

Atmospherics & Engagements

Friday, October 30, 2020

5:08 PM

TUES

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Reminder of another portal to view FYSA: [REDACTED]

USG Joint Statement confirmed CANCELED

[REDACTED]
[REDACTED]

-- On the USPS issue:

FYSA...In regards to the USPS situation, [REDACTED]
determined the USPS IP addresses had been spoofed and did not originate from the USPS enterprise

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

USPS therefore concludes, it would appear that the IP addresses have been spoofed and the activity did not originate from the UPS enterprise.

[REDACTED]

[REDACTED]
[REDACTED]

[REDACTED]
Friday, October 30, 2020 5:10 PM

[REDACTED] RUSSIA [REDACTED]

[REDACTED] IRAN [REDACTED]
[REDACTED]

[REDACTED] report that came out this evening [REDACTED]
[REDACTED]

Open Source: Upon POTUS speaking at 1400 claiming voter fraud -- New York Times reported that "Russian Internet Trolls are amplifying election fraud claims" and is starting to make rounds on sites such as Reddit [REDACTED]
[REDACTED]

[REDACTED] seeing that a nevada judge has rules that several polling places that were delayed opening this morning due to technical issues need to remain open to 8pm Pacific Time. from what I can see it looks like the the poll books not being updated- doesn't look like an issue with voting machines but it caused some really long lines" [REDACTED]

Comms

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

Friday, October 30, 2020 5:10 PM

See below about guidance from the White House on cyber activity they would like to be notified on. [REDACTED]

[REDACTED] Per our conversation, today I had a discussion surrounding the CYBER ad hoc guidance criteria with the WHSR and the topic of [REDACTED] (e.g. ransomware/malware) came up. The WHSR indicated they would like to be notified of any ransomware/malware attacks on U.S. hospitals regardless if the nature of the event meets [REDACTED] criteria or not. The same holds true for Election related information systems. Essentially if there is an attack on critical infrastructure, specifically Election and Health care related information systems, [REDACTED] still proceed with notifying the WHSR for tracking purposes.

- [REDACTED]
- [REDACTED]
- [REDACTED] engaged in media interviews today, see PAO emails from [REDACTED] that include WaPo, WSJ, NYT news articles and transcript of [REDACTED] media engagement:

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

0700 Email to [REDACTED]

Tuesday, November 3, 2020 7:10 AM

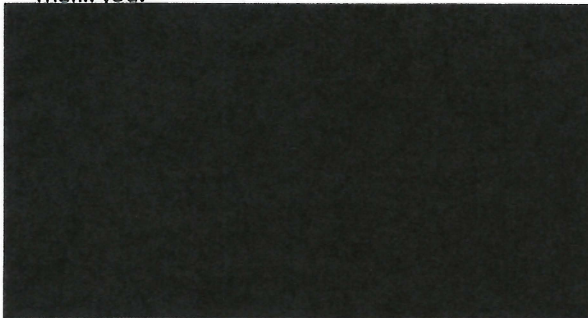
[REDACTED] 0700 [REDACTED] SITREP

believed 600k voter records had been exposed during an intrusion on the county's network," and that this was being considered a "data breach."

- We immediately contacted [REDACTED], [REDACTED] -- who found no information; and requested it be added to [REDACTED] (FBI tipped eventually at 0506)
- Per guidance from the White House [REDACTED] was originally interested in providing this update to the WHSR. We drafted language; however, this was not sent due to the lack of/fragmented information (below):
- Upon identifying the website is where one *checks* their voter registration status -- we inquired:
 - Where did the 600k voter records came into play. → "It's initial reporting. I would think those numbers will change. The 600k was in the initial word of mouth and was not mentioned in the Intake report, they are still confirming these numbers."
 - What time 1617 (Local? MST?) → It was unknown/no clarity was provided.
 - Was the attempt successful? → No.
 - This "breach" did not affect anyone's ability to vote? → Went from "No" to "Unknown"
 - Does this site touch any actual election network (registration database, tabulators, etc.) → "Voter registration database information"
 - How long was the page down? → Unconfirmed
- The information/updates above were provided in fragments in the chat, causing confusion. [REDACTED] to control the updates and provided a summary -- which is the paragraph above and the latest we are tracking. This is the same update that FBI provided in [REDACTED] at 0506.
- Other Info FYI
 - Directions to see website that was down: "If you click on "where do I vote," and then go to the highlighted section in purple "Beballotready.vot," then "check your status," you can enter your information and find your own voter registration information on the website.
 - This is not related to IIR 4 007 0101 21
 - [REDACTED] is on day shift today for any follow-up

Please let us know if there are any questions.

Thank you!



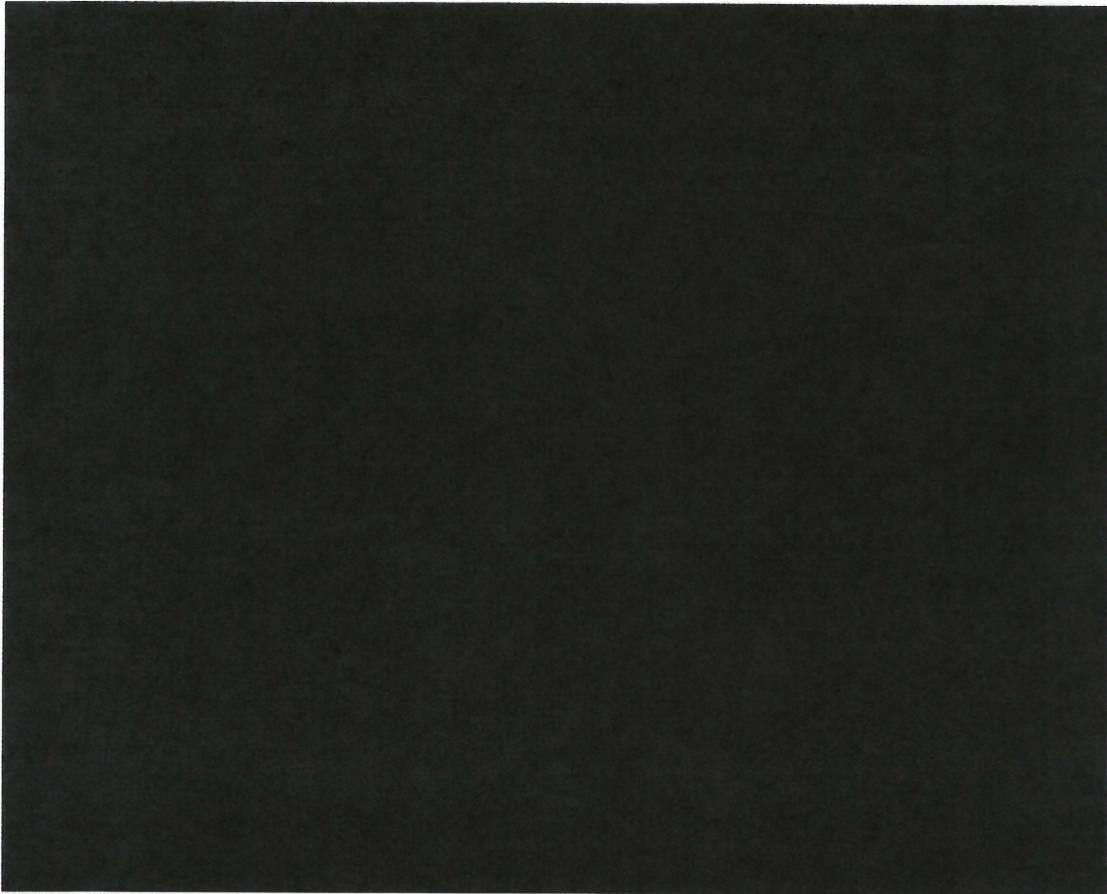
SUBJ: [REDACTED] Update, 0800 - 3 November 2020

Good Morning [REDACTED]

0800 SITREP [REDACTED]

Tuesday, November 3, 2020 12:45 AM

[REDACTED] Update 0910 - 3 November 2020



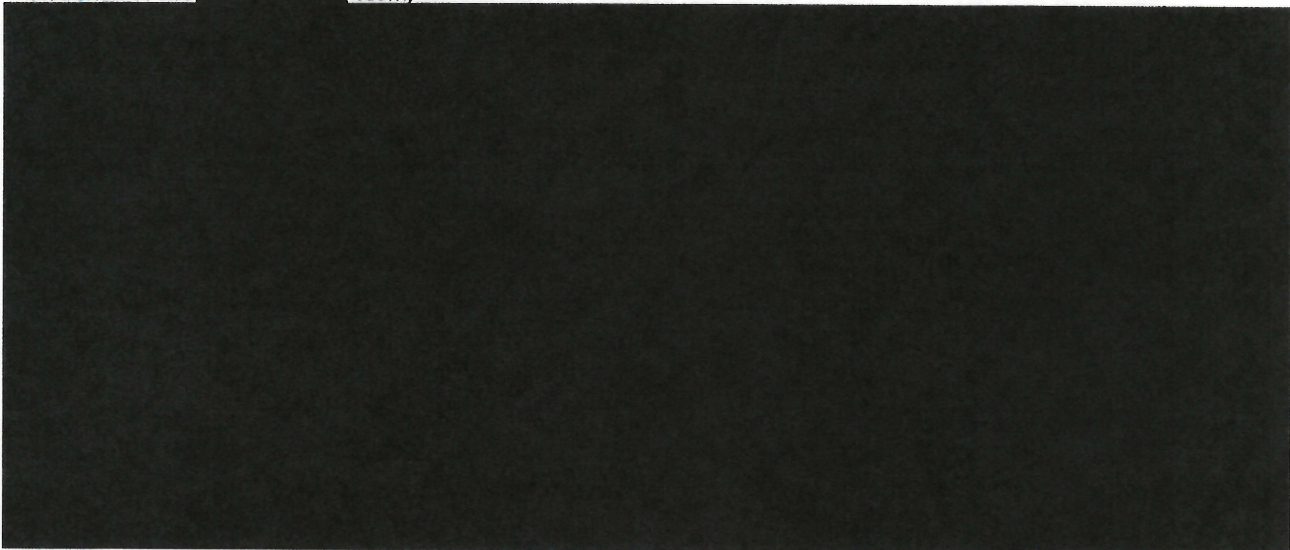
Good Morning [REDACTED]

[REDACTED] Since last night's update, we have not observed any new, malicious foreign influence or interference operations relating to the elections. We would like to highlight the items below for your first update today, which will be followed by additional, continuous updates roughly every four hours throughout the day at 1200, 1600, 2000, and 0000:

- [REDACTED] Russia: There are no significant updates since yesterday evening. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
[REDACTED] UNCLASSIFIED language for FBI to pass to industry partners yesterday regarding previously known websites/platforms used by Russian actors to conduct malign influence activities.
- [REDACTED] Iran: We confirmed that industry received our tearlines last night via FBI/FITF regarding Iranian influence efforts emanating from Iranian [REDACTED]
[REDACTED] actors, [REDACTED]
[REDACTED] Additionally, [REDACTED] UNCLASSIFIED language for FBI to pass to industry partners yesterday regarding previously known websites used by Iranian actors to conduct malign influence activities.

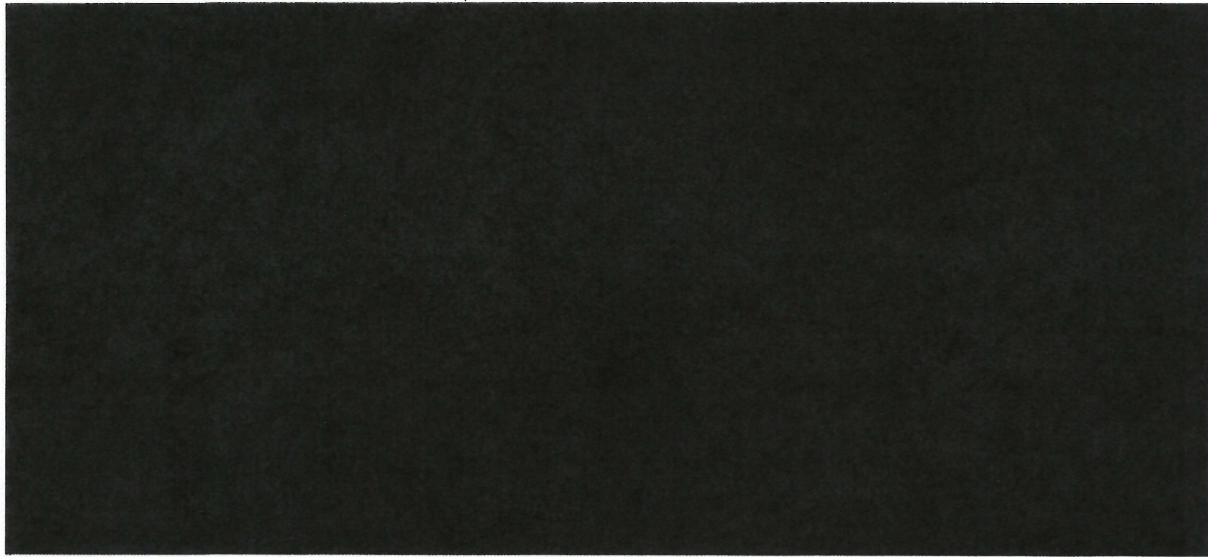
- [REDACTED] Engagements: At the 0800 ODNI-led Sync, FBI indicated that they are investigating voter suppression leads and low level cyber activity, both are considered investigatory at this time. No other significant items to report [REDACTED] will attend multiple interagency syncs today: ODNI [REDACTED] will lead five inter-agency syncs with FBI, CIA, and CTIC at 0800, 1100, 1530, 2000, and 2300; the NSC will lead three interagency syncs at 1000, 1630, and 2100; and DHS CISA will lead two inter-agency partner syncs at 1200 and 1800.
- [REDACTED] Operational Posture: This morning at 0600, [REDACTED]
[REDACTED]
[REDACTED] Elements on alert to support DHS Requests for Assistance. [REDACTED] personnel will support 24x7 operations [REDACTED]

On behalf of the [REDACTED] team,



[REDACTED]

FBI asked if [REDACTED] was elections related



Team,

Below are the notes from today's 0845 [REDACTED] Standup: Tuesday, 3 November.

- Today is Election Day. A portion of [REDACTED] is operating 24/7 out of the [REDACTED] and LOE2 is working out of the ICC.
- You can reach [REDACTED] on the Battlebridge via [REDACTED] [REDACTED] That will be open all day. Please [REDACTED] our team if there are any issues connected or with us not responding on that VMR.
- Please continue to use the [REDACTED] room for tipping and updates.
- There are multiple syncs today with ODNI, NSC, and DHS CISA. [REDACTED] will keep the group updated with quick readouts via chat room.

Campaign Lead

- ID'ed new Twitter account [REDACTED] Immediately serialized and tipped to FB [REDACTED]
- Got a tip from [REDACTED] partner on [REDACTED] capability to disrupt some access to various social media platforms around elections
- [REDACTED] interested in amplifying intended effects of campaign ops using their authorities
- Private Sector highlighted RT and Sputnik already jumping on election topics, as well as covert influence platforms

- Continue to monitor [REDACTED] leaks sites
- Finishing up coordination [REDACTED] this morning

- Continue to monitor targets. [REDACTED]
- [REDACTED]

Campaign Lead

- New [REDACTED] out - selectors for [REDACTED] cyber actors

- [REDACTED]
- Today is Election Day. A portion of [REDACTED] is operating 24/7 out of the [REDACTED] and LOE2 is working out of the [REDACTED]
- You can reach [REDACTED] on the Battlebridge [REDACTED] [REDACTED] That will be open all day. Please Skype our team if there any issues connected or with us not responding on that VMR.
- Please continue to use the [REDACTED] [REDACTED] chat room for tipping and updates.
- There are multiple syncs today with ODNI, NSC, and DHS CISA. [REDACTED] will keep the group updated with quick readouts via chat room.

[REDACTED]
Campaign Lead

- ID'ed new Twitter account [REDACTED]
[REDACTED]
[REDACTED]
- Got a tip from [REDACTED] partner on [REDACTED] capability to disrupt some access to various social media platforms around elections
- [REDACTED] interested in amplifying intended effects of campaign ops using their authorities
- Private Sector highlighted RT and Sputnik already jumping on election topics, as well as covert influence platforms

- [REDACTED]
- Continue to monitor [REDACTED] leaks sites
- Finishing up coordination [REDACTED] this morning

- [REDACTED]
- Continue to monitor targets [REDACTED]
- Maybe will restrike [REDACTED] (at a later date)

[REDACTED]
Campaign Lead

- New [REDACTED] out - selectors for [REDACTED] cyber actors

- [REDACTED]
- [REDACTED]

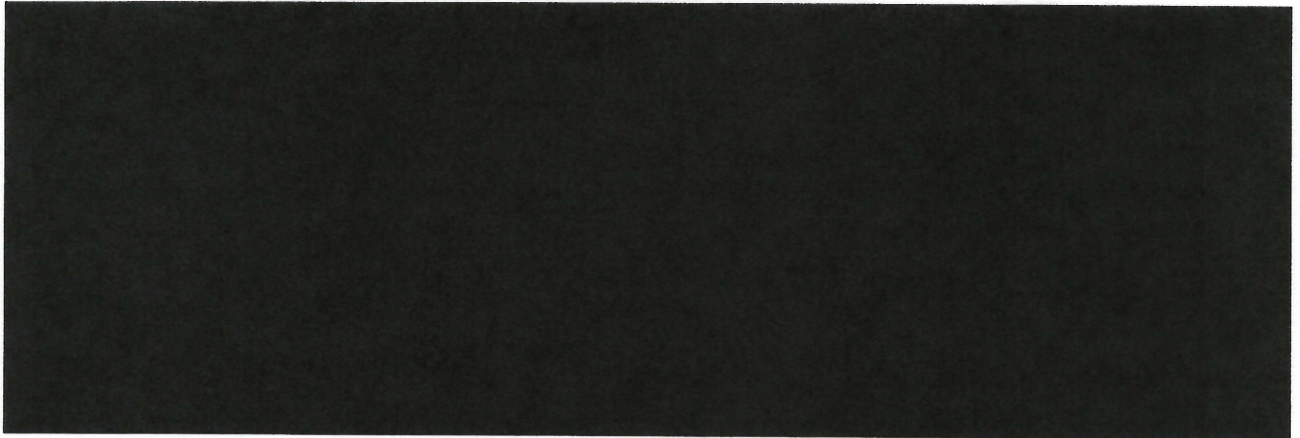


1000 NSC Meeting Notes - [REDACTED]

Tuesday, November 3, 2020 7:06 AM



[REDACTED] 1000 NSC Readout



The following updates were provided at the 1000 NSC [REDACTED] PCC --

DHS/CISA

- Several counties down in GA, expecting those will be back up in the next few hours, not a technical issue. Knowink it is resolving itself it is a load issue on their side not a malicious cyber. Arizona and California use Knowink we are confident that the load issue will not apply but we don't think this is a issue. They are working east to west. They are seeing a resolution and improvement.
- Florida Ransomware - Merrian county affecting the county system no election impact/connection at this time.

FBI

- Command post up and running 24 hour status, hundreds of leads coming in on the criminal side. Open source stories about robo calls to voters, reminding voters to stay home, states reporting this as well. Nothing of significance to update or to link to foreign adversaries at this time.
- PBVCA command post is up and running looking at violence and criminal activity. Referrals have gone to them.

FBI - Cyber

- Maricopa county polling place was shut down for 2-3 hours. Site is now operational. People were able to exfil registration data, possibly 600,000 records were taken. FBI is working this. They have a IP (it is not a foreign IP at this time). Waiting on additional details from FBI for analysis.
- At least one voter address had an unauthorized change in Florida county using a website vulnerability that CISA/FBI previously identified.

ODNI

- NSTR

Media Engagements

- DHS media engagement occurred / mostly fielding are questions about the technology challenges reports. 1230 is the next media touchpoint.
- No FBI Press engagements

[REDACTED]

Next update will take place at 1630.

[REDACTED]

Press/Private Sector/Social Media

CISA: 2 media events (press conf with Wolf and Krebs) - few Qs
nothing rough

Then a media touchpoint - background calls with [REDACTED] [REDACTED]
and Krebs

Asked about tech challenges

Next touchpoint at 1230

FBI: FBI FITF: received tearlines form [REDACTED] and pushed to social
media - NSTR from social media so far - making queries every hour
to social media

Compartmented update:

The following updates were provided at the 1000 NSC

[REDACTED] PCC --

DHS/CISA

- Several counties down in GA, expecting those will be back up in the next few hours, not a technical issue. Knowink it is resolving itself it is a load issue on their side not a malicious cyber. Arizona and California use Knowink we are confident that the load issue will not apply but we don't think this is a issue. They are working east to west. They are seeing a resolution and improvement.
- Florida Ransomware - Merrian county affecting the county system no election impact/connection at this time.

FBI

- Command post up and running 24 hour status, hundreds of leads coming in on the criminal side. Open source stories about robo calls to voters, reminding voters to stay home, states reporting this as well. Nothing of significance to update or to link to foreign adversaries at this time.
- PBVCA command post is up and running looking at violence and criminal activity. Referrals have gone to them.

FBI - Cyber

- Maricopa county polling place was shut down for 2-3 hours. Site is now operational. People were able to exfil registration data, possibly 600,000 records were taken. FBI is working this. They have a IP (it is not a foreign IP at this time). Waiting on additional details from FBI for analysis.
- At least one voter address had an unauthorized change

1000 LOE Check in - [REDACTED]

Tuesday, November 3, 2020 7:39 AM

BLUF: NSTR at 1000 --- LOEs are updating chat ad hoc/real time

[11/3/2020 9:58 AM] [REDACTED]

Good Morning Everyone - this is the 1000 LOE Check In

[11/3/2020 9:59 AM] [REDACTED]

nothing from LOE1 [REDACTED]

[11/3/2020 9:59 AM] [REDACTED]

LOE 1 [REDACTED] NSTR

[11/3/2020 9:59 AM] [REDACTED]

morning! nothing in addition to all the updates i have been passing from LOE2

[11/3/2020 9:59 AM] [REDACTED]

Good Morning! Everything we are tracking has been posted in this chat. Nothing new to add.

[11/3/2020 10:00 AM] [REDACTED]

Checking in for [REDACTED] NSTR.

[11/3/2020 10:04 AM] [REDACTED]

Thank you, all!

[11/3/2020 10:05 AM] [REDACTED]

LOE 3 NSTR

[11/3/2020 10:05 AM] [REDACTED]

LOE 2 / [REDACTED] - any updates?

Thank you, [REDACTED]

[11/3/2020 10:12 AM] [REDACTED]

not sure if he does but looks like [REDACTED] said no updates from LOE 2 other than the chat

[11/3/2020 10:12 AM] [REDACTED]

(y) thx

[11/3/2020 10:16 AM] [REDACTED]

On behalf of [REDACTED] - LOE 2 is NSTR

[11/3/2020 10:16 AM] [REDACTED]

thank you

1100 Email to [REDACTED] SLT - [REDACTED]

Tuesday, November 3, 2020 7:08 AM

UPDATE: [REDACTED]

Sir,

[REDACTED] Since this morning's update, we have not observed any new, malicious foreign influence or interference operations relating to the elections.

- [REDACTED] **Atmospherics:** FBI received a report that a Maricopa County elections-related website was shut down for two to three hours. The site is now operational. Further investigation from FBI revealed a single US IP address bypassed the website's authentication measures and exfiltrated voter registration data, including name, address, voting district and party affiliation. Maricopa County estimates over 600,000 records were taken between 21 October and Tuesday 2 November. FBI is actively pursuing this matter and has notified the Arizona Secretary of State and DHS CISA. Additionally, one report about suspicious robo calls in Virginia, Nebraska, and Michigan and a non-election related report about Ransomware in Florida
- [REDACTED] **Russia:** There are no significant updates since this morning. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
[REDACTED]
- [REDACTED] **Iran:** There are no significant updates since this morning.
- [REDACTED] **Lead Evaluation in Support of FBI and DHS:** We have evaluated 5 tips from FBI and DHS of anomalous cyber activity directed at state and local infrastructure. No attribution of a foreign actor nexus at this time.
- [REDACTED] **Engagements:** [REDACTED] will attend the ODNI [REDACTED] inter-agency syncs with FBI, CIA, and CTIIC at 1530, 2000, and 2300; the NSC interagency syncs at 1630, and 2100; and the DHS CISA inter-agency partner syncs at 1200 and 1800.
- [REDACTED] **Operational Posture:** OCO teams remain postured at [REDACTED] while [REDACTED] and [REDACTED] remain on alert to support DHS Requests for Assistance.

[REDACTED] Our next update will be at 1600.

• [REDACTED] Russia: There are no significant updates since this morning. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
[REDACTED]

1

UPDATE: [REDACTED] SENT // [REDACTED] flipped email

Sir,

[REDACTED] Since this morning's update, we have not observed any new, malicious foreign influence or interference operations relating to the elections.

[REDACTED] **Atmospherics:** FBI received a report that a Maricopa County elections-related website was shut down for two to three hours. The site is now operational. Further investigation from FBI revealed a single U.S. IP address bypassed the website's authentication measures and exfiltrated voter registration data, including name, address, voting district and party affiliation. Maricopa County estimates over 600,000 records were taken between 21 October and Tuesday 2 November. FBI is actively pursuing this matter and has notified the Arizona Secretary of State and DHS CISA. Additionally, we have received reports about suspicious robo calls in Virginia, Nebraska, and Michigan and a non-election related report about Ransomware in Florida. Several counties in several States have gone to paper ballots due to technical issues with e-Pollbooks. No malicious activity is suspected, and no impact.

- [REDACTED] **Russia:** There are no significant updates since this morning. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
[REDACTED]
- [REDACTED] **Iran:** There are no significant updates since this morning.
- [REDACTED] **Lead Evaluation in Support of FBI and DHS:** We have evaluated 5 tips from FBI and DHS of anomalous cyber activity directed at state and local infrastructure. No attribution of a foreign actor nexus at this time.
- [REDACTED] **Engagements:** [REDACTED] will attend the ODNI [REDACTED] inter-agency syncs at 1530, 2000, and 2300; the NSC interagency syncs at 1630, and 2100; and the DHS CISA inter-agency partner syncs at 1200 and 1800.
- [REDACTED] **Operational Posture:** OCO teams remain postured [REDACTED] while [REDACTED] and [REDACTED]
[REDACTED] remain on alert to support DHS Requests for Assistance.

[REDACTED] Our next update will be at 1600.

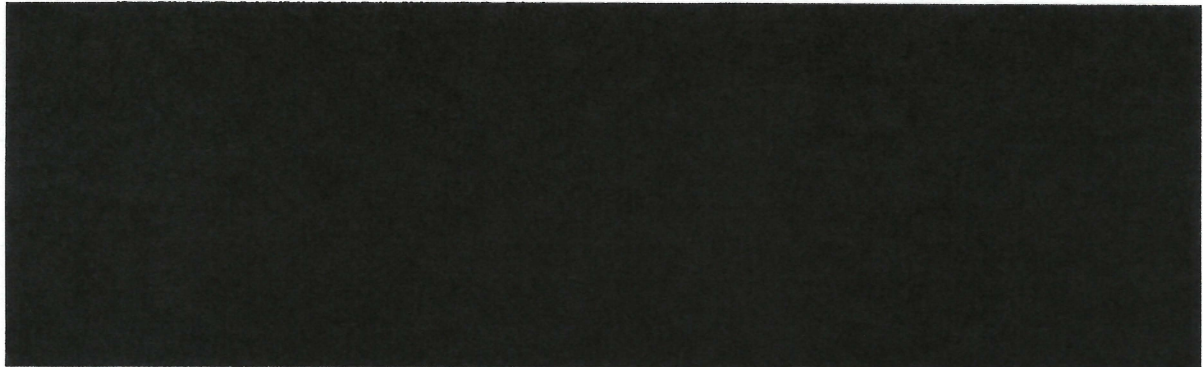
On behalf of the [REDACTED],

1200 Interagency Partners Sync - [REDACTED]

Tuesday, November 3, 2020 7:08 AM



[REDACTED] 1200 DHS CISA Interagency Sync Readout



The following updates were provided at the 1200 DHS CISA-led Interagency Sync:

BLUF: CISA briefly recapped all of the current tips they were tracking. [REDACTED] tracking all.

DHS CISA

- Knowlnk having technical IT issues. Many states have gone to paper ballot backups. No impact to voting.
- AZ county website incident occurred last week. FBI reported that this was an information leak by leveraging URL configuration vulnerability not an exfil of data. IIR: 4 007 0163 21
- Typhon malware identified in a development sandbox believed to be [REDACTED] but [REDACTED] does not have any confirmation that is accurate
- Rhode Island reported IP listed in the FBI Flash. [REDACTED] That attempts were made on our voter information center app. FBI and CISA agreed they are currently unable to determine if this is legitimate or malicious. [REDACTED] of this Luxembourg IP to US. Asked CISA for the domain/IP of the voter system.

[REDACTED] (DHS LNO):

- Following [REDACTED] and all tips from DHS

[REDACTED]

- DHS confirmed it is currently not waiting for [REDACTED] on any action items
- Tracking AZ IP address is U.S. (not foreign) – [REDACTED] awaiting any foreign nexus to continue to evaluate
- [REDACTED] working to share additional malicious domains to share for defensive use, which we will get to MS-ISAC in the next couple of hours

FBI

- AZ incident appears to be info leakage vice an intrusion. The actor was able to edit the URL line to access information that way. Actor did access non-publicly available information but due to an insecure connection, not due to a computer intrusion.

CIA Cyber: NSTR

MS-ISAC:

- This morning in SLTT Sit Room, some states hit by [REDACTED] IP address. MS-ISAC identified 117 hits over 10 sensors; however, no sensors were election related. There are 3 IP addresses that could not be resolved and MS-ISAC is trying to verify; however, not deemed elections related at this time.
- FBI Cyber is working to determine connections to this Iranian activity because not certain if that [REDACTED] is still in use. [REDACTED] For example, the [REDACTED] recently visited a WordPress site, which could indicate legitimate, [REDACTED] use.

- This morning in SLTT Sit Room, some states hit by [REDACTED] 117 hits over 10 sensors; however, no sensors were election related. There are 3 IP addresses that could not be resolved and MS-ISAC is trying to verify; however, not deemed elections related at this time.
- FBI Cyber is working to determine connections between [REDACTED] [REDACTED] For example, the [REDACTED] IP recently visited a WordPress site, which could indicate legitimate, non-Iranian use.

Next update will take place at 1800.

[REDACTED]

Readout from the 1200 CISA Interagency call

CISA briefly recapped all of the current tips they were tracking. [REDACTED] was tracking all of the same information – GOOD

Knowlnk having technical IT issues – many states have gone to paper ballot backups – No impact to voting

AZ county website occurred last week. FBI reported that this was an Information leak by leveraging URL configuration vulnerability not an exfil of data. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] That attempts were made on our voter information center app. FBI and CISA agreed they are currently unable to determine if this is legitimate or malicious. [REDACTED]

[REDACTED] of this Luxemburg IP to US. Asked CISA for the domain/IP of the voter system.

Next update at 1800

Thanks,
[REDACTED]

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

RE ■ Readout DHS CISA Krebs Elec Sec Media Update C...



1230 CISA Media Call
Wednesday, November 4, 2020 12:32 AM

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

Director Krebs opened with a very brief statement that amounted to that CISA wasn't seeing much new in terms of election interference issues.

- several technical issues have been reported and resolved, and that shows resilience of election systems is working
- technical issues with an electronic poll book affecting localities in Ohio and Texas had been resolved
- another poll book issue in Clark County Nevada had been resolved
- FBI is investigating reports of robocalls and texts to voters in Michigan saying "stay safe, stay home".

Detail on press questions below. (paraphrased)

- Q: (CNN) What are the "stay safe, stay home" robocalls that voters are getting? Where are they from?
 - A: It's a voter intimidation tactic, and that falls in FBI's remit. But understand, calls like that happen every election—it's nothing new. Keep calm and vote on.
- Q: (WSJ-Dustin Volz) Are you aware of indications that there may be IRA content on the Parler and Gab social media platforms reaching some groups of voters?
 - A: We're looking into it. But, note that we're seeing this activity in non-mainstream, small platforms thanks in part to social media and USG efforts to make sure it isn't effective more broadly.
- Q: (AP-Frank Bajak) Regarding the text messages in Dearborn, Michigan and ballot misinformation—have you seen more of this activity?
 - A: We're not seeing more. Credit goes to the Michigan Secretary of State and team for handling it. The success is about a community of practice and rapid crisis communication techniques.
- Q: (CNET-Alfred Ng) In light of the technical breakdowns in Spalding County (GA), and Franklin County (OH), do you think that calls for patience are getting through to voters?
 - A: With over 100 million votes so far, yes, I think voters are confident and that the message is resonating. US government efforts, and media reporting are helping.
- Q: (ProPublica-Jack Gillum) Have you seen any websites, e-poll books within the last 24 hours downed by DDOS attacks or other intentional interference?
 - A: No. Haven't seen more, but we're keeping an eye out, as are state and local officials.
- Q: (VoA - Jeff Seldin) How helpful are USCYBERCOM's hunt-forward efforts for limiting interference? Also, are you worried about misinformation from foreign state's propaganda platforms?
 - A: The IC and USCYBERCOM have been great partners. Hunt Forward has gone to various countries and they've seen adversaries, like Russia, operating in the wild. They've seen how Russian actors do it, and brought back malware samples we can share, and given us a sense of what infrastructure those actors target. It helps us advise election security officials where to prioritize security investment and efforts. It's a credit to [REDACTED] and [REDACTED].
 - A2: Disinformation from state outlets — it's more of the same. Stuff we've seen time and again. It's aimed at undermining confidence and promoting conflict. But, the common bond that voters have as Americans helps us resist it.
- Q: (WaPo Ellen Nakashima) Are you seeing lower or higher level of coordinated activity from Russia than in 2016?
 - It's quieter. But we don't discount it. For example we recently warned about Energetic Bear scanning state and local networks. We'll continue to push out alerts.

1400 LOE Check In - [REDACTED]

Tuesday, November 3, 2020 7:39 AM

- Brute force attempts were unsuccessful, several counties. Illinois has exposed domain controllers. Addressing the issues
- Suspected malicious website in Bangor, Maine. Hit a malware attachment. DHS/CISA support is ongoing.
- Attempt SQL injection in NY state.
- Disinformation SMS messages in Florida, claiming protestors causing violence.
- Multiple states seeing RDP connection, none successful.
- Phishing attempt in Washington State, we do not know what is in the email.

ODNI ransomware? DHS – No.

ODNI looking for guidance from [REDACTED] on what type of additional support they need this evening as the calls for violence occur.

- [REDACTED]
- NSTR
 - No products ginned up from overnight? No nothing from the all source. OSC will be putting out a foreign reactions piece in the morning.
- [REDACTED]
- Few [REDACTED] reports talking about unspecified emails, unclear why they did not go out. Another report talking about having the ops done by the 5th. Additional reporting about the operations being done.

[REDACTED] JOE –
Investigating the activity, executed ops and supporting requirements

ODNI

Mr. Evanina has jointed us. Share a couple of thoughts, thank you to everyone out there from my perspective we are greatly appreciated for the efforts of the governemt for the election. Shout out to NSC, the interagency community the support from the team was incredible. I feel like we are ready to respond and react to anythign the advbersary will throw to us. We are prepared. Personally thank you for your efforts. Please pass this pride and thanks to the rest of the time.

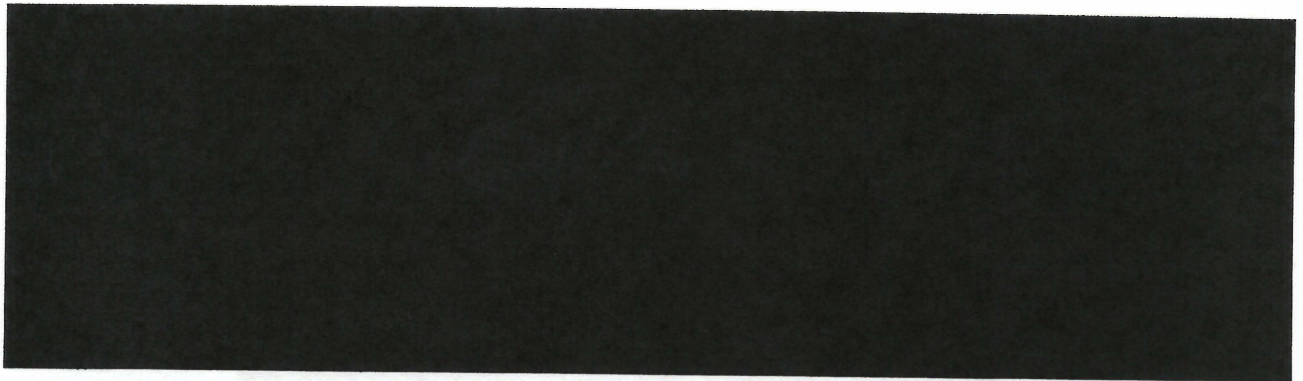
[REDACTED] update

New [REDACTED] reports that have gone out about email campaigns that they have conducted

No details on the details of the content. Reference to the actors talking to the operation. Wrapping up by 5 November.

Following up with [REDACTED] on potential [REDACTED] limited IP.

Here are the atmopsherics [REDACTED] will talk to the Task Forces [REDACTED] responssses



Details from 1600 CISA media call:

TPs

- Voters are turning out – continued increase in votes cast
- American voters have confidence in process
- Same tech issues we've seen in other elections – nothing significant thus far and not cyber
- States are practicing resilience – keeping calm
- On social media – it has been quiet – but we aren't out of the woods yet
- Disruption during the counting process could come in the form of 3 Ds - demand, defacement or DDOS attacks

Qs

CNN (Zack Cohen) – FBI said they are aware of Robocalls – but haven't said they are investigation. Can you confirm if they are investigation? No

ABC (Luke Barwith) – any idea on attribution on Robocalls – No check w/FBI

WaPo (Joe Marks) – do you have any sense why we haven't seen more activity by foreign actors? We can't speak to that. We are focused on our partners and the work we've done/are doing. On disinfo front, the national conversations, social media companies, media – all make it harder for the disinfo to stick

Congressional Quarterly (Gopal Ratnam) – Do you think foreign interference is smaller than in 2018 and before? We aren't out of this yet. Attack surface extends into the next month or two. Based on what we're seeing, this is below what we have seen.

CyberScoop (Sean Lyngass) – Have you been in touch with Nat. Guard today? Is there an open line there? Guard has been part of planning for the past several months. They should speak to what they are doing. CISA is embedded in many states and work alongside Guard

AP (Eric Tucker) – which of the 3Ds is speculative and which is most concerning? Might add 4th D – disinfo. Stress on system is very much something we are watching.

Wash. Examiner (Jerry Dunlevy) – Assuming tonight isn't a landslide, what is concerning most about the delay in results due to longer count? What is being done to protect against that? Go to CISA Rumor Control web page we've worked on a number of scenarios.

MPR (Miles Park) – What are some things you don't know? What is possibility of attacks you may not have identified yet? We've built in resiliency into the process. Layered defense that hopefully accounts for the unknown attacks.

Tuesday, November 3, 2020 7:10 AM

Leaders,

As of 1500, we have not observed any new, malicious foreign influence or interference operations related to the elections. [REDACTED] indicating that [REDACTED] actors continue work on influence operations relating to the elections. The draft [REDACTED] Update to [REDACTED] for sending at 1600 is below for your review.

Sir,

[REDACTED] Since your 1200 update, we have not observed any new, malicious foreign interference operations related to the elections. [REDACTED] indicating that Iranian [REDACTED] actors continue work on influence operations relating to the elections. We would like to highlight the items below:

- [REDACTED]
 - [REDACTED] actors on 1 November claimed that unspecified work would be completed by 5 November despite pending government mandated travel restrictions in [REDACTED]
 - [REDACTED]
 - [REDACTED] Two Iranian IPs are reportedly conducting a low-level DDOS against a U.S. media entity. As of now, no known link to [REDACTED] but teams are investigating. FBI has been on-site assisting in [REDACTED] mitigation efforts since last week. [REDACTED] is also conducting analysis.
- [REDACTED] **Russia:** There are no significant updates since this morning. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
- [REDACTED] **Actions:**
 - [REDACTED] Task Force 1 continues to monitor [REDACTED] activities, as well as unattributed fragmented reports of Ransomware and Denial of Service activities. [REDACTED] offensive cyber teams are postured in [REDACTED] to pursue and impose costs.
 - [REDACTED] Task Force 3 evaluated suspicious Moldavian IP activity linked to RDP brute force attempts; initial results appear to be targeting IPs around the world and not specifically targeting elections.
 - [REDACTED] Task Force 5 continues to develop suspicious Netherlands based IP's; initial results are linked to an unknown actors previous attempts to exploit an identified Midwestern US financial services provider. No known election nexus at this time.
- [REDACTED] **Lead Evaluation in Support of FBI and DHS:** Task Force 2, Task Force 5, and [REDACTED] have evaluated 3 additional tips from FBI and DHS of anomalous cyber activity directed at state and local infrastructure. Although all 3 tips are foreign, we have not been able to attribute the activity to known foreign actors and there is no elections nexus at this time.
- [REDACTED] **Engagements:** [REDACTED] will attend the ODNI [REDACTED] interagency syncs with FBI, CIA, and CTIIC at 1530, 2000, and 2300; the NSC interagency syncs at 1630 and 2100; and the DHS CISA interagency partner sync at 1800.
- [REDACTED] **Operational Posture:** OCO teams remain postured at [REDACTED] while [REDACTED] [REDACTED] [REDACTED] [REDACTED] remain on alert to support DHS Requests for Assistance.

Tuesday, November 3, 2020 7:10 AM

Good Afternoon Sir,

- [REDACTED] Russia: There are no significant updates since this morning. Our teams remain on heightened alert for malign Russian activity. [REDACTED]
- [REDACTED] Actions: Our cyber response forces have conducted multiple scanning operations against suspicious IP addresses tipped from various interagency and industry partners. [REDACTED]
 - [REDACTED] Task Force 1 continues to monitor [REDACTED] activities, as well as unattributed fragmented reports of Ransomware and Denial of Service activities. [REDACTED] offensive cyber teams are postured in [REDACTED] to pursue and impose costs.
 - [REDACTED] evaluated suspicious Moldavian IP activity linked to RDP brute force attempts; initial results appear to be targeting IPs around the world and not specifically targeting elections.
 - [REDACTED] continues to develop suspicious Netherlands based IPs; initial results are linked to an unknown actors previous attempts to exploit an identified Midwestern U.S. financial services provider. No known election nexus at this time.
 - [REDACTED] executed scanning operations in response to an unsuccessful NY State SQL injection attempt from an IP initially reported to be in China. No election nexus discovered.
- [REDACTED] Lead Evaluation in Support of FBI and DHS: [REDACTED] evaluated 3 additional tips from FBI and DHS of anomalous cyber activity directed at state and local infrastructure. Although all 3 tips are foreign, we have not been able to attribute the activity to known foreign actors and there is no elections nexus at this time.

1630 NSC Meeting Notes - [REDACTED]

Tuesday, November 3, 2020 7:10 AM

Team:

Below are the notes from today 1530 Election Security Sync hosted by ODNI [REDACTED] and the 1630 NSC [REDACTED] Meeting. These meetings covered the same material:

ODNI:

- No immediate reports in the IC about imminent threats to the election.
- [REDACTED]
- A call between ODNI and Congressional members occurred issued raised were:
 - o Congressional members asked about the Robo calls in the Midwest have been asked about it
 - o Members were aware of the Iran reporting in generalities, but had no in-depth questions
- [REDACTED] thanked the group for our efforts to secure the 2020 Elections. He is confident that we are ready to respond and react to anything the adversary will throw to us. He requested that the teams pass this appreciation and thanks to the interagency teams.

FBI – Influence:

- Social Media companies have indicated that they appreciated the tearlines on the Iran influence activity; however, they were not able to take action / could not find anything to match the reporting.
- NSTR on the [REDACTED] activity as it relates to Elections influence.

FBI – Cyber

- Facebook was not able to find additional information on the tearline shared re: Iranian video production due to the vague nature of the tearline.
- Investigating low-level DDoS attempts from Iran geo-located IPs against an identified media company [REDACTED], coming from Iran located IPs. [REDACTED] has been provided the lead information.

DHS/CISA

- A few intermittent issues remain regarding the e-pollbooks.
- Spaulding and Morgan county Georgia have experienced voting machine issues.
- Possible infection of a website in Moscow, Maine (NFI), no indication it is affecting elections.
- Several States are getting the Robo Calls, FBI is investigating.
- Oracle vulnerabilities were not successful, DHS/CISA following up to ensure safe.
- Brute force attempts were unsuccessful, several counties.
- Suspected malicious website in Bangor, Maine. Hit a malware attachment. DHS/CISA support is ongoing.
- Attempt SQL injection in NY state.
- Disinformation SMS messages in Florida, claiming protestors causing violence.

CIA

- OSC will be putting out a foreign reactions piece in the morning.

- [REDACTED]
- We have issued multiple [REDACTED] reports today. One referenced the sending of unspecified emails and another about having the ops done by the 5th.

NSC:

- No actions for the teams at this time.

1800 Interagency Partners Sync - [REDACTED]

Tuesday, November 3, 2020 7:11 AM

FYSA [REDACTED] did not attend due to 1830 in-person [REDACTED] brief
[REDACTED] was in attendance - can get readout from [REDACTED] / [REDACTED]

Over night shift, we're not tracking that a readout was provided

Recommendation:

Execute a scan op now to further characterize the IPs. Continue to develop the intelligence associated with this IP as it does not pose an immediate threat to elections.

██████████ is coordinating now for the scan op.

[11/3/2020 5:39 PM] ██████████

██████████ rgr. ██████████ ██████████ is tracking and passing to QRF for pursuit

<--- This is ██████████ article

[11/3/2020 5:42 PM] ██████████

Press from Washington Post: (UNCLASSIFIED) Discovery Service link: U.S. undertook cyber operation against Iran as part of effort to secure the 2020 election <https://medr-lb.discovery.proj.██████████.ic.gov/discovery/resource/FACWPCOM00020201103EGB30066I/3251633773b660490edd814e88bc93c3>

[11/3/2020 5:43 PM] ██████████:

Regarding QRF actions against Panamanian and Netherlands IPs, unable to exploit using available T10 capabilities. No attribution of activity to a known APT

[11/3/2020 5:45 PM] ██████████:

@Arner interesting that one of the IPs is a possible cell phone and ██████████ was provisioning SIM Cards in recent reporting? any possible relation? ██████████

[11/3/2020 5:58 PM] ██████████

NSTR for ██████████ LOE1 1800 update

[REDACTED]

Departing at 0600

Note to DNI - quick update tomorrow morning

- No interference broadly right no
- One exception is what we find out from [REDACTED] and 1 router against [REDACTED]

[REDACTED]

Rus

Focus on [REDACTED] - nothing on [REDACTED] -- nothing above normal, has been minimal

No new china reporting

Black swan of malware -- [REDACTED] is developmental;

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

If there is no call on winner -- are we seeing

[REDACTED] could use social media companies -- would generate content. Domestic content will be generated; will see
RUS (RT Sputnik) amplify content
Fringe platforms would do so also

Into conservative private messaging groups

ie actors see stand up social media; not having infra will stop from established accounts

Rus - would inject new narratives of ballots lost, gin up stories

Avant team has been watching today; based on past TTPs - If see RT Sputnik inc narrative -- it's a general narrative we have seen more

Wed worry of [REDACTED] execute /inject chaos into [REDACTED]

Ballots misdirected, delayed, lost

Source of [REDACTED] report?

Looking at [REDACTED] -- analysis led to [REDACTED] connx based on IP

More widespread based off of 1 router/? No- based on infra from CISA

Assess isolated incident based on info we have

Check in post 2100 -- call from [REDACTED]

2000 ODNI Meeting Notes

Tuesday, November 3, 2020 7:11 AM

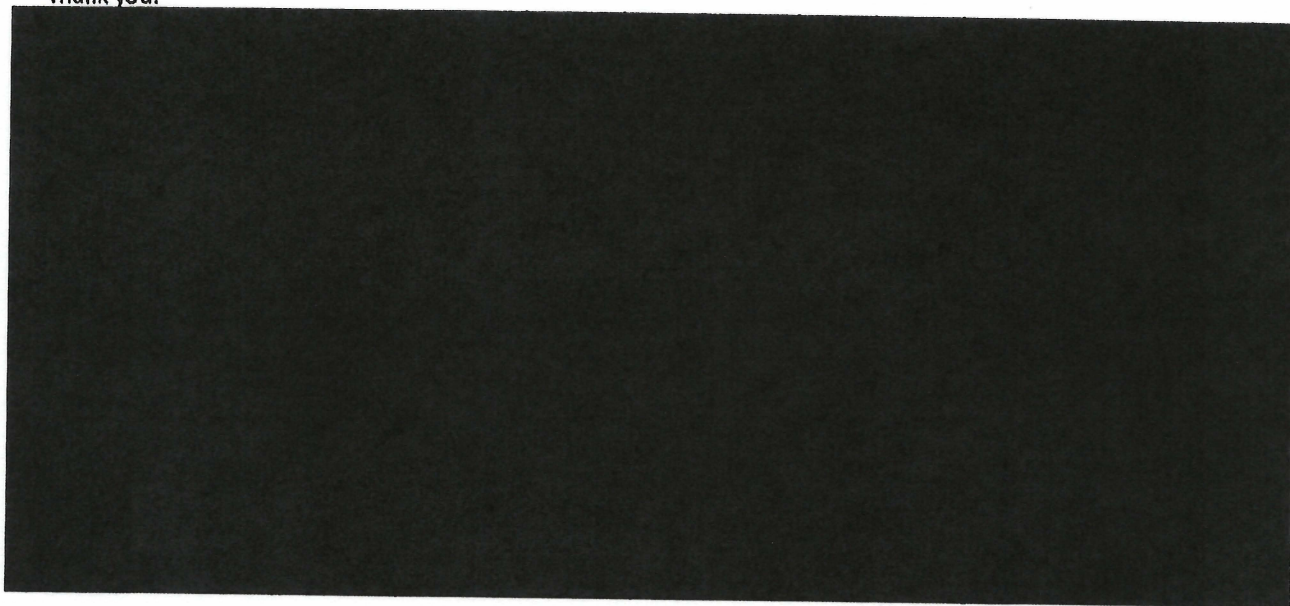
 (U FOUO) Readout -- 2000 Election Security Sync hosted b...

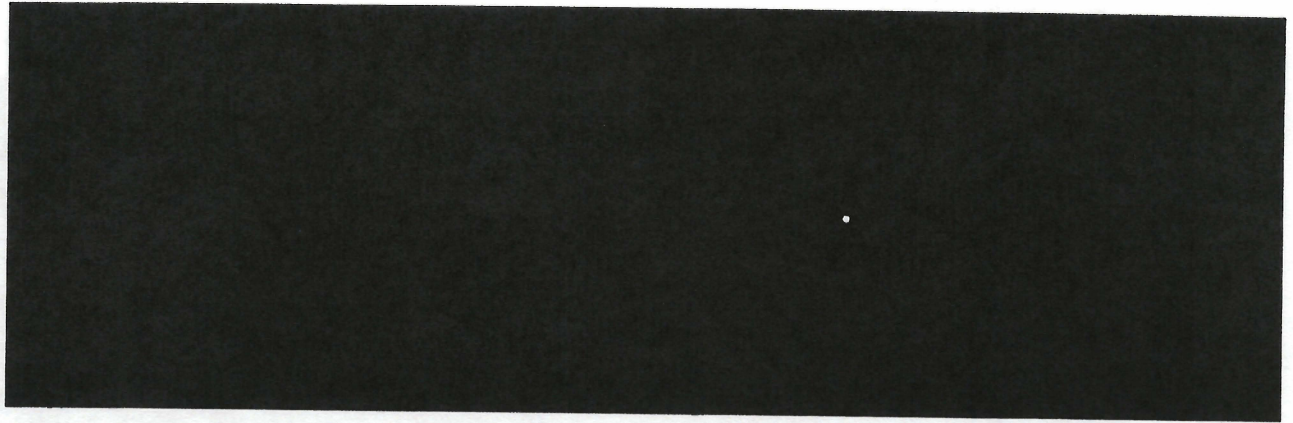
DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

DECLASSIFIED BY COUNSEL TO THE PRESIDENT WARRINGTON ON 30 JULY 2026

Please let us know if there are any questions.

Thank you!





Team,

Below are the notes from yesterday's 2000 Election Security Sync hosted by ODNI [REDACTED] and the 2100 NSC [REDACTED] Meeting. These meetings covered the same material:

ODNI

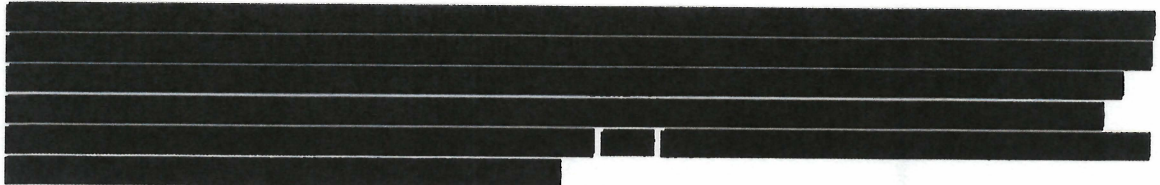
- The 2300 Interagency Sync led by ODNI will be cancelled
- No significant threats are being tracked at this time

DHS

- The USPS LNO indicated that the compromise of the supposed USPS IP space was not a true compromise as it was assessed at the time that the USPS did not actively use that space (two IPs were compromised)
- Two phishing attempts have been conducted against the Board of Elections in New York; it is assessed that Emotet is responsible, and the attempt was unsuccessful
- DHS tipped that Texas reporting is down due to a back-end server. In response, Texas officials are working from a static webpage from now. There is no cyber nexus at this time; similar, internal activity took place in the Texas primaries.
- A few intermittent issues remain regarding the e-pollbooks - but it has not impacted any voting tallies

FBI

- FBI is focused on any violent, physical threats
- Expect social media to tip them if they see any influence activity, and they are standing by to receive tips from industry partners
- Social media companies will work through the night
- San Francisco is 24 hours and able to respond as needed
- Regarding Maricopa County, FBI is continuing to investigate; no further updates



NSC:

- No actions for the teams at this time.

2200 SecDef Update

Tuesday, November 3, 2020 9:00 PM

RE [REDACTED] Secretary and Chairman Note

[REDACTED]

Sir,

Updated note w/ operational capability bullet.

v/r,
[REDACTED]

Mr. Secretary and Chairman,

[REDACTED] Here is our first post-Election Day update. I will provide updates throughout the day if conditions change.

Current Situation:

[REDACTED] Over the last 24 hours, we have not observed successful foreign interference or significant foreign adversary influence operations against the elections. We continue 24/7 operations and remain synchronized with interagency, industry, and foreign partners. My main concern this morning is an adversary amplifying and/or stoking disinformation surrounding the results or legitimacy of the elections.

Quick Intelligence / Operations Summary:

- [REDACTED] We are aware that a Russian [REDACTED] actor has compromised a router that may be associated with the U.S. Postal Service. [REDACTED], we are proactively addressing this threat with FBI and DHS. We remain on alert for other malign Russian activity and continue to see disparate Russian [REDACTED] efforts to leverage social media as a vector for election influence.

- [REDACTED] Iranian malicious cyber actor aspirational efforts against our elections continue. We are aware of a possible Iranian malicious cyber actor executing a unsuccessful low-level denial of service attack against a U.S. media entity. We are conducting [REDACTED] to gather additional information. The FBI is leading the domestic actions, and we remain in support.

- [REDACTED] We have observed no significant nefarious Chinese election-related activities at this time.

- [REDACTED] Finally, we remain highly attuned to Ransomware attacks. We have seen no indications of Ransomware attacks against election infrastructure; however, we remain postured to quickly respond and act.

Operational Capability:

Mr. Secretary and Chairman,

[REDACTED] Here is our first post-Election Day update. I will provide updates throughout the day if conditions change.

Current Situation:

[REDACTED] Over the last 24 hours, we have not observed successful foreign interference or significant foreign adversary influence operations against the elections. We continue 24/7 operations and remain synchronized with interagency, industry, and foreign partners. My main concern this morning is an adversary amplifying and/or stoking disinformation surrounding the results or legitimacy of the elections.

Quick Intelligence / Operations Summary

- [REDACTED] [REDACTED] we are proactively addressing this threat with FBI and DHS. We remain on alert for other malign Russian activity and continue to see disparate Russian [REDACTED] efforts to leverage social media as a vector for election influence.

- [REDACTED] [REDACTED] We are conducting [REDACTED] to gather additional information. The FBI is leading the domestic actions, and we remain in support.

- [REDACTED] We have observed no significant nefarious Chinese election-related activities at this time.

- [REDACTED] Finally, we remain highly attuned to Ransomware attacks. We have seen no indications of Ransomware attacks against election infrastructure; however, we remain postured to quickly respond and act.

Next 24 hours:

[REDACTED] We remain postured for extended operations to understand and act against foreign adversary attempts to propagate disinformation, sow discord, or foment violence.

v/r,

[REDACTED]