s47F

From: Andrew Brooks
Sent: Wednesday, 30 November 2022 3:36 PM
To: s47F
Cc: s47F
Subject: RE: INC11744 summary - AEC spear phishing campaign [SEC=OFFICIAL:Sensitive]

I'm ok with the revised wording if you want to get back to EIAT and cc me in

Andrew Brooks | Director (ITSA)
Cyber Security & Assurance Section | Electoral Integrity and Communications Branch
Australian Electoral Commission
s47F

From: s47F
Sent: Wednesday, 30 November 2022 3:33 PM
To: Andrew Brooks s47F
Cc: s47F
Subject: RE: INC11744 summary - AEC spear phishing campaign [SEC=OFFICIAL:Sensitive]

Please see below

s47F **| Deputy ITSA**
Cyber Security & Assurance Section | Electoral Integrity & Communications Branch
Australian Electoral Commission
s47F

From: s47F
Sent: Monday, 21 November 2022 1:24 PM
To: Andrew Brooks s47F
Cc: s47F
Subject: RE: INC11744 summary - AEC spear phishing campaign [SEC=OFFICIAL:Sensitive]

Are you happy to share this with EIAT? I've edited their proposed wording and cut out a lot of the summary, below:

> Dear EIAT members
>
> For your information and awareness, we would like to bring to your attention a recent 'spear phishing' email campaign at the AEC. The detail of these emails is below.

AEC systems were **not** compromised in any way. We believe this is worthwhile sharing with the EIAT on the basis that despite being contained by the AEC, the campaign appears targeted and somewhat sophisticated. It is possible it relates to the proposed referendum given the targeting of AEC's Indigenous Electoral Participation Program mailboxes. [redacted] s47E [redacted]

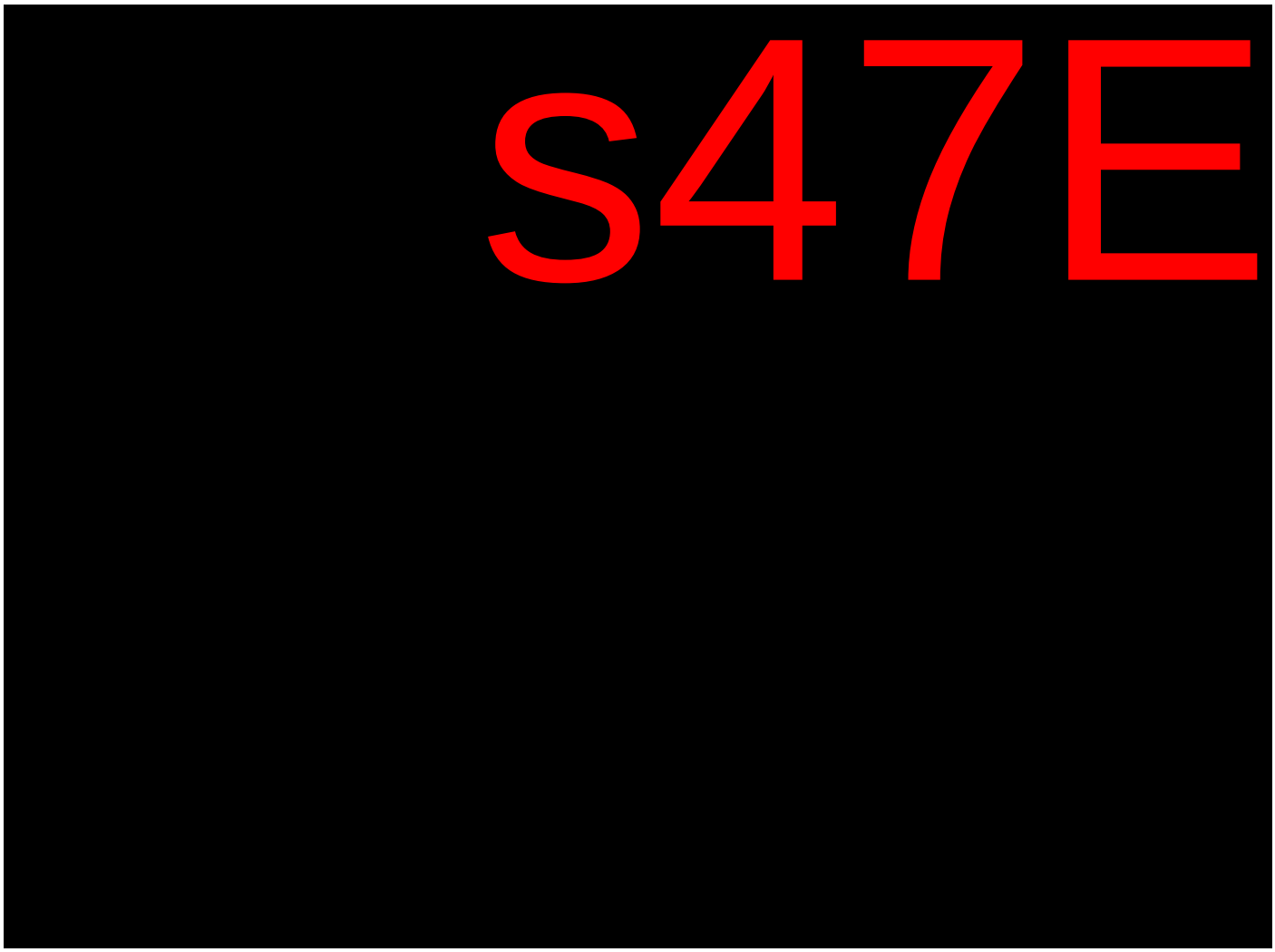
It is a reminder that the cyber threat environment for the proposed referendum is unlikely to be lower than for a federal election.

Email details

On 14 November 2022, at 22:52, a series of emails were sent to the AEC's eight IEPP mailboxes, from the falsified email address support[@]aec.gov.au, with the subject '[email address] have 12 Pending incoming emails'. The list of recipients is as follows:

- indigenous@aec.gov.au
- indigenous-sa@aec.gov.au
- indigenous-wa@aec.gov.au
- indigenous-vic@aec.gov.au
- indigenous-tas@aec.gov.au
- indigenous-qld@aec.gov.au
- indigenous-nt@aec.gov.au
- indigenous-nsw@aec.gov.au

[redacted] s47E [redacted]



[redacted] | **Deputy ITSA**
Cyber Security & Assurance Section | Electoral Integrity & Communications Branch
Australian Electoral Commission
[redacted]

From: EIAT <EIAT@aec.gov.au>
Sent: Friday, 18 November 2022 2:35 PM
To: Andrew Brooks <[redacted]
Cc: [redacted] Julie Igglesden [redacted]
Subject: FW: INC11744 summary - AEC spear phishing campaign [SEC=OFFICIAL:Sensitive]

Hi Andrew

I think [redacted] may have discussed this with you.

Are you supportive if we notify EIAT members of this incident? The benefit would be to ensure EIAT members remain alert to the threats in the referendum environment and particularly reinforce that it is not necessarily a lower cyber threat environment compared to a federal election.

We would propose sharing the incident summary below (happy if you have a more recent version) and introduce it along the lines below so as not to alarm anyone or otherwise imply that the AEC was compromised.

> Dear EIAT members
>
> For your information and awareness, we would like to bring to your attention a recent 'spear phishing' attempt at the AEC. The incident summary is below.
>
> AEC systems were **not** compromised in anyway. The attempt appears targeted and somewhat sophisticated. It is possible it relates to the proposed referendum given the targeting of AEC's Indigenous Electoral Participation Program mailboxes. [redacted]
>
> It is a reminder that the cyber threat environment for the proposed referendum is unlikely to be lower than for a federal election.

Grateful for your thoughts.

Regards

[redacted] | **Assistant Director**
Defending Democracy Unit | Electoral Integrity and Communications Branch
Australian Electoral Commission
[redacted]

From: Andrew Brooks [redacted]s47F
Sent: Thursday, 17 November 2022 11:14 AM
To: John Forrest [redacted]s47F Brian Foo [redacted]s47F Toby Wright [redacted]s47F Julie Igglesden [redacted]s47F
Subject: INC11744 summary - AEC spear phishing campaign [SEC=OFFICIAL:Sensitive]

Good Morning

Please refer below for a high level summary that consolidates yesterday's incident response so we are all on the same page as to what happened including the resulting mitigation actions. While the incident has now been closed from a response perspective, [redacted]s47E.

The nature of the targeted phishing campaign and the resulting incident response may make an excellent case study for broader awareness activities in the future.

Let me know if additional information is required and note we've purposely left the more technical details out of this summary.

Regards

Andrew

Andrew Brooks | Director (ITSA)
Cyber Security & Assurance Section | Electoral Integrity and Communications Branch
Australian Electoral Commission
[redacted]s47F

AEC Australian Electoral Commission
Make sure you're **enrolled to vote.**
Visit www.aec.gov.au

INC11744 summary - AEC spear phishing campaign

Email details

On 14 November 2022, at 22:52, a series of emails were sent to the AEC's eight IEPP mailboxes, from the falsified email address support[@]aec.gov.au, with the subject '[email address] have 12 Pending incoming emails'. The list of recipients is as follows:

- indigenous@aec.gov.au
- indigenous-sa@aec.gov.au
- indigenous-wa@aec.gov.au
- indigenous-vic@aec.gov.au
- indigenous-tas@aec.gov.au
- indigenous-qld@aec.gov.au
- indigenous-nt@aec.gov.au

- indigenous-nsw@aec.gov.au

[redacted] s47E

[redacted] s47E

[redacted] s47E

[redacted]

[redacted] s47E

[redacted]

[redacted]

s47E

s47E