

(b)(6) - Gary Barnett email

From: (b)(6) - Gary Barnett email
Sent: Monday, January 28, 2019 3:46 PM
To: Raimondi, Marc (OPA)
Cc: Benczkowski, Brian (CRM)
Subject: Re: 2019 01 28 1000 Media Advisory DRAFT

Please go with:

“Today we are announcing that we are bringing criminal charges against telecommunications giant Huawei and its associates for nearly two dozen alleged crimes. As I told Chinese officials in August, China must hold its citizens and Chinese companies accountable for complying with the law. I’d like to thank the many dedicated criminal investigators from several different federal agencies who contributed to this investigation and the Department of Justice attorneys who are moving the prosecution efforts forward. They are helping us uphold the rule of law with integrity.”

On Jan 28, 2019, at 3:25 PM, Raimondi, Marc (OPA) (b)(6) wrote:

Duplicates of 27225 and CRM Bates 131-36

Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



Kupec, Kerri (OPA)

From: Kupec, Kerri (OPA)
Sent: Monday, January 28, 2019 3:46 PM
To: Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM)
Cc: Driscoll, Kevin (CRM); Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD (b)(6) (NSD (b)(6) (NSD); Navas, Nicole (OPA); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Folks, I just received CRM's edit (b)(5) DPP We are WAY past the time to be making these kinds of edits to the A/AG's speech he is set to deliver in 45 mins.

Duplicates of 27225 and CRM Bates 131-36

Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



Duplicates of 27225 and CRM Bates 131-36



From: Raimondi, Marc (OPA)
Sent: Monday, January 28, 2019 3:47 PM
To: Barnett, Gary E. (OAG)
Cc: Benczkowski, Brian (CRM)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Ok re-printing now.

Duplicates of 27248



Duplicates of 27248



Duplicates of 27248



Duplicates of 27248



Duplicates of 27248



Kupec, Kerri (OPA)

From: Kupec, Kerri (OPA)
Sent: Monday, January 28, 2019 3:48 PM
To: Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM)
Cc: Driscoll, Kevin (CRM); Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD (b)(6) (NSD (b)(6) (NSD); Navas, Nicole (OPA); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

And as I've now repeated multiple times, ODAG needs to stay on these threads.

Duplicates of 27253



Subject: Re: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27253



Duplicates of 27253



Duplicates of 27253



Duplicates of 27253



Raimondi, Marc (OPA)

From: Raimondi, Marc (OPA)
Sent: Monday, January 28, 2019 3:48 PM
To: Keshwani, Sonya (OPA); Mangum, Anela (OPA)
Cc: Kupec, Kerri (OPA); Stafford, Steven (OPA)
Subject: FW: 2019 01 28 1000 Media Advisory DRAFT

Anela/Sonya, quote changed again. Please recycle the print outs and re-print 35 copies.
Very sorry,
MR

Duplicates of 27248



Duplicates of 27248



Duplicates of 27248



Duplicates of 27248



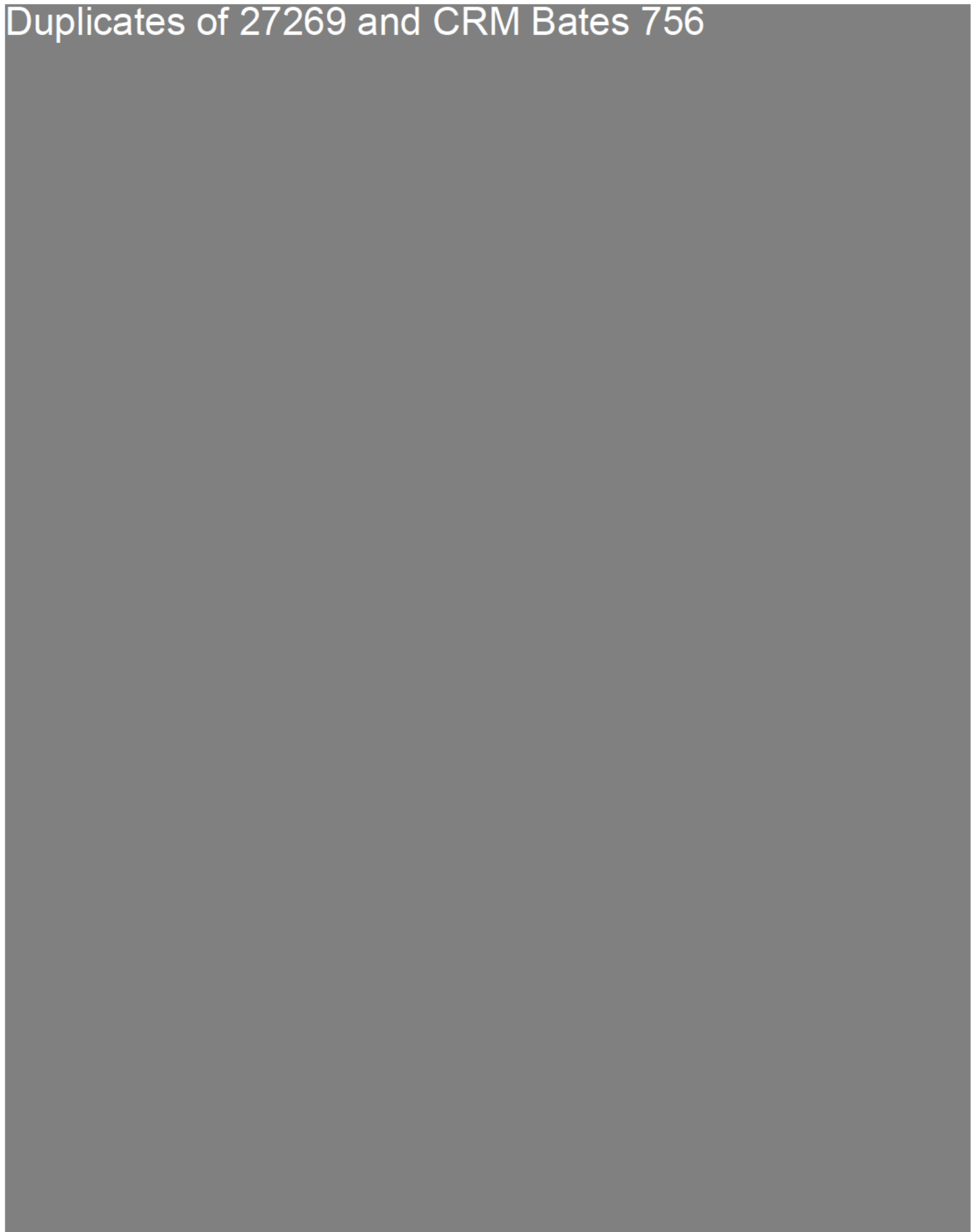
Duplicates of 27248



From: Driscoll, Kevin (CRM)
Sent: Monday, January 28, 2019 3:49 PM
To: Kupec, Kerri (OPA); Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM)
Cc: Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD) (b)(6) per NSD (NSD); (b)(6) per NSD (NSD); Navas, Nicole (OPA); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27269 and CRM Bates 756

Duplicates of 27269 and CRM Bates 756




Duplicates of 27269 and CRM Bates 756



Duplicates of 27269 and CRM Bates 756



Duplicates of 27269 and CRM Bates 756



Hornbuckle, Wyn (OPA)

From: Hornbuckle, Wyn (OPA)
Sent: Monday, January 28, 2019 3:57 PM
To: Driscoll, Kevin (CRM); Kupec, Kerri (OPA); Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM)
Cc: Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD (b)(6) (NSD); (b)(6) (NSD); Navas, Nicole (OPA); Mangum, Anela (OPA); Keshwani, Sonya (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27279 and CRM Bates 756, 785

Duplicates of 27279 and CRM Bates 756, 785



Duplicates of 27279 and CRM Bates 756, 785



Duplicates of 27279 and CRM Bates 756, 785



Duplicates of 27279 and CRM Bates 756, 785



Duplicates of 27279 and CRM Bates 756, 785



From: Kupec, Kerri (OPA)
Sent: Monday, January 28, 2019 3:59 PM
To: Hombuckle, Wyn (OPA)
Cc: Driscoll, Kevin (CRM); Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM); Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD) (b)(6) (NSD) (b)(6) (NSD); Navas, Nicole (OPA); Mangum, Anela (OPA); Keshwani, Sonya (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: Re: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27284 and CRM Bates 756, 785

Duplicates of 27284 and CRM Bates 756, 785



Duplicates of 27284 and CRM Bates 756, 785



Duplicates of 27284 and CRM Bates 756, 785



Duplicates of 27284 and CRM Bates 756, 785



Duplicates of 27284 and CRM Bates 756, 785



Navas, Nicole (OPA)

From: Navas, Nicole (OPA)
Sent: Monday, January 28, 2019 4:00 PM
To: Driscoll, Kevin (CRM); Kupec, Kerri (OPA); Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Benczkowski, Brian (CRM)
Cc: Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NS (b)(6) (NSD); (b)(6) (NSD); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27279 and CRM Bates 753-58

investigative work.

- Ensuring our nation's laws are upheld takes the full-force of all our federal, state, and local partners. I'd

Duplicates of 27279 and CRM Bates 753-58



Duplicates of 27279 and CRM Bates 753-58



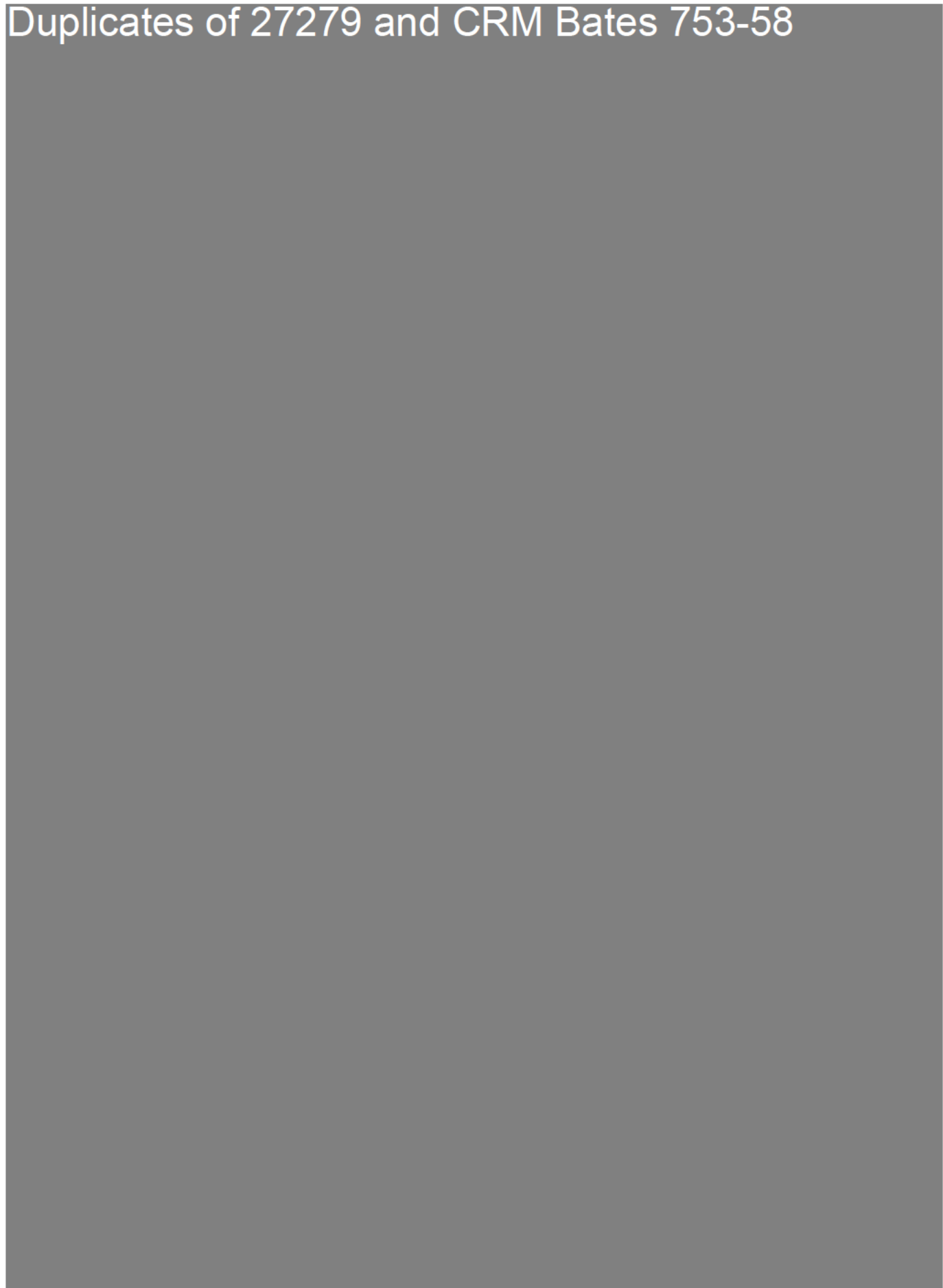
Duplicates of 27279 and CRM Bates 753-58



Duplicates of 27279 and CRM Bates 753-58



Duplicates of 27279 and CRM Bates 753-58



Duplicates of 27279 and CRM Bates 753-58

Duplicates of 27279 and CRM Bates 753-58



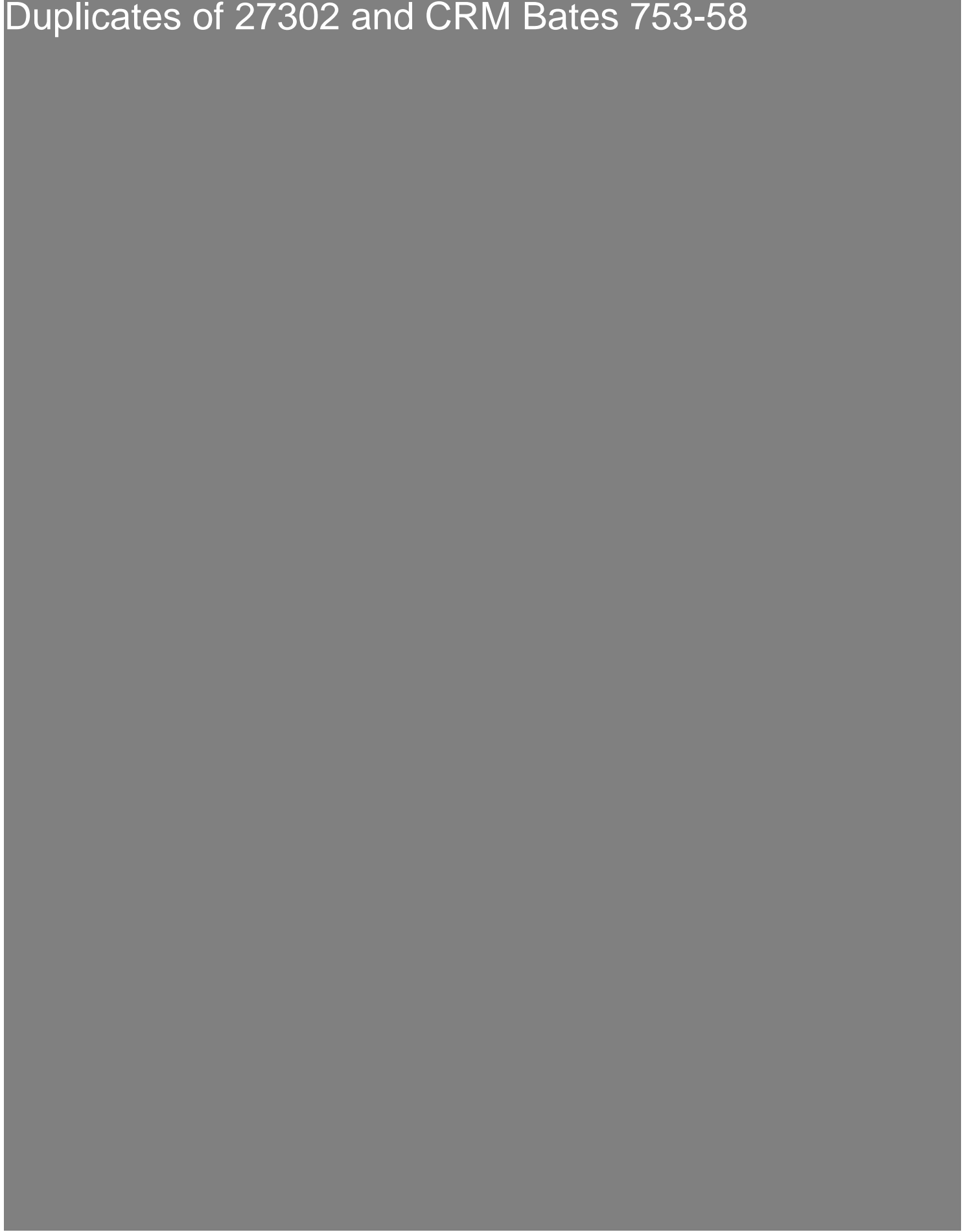
From: Raimondi, Marc (OPA)
Sent: Monday, January 28, 2019 6:05 PM
To: Barnett, Gary E. (OAG); Navas, Nicole (OPA); Driscoll, Kevin (CRM); Kupec, Kerri (OPA); Benczkowski, Brian (CRM)
Cc: Hickey, Adam (NSD); Stafford, Steven (OPA); Demers, John C. (NSD) (b)(6) (NSD); (b)(6) (NSD); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27302 and CRM Bates 753-58

Duplicates of 27302 and CRM Bates 753-58



Duplicates of 27302 and CRM Bates 753-58



Duplicates of 27302 and CRM Bates 753-58



Duplicates of 27302 and CRM Bates 753-58

Duplicates of 27302 and CRM Bates 753-58



Duplicates of 27302 and CRM Bates 753-58



Duplicates of 27302 and CRM Bates 753-58



From: Hickey, Adam (NSD)
Sent: Monday, January 28, 2019 6:05 PM
To: Raimondi, Marc (OPA); Barnett, Gary E. (OAG); Navas, Nicole (OPA); Driscoll, Kevin (CRM); Kupec, Kerri (OPA); Benczkowski, Brian (CRM)
Cc: Stafford, Steven (OPA); Demers, John C. (NSD) (b)(6) (NSD) (b)(6) (NSD); Mangum, Anela (OPA); Keshwani, Sonya (OPA); Hornbuckle, Wyn (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)
Subject: RE: 2019 01 28 1000 Media Advisory DRAFT

Duplicates of 27311 and CRM Bates 753-58, 763

Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



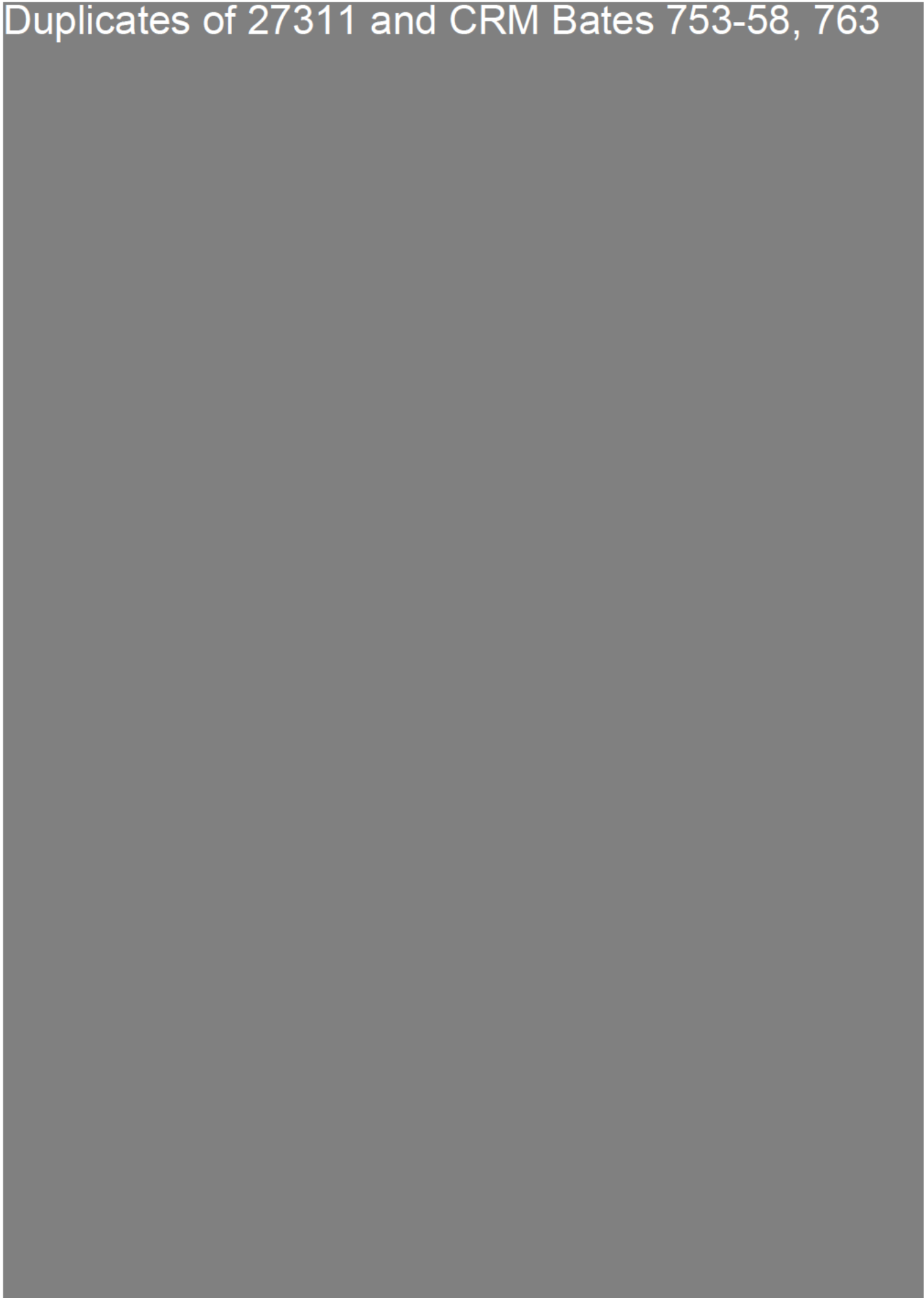
Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



Duplicates of 27311 and CRM Bates 753-58, 763



From: Cronan, John (CRM)
Sent: Thursday, February 14, 2019 8:59 AM
To: Lan, Iris (ODAG)
Cc: Driscoll, Kevin (CRM)
Subject: AG Barr Overview Materials CRM.Final.2.14.19
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx

Iris Here is the CRM overview. Thanks again!

John

From: Lan, Iris (ODAG)
Sent: Thursday, February 14, 2019 9:13 AM
To: Ellis, Corey F. (ODAG)
Subject: CRM Paper for new AG
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx

As promised thanks. Iris

From: Lan, Iris (ODAG)
Sent: Thursday, February 14, 2019 10:30 AM
To: Ellis, Corey F. (ODAG)
Subject: FW: CRM Paper for new AG
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx; CRM Org Chart - SES SL - 2.14.19.pdf

(Adding CRM Org Chart)

From: Lan, Iris (ODAG)
Sent: Thursday, February 14, 2019 9:13 AM
To: Ellis, Corey F. (ODAG (b)(6))
Subject: CRM Paper for new AG

As promised thanks. Iris

From: Ellis, Corey F. (ODAG)
(b)(6)
To: Leeman, Gabrielle (ODAG)
(b)(6); Heane, Kristen (ODAG)
(b)(6)
Cc:
Bcc:
Subject: FW: CRM Paper for new AG
Date: Thu Feb 14 2019 10:31:41 EST
Attachments: AG Barr Overview Materials_CRM.Final.2.14.19.docx
CRM Org Chart - SES SL - 2.14.19.pdf

From: Lan, Iris (ODAG) (b)(6)
Sent: Thursday, February 14, 2019 10:30 AM
To: Ellis, Corey F. (ODAG) (b)(6)
Subject: FW: CRM Paper for new AG

(Adding CRM Org Chart)

From: Lan, Iris (ODAG)
Sent: Thursday, February 14, 2019 9:13 AM
To: Ellis, Corey F. (ODAG) (b)(6)
Subject: CRM Paper for new AG

As promised - thanks. Iris

From: Cronan, John (CRM)
Sent: Thursday, February 14, 2019 5:11 PM
To: Lan, Iris (ODAG)
Subject: AG Barr Overview Materials CRM.Final.2.14.19
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx

Follow Up Flag: Flag for follow up
Flag Status: Flagged

It may be too late, but I made a couple of tiny changes to our overview (b)(5) DPP, (b)(6), (b)(7)(C) per CRM [REDACTED] in case you are able to replace with the attached document.

From: Lan, Iris (ODAG)
Sent: Thursday, February 14, 2019 5:15 PM
To: Ellis, Corey F. (ODAG)
Subject: Revised CRM Paper for New AG
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx

Just in from CRM, with minor edits, in case not too late.

Duplicate of 27523

From: (b)(6) - Corey Ellis email
Sent: Thursday, February 14, 2019 5:19 PM
To: Leeman, Gabrielle (ODAG); Heane, Kristen (USAEO); Peterson, Andrew (ODAG)
Subject: Fwd: Revised CRM Paper for New AG
Attachments: AG Barr Overview Materials CRM.Final.2.14.19.docx; ATT00001.htm

Corey F. Ellis

(b)(6)

Begin forwarded message:

Duplicates of 27529

From: (b)(6) per NSD (NSD)
Sent: Tuesday, February 19, 2019 10:27 AM
To: Levi, William (OAG)
Cc: Demers, John C. (NSD); Wiegmann, Brad (NSD)
Subject: NSD Summary Topical material for AG
Attachments: NSD Topics 2019 Transition 2 19 19.docx

Hi Will,

Enclosed is a summary memo of the NSD matters that fit within the three areas we discussed: (1) Hot Topics; (2) Steady State topics, and (3) Fast Approaching topics. I have also sent you on the TS system the addendum referenced in this memo.

We hope this is helpful and let me know if you need any further information.

(b)(6) per

(b)(6) per NSD
Chief of Staff and Senior Counsel
U.S. Department of Justice
National Security Division
(b)(6) per NSD (desk)
(b)(6) per NSD (cell)

From: Navas, Nicole (OPA)
<(b)(6)>
To: Sutton, Sarah E. (OPA)
(b)(6); Raimondi, Marc (OPA)
<(b)(6)>
Cc: Kupec, Kerri (OPA)
<(b)(6)> Hornbuckle, Wyn (OPA)
<(b)(6)>
Bcc:
Subject: RE: Rosenstein contact
Date: Tue Feb 26 2019 11:44:01 EST
Attachments:

Thank you. (b)(5)

From: Sutton, Sarah E. (OPA) <(b)(6)>
Sent: Monday, February 25, 2019 10:12 AM
To: Navas, Nicole (OPA) <(b)(6)> Raimondi, Marc (OPA) <(b)(6)>
Subject: FW: Rosenstein contact

Wyn and I discussed this with Kerri and declined to interview on this at this time, but I wanted to flag for both of your awarenesses.

From: Sutton, Sarah E. (OPA)
Sent: Monday, February 25, 2019 10:10 AM
To: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com<mailto:Karen.Freifeld@thomsonreuters.com>>
Subject: Re: Rosenstein contact

Hi Karen,

Appreciate your patience on this. At this time we're going to decline to interview. If something changes in the future, we will reach out.

Best,

Sarah
Sent from my iPhone

On Feb 24, 2019, at 20:02, Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com<mailto:Karen.Freifeld@thomsonreuters.com>> wrote:
I appreciate that. Thank you.

Karen Freifeld
Reuters
(b)(6)

From: Sutton, Sarah E. (OPA) [mailto:(b)(6)]

Sent: Sunday, February 24, 2019 7:59 PM
To: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com<mailto:Karen.Freifeld@thomsonreuters.com>>
Subject: Re: Rosenstein contact

I can't promise it, but I will check to see if we can make that work.
Sent from my iPhone

On Feb 24, 2019, at 19:17, Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com<mailto:Karen.Freifeld@thomsonreuters.com>> wrote:
Thanks for responding on Sunday.

I will look out for the remarks, thanks. I have more specific questions involving him.

Any chance of a few minutes tomorrow?

Karen

(b)(6)

Get Outlook for iOS<https://urldefense.proofpoint.com/v2/url?u=https-3A__aka.ms_o0ukef&d=DwMGaQ&c=4ZIZThykDLcoWk-GVjSLmy8-1Cr1I4FWIvbLFebwKgY&r=_mDyr8pJyje9qKuiYqSqktlSzh5zE_VVqi9sUEbnqnP40q_h9V_9_XaO9AZQ2LbX&m=AJ9Smd0mbZW5ptKGdYETK9kH_yq21GuNGtsXwhHjznc&s=J7GOTBP0ch7Yg8e2AHtCdd5BGhib795z1lcwKn-A1y0&e=>>

From: Sutton, Sarah E. (OPA) (b)(6)
Sent: Sunday, February 24, 2019 7:07 PM
To: Freifeld, Karen (Reuters)
Subject: Re: Rosenstein contact

Karen,

Thanks for reaching out!

I will see if we can get some time on his schedule for you. In the mean time, if you didn't get our advisory for his remarks at CSIS this Monday I would check that out as well.

Best,

Sarah
Sent from my iPhone

On Feb 24, 2019, at 10:16, Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com<mailto:Karen.Freifeld@thomsonreuters.com>> wrote:
Hi, Sarah,

I'm a veteran law enforcement reporter with Reuters.

I'm working on stories involving Huawei and DOJ's China initiative and I am hoping to talk to Rod Rosenstein about the subject. Background or off the record is fine.

I have done extensive reporting on ZTE and Huawei (as has my colleague Steve Stecklow who wrote the original stories that were credited in both indictments).

Another colleague Sarah Lynch said she mentioned me to you and the DAG on Friday and that he

seemed willing to talk (particularly about something other than Mueller!).

Is it possible for me to grab a few minutes with him either on the phone or in person?

I am available anytime (including today; I actually sent this message earlier but left out your middle initial and it bounced back). Obviously, the sooner the better. I am planning to publish in the next few days.

Thanks for your consideration.

Karen Freifeld

(b)(6)

Karen Freifeld

Reuters

(b)(6)

From: Levi, William (OAG) (b)(6)
To: Washington, Tracy T (OAG) (b)(6)
Cc: Watson, Theresa (OAG) (b)(6); Bryant, Errical (OAG) (b)(6)
Bcc:
Subject: FW: AG Briefing Materials for Thursday, February 28, 2019
Date: Wed Feb 27 2019 11:02:18 EST
Attachments: NSD Topics 2019 Transition 2 19 19.docx
NCW.docx

Please see attached materials for tomorrow. I may follow-up with materials for Dan Coats, as well. There are none for the Paper PC / 702 as those are classified. Thanks!

From: Watson, Theresa (OAG) (b)(6)
Sent: Tuesday, February 26, 2019 6:45 PM
To: Levi, William (OAG) (b)(6); Hamilton, Gene (OAG) (b)(6)
Cc: Rabbitt, Brian (OAG) (b)(6); Bryant, Errical (OAG) (b)(6);
Washington, Tracy T (OAG) (b)(6); Jackson, Wykema C. (OAG) (b)(6)
Subject: AG Briefing Materials for Thursday, February 28, 2019

You are listed as the POC for the events listed below on the A/AG's schedule for Thursday, and we are expecting briefing materials from you. Please send an email with a copy of your complete package, (including tabs if appropriate, by 4:30 pm, tomorrow, so that we can prepare the binder. If you do not have any materials, or if you have a separate binder, please reply to this message so that we know not to include them in our table of contents. Thanks.

IF YOU DO NOT HAVE MATERIALS, PLEASE LET US KNOW.

Will Levi

- *Time Sensitive National Security Topics
- *USA Meet/Greet: Andrew Murray, WD/NC
- *Paper PC/ 702 Semi-Annual Report
- *Meeting: Dan Coats, Director DNI

Gene Hamilton

- *Regulations Discussion

Sutton, Sarah E. (OPA)

From: Sutton, Sarah E. (OPA)
Sent: Monday, March 18, 2019 11:09 AM
To: Hornbuckle, Wyn (OPA); Raimondi, Marc (OPA); Navas, Nicole (OPA)
Subject: FW: Rosenstein contact

(b)(5) DPP [REDACTED] but I passing along since the subject matter isn't my lane.

From: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com>
Sent: Monday, March 18, 2019 11:02 AM
To: Sutton, Sarah E. (OPA) (b)(6) [REDACTED]
Subject: RE: Rosenstein contact

And/or other matters....including the Mueller probe. I have a couple of questions OTR that I think have not been addressed.

Karen Freifeld
Reuters

(b)(6) [REDACTED]

From: Sutton, Sarah E. (OPA) [[mailto:](#)(b)(6) [REDACTED]]
Sent: Monday, March 18, 2019 11:00 AM
To: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com>
Subject: RE: Rosenstein contact

Thanks Karen. Are you wanting to speak to him on Huawei?

From: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com>
Sent: Monday, March 18, 2019 9:12 AM
To: Sutton, Sarah E. (OPA) (b)(6) [REDACTED]
Subject: RE: Rosenstein contact

Hi, Sarah,

I will be in DC this week.

Any chance of my getting some time with Rosenstein?

Thanks for your consideration.

Karen Freifeld
Reuters

(b)(6) [REDACTED]

From: Sutton, Sarah E. (OPA) [[mailto:](#)(b)(6) [REDACTED]]

Sent: Monday, February 25, 2019 10:21 AM
To: Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com>
Subject: Re: Rosenstein contact

Sorry, we have to pass at this time.

Sent from my iPhone

On Feb 25, 2019, at 10:16, Freifeld, Karen (Reuters) <Karen.Freifeld@thomsonreuters.com> wrote:

I'm disappointed. Not even five minutes?

Get [Outlook for iOS](#)

Duplicates of 27553



Duplicates of 27553



Duplicates of 27553



Hankey, Mary Blanche (OLA)

From: Hankey, Mary Blanche (OLA)
Sent: Tuesday, March 26, 2019 10:13 AM
To: Bissex, Rachel (OAG)
Subject: RE: hearing transcript
Attachments: 2019.01.15 AG Barr confirmation hearing.pdf; 2019.01.16 AG Barr confirmation hearing.pdf

[Attached.](#)

From: Bissex, Rachel (OAG (b)(6))
Sent: Tuesday, March 26, 2019 10:09 AM
To: Hankey, Mary Blanche (OLA (b)(6))
Subject: hearing transcript

Hi Mary Blanche,

Do you all have a transcript from the AG's confirmation hearing?

Rachel P. Bissex
Counselor to the Attorney General & White House Liaison
(b)(6) (work)
(b)(6) (cell)

Raimondi, Marc (OPA)

From: Raimondi, Marc (OPA)
Sent: Monday, April 29, 2019 5:48 PM
To: Chon, Gina (Reuters)
Subject: Re: Milken

Where shall we meet? Lobby bar and then go find someplace?

On Apr 29, 2019, at 2:46 PM, Chon, Gina (Reuters) (b)(6) > wrote:

Yep and can get there 10 mins early if that works.

Gina Chon
Columnist, San Francisco
Reuters Breakingviews
Mobil (b)(6)
Twitter: @GinaChon

From: Raimondi, Marc (OPA (b)(6))
Sent: Monday, April 29, 2019 2:26 PM
To: Chon, Gina (Reuters)
Subject: Re: Milken

Still good for 3? We could meet a bit sooner if you'd like

On Apr 29, 2019, at 5:50 AM, Chon, Gina (Reuters) (b)(6) > wrote:

(b)(6)

Hope all has been well with you though I imagine pretty hectic.

From: Raimondi, Marc (OPA (b)(6))
Sent: Monday, April 29, 2019 5:45 AM
To: Chon, Gina (Reuters)
Subject: Re: Milken

I am so linking to catch up? What got you out west?

On Apr 29, 2019, at 5:37 AM, Chon, Gina (Reuter (b)(6) > wrote:

Sounds good and not sure yet. May have a meeting then but waiting to hear back.

Gina Chon
Columnist, San Francisco
Reuters Breakingviews
Mobil (b)(6)
Twitter: @GinaChon

From: Raimondi, Marc (OPA) (b)(6) >
Sent: Monday, April 29, 2019 5:15 AM
To: Chon, Gina (Reuters)
Subject: Re: Milken

Yes. That works. Lobby bar at the hotel? Also, are you coming to John's session at 1045?

<image1.png>

Marc Raimondi
U.S. Department of Justice

(b)(6)
Mobil (b)(6)

Sent from an iPhone, pls excuse typos and errant autocorrects.

On Apr 29, 2019, at 4:19 AM, Chon, Gina (Reuter (b)(6)) wrote:

Hi Marc,

Great to hear from you and thanks for letting me know as I didn't hear. Would he have time today at 3 pm?

Thanks and would be nice to see you.

Cheers,

Gina

Gina Chon
Columnist, San Francisco
Reuters Breakingviews
Mobil (b)(6)
Twitter: @GinaChon

From: Gina Cho (b)(6)
Sent: Monday, April 29, 2019 4:14 AM
To: Chon, Gina (Reuters)
Subject: Fwd: Milken

----- Forwarded message -----

From: Raimondi, Marc (OPA) (b)(6)
Date: Fri, Apr 26, 2019, 8:26 PM
Subject: Milken
To: Gina Cho (b)(6)

Gina! long time no hear or see. I think I was at the White House last time we chatted. Im back at my regular gig at the Justice Department now. I sent this out earlier to DOJ Reuters reporter to forward to the team at Milken. In case it didn't reach you please see what follows. I hope we can link up in LA.

Original note:

I'm going to be at the Milken Conference this Monday with Assistant Attorney General John Demers. John is presenting at 10:45 AM in the Whittier Room on a panel titled: *Cyber Attacks by Nation States: The View From Inside America's National Security Network*. John will focus on national security cyber threats and the continued malfeasance posed by nation states. A particular focus of the presentation will be on Chinese state actors targeting US companies for economic espionage. John is the Department of Justice lead for the Attorney General's China Initiative effort which is detailed below. I've also attached cases for the last 15 or so months that show a clear and continuing pattern of Chinese economic aggression. We are not able to have a media availability while at the conference but I do have some time set aside for media interviews on the topic of our China Initiative. Please shoot me a note if you would like to interview John.

Thanks!

Marc Raimondi

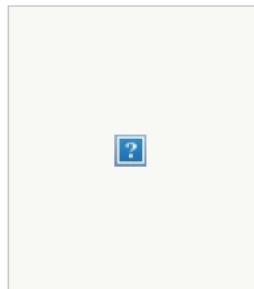
Senior Advisor for National Security Communications and External Affairs

U.S. Department of Justice

Mobil (b)(6)

(b)(6)

More about John and the China Initiative



John Demers became Assistant Attorney General for National Security on February 22, 2018. In that capacity, he leads the Department of Justice's efforts to combat national security related cyber-crime, terrorism and espionage, to enforce export control and sanctions laws, to use the authorities of the Foreign Intelligence Surveillance Act, and to conduct national security review of foreign investments. In November 2018, John was selected to lead the Attorney General's China Initiative, put in place to counter the Peoples Republic of China's persistent and aggressive economic espionage, trade secret theft, hacking and other related crimes.

Prior to rejoining the Department, John was Vice President and Assistant General Counsel at The Boeing Company, where he held several senior positions including in Boeing Defense, Space, and Security and as lead lawyer and head of international government affairs for Boeing International.

From 2006 to 2009, John served on the first leadership team of the National Security Division, first as Senior Counsel to the Assistant Attorney General and then as Deputy Assistant Attorney General for the Office of Law & Policy. In addition, he has served in the Office of Legal Counsel and the Office of the Deputy Attorney General. From 2010 to 2017, he taught national security law as an adjunct professor at the Georgetown University Law Center. John worked in private practice in Boston and clerked for Associate Justice Antonin Scalia of the U.S. Supreme Court and Judge Diarmuid O'Scannlain of the U.S. Court of

Appeals for the Ninth Circuit. He graduated from Harvard Law School and the College of the Holy Cross.

Attorney General China Initiative Fact Sheet

Background

The Attorney General's Initiative reflects the Department's strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy. The Initiative is launched against the background of previous findings by the Administration concerning China's practices. In March 2018, the Office of the U.S. Trade Representative announced the results of a months' long investigation of China's trade practices under Section 301 of the Trade Act of 1974. It concluded, among other things, that a combination of China's practices are unreasonable, including its outbound investment policies and sponsorship of unauthorized computer intrusions, and that "[a] range of tools may be appropriate to address these serious matters."

In June 2018, the White House Office of Trade and Manufacturing Policy issued a report on "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," documenting "the two major strategies and various acts, policies, and practices Chinese industrial policy uses in seeking to acquire the intellectual property and technologies of the world and to capture the emerging high-technology industries that will drive future economic growth."

The National Security Division (NSD) is responsible for countering nation state threats to the country's critical infrastructure and private sector. In addition to identifying and prosecuting those engaged in trade secret theft, hacking and economic espionage, the initiative will increase efforts to protect our critical infrastructure against external threats including foreign direct investment, supply chain threats and the foreign agents seeking to influence the American public and policymakers without proper registration.

Statements

Assistant Attorney for National Security John C. Demers

"China wants the fruits of America's brainpower to harvest the seeds of its planned economic dominance. Preventing this from happening will take all of us, here at the Justice Department, across the U.S. government, and within the private sector. With the Attorney General's initiative, we will confront China's malign behaviors and encourage them to conduct themselves as they aspire to be: one of the world's leading nations."

FBI Director Christopher Wray

"No country presents a broader, more severe threat to our ideas, our innovation, and our economic security than China," said FBI Director Christopher Wray. "The Chinese government is determined to acquire American technology, and they're willing use a variety of means to do that from foreign investments, corporate acquisitions, and cyber intrusions to obtaining the services of current or former company employees to get inside information. If China acquires an American company's most important technology the very technology that makes it the leader in a field that company will suffer severe losses, and our national security could even be impacted. We are committed to continuing to work closely with our federal, state, local, and private sector partners to counter this threat from China."

US Attorneys in Working Group

- Andrew E. Lelling (District of Massachusetts)

- Jay E. Town (Northern District of Alabama)
- Alex G. Tse (Northern District of California)
- Richard P. Donoghue (Eastern District of New York)
- Erin Nealy Cox (Northern District of Texas)

Components of Initiative

The Attorney General has set the following goals for the Initiative:

Identify priority trade secret theft cases, ensure that investigations are adequately resourced; and work to bring them to fruition in a timely manner and according to the facts and applicable law;

Develop an enforcement strategy concerning non-traditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests;

Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus;

Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate;

Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their Districts and support their outreach efforts;

-- Implement the Foreign Investment Risk Review Modernization Act (FIRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow);

Identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks;

Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses;

Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States; and

Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.

To launch the initiative, Assistant Attorney General Demers will convene a meeting of the above-mentioned U.S. Attorneys, senior FBI officials, and his counterpart in the Criminal Division, Assistant Attorney General Brian Benczkowski.

China-Related Cases since January 2018

Tuesday, April 23, 2019

Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's

Trade Secrets

An indictment unsealed today charges Xiaoqing Zheng, 56, of Niskayuna, New York, and Zhaoxi Zhang, 47, of Liaoning Province, China, with economic espionage and conspiring to steal General Electric's (GE's) trade secrets surrounding turbine technologies, knowing and intending that those stolen trade secrets would be used to benefit the People's Republic of China. Assistant Attorney General for National Security John C. Demers, U.S. Attorney Grant C. Jaquith for the Northern District of New York, Assistant Director John Brown of the FBI's Counterintelligence Division and Special Agent in Charge James N. Hendricks of the FBI's Albany Field Office made the announcement.

According to the 14-count indictment, Zheng, while employed at GE Power & Water in Schenectady, New York as an engineer specializing in sealing technology, exploited his access to GE's files by stealing multiple electronic files, including proprietary files involving design models, engineering drawings, configuration files, and material specifications having to do with various components and testing systems associated with GE gas and steam turbines. Zheng e-mailed and transferred many of the stolen GE files to his business partner, Chinese businessman Zhaoxi Zhang, who was located in China. Zheng and Zhang used the stolen GE trade secrets to advance their own business interests in two Chinese companies - Liaoning Tianyi Aviation Technology Co., Ltd. (LTAT) and Nanjing Tianyi Avi Tech Co. Ltd. (NTAT), companies which research, develop, and manufacture parts for turbines.

The indictment also alleges that Zheng and Zhang conspired to commit economic espionage, as the thefts of GE's trade secrets surrounding various turbine technologies were done knowing and intending that the thefts would benefit the People's Republic of China and one or more foreign instrumentalities, including LTAT, NTAT, Shenyang Aerospace University, Shenyang Aeroengine Research Institute, and Huaihai Institute of Technology. The defendants, through LTAT and NTAT, received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies.

"The indictment alleges a textbook example of the Chinese government's strategy to rob American companies of their intellectual property and to replicate their products in Chinese factories, enabling Chinese companies to replace the American company first in the Chinese market and later worldwide," said Assistant Attorney General Demers. "We will not stand idly by while the world's second-largest economy engages in state-sponsored theft. As part of the Attorney General's China Initiative, we will partner with the private sector to hold responsible those who violate our laws, and we urge China's leaders to join responsible nations and to act with honesty and integrity when competing in the global marketplace."

"As alleged, the thefts of trade secrets to benefit the People's Republic of China are serious crimes against the victimized company and our country," said U.S. Attorney Jaquith. "Both fair competition and incentivized innovation require that American companies be able to rely on the secrecy of technological advances forged through their talent and tenacity. When technology is taken through treachery, we will continue to work with the National Security Division and the FBI to prosecute the perpetrators."

"American businesses spend many hours and large amounts of money developing unique technology. When such technology is stolen it can be devastating to U.S. businesses and can result in American workers losing jobs," said FBI Assistant Director Brown. "China continues to support behavior that violates the rule of law. This case demonstrates the FBI will continue to pursue China's efforts to steal American technology."

"Economic espionage and the theft of trade secrets have a profound impact on our companies and communities," said FBI Special Agent in Charge Hendricks. "We view this as a grave threat to our economic

and national security and the FBI will work tirelessly to prevent the loss of American technology and American jobs.”

Zheng was arraigned today in Albany, New York, before United States Magistrate Judge Christian F. Hummel, and released with conditions pending a trial before United States District Judge Mae A. D’Agostino.

The economic espionage counts (Counts One, Three, Four, Seven, Eight and Eleven) carry a maximum sentence of 15 years in prison, a fine of up to \$5,000,000, and a term of supervised release of up to three years. The trade secrets theft counts (Counts Two, Five, Six, Nine, Ten, Twelve and Thirteen) carry a maximum sentence of 10 years in prison, a fine of up to \$250,000, and a term of supervised release of up to three years. Count Fourteen of the indictment, which charges Zheng with making false statements to the FBI during a voluntary interview, carries a maximum sentence of 5 years in prison, a fine of up to \$250,000, and a term of supervised release of up to three years.

The charges in the indictment are merely accusations. The defendants are presumed innocent unless and until proven guilty.

This case is being investigated by the Federal Bureau of Investigation, and is being prosecuted by Assistant U.S. Attorney Rick Belliss, and National Security Division Trial Attorneys Jason McCullough and Matthew Chang.

Wednesday, April 17, 2019

Former Manager for International Airline Pleads Guilty to Acting as an Agent of the Chinese Government

Defendant Placed Packages on Flights from JFK Airport to Beijing at the Direction of Military Officers Assigned to the Chinese Mission to the United Nations

Earlier today, in federal court in Brooklyn, New York, Ying Lin pleaded guilty to acting as an agent of the People’s Republic of China (PRC), without notification to the Attorney General, by working at the direction and control of military officers assigned to the Permanent Mission of the People’s Republic of China to the United Nations. Lin, a former manager with an international air carrier headquartered in the PRC (the Air Carrier), abused her privileges to transport packages from John F. Kennedy International Airport (JFK Airport) to the PRC aboard Air Carrier flights at the behest of the PRC military officers and in violation of Transportation Security Administration (TSA) regulations. The proceeding was held before United States District Judge Ann M. Donnelly.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, Assistant Director in Charge William F. Sweeney, Jr of the FBI’s New York Field Office, and Special Agent in Charge Angel M. Melendez, Department of Homeland Security, Homeland Security Investigations (HSI) announced the guilty plea.

“This case is a stark example of the Chinese government using the employees of Chinese companies doing business here to engage in illegal activity,” said Assistant Attorney General Demers. “Covertly doing the Chinese military’s bidding on U.S. soil is a crime, and Lin and the Chinese military took advantage of a commercial enterprise to evade legitimate U.S. government oversight.”

“The defendant’s actions as an agent of the Chinese government helped Chinese military officers to evade U.S. law enforcement scrutiny of packages that they sent from New York to Beijing,” stated United

States Attorney Donoghue. “This case demonstrates how seriously we address counterintelligence threats posed by individuals in the United States who work for foreign governments, such as China.”

“The FBI and our law enforcement partners do all we can every day to protect this country from the threats we can see, and we work even harder to find the threats we can’t see,” said FBI Assistant Director-in-Charge Sweeney. “Ms. Lin was secreting packages through some of the country’s busiest airports, using her work with the Chinese government to thwart our security measures. We believe this case isn’t unique and hope it serves as an example that the Chinese and other foreign governments can’t break our laws with impunity.”

“Lin’s criminal actions exploited the international boundary of the United States as she used her position to smuggle packages onto planes headed to China,” said HSI Special Agent-in-Charge Melendez. “We are committed to ensuring the integrity of our international airports so they are not used as a front for illicit activities.”

Lin worked for the Air Carrier from 2002 through the fall of 2015 as a counter agent at JFK Airport and from the fall of 2015 through April 2016 as the station manager at Newark Liberty International Airport. During her employment with the Air Carrier, Lin accepted packages from the PRC military officers, and placed those packages aboard Air Carrier flights to the PRC as unaccompanied luggage or checked in the packages under the names of other passengers flying on those flights. As the PRC military officers did not travel on those flights, Lin’s actions were contrary to a security program that required that checked baggage be accepted only from ticketed passengers, thereby violating TSA regulations. In addition, Lin encouraged other Air Carrier employees to assist the PRC military officers, instructing those employees that because the Air Carrier was a PRC company, their primary loyalty should be to the PRC.

In exchange for her work at the direction and under the control of PRC military officers and other PRC government officials, Lin received benefits from the PRC Mission and PRC Consulate in New York. These benefits included tax-exempt purchases of liquor, cigarettes and electronic devices worth tens of thousands of dollars. These benefits also included free contracting work at the defendant’s two residences in Queens, New York, by PRC construction workers who were permitted under the terms of their visas to work only on PRC government facilities.

When sentenced, Lin faces up to 10 years’ imprisonment. As part of the guilty plea, Lin agreed to forfeit approximately \$25,000 as well as an additional \$145,000 in connection with her resolution of the government’s forfeiture verdict in *United States v. Zhong*, No. 16-CR-614 (AMD).

Mr. Demers and Mr. Donoghue expressed their appreciation to the Transportation Security Administration for their assistance on the case. The government’s case is being handled by the National Security and Cybercrime Section. Assistant United States Attorneys Douglas M. Pravda, Alexander A. Solomon, Ian C. Richardson and Sarah M. Evans are in charge of the prosecution, with assistance from Trial Attorney Matthew R. Walczewski of the Department of Justice’s Counterintelligence and Export Control Section. The forfeiture aspect of the case is being handled by EDNY Assistant United States Attorney Brian Morris of the Office’s Civil Division.

Friday, March 15, 2019

Former Defense Intelligence Officer Pleads Guilty to Attempted Espionage

Ron Rockwell Hansen, 58, a resident of Syracuse, Utah, and a former Defense Intelligence Agency (DIA) officer, pleaded guilty today in the District of Utah in connection with his attempted transmission of

national defense information to the People's Republic of China. Sentencing is set for Sept. 24, 2019.

Assistant Attorney General for National Security John C. Demers, U.S. Attorney John Huber for the District of Utah and Special Agent in Charge Paul Haertel of the FBI's Salt Lake City Field Office announced the charges.

Hansen retired from the U.S. Army as a Warrant Officer with a background in signals intelligence and human intelligence. He speaks fluent Mandarin-Chinese and Russian. DIA hired Hansen as a civilian intelligence case officer in 2006. Hansen held a Top Secret clearance for many years, and signed several non-disclosure agreements during his tenure at DIA and as a government contractor.

As Hansen admitted in the plea agreement, in early 2014, agents of a Chinese intelligence service targeted Hansen for recruitment and he began meeting with them regularly in China. During those meetings, the Chinese agents described to Hansen the type of information that would interest the Chinese intelligence service. During the course of his relationship with the agents of the Chinese intelligence service, Hansen received hundreds of thousands of dollars in compensation for information he provided them, including information he gathered at various industry conferences. Between May 24, 2016 and June 2, 2018, Hansen solicited from an intelligence case officer working for the DIA national defense information that Hansen knew the Chinese intelligence service would find valuable. Hansen agreed to act as a conduit to sell that information to the Chinese. Hansen advised the DIA case officer how to record and transmit classified information without detection, and explained how to hide and launder any funds received as payment for classified information. The DIA case officer reported Hansen's conduct to the DIA and subsequently acted as a confidential human source for the FBI.

As Hansen further admitted in the plea agreement, Hansen met with the DIA case officer on June 2, 2018, and received from that individual documents containing national defense information that Hansen previously solicited. The documents Hansen received were classified. The information in the documents related to the national defense of the United States in that it related to United States military readiness in a particular region and was closely held by the United States government. Hansen reviewed the documents, queried the DIA case officer about their contents, and took written notes about the materials relating to the national defense information. Hansen advised the DIA case officer that he would remember most of the details about the documents he received that day and would conceal some notes about the material in the text of an electronic document that Hansen would prepare at the airport before leaving for China. Hansen intended to provide the information he received to the agents of the Chinese intelligence service with whom he had been meeting, and Hansen knew that the information was to be used to the injury of the United States and to the advantage of a foreign nation.

Hansen pleaded guilty to one count of attempting to gather or deliver national defense information to aid a foreign government. The plea agreement calls for an agreed-upon sentence of 15 years.

Special agents of the FBI, IRS, U.S. Department of Commerce, the Department of Defense, U.S. Army Counterintelligence, and the Defense Intelligence Agency were involved in the investigation.

The prosecution was handled by Assistant U.S. Attorneys Robert A. Lund, Karin Fojtik, Mark K. Vincent and Alicia Cook of the District of Utah, and Trial Attorneys Patrick T. Murphy, Matthew J. McKenzie and Adam L. Small of the National Security Division's Counterintelligence and Export Control Section. Prosecutors from the U.S. Attorney's Office for the Western District of Washington assisted with this case.

Friday, February 15, 2019

Chinese National Sentenced to Prison for Selling Counterfeit Computer Parts

A Beijing, China man was sentenced today to 54 months in federal prison for directing the shipment of counterfeit computer-networking equipment into the Southern District of Texas.

Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and U.S. Attorney Ryan K. Patrick for the Southern District of Texas made the announcement.

Ruiyang Li, 40, was sentenced today to serve 54 months in federal prison by U.S. District Judge Ewing Werlein Jr. The court reserved the determination of restitution to the victims of Li's trademark counterfeiting including Cisco Systems Inc., The Hewlett-Packard Company and Intel Corporation until a later date. Because Li is not a U.S. citizen, he is expected to be deported after serving his prison sentence.

From at least 2007 until in or about June 2017, Li directed the shipment of counterfeit computer-networking equipment into the Southern District of Texas, first when selling to a retailer in Magnolia, Texas, and eventually when selling to law enforcement acting in an undercover capacity. Over this time period, Li sold counterfeit networking products through several business entities, often hiding behind layers of personal and corporate aliases to evade detection by law enforcement. Li also used various means to conceal his unlawful conduct, including by sending and receiving payments using accounts that did not appear connected, at least publicly, to companies trafficking in illicit products. Li and his customers would also agree to mislabel packages, break up shipments into separate components, alter destination addresses and use multiple forwarding companies based in the United States. These methods, in Li's mind, made shipping counterfeit parts "safer," which in practice meant delaying or complicating detection by U.S. authorities.

State and local governments rely on complex computer networking technology, including the transceivers and other parts that were trafficked in this case, to manage critical data and operations. This same technology is also prominent in banks, hospitals, air traffic control installations, power plants and other essential infrastructure. Because counterfeit parts are often not subject to stringent manufacturing requirements, they present a significant health and safety risk to communities across the United States.

The case was investigated by U.S. Immigration and Customs Enforcement's Homeland Security Investigations, with significant assistance from U.S. Customs and Border Protection. The case was prosecuted by Senior Trial Attorney Timothy C. Flowers of the Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Jay Hileman.

Thursday, February 14, 2019

One American and One Chinese National Indicted in Tennessee for Conspiracy to Commit Theft of Trade Secrets and Wire Fraud

A grand jury sitting in Greeneville, Tennessee has returned an indictment against Xiaorong You, a/k/a Shannon You, 56, of Lansing, Michigan, and Liu Xiangchen, 61, of Shandong Province, China for conspiracy to steal trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings. You was also indicted on seven counts of theft of trade secrets and one count of wire fraud.

Assistant Attorney General National Security John C. Demers, U.S. Attorney J. Douglas Overbey of the Eastern District of Tennessee, FBI Executive Assistant Director for the National Security Branch Jay Tabb, and Special Agent in Charge Troy Sowers of the FBI's Knoxville Field Office made the announcement.

"The conduct alleged in today's indictment exemplifies the rob, replicate and replace approach to

technological development,” said Assistant Attorney General Demers. “Xiaorong You is accused of an egregious, premediated theft and transfer of trade secrets worth more than \$100 million for the purpose of setting up a Chinese company that would compete with the American companies from which the trade secrets were stolen. Unfortunately, China continues to use its national programs, like the ‘Thousand Talents,’ to solicit and reward the theft of our nation’s trade secrets and intellectual property, but the Justice Department will continue to prioritize investigations like these, to ensure that China understands that this criminal conduct is not an acceptable business or economic development practice.”

“Our office is committed to working closely with our federal, state and local partners to identify and prosecute those who engage in illegal and deceptive practices to steal trade secret and protected information from companies who spend millions of dollars to develop it,” said U.S. Attorney Overbey. “Not only can theft of this information be potentially devastating to our American companies, it could also pose a threat to our overall national and economic security.”

“The facts laid out in this indictment show the conspirators engaged in blatant criminal activity,” said Executive Assistant Director Tabb. “They didn’t stop at going after technical secrets belonging to just one company. They allegedly targeted multiple companies and made off with trade secrets at an estimated value of almost 120 million dollars. As this case demonstrates, the FBI is determined to do everything possible to bring to justice those who try to steal secrets belonging to American companies.”

"As this indictment highlights, theft of trade secrets from American companies is an emerging economic threat, even here in East Tennessee," said Special Agent in Charge Sowers. "The tireless work of our agents and prosecutors in this case underscores the FBI's commitment to protecting American ingenuity."

The BPA-free trade secrets allegedly stolen by these individuals belonged to multiple owners and cost an estimated total of at least \$119,600,000 to develop. Until recently, bisphenol-A (BPA) was used to coat the inside of cans and other food and beverage containers to help minimize flavor loss, and prevent the container from corroding or reacting with the food or beverage contained therein. However, due to the discovered potential harmful effects of BPA, companies began searching for BPA-free alternatives. These alternatives are difficult and expensive to develop.

From December 2012 through Aug. 31, 2017, You was employed as Principal Engineer for Global Research by a company in Atlanta, which had agreements with numerous companies to conduct research and development, testing, analysis and review of various BPA-free technologies. Due to her extensive education and experience with BPA and BPA-free coating technologies, she was one of a limited number of employees with access to trade secrets belonging to the various owners. From approximately September 2017 through June 2018, You was employed as a packaging application development manager for a company in Kingsport, Tennessee, where she was one of a limited number of employees with access to trade secrets belonging to that company.

Details of the conspiracy are included in the indictment on file with the U.S. District Court. The indictment alleges that You, Liu, and a third co-conspirator formulated a plan in which You would exploit her employment with the two American employers to steal trade secrets and provide the information for the economic benefit of trade secrets the Chinese company that Liu managed, which would manufacture and profit from products developed using the stolen trade secrets. In exchange, Liu would cause the Chinese company to reward You for her theft, by helping her receive the Thousand Talent and another financial award, based on the trade secrets she stole, and by giving You an ownership share of a new company that would “own” the stolen trade secrets in China. The conspirators also agreed to compete with U.S. and foreign companies, including some of the owners of the stolen trade secrets, in China and elsewhere, by selling products designed,

developed and manufactured using the stolen trade secrets.

The charges contained in this indictment are merely allegations, and the defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law.

The case is being investigated by the FBI's Knoxville Field Office.

The government's case is being prosecuted by the Eastern District of Tennessee and the National Security Division's Counterintelligence and Export Control Section.

Monday, January 28, 2019

Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice

Huawei Corporate Entities Conspired to Steal Trade Secret Technology and Offered Bonus to Workers who Stole Confidential Information from Companies Around the World

A 10-count indictment unsealed today in the Western District of Washington State charges Huawei Device Co., Ltd. and Huawei Device Co. USA with theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice. The indictment, returned by a grand jury on January 16, details Huawei's efforts to steal trade secrets from Bellevue, Washington based T-Mobile USA and then obstruct justice when T-Mobile threatened to sue Huawei in U.S. District Court in Seattle. The alleged conduct described in the indictment occurred from 2012 to 2014, and includes an internal Huawei announcement that the company was offering bonuses to employees who succeeded in stealing confidential information from other companies.

"Today we are announcing that we are bringing criminal charges against telecommunications giant Huawei and its associates for nearly two dozen alleged crimes" Acting Attorney General Matthew G. Whitaker said. "As I told Chinese officials in August, China must hold its citizens and Chinese companies accountable for complying with the law. I'd like to thank the many dedicated criminal investigators from several different federal agencies who contributed to this investigation and the Department of Justice attorneys who are moving the prosecution efforts forward. They are helping us uphold the rule of law with integrity."

"The charges unsealed today clearly allege that Huawei intentionally conspired to steal the intellectual property of an American company in an attempt to undermine the free and fair global marketplace," said FBI Director Wray. "To the detriment of American ingenuity, Huawei continually disregarded the laws of the United States in the hopes of gaining an unfair economic advantage. As the volume of these charges prove, the FBI will not tolerate corrupt businesses that violate the laws that allow American companies and the United States to thrive."

"This indictment shines a bright light on Huawei's flagrant abuse of the law especially its efforts to steal valuable intellectual property from T-Mobile to gain unfair advantage in the global marketplace," said First Assistant U.S. Attorney Annette L. Hayes of the Western District of Washington. "We look forward to presenting the evidence of Huawei's crimes in a court of law, and proving our case beyond a reasonable doubt. Fair competition and respect for the rule of law is essential to the functioning of our international economic system."

According to the indictment, in 2012 Huawei began a concerted effort to steal information on a T-Mobile phone-testing robot dubbed "Tappy." In an effort to build their own robot to test phones before they

were shipped to T-Mobile and other wireless carriers, Huawei engineers violated confidentiality and non-disclosure agreements with T-Mobile by secretly taking photos of “Tappy,” taking measurements of parts of the robot, and in one instance, stealing a piece of the robot so that the Huawei engineers in China could try to replicate it. After T-Mobile discovered and interrupted these criminal activities, and then threatened to sue, Huawei produced a report falsely claiming that the theft was the work of rogue actors within the company and not a concerted effort by Huawei corporate entities in the United States and China. As emails obtained in the course of the investigation reveal, the conspiracy to steal secrets from T-Mobile was a company-wide effort involving many engineers and employees within the two charged companies.

As part of its investigation, FBI obtained emails revealing that in July 2013, Huawei offered bonuses to employees based on the value of information they stole from other companies around the world, and provided to Huawei via an encrypted email address.

Under the maximum sentencing provisions applicable to corporate entities, Conspiracy and Attempt to Commit Trade Secret Theft are punishable by a fine of up to \$5,000,000 or three times the value of the stolen trade secret, whichever is greater. Wire Fraud and Obstruction of Justice are punishable by a fine of up to \$500,000.

The charges contained in the indictment are only allegations. A defendant is presumed innocent unless and until proven guilty beyond a reasonable doubt in a court of law. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, the sentencing of the defendants will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

The case is being investigated by the FBI. The case is being prosecuted by Assistant U.S. Attorneys Todd Greenberg and Thomas Woods of the Western District of Washington, with assistance from the Department of Justice’s National Security Division’s Counterintelligence and Export Control Section.

U.S. Attorney Brian T. Moran has been recused from this matter because of legal representations he undertook before he joined the Department of Justice. Per direction from ethics officials in the Department of Justice, First Assistant U.S. Attorney Annette L. Hayes will act as U.S. Attorney with respect to this matter pursuant to the authority conferred by 28 U.S.C. § 515.

Monday, January 28, 2019

Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud

Huawei Device USA Inc. and Huawei’s Iranian Subsidiary Skycom Also Named Defendants

Other Charges Include Money Laundering, Conspiracy to Defraud the United States, Obstruction of Justice and Sanctions Violations

A 13-count indictment was unsealed earlier today in federal court in Brooklyn, New York, charging four defendants,[1] including Huawei Technologies Co. Ltd. (Huawei), the world’s largest telecommunications equipment manufacturer, with headquarters in the People’s Republic of China (PRC) and operations around the world. The indicted defendants include Huawei and two Huawei affiliates – Huawei Device USA Inc. (Huawei USA) and Skycom Tech Co. Ltd. (Skycom) – as well as Huawei’s Chief Financial Officer (CFO) Wanzhou Meng (Meng).

The defendants Huawei and Skycom are charged with bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA are charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern District of New York. Meng is charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud.

Acting U.S. Attorney General Matthew G. Whitaker, Secretary Kirstjen Nielsen of the U.S. Department of Homeland Security, Secretary Wilbur Ross of the U.S. Department of Commerce, U.S. Attorney Richard P. Donoghue for the Eastern District of New York, FBI Director Christopher A. Wray, Assistant Attorney General Brian A. Benzckowski of the Justice Department's Criminal Division and Assistant Attorney General John C. Demers of the National Security Division, announced the charges.

“Today we are announcing that we are bringing criminal charges against telecommunications giant Huawei and its associates for nearly two dozen alleged crimes,” said Acting Attorney General Whitaker. “As I told Chinese officials in August, China must hold its citizens and Chinese companies accountable for complying with the law. I’d like to thank the many dedicated criminal investigators from several different federal agencies who contributed to this investigation and the Department of Justice attorneys who are moving the prosecution efforts forward. They are helping us uphold the rule of law with integrity.”

“As charged in the indictment, Huawei and its Chief Financial Officer broke U.S. law and have engaged in a fraudulent financial scheme that is detrimental to the security of the United States,” said Secretary Nielsen. “They willfully conducted millions of dollars in transactions that were in direct violation of the Iranian Transactions and Sanctions Regulations, and such behavior will not be tolerated. The Department of Homeland Security is focused on preventing nefarious actors from accessing or manipulating our financial system, and we will ensure that legitimate economic activity is not exploited by our adversaries. I would like to thank ICE Homeland Security Investigations for their exceptional work on this case.”

“For years, Chinese firms have broken our export laws and undermined sanctions, often using U.S. financial systems to facilitate their illegal activities,” said Secretary Ross. “This will end. The Trump Administration continues to be tougher on those who violate our export control laws than any administration in history. I commend the Commerce Department’s Office of Export Enforcement, and our partners in the FBI, Justice Department, Department of Defense, and Department of Homeland Security for their excellent work on this case.”

“As charged in the indictment, Huawei and its subsidiaries, with the direct and personal involvement of their executives, engaged in serious fraudulent conduct, including conspiracy, bank fraud, wire fraud, sanctions violations, money laundering and the orchestrated obstruction of justice,” stated U.S. Attorney Donoghue. “For over a decade, Huawei employed a strategy of lies and deceit to conduct and grow its business. This Office will continue to hold accountable companies and their executives, whether here or abroad, that commit fraud against U.S. financial institutions and their international counterparts and violate U.S. laws designed to maintain our national security.” Mr. Donoghue thanked the FBI, U.S. Immigration and Customs Enforcement’s Homeland Security Investigations (HSI), U.S. Department of Commerce Office of Export Enforcement (OEE) and the Defense Criminal Investigative Service (DCIS) agents who are investigating this case for their tireless work and dedication.

“These charges lay bare Huawei’s alleged blatant disregard for the laws of our country and standard global business practices,” said FBI Director Wray. “Companies like Huawei pose a dual threat to both our economic and national security, and the magnitude of these charges make clear just how seriously the FBI takes

this threat. Today should serve as a warning that we will not tolerate businesses that violate our laws, obstruct justice, or jeopardize national and economic well-being.”

* * * *

Overview of the Indictment

The charges in this case relate to a long-running scheme by Huawei, its CFO, and other employees to deceive numerous global financial institutions and the U.S. government regarding Huawei’s business activities in Iran. As alleged in the indictment, beginning in 2007, Huawei employees lied about Huawei’s relationship to a company in Iran called Skycom, falsely asserting it was not an affiliate of Huawei. The company further claimed that Huawei had only limited operations in Iran and that Huawei did not violate U.S. or other laws or regulations related to Iran. Most significantly, after news publications in late 2012 and 2013 disclosed that Huawei operated Skycom as an unofficial affiliate in Iran and that Meng had served on the board of directors of Skycom, Huawei employees, and in particular Meng, continued to lie to Huawei’s banking partners about Huawei’s relationship with Skycom. They falsely claimed that Huawei had sold its interest in Skycom to an unrelated third party in 2007 and that Skycom was merely Huawei’s local business partner in Iran. In reality, Skycom was Huawei’s longstanding Iranian affiliate, and Huawei orchestrated the 2007 sale to appear as an arm’s length transaction between two unrelated parties, when in fact Huawei actually controlled the company that purchased Skycom.

As part of this scheme to defraud, Meng allegedly personally made a presentation in August 2013 to an executive of one of Huawei’s major banking partners in which she repeatedly lied about the relationship between Huawei and Skycom.

According to the indictment, Huawei relied on its global banking relationships for banking services that included processing U.S.-dollar transactions through the United States. U.S. laws and regulations generally prohibited these banks from processing transactions related to Iran through the United States. The banks could have faced civil or criminal penalties for processing transactions that violated U.S. laws or regulations. Relying on the repeated misrepresentations by Huawei, these banks continued their banking relationships with Huawei. One bank cleared more than \$100 million worth of Skycom-related transactions through the United States between 2010 and 2014.

In furtherance of this scheme to defraud, and as alleged in the indictment, Huawei and its principals repeatedly lied to U.S. government authorities about Huawei’s business in Iran in submissions to the U.S. government, and in responses to government inquiries. For example, Huawei provided false information to the U.S. Congress regarding whether Huawei’s business in Iran violated any U.S. law. Similarly, as indicated in the indictment, in 2007 months before Huawei orchestrated the purported sale of Skycom to another Huawei-controlled entity Huawei’s founder falsely stated to FBI agents that Huawei did not have any direct dealings with Iranian companies and that Huawei operated in compliance with all U.S. export laws.

After one of Huawei’s major global banking partners (identified as Financial Institution 1 in the indictment) decided to exit the Huawei relationship in 2017 because of Huawei’s risk profile, Huawei allegedly made additional misrepresentations to several of its remaining banking partners in an effort to maintain and expand those relationships. Huawei and its principals are alleged to have repeatedly and falsely claimed that Huawei had decided to terminate its banking relationship with Financial Institution 1, when in fact it was Financial Institution 1 that had decided to terminate the banking relationship. Through these misrepresentations, Huawei was able to continue its banking relationships with its other banks.

In 2017, when Huawei became aware of the government's investigation, Huawei and its subsidiary Huawei USA allegedly tried to obstruct the investigation by making efforts to move witnesses with knowledge about Huawei's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and by concealing and destroying evidence of Huawei's Iran-based business that was located in the United States.

In December 2018, Canadian authorities apprehended Meng in Vancouver pursuant to a provisional arrest warrant issued under Canadian law. The U.S. government is seeking Meng's extradition to the United States.

The charges in the indictment are merely allegations, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

The indictment unsealed today is assigned to U.S. District Judge Ann M. Donnelly of the Eastern District of New York.

The government's investigation is ongoing.

The investigation is being jointly conducted by the FBI's New York Field Office, HSI's New York Field Office, OEE's New York Field Office, and DCIS's Southwest and Northeast Field Offices. Agents from the FBI, HSI, and OEE offices in Dallas provided significant support and assistance. The government's case is being handled by the National Security and Cybercrime and Business and Securities Fraud Sections of the U.S. Attorney's Office for the Eastern District of New York, the Justice Department's Criminal Division's Money Laundering and Asset Recovery Section (MLARS), and the Justice Department's National Security Division's Counterintelligence and Export Control Section (CES).

Assistant U.S. Attorneys Alexander A. Solomon, Julia Nestor, David K. Kessler, Kaitlin Farrell, and Sarah Evans, MLARS Trial Attorneys Laura Billings and Christian Nauvel, and CES Trial Attorneys Thea D. R. Kendler and David Lim are in charge of the prosecution, with assistance provided by Assistant U.S. Attorney Mark Penley of the Northern District of Texas, Assistant U.S. Attorneys Brian Morris and Brendan King of the Eastern District of New York's Civil Division and Trial Attorneys Andrew Finkelman and Margaret O'Malley of DOJ's Office of International Affairs. Additional Criminal Division and National Security Division Trial Attorneys and Assistant U.S. Attorneys within U.S. Attorney's Offices for the Northern District of Texas, the Eastern District of Texas, and the Northern District of California have provided valuable assistance with various aspects of this investigation.

The Defendants:

Huawei Technologies Co. Ltd.

Huawei Device USA Inc.

Skycom Tech Co. Ltd.

Meng Wanzhou, also known as "Cathy Meng" and "Sabrina Meng"

Age: 46

Residence: People's Republic Of China

E.D.N.Y. Docket No. 18-CR-457 (AMD)

[1] The indictment charges other individuals who have not yet been apprehended and whose names will not be publicly released at this time.

Wednesday, December 5, 2018

Former Head of Organization Backed by Chinese Energy Conglomerate Convicted of International Bribery, Money Laundering Offenses

Schemed to Bribe the President of Chad, President and Foreign Minister of Uganda

A federal jury in New York City today convicted the head of a nongovernmental organization (NGO) based in Hong Kong and Virginia on seven counts for his participation in a multi-year, multimillion-dollar scheme to bribe top officials of Chad and Uganda in exchange for business advantages for a Chinese oil and gas company, announced Assistant Attorney General Brian A. Benczkowski of the Justice Department's Criminal Division and U.S. Attorney Geoffrey S. Berman of the Southern District of New York.

Chi Ping Patrick Ho, aka "Patrick C.P. Ho," aka "He Zhiping," 69, of Hong Kong, China, was found guilty today after a one-week jury trial before U.S. District Judge Loretta A. Preska in the Southern District of New York of one count of conspiring to violate the Foreign Corrupt Practices Act (FCPA), four counts of violating the FCPA, one count of conspiring to commit international money laundering and one count of committing international money laundering. Ho is scheduled to be sentenced before Judge Preska on March 14, 2019, at 10:00 a.m. EDT.

"Patrick Ho paid millions of dollars in bribes to the leaders of two African countries to secure contracts for a Chinese conglomerate," said Assistant Attorney General Benczkowski. "Today's trial conviction demonstrates the Criminal Division's commitment to prosecuting those who seek to utilize our financial system to secure unfair competition advantages through corruption and bribery."

"Patrick Ho now stands convicted of scheming to pay millions in bribes to foreign leaders in Chad and Uganda, all as part of his efforts to corruptly secure unfair business advantages for a multibillion-dollar Chinese energy company," said U.S. Attorney Berman. "As the jury's verdict makes clear, Ho's repeated attempts to corrupt foreign leaders were not business as usual, but criminal efforts to undermine the fairness of international markets and erode the public's faith in its leaders."

According to evidence presented at trial, Ho was involved in two bribery schemes to pay top officials of Chad and Uganda in exchange for business advantages for CEFC China, a Shanghai-based multibillion-dollar conglomerate that operates internationally in multiple sectors, including oil, gas, and banking. At the center of both schemes was Ho, the head of a nongovernmental organization based in Hong Kong and Arlington, Virginia, the China Energy Fund Committee (the "CEFC NGO"), which held "Special Consultative Status" with the United Nations (UN) Economic and Social Council. CEFC NGO was funded by CEFC China.

According to the evidence presented at trial, in the first scheme (the "Chad Scheme"), Ho, on behalf of CEFC China, offered a \$2 million cash bribe, hidden within gift boxes, to Idriss Déby, the President of Chad, in an effort to obtain valuable oil rights from the Chadian government. In the second scheme (the "Uganda Scheme"), Ho caused a \$500,000 bribe to be paid, via wires transmitted through New York, New York, to an account designated by Sam Kutesa, the Minister of Foreign Affairs of Uganda, who had recently completed his term as the President of the UN General Assembly. Ho also schemed to pay a \$500,000 cash bribe to Yoweri Museveni, the President of Uganda, and offered to provide both Kutesa and Museveni with additional corrupt benefits by "partnering" with them in future joint ventures in Uganda.

The Chad Scheme

According to the evidence presented at trial, the Chad Scheme began in or about September 2014 when Ho flew into New York, New York to attend the annual UN General Assembly. At that time, CEFC China was working to expand its operations to Chad and wanted to meet with President Déby as quickly as possible. Through a connection, Ho was introduced to Cheikh Gadio, the former Minister of Foreign Affairs of Senegal, who had a personal relationship with President Déby. Ho and Gadio met in midtown Manhattan, New York where Ho enlisted Gadio to assist CEFC China in obtaining access to President Déby.

Gadio connected Ho and CEFC China to President Déby. In an initial meeting in Chad in November 2014, President Déby described to Ho and CEFC China executives certain lucrative oil rights that were available for CEFC China to acquire. Following that meeting, Gadio advised Ho and CEFC China to send a technical team to Chad to investigate the oil rights and make an offer to President Déby. Instead, Ho insisted on a prompt second meeting with the President. The second meeting took place a few weeks later, in December 2014. Ho led a CEFC China delegation, which flew into Chad on a corporate jet with \$2 million cash concealed within several gift boxes. At the conclusion of a business meeting with President Déby, Ho and the CEFC China executives presented President Déby with the gift boxes.

To the surprise of Ho and the CEFC China executives, President Déby rejected the \$2 million bribe offer. Ho subsequently drafted a letter to President Déby claiming that the cash had been intended as a donation to Chad. Ultimately, Ho and CEFC China did not obtain the unfair advantage that they had sought through the bribe offer, and by mid-2015, Ho had turned his attention to a different “gateway to Africa”: Uganda.

The Uganda Scheme

According to the evidence presented at trial, the Uganda Scheme began around the same time as the Chad Scheme, when Ho was in New York, New York for the annual UN General Assembly. Ho met with Sam Kutesa, who had recently begun his term as the 69th President of the UN General Assembly (“PGA”). Ho, purporting to act on behalf of CEFC NGO, met with Kutesa and began to cultivate a relationship with him. During the year that Kutesa served as PGA, Ho and Kutesa discussed a “strategic partnership” between Uganda and CEFC China for various business ventures, to be formed once Kutesa completed his term as PGA and returned to Uganda.

In or about February 2016 after Kutesa had returned to Uganda and resumed his role as Foreign Minister, and Yoweri Museveni (Kutesa’s relative) had been reelected as the President of Uganda Kutesa solicited a payment from Ho, purportedly for a charitable foundation that Kutesa wished to launch. Ho agreed to provide the requested payment, but simultaneously requested, on behalf of CEFC China, an invitation to Museveni’s inauguration, business meetings with President Museveni and other high-level Ugandan officials, and a list of specific business projects in Uganda that CEFC China could participate in.

Hickey, Adam (NSD)

From: Hickey, Adam (NSD)
Sent: Tuesday, May 7, 2019 7:35 AM
To: Parson, Rusty (JMD)
Cc: Raman, Sujit (ODAG); Champoux, Mark (OLP)
Subject: RE: Army War College visit May 8
Attachments: China Initiative - Army War College 2019.pptx

Rusty, here are some slides I might use for the China Initiative portion of the discussion. Thanks,

Adam

From: Champoux, Mark (OLP (b)(6))
Sent: Wednesday, May 1, 2019 6:14 PM
To: Hickey, Adam (NSD) (b)(6); Raman, Sujit (ODAG (b)(6))
Cc: Parson, Rusty (JMD (b)(6))
Subject: Army War College visit May 8

Adam and Sujit,

Thanks again for making yourselves available to discuss China and Russia issues with the Army War College policy group that will be here on May 8, from 10:15 to 11:15 (followed by cryptocurrency from 11:15 to 11:45 if you want to stick around; Downing will be joining for that part).

Rusty Parson, copied here, is organizing the event and will get you any additional info you need and coordinate any logistics (e.g., if you have any slides you'd like to show, etc.). We'll also get you a calendar invite.

Again, many thanks. We think this will be well worth the time.

MC

(b)(6)