our time.

s. 22(1)(a)(ii)

6.42pm mobile ≒4mins 26/10

- Rang Tim ~~adjust w~~
- Advised him that I just wanted to remind him that all was preliminary as I had to do a walkthrough
- Also advised him that it was going to take time to get it factually correct, as he requested and wanted he need it tomorrow or later?
- Tim reiterated it was important to get the facts correct and take time needed. so if it is early next weeks then that is OK as long as accurate and correct.
- Agreed would update early next week

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

11.40am → 12.48pm mobile 27/10

- Series of short calls between Tim Roy and D

s. 22(1)(a)(ii)

- Tim inquiring about particular facts as he wanted to understand particulars.

s. 22(1)(a)(ii)

- Tim again thanked me and the team for the thoroughness and professionalism in establishing facts.

s. 22(1)(a)(ii)

1256pm Tues 29/10

- Rang Tim Roy - updated where we were at.
- He discussed he had been doing his own review with the advice based on material I provided
- Advised we were doing some more analysis of print logs and event log.
- Tim was very keen to understand what happened
- I said it was complex and we would update where we were at later

6.37pm 29/10

- Rang Tim - he returned my call
- Advised that we know have [redacted] a lot better picture but just now documenting and checking

the logs to make sure facts are correct.

- ~~Fra~~ Fi[illegible] agreed it was important to get Facts right.
- Advised I would aim to get a written response back to him tomorrow.

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)

s. 22(1)(a)(ii) 30/10

s. 22(1)(a)(ii)

5:00pm → Rang Tim [illegible] said just sending through

s. 22(1)(a)(ii)

s. 22(1)(a)(ii)