As far as downgrades/crossposting for ICA purposes—like [redacted] said, as long as we can get to the [redacted] level we're good. NSA has been fantastic about making election-relevant [redacted] usable, and we really appreciate your commitment to that.

[redacted]
Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]
[redacted]
[redacted]

From: [redacted] NSA [redacted] USA GOV [redacted]
Sent: Friday, November 20, 2020 9:20 AM
To: [redacted] NSA [redacted] USA GOV [redacted] @nsa [redacted]
Cc: [redacted] @nsa [redacted] [redacted] @nsa [redacted] DNI- [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted]
Subject: RE: (U) Note to Election Threat 45 day ICA China Section Drafting Team

Classification: [redacted]

[redacted]

OK, thx. Regarding cross-posting into various [redacted] or downgrading to [redacted] for the 45 day piece, if you make sure there are [redacted] versions, we're good.

[redacted]
CNIO for Cyber and Elections

Cryptologic National Intelligence Officer Council [redacted]
Office of Strategic Analysis [redacted]
Information & Intelligence Analysis [redacted]
Directorate of Operations [redacted]
National Security Agency
Secure: [redacted]
Unclass: [redacted]
Team email: [redacted]

Regards,

[redacted]

From: [redacted] NSA [redacted] USA GOV [redacted]
Sent: Friday, November 20, 2020 8:22 AM
To: [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted]
Cc: [redacted] @nsa [redacted] @nsa [redacted]
Subject: RE: (U) Note to Election Threat 45 day ICA China Section Drafting Team

Classification: [redacted]

All,

[redacted] has heard/received nothing.

We have deliberately massaged our one pending PDB to avoid any direct links to the election. The massive report we have been waiting on has been chopped up into 13 reports that likely will not get out until late next week. Many/all of them will be cross-posted into [redacted] or downgraded to [redacted] so that can be more readily incorporated into the 45-day piece, if needed.

----(U[redacted])----
[redacted]
Strategic Intelligence Analyst
[redacted] China & North Korea Strategic Assessments
ICemail: [redacted]
NSTS: [redacted]
Bldg/Room: [redacted]
----(U[redacted])----

From: [redacted] NSA [redacted] USA GOV [redacted] @nsa [redacted]
Sent: Thursday, November 19, 2020 4:25 PM
To: [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted]

[redacted]@nsa[redacted]
Cc: [redacted]@nsa[redacted]
[redacted]@nsa[redacted]
Subject: RE: (U) Note to Election Threat 45 day ICA China Section Drafting Team

Classification: [redacted]

Hello All,

Greetings…just wanted to touch base to see if anyone has contacted you about this and/or if you are doing any work on this product yet. Thanks in advance.

Regards,

[redacted]

[redacted]
CNIO for Cyber and Elections

Cryptologic National Intelligence Officer Council [redacted]
Office of Strategic Analysis [redacted]
Information & Intelligence Analysis [redacted]
Directorate of Operations [redacted]
National Security Agency
Secure: [redacted]
Unclass: [redacted]
Team email: [redacted]

From: [redacted] NSA [redacted] USA GOV [redacted]
Sent: Wednesday, November 4, 2020 12:58 PM
To: [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted] NSA [redacted] USA GOV [redacted]
Cc: [redacted]@nsa[redacted]

[redacted]@nsa[redacted]
Subject: (U) Note to Election Threat 45 day ICA China Section Drafting Team

Classification: [redacted]

All,

Greetings, hope all is well. I just wanted to send you a note with a few thoughts on this coming project. First, thanks in advance for your work on this product. Second, when you begin communicating with co-drafters across the community, please cc those on the cc line so we can maintain visibility on progress, provide assistance where needed, and help alleviate any potential problems. I also wanted to let you know that we optimally would like to keep [redacted] Let us know if you have any questions. Thx!

Regards,

[redacted]

[redacted]
Cryptologic National Intelligence Officer (CNIO) for Cyber and Election Threats & Security

Cryptologic National Intelligence Officer Council [redacted]
Office of Strategic Analysis [redacted]
Information & Intelligence Analysis [redacted]
Directorate of Operations [redacted]
National Security Agency
Secure: [redacted]
Unclass: [redacted]
Team email: [redacted]@nsa[redacted]

//

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]

Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

==========

Classification: [redacted]

==========

Classification: [redacted]

==========

Classification: [redacted]

==========

Classification: [redacted]

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: Everyone"s favorite topic
Date: Thursday, December 23, 2021 12:52:29 PM

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

[redacted]

Take a minute and read through this report. It cites some of the same intel and logic used in 2020 to say that these same units were NOT engaged in election influence but were instead only issue-focused, to now argue that China IS influencing the [redacted] election. The regional influence, focus on issues, etc. They literally cite as support for their argument some of the same reporting used in the mainline assessment in our minority report.

For example, they cite [redacted] activity as being "the Chinese military" even though in 2020 the IC said we didn't know who it was. *This report describes the same unit that* [redacted] *and I said were influencing the US 2020 election and now characterizes it as an election-influence unit and attributes it to the Chinese Government*. That's a weird coincidence, and one we should highlight for oversight. FBI and [redacted]

We should consider how this looks and on what logical, non-partisan basis the IC makes calls one way or the other. Why is this unit engaged in election influence in the [redacted] and [redacted] "to promote China's interests" but when they do it here it's "issue influence" but somehow not election-related? *It's the same personnel doing the same kind of activity.*

[redacted]
National Intelligence Officer - Cyber
ODNI/National Intelligence Council

Secure: [redacted]
Email: [redacted]
Unclass: [redacted]
Unclass email: [redacted]

==========
Classification: [redacted]

SENSITIVE GOVERNMENT AGENCY

[redacted] PRC [redacted] Aware in Mid-2020 of Collection of U.S. Consumer, Military, Voter Registration Databases; [redacted] Capabilities To Conduct Identity Verification Checks of U.S. Persons

[redacted]

DETAILS (U)

[redacted] PRC [redacted] were aware in [redacted] 2020 [redacted] had [redacted] U.S.-origin databases, [redacted] contain the personally identifiable information (PII) of [redacted] million Americans. [redacted] these databases [redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

[redacted]	[redacted]
[redacted]	U.S. Consumer database [redacted]
[redacted]	U.S. Voter Registration database [redacted]
[redacted]	U.S. Voter Registration databases from [redacted] State Governments of [redacted] Georgia, Iowa [redacted].
[redacted]	Registered U.S. Military Personnel Information database [redacted]

[redacted] comprehensive PII baseline on [redacted] U.S. persons—[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

DTG: 2009251123Z
PRECEDENCE: ROUTINE
INFO PRECEDENCE: ROUTINE
FM DIRECTOR FBI
TO ALL FBI FIELD OFFICES/ROUTINE
INFO 24AF LACKLAND AFB TX/ROUTINE/
543 ISR GP LACKLAND AFB TX/ROUTINE/
AMEMBASSY BEIJING/ROUTINE/
CDR USAFRICOM STUTTGART GE/ROUTINE/
CDR USEUCOM INTEL VAIHINGEN GE/ROUTINE/
CDR USEUCOM VAIHINGEN GE//J2///ROUTINE/
CDR USPACOM HONOLULU HI/ROUTINE/
CDR USPACOM JECG HONOLULU HI/ROUTINE/
CDR USPACOM LO WASHINGTON DC/ROUTINE/
CDR USSTRATCOM ABNCP OFFUTT AFB NE/ROUTINE/
CDR USSTRATCOM OFFUTT AFB NE/ROUTINE/
CDR USSTRATCOM OFFUTT AFB NE//J2/ROUTINE/
CDR USTRANSCOM INTEL CELL SCOTT AFB IL/ROUTINE/
CDR USTRANSCOM SCOTT AFB IL/ROUTINE/
CDR USTRANSCOM TCJ2 SCOTT AFB IL/ROUTINE/
CDRINSCOM FT BELVOIR VA /ROUTINE/
CDRNGIC CHARLOTTESVILLE VA/ROUTINE/
CIA WASHINGTON DC/ROUTINE/
COGARD INTELCOORDCEN WASHINGTON DC/ROUTINE/
DA AMHS WASHINGTON DC/ROUTINE/
DA WASHINGTON DC/ROUTINE/
DCIS WASHINGTON DC/ROUTINE/
DEPT OF ENERGY WASHINGTON DC/ROUTINE/
DEPT OF HOMELAND SECURITY WASHINGTON DC/ROUTINE/
DEPT OF JUSTICE WASHINGTON DC/ROUTINE/
DEPT OF STATE WASHINGTON DC/ROUTINE/
DEPT OF TREASURY WASHINGTON DC//INTEL///ROUTINE/
DIA WASHINGTON DC/ROUTINE/
DIRACIC FT GEORGE G MEADE MD/ROUTINE/
DIRMSIC REDSTONE ARSENAL AL/ROUTINE/

[redacted]

[redacted]

DIRNAVCRIMINVSERV WASHINGTON DC/ROUTINE/
DIRNSA FT GEORGE G MEADE MD/ROUTINE/
DNI WASHINGTON DC/ROUTINE/
DRUG ENFORCEMENT ADMIN HQ WASHINGTON DC/ROUTINE/
DTRA OPSCENTER WASHINGTON DC/ROUTINE/
HQ AFOSI ANDREWS AFB MD/ROUTINE/
HQ AFOSI DOQ ANDREWS AFB MD/ROUTINE/
HQ AFOSI QUANTICO VA/ROUTINE/
HQ NORAD USNORTHCOM INTEL PETERSON AFB CO/ROUTINE/
HQ USNORTHCOM//J2///ROUTINE/
HQ USSOUTHCOM SECURITY AND INTEL MIAMI FL/ROUTINE/
JAC MOLESWORTH RAF MOLESWORTH UK/ROUTINE/
JWAC DAHLGREN VA/ROUTINE/
LEGAT BEIJING/ROUTINE/
MDA WASHINGTON DC/ROUTINE/
NASIC WRIGHT PATTERSON AFB OH/ROUTINE/
NATIONAL SECURITY COUNCIL WASHINGTON DC/ROUTINE/
NGA HQ BETHESDA MD/ROUTINE/
NRO WASHINGTON DC/ROUTINE/
NSA FT GEORGE G MEADE MD/ROUTINE/
ONI WASHINGTON DC/ROUTINE/
SECDEF WASHINGTON DC/ROUTINE/
SECSTATE WASHINGTON DC//INR///ROUTINE/
USCENTCOM INTEL CEN MACDILL AFB FL/ROUTINE/
USSOCOM INTEL MACDILL AFB FL/ROUTINE/
WHITE HOUSE SITUATION ROOM WASHINGTON DC/ROUTINE/
BT

SERIAL: [redacted] IIR 4 212 7305 20

DATE OF PUBLICATION: [redacted] 2009251123Z

FEDERAL BUREAU OF INVESTIGATION

INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE

[redacted]

[redacted]

COUNTRY OR NONSTATE ENTITY: [redacted]United States; China

SUBJECT: [redacted] Chinese Government Production and Export of Fraudulent US Drivers Licenses to Chinese Sympathizers in the United States, in Order to Create Tens of Thousands of Fraudulent Mail-in Votes for US Presidential Candidate Joe Biden, in late August 2020

DATE OF INFORMATION: [redacted] 00 AUG 2020

SUMMARY: [redacted] None.

SOURCE: [redacted] A collaborative source with indirect access, none of whose reporting has been corroborated for less than one year.

CONTEXT: [redacted] The source obtained the information from an identified sub-source, who claimed they obtained the information from unidentified PRC government officials.

WARNING: [redacted] This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. Receiving agencies are requested not to take action based on this raw reporting without prior coordination with the FBI. Unless a conviction in a criminal proceeding occurs, a presumption of innocence exists for any person being reported on in this IIR.

TEXT:

1. [redacted] In late August 2020, the Chinese government had produced a large amount of fraudulent United States drivers licenses that were secretly exported to the United States (NFI). The fraudulent drivers licenses would allow tens of thousands of Chinese students and immigrants sympathetic to the Chinese Communist Party to vote for US Presidential Candidate USPER Joe ((Biden)), despite

[redacted]

[redacted]

not being eligible to vote in the United States. China had collected private US user data from millions of TikTok accounts, to include name, ID and address, which would allow the Chinese government to use real US persons' information to create the fraudulent drivers license. The fraudulent drivers licenses were to include true ID number and true address of US citizens, making them difficult to detect. China planned to use the fraudulent drivers licenses to account for tens of thousands of mail-in votes.

COMMENTS:
1. [redacted] FBI COMMENTS: A persons address information was not a valid field when creating a TikTok account. It was unspecified how China would attain US address data from the application.
2. [redacted] Source is available for re-contact.

TOPIC: [redacted]

FUNCTIONAL CODE: [redacted]

[redacted]

INSTR: [redacted] US Yes. Contact FBIHQ for additional details

DATE OF ACQUISITION: [redacted] 24 AUG 2020

POC: [redacted]
Please direct Requests for Information (RFIs) to [redacted] on [redacted] or [redacted] Advise if the request is time-sensitive, and include a date or time-frame required for a

[redacted]

[redacted]

response. Direct comments, evaluations, and SDRs to [redacted] or [redacted] Request for direct declassification should be sent to [redacted] Requests concerning foreign disclosure and ORCON release should be sent to [redacted] and [redacted] Include the serial number and subject line of the report in the correspondence.

WARNING: [redacted] Report classified [redacted]

==========DISSEMINATION==========

AGENCY: [redacted] CIA; Coast Guard; DEA; DHS; Defense; Energy; FBI; Justice; NGA; NRO; NSA; ODNI; State; Treasury; White House

U.S. MISSION: [redacted] Beijing

MILITARY: [redacted] Air Force; Army; DIA; Defense; Navy

STATE/LOCAL: [redacted] None

==========CLASSIFICATION==========

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

SENSITIVE GOVERNMENT AGENCY

[redacted]

[redacted] PRC [redacted] PRC [redacted] discuss targeting 2024 US elections: [redacted] 2023 information

[redacted]

(U) Correction

[redacted]

[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

(U) Key points

[redacted] The essential element in this report is as follows:

- PRC [redacted] to target the 2024 US elections.

(U) [redacted] Analysis

[redacted] It is unknown if [redacted] were instructed to target unidentified 2024 US elections by [redacted]

(U) Details

[redacted]

[redacted] shared [redacted] data with [redacted] PRC [redacted]

[redacted]

[redacted]

[redacted]

The [redacted] data [redacted] shared [redacted] included [redacted], and voter registration information from Named US state entity 1 (US-1).

(U) Election

[redacted] On [redacted] July, [redacted] wanted to [redacted] the election system as the following year was the US election. [redacted] *This is a reference to an unidentified 2024 election, almost certainly the 2024 US Congressional or Presidential elections.* [redacted] to join an effort to [redacted] an unidentified swing state to observe the voting situation ahead of time. [redacted] requested [redacted] a list of swing states. *This is almost certainly a reference to US electoral swing states, suggesting their discussion is regarding the 2024 US Presidential election.*

[redacted]

[redacted]

[redacted]

[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

SENSITIVE GOVERNMENT AGENCY

[redacted]

[redacted] PRC [redacted] Analysis on U.S. Voter Registration Information [redacted] from Multiple States, [redacted] Conduct U.S. Identity Matching and Public Opinion Analysis; 2019

[redacted]

(U) DETAILS

[redacted] PRC [redacted] analysis on U.S. voter registration data [redacted]. [redacted] contained U.S. voter registration records from the [redacted] Mid-term Elections. [redacted] the [redacted] data [redacted] contained [redacted] personal identifiable information (PII). [redacted] it would be used [redacted] for [redacted] mining PII on U.S. citizens. Additionally, [redacted] the data [redacted] could be used [redacted] to analyze, discover, [redacted] the identities of U.S. citizens [redacted]. [redacted] the [redacted] information would be used to conduct [redacted] opinion [redacted] analysis on the U.S. [redacted] General Election. Furthermore, [redacted] to continue [redacted] state voter registration data.

[redacted]

[redacted]

[redacted]

[redacted]

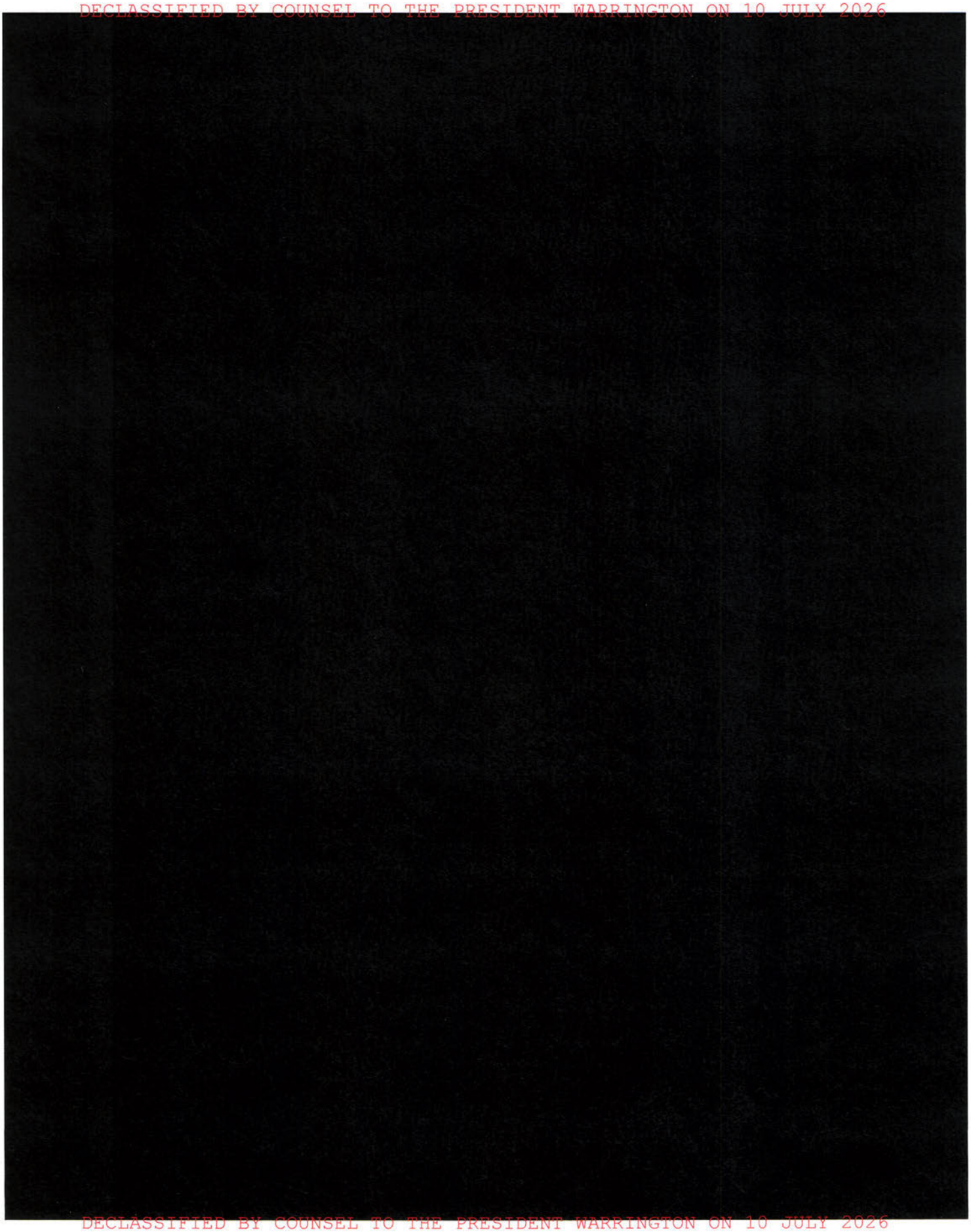
[redacted]

[redacted]

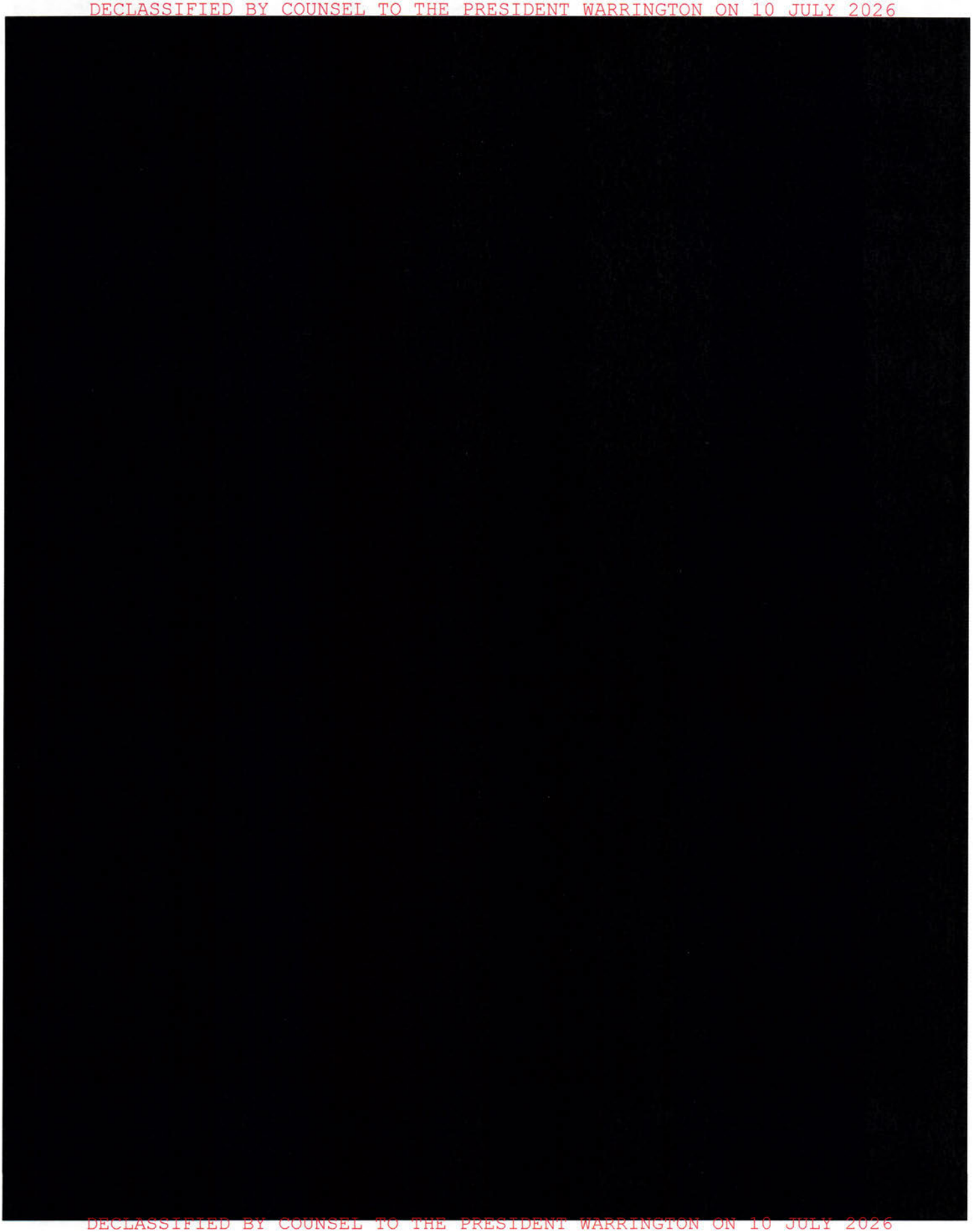
[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

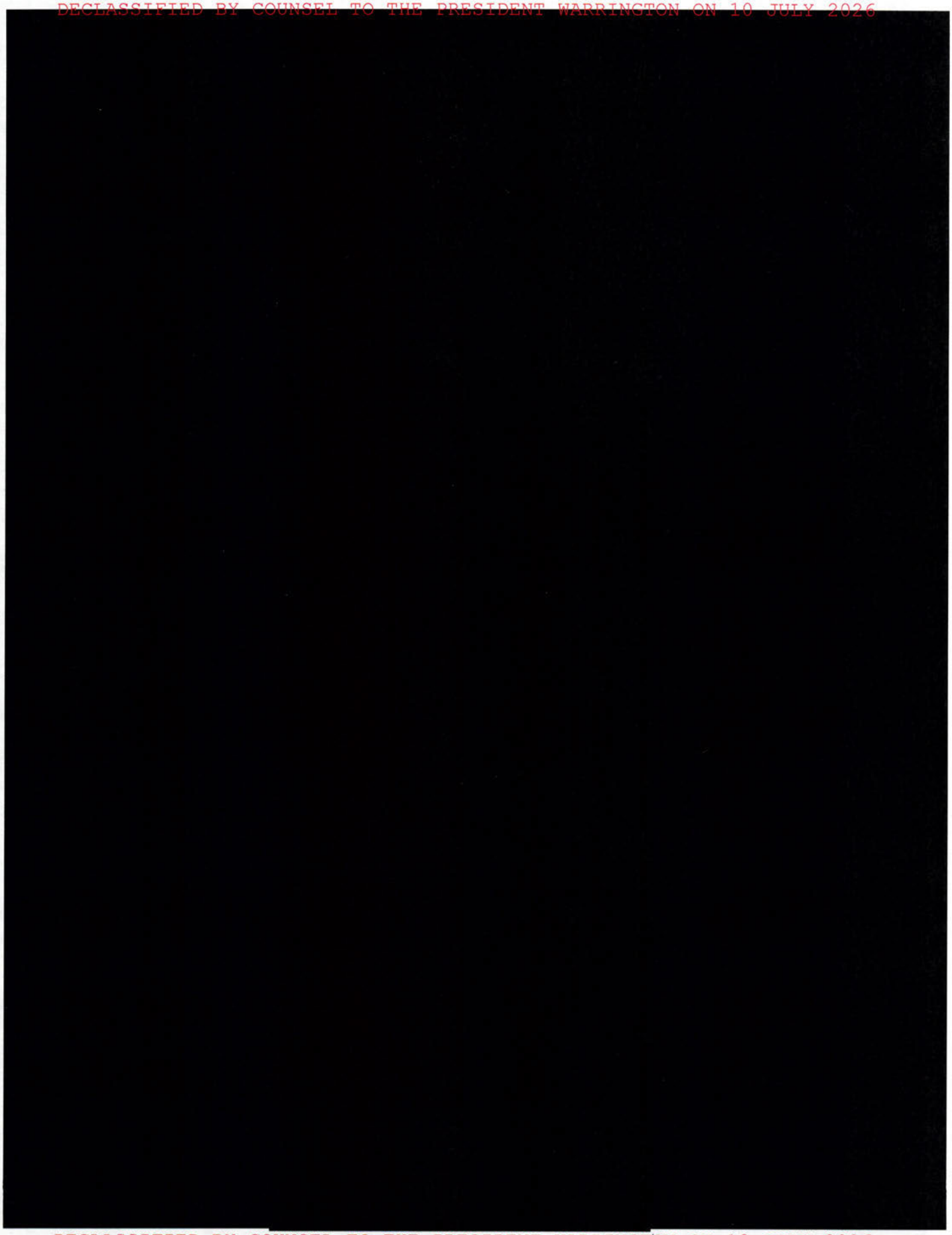


DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026



DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026



DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

From: [redacted] -DNI-
To: [redacted] -DNI- [redacted] -DNI-
Subject: RE: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election
Date: Wednesday, October 07, 2020 9:32:03 AM

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

Hey that is great news. [redacted] is an NSA senior, one of the few seniors that remained analytically focused, so having him on board is a big deal.

From: [redacted] -DNI- [redacted]
Sent: Wednesday, October 7, 2020 9:29 AM
To: [redacted] -DNI- [redacted]
Cc: [redacted] -DNI- [redacted]
Subject: FW: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

[redacted]
Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]
[redacted]
[redacted]

From: [redacted] NSA [redacted]
Sent: Wednesday, October 07, 2020 9:28 AM
To: [redacted] -DNI- [redacted]
Subject: RE: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

I think it speaks exactly to what has been on my mind but what was left out of the mainline IC assessment. I think it looks very good!

[redacted]

****

(U[redacted]

[redacted]

CI SME

East Asia CI Division [redacted]

Operations/IIA/Office of East Asia Pacific

Senior Advocate, English as a Second Language (ESL) Employee Resource Group

[redacted]

(U[redacted]

****

From: [redacted] -DNI- [redacted]

Sent: Tuesday, October 6, 2020 3:40 PM

To: [redacted] NSA [redacted]

Subject: RE: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

[redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========[redacted]==========

Good to know. I've heard a few other similar comments from some analysts in CIA, though not in the main China office. Maybe this will draw them out of the woodwork.

Here's a [redacted] version of the paper. I sent this to [redacted] and [redacted] earlier, but wanted to make sure your team had a chance to take a look.

[redacted]

Director, Election Threat Analysis

National Intelligence Council/DNI Election Threat Executive

[redacted]

[redacted]

[redacted]

From: [redacted] NSA [redacted]

Sent: Tuesday, October 06, 2020 10:48 AM

To: [redacted] -DNI- [redacted]

Subject: RE: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

Thanks. Just for your awareness, as that last COI meeting was going on, everyone around the table at NSA had thoughts similar to what I shared at the meeting. I think many were reticent to express them to the group because FBI and CIA seemed so adamant about their stances. I'm happy to see that we can have the alternative view point. :)

[redacted]

****

(U[redacted]
[redacted]
CI SME
East Asia CI Division [redacted]
Operations/IIA/Office of East Asia Pacific
Senior Advocate, English as a Second Language (ESL) Employee Resource Group
[redacted]
(U[redacted]
****

From: [redacted] -DNI- [redacted]
Sent: Tuesday, October 6, 2020 9:44 AM
To: [redacted] NSA [redacted]
Subject: RE: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========[redacted]==========

Hi[redacted]

Thanks to you too for sharing your thoughts in the last COI meeting. It sounded to me like your take on this is at least somewhat similar to ours. I felt like jumping in to agree with you, but I've burned enough political capital arguing with CIA and FBI about this that I thought it might be more productive for me to sit the discussion out. The positions are not really that far apart, so I'm not sure why so many in the community want to close down the possibility that China might have done or be doing *something.* But, hopefully this piece sparks some more thought and discussion.

[redacted]

Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]

From: [redacted]
Sent: Tuesday, October 06, 2020 8:36 AM
To: [redacted]
Subject: (U) RE: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

I really appreciate this. Thank you very much [redacted]!

[redacted]

****
(U[redacted]
[redacted]
CI SME
East Asia CI Division [redacted]
Operations/IIA/Office of East Asia Pacific
Senior Advocate, English as a Second Language (ESL) Employee Resource Group
[redacted]
(U[redacted]
****

From: [redacted] -DNI- [redacted]
Sent: Monday, October 5, 2020 4:36 PM
To: [redacted]

[redacted]

[redacted]

Cc: [redacted] -DNI- [redacted] -DNI-
[redacted]

Subject: For IC coord by Wed. 7 Oct.: NIC alternative analysis on china/election

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========[redacted]==========

Hello everyone,

As I'm sure many of you have gathered through coord comments, COI discussions, or other conversations, NIO Cyber and I have a somewhat different take on the China/election story than what has appeared in production so far. Rather than continue to argue about this and drive you all nuts, we are opting to publish an alternative analysis NIC memo. We think this is the best way for us to put our perspective on the record while not getting in the way of what the rest of the community wants to say. The lead, in short non-compartmented form, is that we assess that Beijing has taken some low-level, exploratory steps to denigrate the President and shape voter perceptions ahead of the election.

We have really appreciated everyone's efforts to community coord all election-related production, and in that spirit I'd like to offer you all the chance to comment on this piece. However: we are clearly labeling this as alternative analysis and highlighting that it is the perspective of NIO Cyber and myself **only**. Which means that we will most likely not be taking comments on board; we already know most of you disagree. But fear not. We are including a large text box laying out the mainline view. [redacted] and [redacted] have helped us craft this, but we would very much appreciate your input on it to make sure that we're capturing your views accurately. The intention is to show an honest analytic difference, not to set up a straw man version of the IC line to knock down.

Like most of the China/election production, this piece uses [redacted]. The IC Mainline Analysis text box uses [redacted]. Though mostly [redacted] If you have at least [redacted] and would like to coordinate on this box, please let me know. We are looking for input by **COB Wednesday 7 Oct**.

The full piece uses [redacted]. I'm still fixing some formatting issues, but can work with you to get you some version of the paper.

Thank you all—we look forward to continuing conversation on this topic.

[redacted]
Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]
[redacted]
[redacted]

==========

Classification: [redacted]

==========

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

==========

Classification: [redacted]

==========

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

==========

[redacted]

==========

Classified By: [redacted]
Derived From: [redacted]
Dated: [redacted]
Declassify On: [redacted]

Classification: [redacted]

==========

Classification: [redacted]

==========

Classification: [redacted]

==========

Classification: [redacted]

SENSITIVE GOVERNMENT AGENCY

Summary:

Ahead of the 2020 Presidential Elections, China had extensive plans to utilize potential [redacted] and cyber operations to sway public opinion against the Trump Administration and international opinion against the U.S. Government. The China plans were designed to exploit U.S. societal fissures and vulnerabilities, to influence U.S and other audiences, and by extension U.S. government decision-making. The plans addressed several scenarios, including military conflict between the U.S. and China, as well as other potential crises.

The [redacted] operations themes covered a broad range of topics, to exploit what China perceived to be U.S. fissures and vulnerabilities (perceived or real), including:

- Gun proliferation; and
- Immigration policies;
  - Inciting migrant community dissatisfaction with the USG;
  - Instigating demonstrations against the USG's alleged human rights violations against immigrants;
  - Inflaming resentment between anti-immigrant and pro-immigrant communities; and
  - Instigating anti-immigration demonstrations.

China had developed capabilities to project themes on these topics into social media (Tiktok, Facebook, Twitter, YouTube and others), as well as mainstream media through a variety of overt and hidden influencers and media contributors. One of the options included gathering information on senior U.S. government officials to influence public opinion of those officials.

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

SENSITIVE GOVERNMENT AGENCY

[redacted]

[redacted] SUBSTANTIVE REVISION: Network Defense Notice: Publicly Available U.S. Voter Registration Information for Six U.S. States Downloaded from Commercial Websites by PRC CNE Actor in January 2022; Same Actor Attempts to Download Ohio Voter Registration Application; [redacted]

[redacted]

[redacted] This is a revised copy. The State of Oklahoma has been added. In addition, the websites hosting the voter registration records are commercial websites, and that fact has been clarified in the report. Please remove the original report from all manual and computer files.

[redacted]

[redacted] Publicly available U.S. voter registration information for six states was downloaded by a PRC, [redacted], CNE actor on 14 January 2022. The CNE actor [redacted] Colorado, Connecticut, Florida, Michigan, Oklahoma, and Rhode Island voter registration information from U.S. commercial websites and a U.S. IP address. In addition, an Ohio voter registration application was also of interest to the CNE actor, but failed to download.

[redacted]

[redacted]

[redacted]

[redacted]

([redacted]) Voter registration information from at least 2013 through 2021 is publicly available for download from the commercial websites and it appears the PRC CNE actor downloaded the full repositories. This activity represents newly-identified interest by this PRC CNE actor in U.S. elections, and the PII information obtained - to include names, party affiliations, email addresses, physical addresses, and phone numbers - could, in theory, be leveraged to carry out anything from future CNE operations to election influence operations, although the actual motivations for collecting this information is unknown.

[redacted] The victim information was passed to the appropriate agencies for CND response actions.[1]

[redacted]

[redacted] Colorado, Connecticut, Florida, Michigan, Oklahoma, and Rhode Island States' historical U.S. voter registration information from 2013 to 2021 was downloaded by a PRC CNE actor on 14 January 2022 from U.S. commercial websites, and a U.S. IP address hosting, among other things, U.S. state voter registration information. (T1594)[2] On the same day, an Ohio voter registration application was also of interest to the PRC CNE actor, but failed to download from the U.S. State Government's website .

[redacted]

[redacted] While the PRC government has historically demonstrated interest in U.S. elections, this is a newly-identified interest for this individual actor. The U.S. voter registration information is available for public download, with 2021 voter registration information available for some states. The PRC actors could, in theory, leverage the PII information obtained - to include names, party affiliations, email addresses, physical

---

1. [redacted] *CISA and the NCIJTF CYWATCH have established a Victim Notification process that provides a systematic way to contact organizations during cyber incidents. Before anyone outside of the Federal Cybersecurity Centers contacts a U.S. victim, the notification should be deconflicted through CISA and NCIJTF CYWATCH, using the contact information below:* [redacted]

2. [redacted] *According to the MITRE ATT&CK framework, T1594 describes how adversaries may search websites owned by potential victims for information that can be used during targeting. Victim-owned websites may contain a variety of details, including names of departments/divisions, physical locations, and data about key employees such as names, roles, and contact info. These sites may also have details highlighting business operations and relationships.*

[redacted]

[redacted]

[redacted]

addresses, and phone numbers - for anything from future CNE operations to election influence operations, although the actual motivations for collecting this information is unknown.

[redacted]

[redacted] Election security organizations should be aware that U.S. State voter registration information may be hosted on websites outside the control of government agencies, and that APT actors may harvest voter registration information outside the monitoring of election security organizations.

[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

SENSITIVE GOVERNMENT AGENCY

Summary:

Ahead of the 2020 Presidential Elections, China had extensive plans to utilize potential [redacted] and cyber operations to sway public opinion against the Trump Administration and international opinion against the U.S. Government. The China plans were designed to exploit U.S. societal fissures and vulnerabilities, to influence U.S and other audiences, and by extension U.S. government decision-making. The plans addressed several scenarios, including military conflict between the U.S. and China, as well as other potential crises.

The [redacted] operations themes covered a broad range of topics, to exploit what China perceived to be U.S. fissures and vulnerabilities (perceived or real), including:

- Economic recession;
  - Encouraging violent demonstrations and looting, to increase the appearance of social unrest;
  - Intensifying Americans' disapproval of the President of the United States, calling into question his ability to govern; and
  - Overall undermining the legitimacy and public support of the President of the United States.
- Ineffective USG COVID-19 response;
  - Increasing public dissatisfaction with the President of the United States by questioning his fitness to govern and undermining public support for his actions.

China had developed capabilities to project themes on these topics into social media (Tiktok, Facebook, Twitter, YouTube and others), as well as mainstream media through a variety of overt and hidden influencers and media contributors. One of the options included gathering information on senior U.S. government officials to influence public opinion of those officials.

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

WHITE HOUSE TASK FORCE

GOVERNMENT TRANSPARENCY

July 13, 2026

In May 2026, President Trump created the Government Transparency Task Force within the White House Executive Office of the President for the purpose of advising him, through the Counsel to the President, on documents that should be declassified and/or released to the public to further his administration's priorities of transparency and accountability.

Today the Government Transparency Task Force announces the first disclosure of U.S. Intelligence Community records that were declassified last week under the direction of President Trump.

The declassified intelligence reveals that voter registration rolls from at least 18 states (not all identified by name) have been compromised by the People's Republic of China (PRC). Additional intelligence records reveal that more than 200 million voter records were also compromised by the PRC, without state-specific affiliations.

President Trump is alerting Congressional and state government leadership officials to the election infrastructure vulnerabilities in states identified by name in the declassified intelligence records.

- Alaska
- Arkansas
- Colorado
- Connecticut
- District of Columbia
- Florida
- Georgia
- Iowa
- Kansas
- Maryland
- Michigan
- New York
- North Carolina
- Ohio
- Oklahoma
- Rhode Island

SENSITIVE GOVERNMENT AGENCY

Summary:

Ahead of the 2020 Presidential Elections, China had extensive plans to utilize potential [redacted] and cyber operations to sway public opinion against the Trump Administration and international opinion against the U.S. Government. The China plans were designed to exploit U.S. societal fissures and vulnerabilities, to influence U.S and other audiences, and by extension U.S. government decision-making. The plans addressed several scenarios, including military conflict between the U.S. and China, as well as other potential crises.

The [redacted] operations themes covered a broad range of topics, to exploit what China perceived to be U.S. fissures and vulnerabilities (perceived or real), including:

- Racial tensions;
  - Alleging that White people hate Black people;
  - Inciting demonstrations and marches as evidence of racial divides;
  - Increasing the level of conflict between police and anti-racism activists; and
  - Feeding any sense that U.S. law enforcement resents USG and people of color.
- USG tensions with the U.S. military;
- Political party disagreements;
- Congress-Trump Administration conflicts;
- Women's rights;
- U.S. South China Sea policies;
- Alleged U.S. war aspirations; and
- International propaganda.

China had developed capabilities to project themes on these topics into social media (Tiktok, Facebook, Twitter, YouTube and others), as well as mainstream media through a variety of overt and hidden influencers and media contributors. One of the options included gathering information on senior U.S. government officials to influence public opinion of those officials.

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 10 JULY 2026

[redacted]

NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

ALTERNATIVE ANALYSIS

16 October 2020

NICM 2020-09381

[redacted] Making the Case That China Has Taken Some Steps to Influence the Presidential Election

[redacted] ***Scope Note:*** *This memorandum was prepared by the National Intelligence Officer (NIO) for Cyber and the Director, Election Threat Analysis (D/ETA). It offers an alternative perspective to the IC's assessment that China has not attempted to influence the outcome of the 2020 Presidential election. It was provided to the IC for comment before publication but is not an IC-coordinated memorandum.*

[redacted] **The NIO for Cyber and the Director for Election Threat Analysis (D/ETA) assess that Beijing has taken at least some low-level, exploratory steps to undermine the President's reelection chances by denigrating him and shaping voter perceptions. Their assessment differs from the IC's judgment that Beijing has considered but not deployed influence efforts to affect the Presidential election.**

- [redacted] **The NIO and D/ETA assess that Beijing's efforts probably have included overt messaging, nascent online covert influence capabilities, diplomatic measures, and the use of economic leverage.**
- [redacted] **They assess that these efforts probably have not included the use of Beijing's most aggressive options for influencing or interfering in the election, [redacted] because Beijing wants to minimize the risk of blowback and hopes to stabilize the relationship after the election.**
- [redacted] **The NIO and D/ETA have low-to-medium confidence in these assessments because [redacted] much of the available reporting would be consistent with either the mainline or alternative view.**

(U) IC Mainline Judgments

[redacted] The IC, including the NIO for East Asia and other NIC officers, assesses Beijing has not deployed influence efforts intended to change the outcome of the US Presidential election. [redacted] that Chinese leaders desire stability in the US-China relationship and believe they have a range of tools that can achieve their goals regardless of who wins the election. The IC also assesses [redacted] that the election of either candidate will present opportunities and challenges for China probably informs their risk calculus against influencing the election. The IC assesses that Beijing prefers to respond to US actions with restraint to show resolve and preserve the ability to repair relations after the election.

- [redacted]

(U) *This memorandum was prepared by the National Intelligence Officer (NIO) for Cyber and the Director, Election Threat Analysis. Questions may be directed to the NIO* [redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

- In 2019, assessed that "hostile forces" could fabricate claims that Beijing was interfering in the election to demonize China and that no matter who won the election Washington's hardline policies against Beijing were unlikely to change, Chinese noted that Beijing should avoid giving Washington any pretext to "scapegoat" China and to claim that it was interfering in the election, In 2020 also assessed, despite the President's attempts to blame China to divert attention from the pandemic and his electoral prospects, that managing tensions without causing irreparable damage to bilateral relations over the next six months remained in China's interest,

- Chinese leaders may have decided that there is little point to taking the risk of an influence effort because they believe their preferred outcome is probable. As early as this year, Chinese assessed that the pandemic and economic downturn had diminished the President's reelection prospects and since then Beijing has been planning for either electoral outcome and conducting outreach to both candidates and their campaigns,

The IC has seen no indication that Beijing is engaged in an effort to influence the outcome of the presidential election, nor has it observed activity that it assesses is likely the result of such an effort by Beijing. While we have seen Beijing develop other options that could be used to influence the election, we have not seen these capabilities deployed.

- claimed that China had not interfered with the US election and recommended that China speak and act circumspectly when faced with US assertions about Chinese and Russian interference,

- in 2019– to prevent the US President's reelection by suppressing his base,

(U) An Alternative Perspective: Indicators of Influence Efforts

The NIO and D/ETA agree with the large majority of the IC's judgments about China's calculus and approach to the election. They assess, however, that the IC's judgment that no element of the Chinese Government has taken any steps to influence the Presidential election at least through the summer. They also have less confidence than the rest of the IC that China's preparations for influence efforts were not carried out given contradictory reporting

[redacted]

[redacted] The NIO and D/ETA assess [redacted] over the summer [redacted] private sector and open source reporting on influence activities already underway suggest that the Chinese Government has been engaging in at least some level of influence targeting US voters and candidates with the knowledge that their activities could have an effect on the election outcome.

- [redacted] Beijing began taking unspecified steps around [redacted] 2020 to damage the US President's reelection campaign in response to US pressure on China's [redacted] technology sector, [redacted] planning discussions among [redacted] officials to respond to US pressure were taking place at increased frequency, and that senior leaders expected China's semiconductor industry would continue to be damaged if the US President were reelected. Unspecified Chinese Government officials [redacted] that [redacted] Chinese [redacted] expected relief from sanctions if as a result of their efforts, US resolve weakened or a candidate from a named US political party were elected instead of the President being reelected.

- [redacted] 2020, the [redacted] recommended that China collect derogatory "black materials" on the US President, [redacted] and [redacted] official which the [redacted] recommended China "sensationalize" at the appropriate time, [redacted]

[redacted]

- (U//[redacted]) **IC Terminology: Election influence** includes overt and covert influence activities of foreign governments or actors serving as agents of, or on behalf of, foreign governments intended to affect directly or indirectly a US election—including candidates, political parties, voters or their preferences, or political processes. **Election interference** is a subset of election influence targeted at the technical aspects of the election, including voter registration, casting and counting of ballots, and reporting of results.

- [redacted] The NIO and D/ETA assess that China [redacted] intend to at least indirectly affect US candidates, voters' preferences, and political processes, thus meeting the definition of election influence

[redacted]

- [redacted] the Chinese Government had tasked its missions in the US to use Chinese groups and organizations to incite protests in the US to damage the President's public standing and undermine his reelection chances, [redacted]

[redacted]

- The Chinese had assessed that racial conflict would be a large factor in the election, government-affiliated[21] Chinese technology company employees were assisting with a campaign, to covertly incite violence and protests against the US Government.[22][23]

- Chinese were experimenting with the creation of deepfakes intended to denigrate President Trump in response to directives made by to improve Beijing's ability to manipulate public opinion.[24]

During the same period, a pro-China influence network on US social media platforms posted messages supporting Beijing's views that included some English-language content denigrating the President and his Administration's policies. The activities of these networks are consistent with what we would expect to see from intelligence services or similar actors taking steps to build nascent online influence capabilities;[26] the NIO and D/ETA assess that their level of sophistication

- Although we cannot directly tie this network to the Chinese Government, the NIO and D/ETA assess that elements of the government were, at a minimum, aware of and condoned the campaign, and may have directed or conducted it. We base this assessment on the alignment of the content with Beijing's overt messaging themes, its striking similarity to the themes and tactics of previous Chinese influence campaigns that seek to blend their influence operations into broader public discourse, the duration and frequency of the activity spanning several months, the rapidity with which the network created videos in response to world events, and the network's consistent ability to operate outside China's Great Firewall.

- a US social media platform took down a separate cluster of unattributed pro-China accounts that defended a range of Chinese interests, but which also included accounts posing as Americans and posting some US election-focused content. The unidentified actors running these accounts created four groups—one favoring the President, two favoring his opponents, and one that primarily denigrated the President.[28] The accounts have since been shut down, but others could easily take their place and would be difficult to detect;

- The IC assesses that since 2018, China has been researching methods and developing new tools for using online covert influence operations to sway the perspectives of American audiences. Chinese planned a report on the potential impact their covert influence operations could have on the presidential election,

These are developments that the IC has identified as increasing the likelihood that Beijing would seek to influence the election outcome.[c]

China's Possible View of an Influence Campaign

The NIO and D/ETA assess that China may intend much of its broader messaging on issues in US-Chinese relations to also undermine the President's reelection prospects. China probably views as low-risk broad campaigns that emphasize specific issues in the US-China relationship and use a mixture of public statements, diplomatic engagement, private messaging, targeting of campaign donors, and online covert efforts to influence US officials, firms, and the public to oppose the President.[d] Beijing has authorized the conduct of increasingly aggressive overt and covert influence campaigns aimed at criticizing policies of the Administration while trying to avoid blame for interfering in a U.S. Presidential election.

- China, starting in March, launched overt and covert influence efforts to shape the global public narrative regarding Beijing's response to COVID-19 and denigrate the Administration's pandemic response, including by spreading disinformation about the pandemic's origins and publicizing English-language cartoons denigrating the President's handling of the crisis, judging from open source The NIO for Cyber and D/ETA assess that Chinese leaders believe these activities could impact the election.[45]

- In May, a newspaper owned by the Chinese Communist Party claimed that economic measures Beijing could take against supporters of legislation and lawsuits seeking compensation from China over the COVID-19 pandemic may affect US state and congressional races.[46] This was the first time the IC had observed Beijing issue a public warning that suggests it is willing to impose economic costs that could affect US elections, although in 2019 advised to gain leverage over US policy by directing unspecified resources to political swing states

- To help resolve a border dispute with India in Beijing's favor, Chinese planned to disseminate on US social media platforms content" discrediting the President,

[d] The NIO and D/ETA note that in NICM 2019-113 the IC warned that, because China probably would use the same tactics to influence the election as it already uses to influence US policy, we might not detect such a pivot.

- [redacted] Beijing over at least the past year has stepped up its efforts to influence the views and policies of candidates for US political office, [redacted] by targeting their key advisors and financial donors, [redacted] Chinese diplomats acknowledge the sensitivity of targeting donors and have sought to hide such activity from US authorities.[54]

[redacted] Tempering the assessments of the NIO and D/ETA is the fact there is no reporting to suggest that China has engaged in some of the more aggressive measures available to it to influence the US election outcome, such as funneling large donations or trying to compromise voting infrastructure[e] or interfere with mail-in ballots. There are also indications that some elements of state power, such as trade, are being used ambiguously. For example, despite trade disputes, China continues to buy agricultural products as part of the Phase One trade deal which Beijing probably assesses will help the President's reelection bid as well as help stabilize the bilateral relationship. The apparent lack of a whole-of-government campaign to favor one side [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

NIC NATIONAL INTELLIGENCE COUNCIL

[redacted] Comparing Judgments on Chinese Election Influence

[redacted] The NIO for Cyber and the Director for Election Threat Analysis assess that Beijing has taken at least some low-level, exploratory steps to try to undermine the President's reelection chances by denigrating him and shaping voter perceptions ahead of the election. Their assessment differs from the IC's consensus judgments primarily in confidence levels and on whether Beijing has deployed influence efforts to try to affect the outcome of the Presidential election.

[redacted]

✓ Yes ✗ No

China has...	IC JUDGMENT	MINORITY ASSESSMENT
...Broad influence efforts in the United States (diplomatic, business, media)	✓	✓
...Probable preference for Trump's defeat	✓ [redacted]	✓
...Considered an influence effort aimed at the Presidential election	✓	✓
...Prepared options for influence effort in Presidential election	✓	✓
...Concerns about risk versus gain in any influence effort, particularly blowback if discovered	✓ [redacted]	✓ [redacted]
...Prepared for victory by either Trump or Biden	✓	✓ [redacted]
...Avoided a whole-of-government influence effort and any interference with US election systems	✓ [redacted]	✓ [redacted]
...Intends public and diplomatic actions to undercut Trump in election	✗ [redacted]	✓ [redacted]
...Undertaken a few covert influence efforts to undermine Trump's reelection	✗	✓

[redacted]

NIC • 2010-00891

[redacted]

[redacted]

Published online on 01 July 2020

[redacted] China: Cyber Activities Probably Prelude to Election Espionage

[redacted] ***China is probing the presidential campaign for opportunities to tailor collection and gather insight on policy positions on US-Chinese issues.*** US policy on China is a longstanding high collection priority for Beijing, and Chinese cyber actors have conducted such activity in every US presidential election campaign since at least 2008, according to [redacted] open-source reporting.

[redacted] *Chinese cyber actors are targeting US presidential campaign information, probably to gather intelligence that enables future operations.*

- [redacted] Since [redacted] 2018, Chinese cyber actors known in the private sector as APT31—[redacted]—have targeted the personal e-mail accounts of senior US leadership, including officials in the Executive Office of the President and high-ranking officials in multiple Executive Branch organizations, Congress, and the federal judiciary, [redacted]
- [redacted] Since 2017, a separate [redacted] has worked with the [redacted] to enable more stealthy operations by identifying the e-mail addresses of high-level US officials, then requesting that [redacted] obtain or crack the passwords for targeted accounts, [redacted]

[redacted] ***As the 2020 election approaches, the IC has detected Chinese state-sponsored cyber actors targeting the former Vice President's presidential campaign, probably to gather intelligence that could enable future operations, the first instance this election cycle that we have seen them directly targeting a US presidential campaign*** China has also conducted cyber espionage against other US election-related entities, [redacted] The IC assesses that China does not currently intend to covertly interfere to try to sway the outcome of the election, although this activity could enable such operations, if Beijing made a decision to do so.

- [redacted] As of 20 May, APT31 actors had sent spear-phishing e-mails containing tracking links to the G-mail accounts of staffers associated with a presidential campaign, [redacted] On 4 June, Google announced that APT31 was targeting the campaign.
- [redacted] Google and the FBI both briefed campaign officials on the Chinese cyber operations shortly after discovering the activity. Google officials have publicly stated that the spear-phishing attempts were unsuccessful; [redacted]
- [redacted] During the past year, Chinese cyber actors have collected US election-related information from US voter databases, a polling data company, political and nonprofit organizations, fundraisers, and advisory organizations for political campaigns, [redacted]

[redacted] ***APT31's method of sending tracking links suggests that the Chinese operators are mapping out the target network for follow-on approaches, possibly including tasking campaign staffers' e-mail accounts in the Chinese military's signals intelligence system for collection.*** Tracking links collect metadata such as

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]

[redacted]

Internet activity and system information that the operators can use to exploit the accounts and identify other targets of interest.

- [redacted] Knowledge of a campaign official's operating system and software would allow cyber actors to determine whether they could quickly exploit known vulnerabilities or if they needed to develop malware to gain undetected access to the victim's machine.
- [redacted] If a target opened a spear-phishing e-mail with a tracking link—even without clicking on any links—it would confirm an active account for the cyber actors, potentially narrowing the target set for future [redacted] operations.

(U) *For additional information:*

[redacted]

(U) *Produced jointly under the auspices of the Chief of Analysis,* [redacted] *the Federal Bureau of Investigation, and the National Security Agency.*

[redacted]

[redacted]OCUMENT DETAILS

CONTENTS

Produced By: CIA **Product Type:** World Intelligence Review **Document Number:** WIRe2020-05063

Publication Date: 01 Jul 2020

Contact: [redacted] (secure), [redacted] (open)

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: Everyone"s favorite topic
Date: Thursday, December 23, 2021 12:52:29 PM

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

[redacted]

Take a minute and read through this report. It cites some of the same intel and logic used in 2020 to say that these same units were NOT engaged in election influence but were instead only issue-focused, to now argue that China IS influencing the [redacted] election. The regional influence, focus on issues, etc. They literally cite as support for their argument some of the same reporting used in the mainline assessment in our minority report.

For example, they cite [redacted] activity as being "the Chinese military" even though in 2020 the IC said we didn't know who it was. *This report describes the same unit that* [redacted] *and I said were influencing the US 2020 election and now characterizes it as an election-influence unit and attributes it to the Chinese Government*. That's a weird coincidence, and one we should highlight for oversight. FBI and [redacted]

We should consider how this looks and on what logical, non-partisan basis the IC makes calls one way or the other. Why is this unit engaged in election influence in the [redacted] and [redacted] "to promote China's interests" but when they do it here it's "issue influence" but somehow not election-related? *It's the same personnel doing the same kind of activity.*

[redacted]
National Intelligence Officer - Cyber
ODNI/National Intelligence Council

Secure: [redacted]
Email: [redacted]
Unclass: [redacted]
Unclass email: [redacted]

==========
Classification: [redacted]

To: [redacted]
Cc: [redacted]
Subject: FW: ICA Comments

Classification: [redacted]

[redacted]

==========

Hi [redacted]– Forwarding these comments from FBI for your awareness. They had previously told me that Director Wray signed off on the ICA text, and the only changes since then have been downgrades of [redacted] reporting and the DNI's minor initial edits. Most of this we've been over numerous times already. So it's not clear to me if they're backtracking or just commenting for the record.

[redacted]
Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]

From: FLORIS, NIKKI L. (CD) (FBI) [redacted]
Sent: Wednesday, December 30, 2020 1:42 PM
To: [redacted]
Cc: UGORETZ TONYA FBI USA GOV [redacted]
Subject: ICA Comments --[redacted]

Classification: [redacted]

[redacted]

==========

Hi [redacted]

Couple of thoughts on the updated ICA draft, all of which center on the minority view and some of which you have previously heard from the FBI team. Generally speaking, while we are fine with the inclusion of the minority view textbox, we firmly believe the analysis in said text box must comport to the same analytic standards as the rest of the ICA. This is an absolute red line for the FBI. Additionally, we do not support the inclusion of the minority view in the KJs; without proper context and source descriptions, the minority view is given parody to the ICA assessments. Below are some more specific points:

In the first para, the NIO notes that China's leaders also "intended" some of Beijing's efforts to indirectly affect US candidates, etc. The IC has repeatedly stated, based on a body of intelligence, there is no evidence of said intention, though we note there was an awareness of this potential effect. To state this as bluntly as the NIO does, without evidence to support this claim, is extremely misleading.

In the second para, the NIO notes he gives move weight to several clandestine and liaison reports, without any sort of source description whatsoever. By minimizing the source descriptions, clandestine reporting from US or liaison sources of dubious credibility, poorly identified sourcing chains, and minimal track records of reporting is given the same weight as signals intelligence of identified senior Chinese diplomatic and intelligence figures, as well as clandestine reporting of decision making in Beijing from sources with established records of reporting that is generally reliable.

In the last tic, the NIO assesses China "may" also have encouraged protests. There is no evidence of this in the reporting, and the citations associated with this tic certainly do not support this assessment. This is highly misleading and a misrepresentation of the underlying reports.

The final para in the dissent argues that we have collection gaps on the entities that would probably execute influence operations. This point appears to acknowledge that IC collection demonstrated that China's leaders practiced restraint and did not intend to influence the outcome of the election and instead focuses on where collection gaps might miss evidence of the execution of influence ops. This shift in focus by the NIO is inconsistent with earlier portions of the dissent argumentation and argues that US collection did not find what China has actually done. As we've said before, citing the absence of evidence is an absolute red line for us.

Thanks again for all the work on this [redacted]. . . we will continue to stand by for any additional drafts, etc. On a more positive note, the Iran section edits are much improved and we greatly appreciate you working with us on this! I am out of the office tomorrow, but Cynthia is in should you need to reach anyone on the team. We will be back in full force Monday.

Have a wonderful New Year,
Nikki

DAD Nikki L. Floris
Counterintelligence Division
Open: [redacted]
NSTS: [redacted]
FBIHQ Rm [redacted]

==========
Classification: [redacted]