From: (b) (6) (OLA)
Subject: RE: [EXTERNAL] Threats against school personnel
To: Pietranton, Kelsey (PAO); Hanson, Alan R. (JMD)
Cc: Coley, Anthony D. (PAO); Iverson, Dena (PAO); Hornbuckle, Wyn (PAO)
Sent: October 7, 2021 2:34 PM (UTC-04:00)

Thanks; I was just connecting you up with Alan Hanson. But disregard. It looks like his question is being resolved. Thanks, (b) (6)

From: Pietranton, Kelsey (PAO) (b) (6)
Sent: Thursday, October 7, 2021 2:32 PM
To: (b) (6) (OLA) (b) (6)
Cc: Coley, Anthony D. (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6)
Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

Hey (b) (6),

We just wrapped a meeting and I listened to your voicemail. I am about to run to another meeting but wanted to send a note because it's really hard to hear you in the message!

What do you need from OPA?

Thanks!
Kelsey

From: Pietranton, Kelsey (PAO)
Sent: Thursday, October 7, 2021 1:32 PM
To: (b) (6) (OLA) (b) (6)
Cc: Coley, Anthony D. (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ;
Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

I have not been working with anyone in FBI OCA. I know FBI OPA has been providing more info, and I think that has been shared with FBI OCA, hence my suggestion to reach out to them!

From: (b) (6) (OLA) (b) (6)
Sent: Thursday, October 7, 2021 1:30 PM
To: Pietranton, Kelsey (PAO) (b) (6)
Cc: Coley, Anthony D. (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ;
Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

Thanks. Who in FBI OCA have you been working with? Thank you, (b) (6)

From: Pietranton, Kelsey (PAO) (b) (6)
Sent: Thursday, October 7, 2021 1:29 PM
To: (b) (6) (OLA) (b) (6)
Cc: Coley, Anthony D. (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ;
Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

+ Anthony, Dena, and Wyn. Have you reached out to FBI OCA yet on this? I believe they have more info.

From: (b) (6) . (OLA) (b) (6) >
Sent: Thursday, October 7, 2021 1:27 PM
To: Pietranton, Kelsey (PAO) (b) (6)
Subject: FW: [EXTERNAL] Threats against school personnel

Kelsey – See the press release that Alan cites below. Who was OPA working with on this matter? Alan needs a POC to learn more information. Thanks, (b) (6)

From: Hanson, Alan R. (JMD) (b) (6)
Sent: Thursday, October 7, 2021 1:12 PM
To: (b) (6) (OLA) (b) (6) ; Calce, Christina M. (OLA) (b) (6) ; Greenfeld, Helaine A. (OLA) (b) (6) ; Gaeta, Joseph (OLA) (b) (6) ; Antell, Kira M. (OLA) (b) (6)
Cc: Lucas, Daniel (JMD) (b) (6) ;(b) (6) (OLA) (b) (6) ; (b) (6) (OLA) (b) (6) ;(b) (6) (OLA) (b) (6) ;(b) (6) (OLA) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

Now adding (b) (6) , as suggested, to see if anybody has information we can share back to Senate CJS Majority staff who sent us the inquiry at the bottom of this email chain. Even if you guys are just able to provide us an appropriate contact so that we can respond to this inquiry will be helpful.

Thanks.

From: (b) (6) (OLA) (b) (6)
Sent: Tuesday, October 5, 2021 1:17 PM
To: Calce, Christina M. (OLA) (b) (6) ; Hanson, Alan R. (JMD) (b) (6) ; Greenfeld, Helaine A. (OLA) (b) (6) ; Gaeta, Joseph (OLA) (b) (6) ; Antell, Kira M. (OLA) (b) (6)
Cc: Lucas, Daniel (JMD) (b) (6) ;(b) (6) (OLA) (b) (6) (b) (6) (OLA) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

The AG memo says the efforts are FBI-led so maybe ask (b) (6) ? It says they will be announcing things in the coming days – maybe that is the answer for now?

Or, looks like the press release came out of the AG's office – maybe ask OPA who the POC was in OAG?

From: Calce, Christina M. (OLA) (b) (6)
Sent: Tuesday, October 5, 2021 12:21 PM
To: Hanson, Alan R. (JMD) (b) (6) ; Greenfeld, Helaine A. (OLA) (b) (6) ; Gaeta, Joseph (OLA) (b) (6) ; Antell, Kira M. (OLA) (b) (6)
Cc: Lucas, Daniel (JMD) (b) (6) ;(b) (6) (OLA) (b) (6) ;(b) (6) (OLA) (b) (6) ;(b) (6) (OLA) (b) (6)
Subject: RE: [EXTERNAL] Threats against school personnel

Adding in (b) (6) from our team. I'm not familiar w/this – do any of you have any insights?

From: Hanson, Alan R. (JMD) (b) (6)
Sent: Tuesday, October 5, 2021 9:31 AM
To: Greenfeld, Helaine A. (OLA) (b) (6) ; Gaeta, Joseph (OLA) (b) (6) ; Calce, Christina M. (OLA) (b) (6) ; Antell, Kira M. (OLA) (b) (6)
Cc: Lucas, Daniel (JMD) (b) (6)
Subject: Fwd: [EXTERNAL] Threats against school personnel

Helaine, Joe, Christina, and Kira,

Please see the below inquiries we have received from Senate CJS Majority staff regarding the Department's recent school personnel safety announcement. ALO is unfamiliar with this effort and are hoping you guys can help us with responding to these, or, if you prefer, kindly directing us to where we can best get responses.

Thanks much.

Begin forwarded message:

> **Date:** October 5, 2021 at 7:49:34 AM EDT
> **Subject: [EXTERNAL] Threats against school personnel**
>
> Good morning—
>
> Noticed this in my DOJ news round up (https://www.justice.gov/opa/pr/justice-department-addresses-violent-threats-against-school-officials-and-teachers). The AG memo doesn't have much detail soooo what the plan for outreach? Are FBI FOs and USAOs just issuing press releases to raise awareness? Holding "listening" sessions? Are agents and AUSAs visiting schools?
>
> How are these threats being tracked? As the number for NTOC is being provided, is there now a code to parse out threats against educators, school administrators or school board members?
>
> Theoretically, what types of charges would result for credible threats against those working for/with schools (civil rights violations, terrorism changes, etc)? Approximately how many cases like this (individuals threatening public K-12 school staff) are currently being investigated and prosecuted by DOJ?
>
> Thanks.

From: Roberts, Alivia P. (PAO)
Subject: 10.5 Nightly Look Ahead
To: Coley, Anthony D. (PAO)
Sent: October 5, 2021 9:10 PM (UTC-04:00)
Attached: Nightly Look Ahead 10.5_7.04.docx

Nightly look ahead attached. Will print to your desk.

Alivia

From: Singh, Anita M. (ODAG)
Subject: Fwd: OPA Nightly Look Ahead October 5, 2021
To: Wagner, Rose (JMD)
Sent: October 5, 2021 8:47 PM (UTC-04:00)

Anita M. Singh
Chief of Staff
Office of the Deputy Attorney General
U.S. Department of Justice

C: (b) (6)
O: (b) (6)

Begin forwarded message:

From: "Iverson, Dena (PAO)" (b) (6)
Date: October 5, 2021 at 8:38:27 PM EDT
To: "Hornbuckle, Wyn (PAO)" (b) (6), "Coley, Anthony D. (PAO)" (b) (6), "Klapper, Matthew B. (OAG)" (b) (6), "Heinzelman, Kate (OAG)" (b) (6), "Carlin, John P. (ODAG)" (b) (6), "Singh, Anita M. (ODAG)" (b) (6), "Gupta, Vanita (OASG)" (b) (6), "Colangelo, Matthew (OASG)" (b) (6), "Gaeta, Joseph (OLA)" (b) (6), "Greenfeld, Helaine A. (OLA)" (b) (6)
Subject: OPA Nightly Look Ahead October 5, 2021

DOCUMENT CONTAINS LAW ENFORCEMENT SENSITIVE AND/OR SEALED INFORMATION
DO NOT SHARE OUTSIDE OF ORIGINAL RECIPIENT LIST

OPA Nightly Look Ahead
October 5

Stories of Note:

- ***CNBC.com* op-ed from DAG Monaco**
  CNBC.com is running an op-ed from the DAG on the need for congress to enact legislation to create a national standard for reporting cyber incidents, including ransomware. (Pietranton)

- ***New York Times* profile on Jonathan Kanter**
  The New York Times is expected to run a profile on Jonathan Kanter tomorrow morning in advance of his confirmation hearing tomorrow to head the Antitrust Division. Neither Kanter nor the department participated in the profile. (Iverson)

- **Reporting on school board threats memo**
  Numerous outlets reported on the Attorney General's memo addressing violent threats against school board members, officials, and other school personnel. Editorialists on FOX news and other outlets mischaracterized the memo as targeting parents' free speech and those opposing "critical race theory" curricula and COVID-19 public health measures. A department spokesperson pushed back: "There has been misinformation circulated that the Attorney General's directive is an effort to silence those with particular views about COVID-related policies, school curricula, or other topics of public discussion. This is simply not true. As stated clearly in the Attorney General's guidance to the FBI and United States Attorney's Offices, the Department's efforts are about rooting out criminal threats

of violence, not about any particular ideology." FOX modified an opinion segment on air and apologized to OPA for a headline that falsely stated DOJ was considering "labeling parents as 'terrorists'" (Hornbuckle)

- **Reporting on Deputy Attorney General's testimony**
  Numerous outlets reported on the Deputy Attorney General's testimony at the Senate Judiciary Committee hearing on the reauthorization of VAWA, coverage focused on her announcement of the decision to review the declination to prosecute Larry Nassar. (Pietranton)

- **Washington Post on advocate calls for pattern or practice investigations**
  The Washington Post is working on a piece for the weekend about advocates in Kansas City, Kansas, and, separately, Kansas City, Missouri, calling for DOJ to investigate their respective police departments, including in a full page advertisement on page A30 of today's paper calling on the Associate Attorney General to open an investigation into KC, Kansas. The story will explore the question of whether there has been a rush of requests like this across the country after the Trump era and after the 2020 social justice protests. How the department is responding to, assessing and prioritizing these requests and whether there are concerns about a staffing levels. OPA will coordinate a response. (Iverson/Bradford)

- (b) (5) [redacted]

- ***Wall Street Journal* story on private prisons**
  The Wall Street Journal is working on a piece about private prisons. DOJ response: "The Department of Justice is committed to implementing the President's Executive Order on private detention facilities. The U.S. Marshals Service is carefully examining its existing contracts with these facilities, mindful that any plans should avoid unnecessarily disrupting court appearances, access to counsel, and family support. Generally speaking, the U.S. Marshals are responsible for providing safe, secure and humane housing for federal prisoners remanded to its custody. The Marshals make housing decisions based upon various factors such as court appearances, security, availability of bed space in a particular facility and other factors." (Mastropasqua)

- ***Reuters* CARES Act inquiry**
  Reuters has been inquiring about the number of folks on home confinement pursuant to CARES ACT who are eligible for clemency. (Mastropasqua)

- ***The New York Times* to run obituary on former OSI Director Neal Sher**
  Eli Rosenbaum was interviewed by the *New York Times* on the passing of his predecessor former OSI Director Neal Sher. Eli spoke about Sher's 11-years at the Justice Department and how he implemented OSI's investigative program and tried the first case in the 1980s of participant in World War II era Nazi sponsored human rights abuses. (Navas Oxman)

Leading the Day:

- *The Senate Judiciary Committee will hold a nomination hearing for Antitrust Division Assistant Attorney General nominee Jonathan Kanter at 10 am.*
- *At 2:00 p.m. ET, Assistant Attorney General Kristen Clarke will testify before the Senate Committee on the Judiciary on voting rights.*
- *The Deputy Attorney General will deliver remarks virtually to the Aspen Security Forum at 11am, emphasizing cyber security.*
- *The U.S. Court for the Middle District of Georgia will hold a status conference in this case against three white men charged with killing Ahmaud Arbery, a young Black man who was jogging through a mostly-white neighborhood when he was killed. [A state trial in this matter is set to begin on Oct. 18, 2021, in Brunswick, GA.]*

Other Events:

- Deputy Assistant Attorney General Adam Hickey for the Justice Department's National Security Division will appear as a panelist at the 12th Annual Billington Cybersecurity Conference. His pre-recorded panel titled, "The Ransomware Threat" will air Oct. 6 at 2:15 p.m. Press register here.

- USAO SDNY will announce the extradition from the Netherlands of Napoleon Grier, who is wanted in an advance free fraud scheme. (Press release attached)
- The State Department's Bureau of International Narcotics and Law Enforcement Affairs and HSI plan to announce two Transnational Organized Crime Rewards Program (TOCRP) rewards for Pakistani national and human smuggler Abid Ali Kahn. A reward offer of up to $1 million is offered for information leading to the arrest and/or conviction of Abid Ali Khan and a second $1 million reward is offered for information leading to the financial disruption of Ali Khan's human smuggling network. Ali Khan allegedly operates a Pakistani-based smuggling network to facilitate the travel of undocumented individuals into the United States from the Middle East and southwest Asia in exchange for payment. In April, DOJ announced unsealing of federal indictment in EDVA, charging Kahn with conspiracy to encourage and induce an alien to unlawfully enter the United States, encouraging and inducing an alien to unlawfully enter the United States, and bringing an alien to the United States.
- The DAG will deliver remarks at Major Cities Chiefs Association (MCCA). After her speech, OPA will post her remarks. Following that:
  - OJP will put out a release about their public safety partnership sites.
  - (b) (5) [redacted]
  - [redacted]

Expected Releases Tomorrow:

Division/Component: COPS/OAG
Topic/Summary: The COPS Office will announce over $33 million in funding to advance the practice of community policing in law enforcement

Division/Component: CRM
USAO: EDVA
Topic/Summary: A Virginia man will be sentenced to prison for production and receipt of child pornography.

Division/Component: ENRD
Topic/Summary: Kang Juntao, 25, of Hangzhou City, China, will be sentenced to prison on a federal money laundering conviction. Kang had previously pleaded guilty in U.S. District Court in Camden, New Jersey, to financing a nationwide ring of individuals who smuggled at least 1,500 protected turtles, valued at more than $2,250,000, from the United States to Hong Kong. The court also ordered Kang to pay a $10,000 fine. (

-

From: Gelber, Sophie (PAO)
Subject: RE: Nightly Look Ahead 10.5
To: Pietranton, Kelsey (PAO); Iverson, Dena (PAO); Hornbuckle, Wyn (PAO)
Cc: McGowan, Ashley L. (PAO); Roberts, Alivia P. (PAO); Bradford, Aryele (PAO); Blevins, Danielle (PAO); Mastropasqua, Kristina (PAO); Navas, Nicole (PAO)
Sent: October 5, 2021 7:05 PM (UTC-04:00)
Attached: Nightly Look Ahead 10.5_7.04.docx

Another update attached.

From: Gelber, Sophie (PAO)
Sent: Tuesday, October 5, 2021 6:11 PM
To: Pietranton, Kelsey (PAO) (b) (6) Iverson, Dena (PAO) (b) (6) Hornbuckle, Wyn (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6) ; Roberts, Alivia P. (PAO) (b) (6) Bradford, Aryele (PAO) (b) (6) Blevins, Danielle (PAO) (b) (6) ; Mastropasqua, Kristina (PAO) (b) (6) Navas, Nicole (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

Small updates attached.

From: Pietranton, Kelsey (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 5:38 PM
To: Gelber, Sophie (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ; Hornbuckle, Wyn (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6) ; Roberts, Alivia P. (PAO) (b) (6) ; Bradford, Aryele (PAO) (b) (6) ; Blevins, Danielle (PAO) (b) (6) Mastropasqua, Kristina (PAO) (b) (6) ; Navas, Nicole (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

Can we put times in for DAG entries?

From: Gelber, Sophie (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 5:26 PM
To: Iverson, Dena (PAO) (b) (6) ; Hornbuckle, Wyn (PAO) (b) (6)
Cc: Pietranton, Kelsey (PAO) (b) (6) McGowan, Ashley L. (PAO) (b) (6) ; Roberts, Alivia P. (PAO) (b) (6) ; Bradford, Aryele (PAO) (b) (6) ; Blevins, Danielle (PAO) (b) (6) ; Mastropasqua, Kristina (PAO) (b) (6) ; Navas, Nicole (PAO) (b) (6)
Subject: Nightly Look Ahead 10.5

Hi all,
See attached for the Nightly Look Ahead. Let me know if you have any edits.
Best,
Sophie

Sophie Gelber
Press Assistant, Office of Public Affairs
U.S. Department of Justice
(b) (6)
(b) (6)

From: Gelber, Sophie (PAO)
Subject: RE: Nightly Look Ahead 10.5
To: Pietranton, Kelsey (PAO); Iverson, Dena (PAO); Hornbuckle, Wyn (PAO)
Cc: McGowan, Ashley L. (PAO); Roberts, Alivia P. (PAO); Bradford, Aryele (PAO); Blevins, Danielle (PAO); Mastropasqua, Kristina (PAO); Navas, Nicole (PAO)
Sent: October 5, 2021 6:37 PM (UTC-04:00)
Attached: Nightly Look Ahead 10.5_6.37.docx

Another update!

From: Gelber, Sophie (PAO)
Sent: Tuesday, October 5, 2021 6:11 PM
To: Pietranton, Kelsey (PAO) (b) (6); Iverson, Dena (PAO) (b) (6); Hornbuckle, Wyn (PAO) (b) (6)
Cc: McGowan, Ashley L. (PAO) (b) (6); Roberts, Alivia P. (PAO) (b) (6); Bradford, Aryele (PAO) (b) (6); Blevins, Danielle (PAO) (b) (6); Mastropasqua, Kristina (PAO) (b) (6); Navas, Nicole (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

From: Gelber, Sophie (PAO)
Subject: RE: Nightly Look Ahead 10.5
To: Hornbuckle, Wyn (PAO)
Sent: October 5, 2021 6:10 PM (UTC-04:00)
Attached: Nightly Look Ahead 10.5_6.09.docx

Small update attached.

From: Gelber, Sophie (PAO)
Sent: Tuesday, October 5, 2021 5:47 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

Some additions plus Wyn & Kelsey's changes.

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 5:43 PM
To: Gelber, Sophie (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

Quick addition to stories of note:

(b) (5)

From: Gelber, Sophie (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 5:26 PM
To: Iverson, Dena (PAO) (b) (6) Hornbuckle, Wyn (PAO) (b) (6)
Cc: Pietranton, Kelsey (PAO) (b) (6) ; McGowan, Ashley L. (PAO) (b) (6) ; Roberts, Alivia P. (PAO) (b) (6) ; Bradford, Aryele (PAO) (b) (6) ; Blevins, Danielle (PAO) (b) (6) ; Mastropasqua, Kristina (PAO) (b) (6) ; Navas, Nicole (PAO) (b) (6)
Subject: Nightly Look Ahead 10.5

From: Hornbuckle, Wyn (PAO)
Subject: RE: Nightly Look Ahead 10.5
To: Gelber, Sophie (PAO)
Sent: October 5, 2021 6:10 PM (UTC-04:00)

Correct! Thank you!

From: Gelber, Sophie (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 6:09 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

You mean this item right:

- **Reporting on school board threats memo**
  Numerous outlets reported on the Attorney General's memo addressing violent threats against school board members, officials, and other school personnel. Editorialists on FOX news and other outlets mischaracterized the memo as targeting parents' free speech and those opposing "critical race theory" curricula and COVID-19 public health measures. A department spokesperson pushed back: "There has been misinformation circulated that the Attorney General's directive is an effort to silence those with particular views about COVID-related policies, school curricula, or other topics of public discussion. This is simply not true. As stated clearly in the Attorney General's guidance to the FBI and United States Attorney's Offices, the Department's efforts are about rooting out criminal threats of violence, not about any particular ideology." FOX modified an opinion segment on air and apologized to OPA for a headline that falsely stated DOJ was considering "labeling parents as 'terrorists'" (Hornbuckle)

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 6:07 PM
To: Gelber, Sophie (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

To the bottom of the first item. Can you add the following: FOX modified an opinion segment on air and apologized to OPA for a headline that falsely stated DOJ was considering "labeling parents as 'terrorists'"

From: Gelber, Sophie (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 5:47 PM
To: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: Nightly Look Ahead 10.5

From: Hornbuckle, Wyn (PAO)
Subject: RE: Nightly Look Ahead by 4:45pm
To: Gelber, Sophie (PAO)
Cc: Iverson, Dena (PAO); Coley, Anthony D. (PAO)
Sent: October 5, 2021 4:44 PM (UTC-04:00)

Numerous outlets reported on the Attorney General's memo addressing violent threats against school board members, officials, and other school personnel. Editorialists on FOX news and other outlets mischaracterized the memo as targeting parents' free speech and those opposing "critical race theory" curricula and COVID-19 public health measures. A department spokesperson pushed back: "There has been misinformation circulated that the Attorney General's directive is an effort to silence those with particular views about COVID-related policies, school curricula, or other topics of public discussion. This is simply not true. As stated clearly in the Attorney General's guidance to the FBI and United States Attorney's Offices, the Department's efforts are about rooting out criminal threats of violence, not about any particular ideology."

From: Gelber, Sophie (PAO) (b) (6)
Sent: Tuesday, October 5, 2021 4:31 PM
To: Mitchell, Kendall M. (PAO) (b) (6) ; Li, Kaei (PAO) (b) (6) ; Shevlin, Shannon (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ; Hornbuckle, Wyn (PAO) (b) (6) >; Coley, Anthony D. (PAO) (b) (6) ; Mastropasqua, Kristina (PAO) (b) (6) ; Pietranton, Kelsey (PAO) (b) (6) ; McGowan, Ashley L. (PAO) (b) (6) Bradford, Aryele (PAO) (b) (6) Morales, Arlen M. (PAO) (b) (6) ; Fauntleroy, Priscilla M. (PAO) (b) (6) >; Stueve, Joshua (PAO) (b) (6) ; Roberts, Alivia P. (PAO) (b) (6) >; Blevins, Danielle (PAO) (b) (6) >; Navas, Nicole (PAO) (b) (6) >
Subject: RE: Nightly Look Ahead by 4:45pm

Reminder to submit if you have not yet please!

From: Gelber, Sophie (PAO)
Sent: Tuesday, October 5, 2021 2:19 PM
To: Mitchell, Kendall M. (PAO) (b) (6) ; Li, Kaei (PAO) (b) (6) ; Shevlin, Shannon (PAO) (b) (6) ; Iverson, Dena (PAO) (b) (6) ; Hornbuckle, Wyn (PAO) (b) (6) ; Coley, Anthony D. (PAO) (b) (6) ; Mastropasqua, Kristina (PAO) (b) (6) Pietranton, Kelsey (PAO) (b) (6) ; McGowan, Ashley L. (PAO) (b) (6) >; Bradford, Aryele (PAO) (b) (6) ; Morales, Arlen M. (PAO) (b) (6) >; Fauntleroy, Priscilla M. (PAO) (b) (6) ; Stueve, Joshua (PAO) (b) (6) >; Roberts, Alivia P. (PAO) (b) (6) ; Blevins, Danielle (PAO) (b) (6) >; Navas, Nicole (PAO) (b) (6) >
Subject: Nightly Look Ahead by 4:45pm

Hi all,

Please submit your Nightly Look Ahead entries + PR drafts/upcoming interviews or news stories **by 4:45 pm.**

Thank you!
Sophie

Sophie Gelber
Press Assistant, Office of Public Affairs
U.S. Department of Justice
(b) (6) – work

(b) (6)

From: Saupp, Kevin
Subject: [EXTERNAL] RE: AG Memo - Threats Against Schools
To: Gannon, Anne (ODAG)
Sent: October 5, 2021 12:09 PM (UTC-04:00)

Thank you!

From: Gannon, Anne (ODAG) (b) (6)
Sent: Tuesday, October 5, 2021 12:04 PM
To: Saupp, Kevin (b) (6); Thiemann, Robyn (OLP) (b) (6); Thiemann, Robyn (ODAG) (b) (6)
Subject: RE: AG Memo - Threats Against Schools

The full memo should be attached.

From: Saupp, Kevin (b) (6)
Sent: Tuesday, October 5, 2021 8:52 AM
To: Gannon, Anne (ODAG) (b) (6); Thiemann, Robyn (OLP) (b) (6); Thiemann, Robyn (ODAG) (b) (6)
Subject: [EXTERNAL] AG Memo - Threats Against Schools

Hi all, by chance – can you share the full memo, noted below?

From: Lan, Iris (ODAG)
Subject: RE: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release
To: Jay Greenberg; Driscoll, Kevin (CRM)
Sent: October 4, 2021 5:49 PM (UTC-04:00)

Just picking this up and will call.

From: Jay Greenberg (b)(6); (b)(7)(E) per FBI
Sent: Monday, October 4, 2021 5:05 PM
To: Lan, Iris (ODAG) (b) (6) ; Driscoll, Kevin (CRM) (b) (6)
Subject: FW: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

Iris/Kevin – we have some concern with the attached and would like additional time to engage with you before this messaging is released. CTD has been leading the charge on this for our engagement across the street with Kevin Chambers, but I would ask for any assistance you can provide in helping us get time to find common ground we can all support. None of us wants to see any threats of violence tolerated, and I am sure we can find a way to stand together on that messaging given appropriate time to work through any concerns.

Thanks.

Jay

Deputy Assistant Director
Public Corruption and Civil Rights
Financial Crimes
Undercover Operations
(b)(6); (b)(7)(E) per FBI

(b)(6), (b)(7)(C), (b)(7)(E) per FBI

From: Shevlin, Shannon (PAO)
Subject: RE: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST
To: Hornbuckle, Wyn (PAO); Li, Kaei (PAO); Mitchell, Kendall M. (PAO); Gelber, Sophie (PAO); Morris, Catherine (PAO)
Sent: October 4, 2021 5:49 PM (UTC-04:00)

Probably because it's a .com not .gov? I'll change it and try again.

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Monday, October 4, 2021 5:44 PM
To: Li, Kaei (PAO) (b) (6); Shevlin, Shannon (PAO) (b) (6); Mitchell, Kendall M. (PAO) (b) (6); Gelber, Sophie (PAO) (b) (6); Morris, Catherine (PAO) (b) (6)
Subject: RE: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

Thanks we're still holding. Does the FBI link below work for others? Im getting blocked?

From: Li, Kaei (PAO) (b) (6)
Sent: Monday, October 4, 2021 5:42 PM
To: Shevlin, Shannon (PAO) (b) (6); Mitchell, Kendall M. (PAO) (b) (6); Gelber, Sophie (PAO) (b) (6); Morris, Catherine (PAO) (b) (6)
Cc: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

Also attach a copy of the memo if it's public.

From: Shevlin, Shannon (PAO) (b) (6)
Sent: Monday, October 4, 2021 5:34 PM
To: Li, Kaei (PAO) (b) (6); Mitchell, Kendall M. (PAO) (b) (6) Gelber, Sophie (PAO) (b) (6); Morris, Catherine (PAO) (b) (6)
Cc: Hornbuckle, Wyn (PAO) (b) (6)
Subject: FW: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

Any edits?

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: USDOJ-Office of Public Affairs <USDOJ-OfficeofPublicAffairs@public.govdelivery.com>
Sent: Monday, October 4, 2021 5:31 PM
To: Shevlin, Shannon (PAO) (b) (6)
Subject: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

October 4, 2021

Justice Department Addresses Violent Threats Against School Officials and Teachers

WASHINGTON – Citing an increase in harassment, intimidation and threats of violence against school board members, teachers and workers in our nation's public schools, today Attorney General Merrick B. Garland directed the FBI and U.S. Attorneys' Offices to meet in the next 30 days with federal, state, tribal, territorial and local law enforcement leaders to discuss strategies for addressing this disturbing trend. These sessions will open dedicated lines of communication for threat reporting, assessment, and response by law enforcement.

"Threats against public servants are not only illegal, they run counter to our nation's core values," wrote Attorney General Garland. "Those who dedicate their time and energy to ensuring that our children receive a proper education in a safe environment deserve to be able to do their work without fear for their safety."

According to the Attorney General's memorandum, the Justice Department will launch a series of additional efforts in the coming days designed to address the rise in criminal conduct directed toward school personnel. Those efforts are expected to include the creation of a task force, consisting of representatives from the department's Criminal Division, National Security Division, Civil Rights Division, the Executive Office for U.S. Attorneys, the FBI, the Community Relations Service, and the Office of Justice Programs, to determine how federal enforcement tools can be used to prosecute these crimes, and ways to assist state, tribal, territorial and local law enforcement where threats of violence may not constitute federal crimes.

The Justice Department will also create specialized training and guidance for local school boards and school administrators. This training will help school board members and other potential threats victims understand the type of behavior that constitutes threats, how to report threatening conduct to the appropriate law enforcement agencies, and how to capture and preserve evidence of threatening conduct to aid in the investigation and prosecution of these crimes.

Threats of violence against school board members, officials and workers in our nation's public schools can be reported by the public to the FBI's National Threat Operations Center (NTOC) via its national tip line (1-800-CALL-FBI) and online through the FBI website (http://fbi.com/tips). To ensure that threats are communicated to the appropriate authorities, NTOC will direct credible threats to FBI field offices, for coordination with the U.S. Attorney's Office and law enforcement partners as appropriate. Reporting threats of violence through NTOC will help the federal government identify increased threats in specific jurisdictions as well as coordinated widespread efforts to intimidate educators and education workers.

###

OAG

21-960

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

THE UNITED STATES DEPARTMENT of JUSTICE

FOR IMMEDIATE RELEASE
October 4, 2021
www.justice.gov

OAG
202-514-2007
TTY 866-544-5309

Justice Department Addresses Violent Threats Against School Officials and Teachers

WASHINGTON Citing an increase in harassment, intimidation, and threats of violence against school board members, teachers, and workers in our nation's public schools, today Attorney General Merrick B. Garland directed the FBI and U.S. Attorneys' Offices to meet in the next 30 days with federal, state, Tribal, territorial and local law enforcement leaders to discuss strategies for addressing this disturbing trend. These sessions will open dedicated lines of communication for threat reporting, assessment, and response by law enforcement.

"Threats against public servants are not only illegal, they run counter to our nation's core values," wrote Attorney General Garland. "Those who dedicate their time and energy to ensuring that our children receive a proper education in a safe environment deserve to be able to do their work without fear for their safety."

According to the Attorney General's memorandum, the Justice Department will launch a series of additional efforts in the coming days designed to address the rise in criminal conduct directed toward school personnel. Those efforts are expected to include the creation of a task force, consisting of representatives from the department's Criminal Division, National Security Division, Civil Rights Division, the Executive Office for U.S. Attorneys, the FBI, the Community Relations Service, and the Office of Justice Programs, to determine how federal enforcement tools can be used to prosecute these crimes, and ways to assist state, Tribal, territorial and local law enforcement where threats of violence may not constitute federal crimes.

The Justice Department will also create specialized training and guidance for local school boards and school administrators. This training will help school board members and other potential victims understand the type of behavior that constitutes threats, how to report threatening conduct to the appropriate law enforcement agencies, and how to capture and preserve evidence of threatening conduct to aid in the investigation and prosecution of these crimes.

Threats of violence against school board members, officials, and workers in our nation's public schools can be reported by the public to the FBI's National Threat Operations Center (NTOC) via its national tip line (1-800-CALL-FBI) and online through the FBI website (http://fbi.com/tips). To ensure that threats are communicated to the appropriate authorities, NTOC will direct credible threats to FBI field offices, for coordination with the U.S. Attorney's

Office and law enforcement partners as appropriate. Reporting threats of violence through NTOC will help the federal government identify increased threats in specific jurisdictions as well as coordinated widespread efforts to intimidate educators and education workers.

###

From: Shevlin, Shannon (PAO)
Subject: FW: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST
To: (b)(6) Shannon Shevlin (PAO)
Sent: October 4, 2021 5:46 PM (UTC-04:00)

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: Shevlin, Shannon (PAO) (b) (6)
Sent: Monday, October 4, 2021 5:46 PM
To: Shevlin, Shannon (PAO) (b) (6)
Subject: FW: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

Shannon R. Shevlin
Press Assistant
Office of Public Affairs | U.S. Department of Justice
(m) (b) (6)

From: Li, Kaei (PAO) (b) (6)
Sent: Monday, October 4, 2021 5:42 PM
To: Shevlin, Shannon (PAO) (b) (6) ; Mitchell, Kendall M. (PAO) (b) (6) ; Gelber, Sophie (PAO) (b) (6) ; Morris, Catherine (PAO) (b) (6)
Cc: Hornbuckle, Wyn (PAO) (b) (6)
Subject: RE: [EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers: TEST

Duplicative Material, Document ID: 0.7.1451.10368

From: Chambers, Kevin (ODAG)
Subject: FW: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release
To: Greenberg, Jay (CID) (FBI)
Sent: October 4, 2021 5:33 PM (UTC-04:00)
Attached: Final.AG MEMO TO USAOs AND SACs (10.4.21).docx, DRAFT PRESS RELEASE - Threats Against School Workers (version to components).docx

FYI. See draft PR for what I called "strategies"

From: Chambers, Kevin (ODAG)
Sent: Monday, October 4, 2021 3:00 PM
To: Jensen, Steven J. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; McQuaid, Nicholas (CRM) (b) (6); Moossy, Robert (CRT) (b) (6); Wilkinson, Monty (USAEO) (b)(6), (b)(7)(C) per EOUSA; Toscas, George (NSD) (b) (6); Darke Schmitt, Katherine (OJP/OVC) (b) (6); Tarasca, James A. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Blue, Matt (NSD) (b) (6) Langan, Timothy R. Jr. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; (b)(6), (b)(7)(C), (b)(7)(E) per FBI; (b)(6), (b)(7)(C), (b)(7)(E) per FBI Vorndran, Kevin (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Lesko, Mark (NSD) (b) (6) Wiegmann, Brad (NSD) (b) (6); 'Driscoll, Kevin (CRM)' (b) (6) >; Rossi, Rachel (OASG) (b) (6); Monroe, Becky (OASG) (b) (6) >; Wong, Norman (USAEO) (b)(6), (b)(7)(C) per EOUSA
Cc: Braden, Myesha (ODAG) (b) (6) >; Newman, David A. (ODAG) (b) (6); Lan, Iris (ODAG) (b) (6)
Subject: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

Duplicative Material, Document ID: 0.7.1451.5740

From: Hornbuckle, Wyn (PAO)
Subject: Final PR on Threats to School Officials
To: Klapper, Matthew B. (OAG)
Cc: Coley, Anthony D. (PAO)
Sent: October 4, 2021 3:31 PM (UTC-04:00)
Attached: AG Memo Threats Against School Workers 10-4-2021 1515.docx

Matt,

ODAG has cleared. For OAG review/ final clearance.

Components and USAOs will be notified around 3:45.

Plan to release at 5 p.m.

Wyn Hornbuckle
Deputy Director, Office of Public Affairs
U.S. Department of Justice
O: (b) (6)
M: (b) (6)

From: Greenfeld, Helaine A. (OLA)
To: McKay, Shirley A (OLA)
Cc: Calce, Christina M. (OLA)
Subject: RE: Letter Regarding Memorandum Dated October 4.
Date: Friday, October 8, 2021 11:26:42 AM
Attachments: image001.png

You can assign these all to me. We are drafting a response here in OLA. Thanks, Shirley.

From: McKay, Shirley A (OLA) (b) (6)
Sent: Friday, October 8, 2021 10:55 AM
To: Greenfeld, Helaine A. (OLA) (b) (6)
Cc: Calce, Christina M. (OLA) (b) (6)
Subject: RE: Letter Regarding Memorandum Dated October 4.
Importance: High

Hi Helaine

We have received several of these letters regarding public school officials that reference DOJ 10/4 memo & I have I not received any guidance. Pls advise. Thanks.

From: Greenfeld, Helaine A. (OLA) (b) (6)
Sent: Friday, October 8, 2021 10:35 AM
To: McKay, Shirley A (OLA) (b) (6)
Cc: Gaeta, Joseph (OLA) (b) (6) ; Calce, Christina M. (OLA) (b) (6)
Subject: FW: Letter Regarding Memorandum Dated October 4.

Another for logging. Assign to me.

From: Stewart, Tucker (Marshall) (b) (6)
Sent: Friday, October 8, 2021 10:14 AM
To: Greenfeld, Helaine A. (OLA) (b) (6)
Cc: McMullan, Pace (Marshall) (b) (6)
Subject: [EXTERNAL] Letter Regarding Memorandum Dated October 4.

Hello Helaine,

Please see the attached letter from Senator Marshall and colleagues. Thanks.

Best Regards,

(b) (6)

Tucker A. Stewart, Esq.
Senior Agricultural Policy Advisor
Office of U.S. Senator Roger Marshall, M.D.
(b) (6) (cell)
(b) (6) (office)
(b) (6)

From:	McKay, Shirley A (OLA)
To:	DOJExecSec (JMD)
Cc:	Tolson, Kimberly G (JMD)
Subject:	FW: SJC to DOJ re Schools (21.10.07)
Date:	Friday, October 8, 2021 12:21:01 PM
Attachments:	SJC to DOJ re Schools (21.10.07).pdf OLA.Greenfeld.assignment.guidance.public.school.officials.10.4.memo.pdf
Importance:	High

Pls log & assign to OLA for appropriate handling. OLA (Greenfeld) will be handling this matter. Thanks.

From: Gaeta, Joseph (OLA) (b) (6)
Sent: Thursday, October 7, 2021 3:20 PM
To: McKay, Shirley A (OLA) (b) (6)
Cc: (b) (6) (OLA) (b) (6) ; Greenfeld, Helaine A. (OLA) (b) (6) ; Antell, Kira M. (OLA) (b) (6)
Subject: FW: SJC to DOJ re Schools (21.10.07)

Stand by for assignment of this and the other school board letters.

From: Schoenecker, John (Judiciary-Rep) (b) (6)
Sent: Thursday, October 7, 2021 11:53 AM
To: Gaeta, Joseph (OLA) (b) (6)
Subject: [EXTERNAL] SJC to DOJ re Schools (21.10.07)

Mr. Gaeta,

This is to kindly request that you deliver the attached letter from the Republican Members of the Senate Committee on the Judiciary to Attorney General Garland. Also, please confirm your receipt of this email.

Best regards,

John L. Schoenecker
Counsel
Ranking Member Charles E. Grassley
U.S. Senate Committee on Judiciary
(b) (6)

From: Jay Greenberg
Subject: FW: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release
To: Lan, Iris (ODAG); Driscoll, Kevin (CRM)
Sent: October 4, 2021 5:05 PM (UTC-04:00)
Attached: Final.AG MEMO TO USAOs AND SACs (10.4.21).docx, DRAFT PRESS RELEASE - Threats Against School Workers (version to components).docx

Iris/Kevin – we have some concern with the attached and would like additional time to engage with you before this messaging is released. CTD has been leading the charge on this for our engagement across the street with Kevin Chambers, but I would ask for any assistance you can provide in helping us get time to find common ground we can all support. None of us wants to see any threats of violence tolerated, and I am sure we can find a way to stand together on that messaging given appropriate time to work through any concerns.

Thanks.

Jay

Deputy Assistant Director
Public Corruption and Civil Rights
Financial Crimes
Undercover Operations
(b)(6); (b)(7)(E) per FBI
(b)(6); (b)(7)(E) per FBI
(b)(6), (b)(7)(C), (b)(7)(E) per FBI

From: Langan, Timothy R. Jr. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI
Sent: Monday, October 4, 2021 3:54 PM
To: Greenberg, Jay (CID) (FBI) (b)(6); (b)(7)(E) per FBI; Coakley, Miriam M. (OGC) (FBI) (b)(6); (b)(7)(E) per FBI; McCarthy, Dawn L. (OGC) (FBI) (b)(6); (b)(7)(E) per FBI
Subject: FW: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

Making sure you all had this from today. I'm trying to track down additional on this from today.

Tim Langan
Assistant Director
FBI Counterterrorism Division

From: Chambers, Kevin (ODAG) (b) (6)
Sent: Monday, October 4, 2021 3:00 PM
To: Jensen, Steven J. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; McQuaid, Nicholas (CRM) (b) (6) Moossy, Robert (CRT) (b) (6) Wilkinson, Monty (USAEO) (b)(6), (b)(7)(C) per EOUSA; Toscas, George (NSD) (JMD) (b) (6) ; Darke Schmitt, Katherine (OJP/OVC) (b) (6) ; Tarasca, James A. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Blue, Matt (NSD) (JMD) (b) (6) ; Langan, Timothy R. Jr. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; (b)(6), (b)(7)(C), (b)(7)(E) per FBI (b)(6), (b)(7)(C), (b)(7)(E) per FBI Vorndran, Kevin (CTD) (FBI) (b)(6); (b)(7)(E) per FBI Lesko, Mark (NSD) (JMD) (b) (6) Wiegmann, Brad (NSD) (JMD) (b) (6) ; Driscoll, Kevin (CRM) (b) (6) ; Rossi, Rachel (OASG) (JMD) (b) (6) ; Monroe, Becky (OASG) (JMD) (b) (6) ; Wong, Norman (USAEO)

(b)(6), (b)(7)(C) per EOUSA

Cc: Braden, Myesha (ODAG) (JMD) (b) (6) >; Newman, David A. (ODAG) (JMD) (b) (6) Lan, Iris (ODAG) (JMD) (b) (6)

Subject: [EXTERNAL EMAIL] - FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

From:
Subject: RE: Final PR on Threats to School Officials
To: Matthews-Johnson, Tamarra D. (OAG); Hornbuckle, Wyn (PAO); Klapper, Matthew B. (OAG)
Cc: Coley, Anthony D. (PAO)
Sent: October 4, 2021 4:45 PM (UTC-04:00)

I'm fine; it looks good. But Matt has final pen/call on this.

From: Matthews-Johnson, Tamarra D. (OAG) (b) (6)
Sent: Monday, October 4, 2021 4:40 PM
To: Hornbuckle, Wyn (PAO) (b) (6) ; Klapper, Matthew B. (OAG)
(b) (6)
Cc: Heinzelman, Kate (OAG) (b) (6) ; Coley, Anthony D. (PAO) (b) (6)
Subject: RE: Final PR on Threats to School Officials

From:
Subject: RE: Final PR on Threats to School Officials
To: Hornbuckle, Wyn (PAO); Matthews-Johnson, Tamarra D. (OAG); Klapper, Matthew B. (OAG)
Cc: Heinzelman, Kate (OAG)
Sent: October 4, 2021 4:41 PM (UTC-04:00)

Maybe tweak the headline from the creation TF to Justice Department Addresses Violent

---

From: Hornbuckle, Wyn (PAO) (b) (6)
Sent: Monday, October 4, 2021 4:37 PM
To: Matthews-Johnson, Tamarra D. (OAG) (b) (6) ; Klapper, Matthew B. (OAG) (b) (6)
Cc: Heinzelman, Kate (OAG) (b) (6) ; Coley, Anthony D. (PAO) (b) (6)
Subject: RE: Final PR on Threats to School Officials

Duplicative Material, Document ID: 0.7.1451.9797

From:
Subject: RE: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release
To: Chambers, Kevin (ODAG)
Sent: October 4, 2021 3:25 PM (UTC-04:00)

Understood. But once we say it and school boards ask for it, Lisa will be on the hook to testify about it.

From: Chambers, Kevin (ODAG) (b) (6)
Sent: Monday, October 4, 2021 3:21 PM
To: Braden, Myesha (ODAG) (b) (6)
Subject: RE: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

From:
Subject:
To:
Sent: October 4, 2021 2:10 PM (UTC-04:00)

In the coming days, the Department will announce a series of measures designed to address the rise in criminal conduct directed toward school personnel

Anthony D. Coley, Director
Office of Public Affairs &
Sr. Advisor to the Attorney General
U.S. Department of Justice
Direct: (b) (6)
Cell: (b) (6)
@AnthonyColeyDOJ

From: Klapper, Matthew B. (OAG)
Subject: FW: state and local partners
To: Davidson, Marcia A. (OAG)
Sent: October 4, 2021 11:49 AM (UTC-04:00)

Please include "Tribal, and territorial" after "State, Local"

Thanks

From: Chambers, Kevin (ODAG) (b) (6)
Sent: Monday, October 4, 2021 11:47 AM
To: Klapper, Matthew B. (OAG) (b) (6) ; Matthews-Johnson, Tamarra D. (OAG) (b) (6) ; Stamper, Gwendolyn (CRM) (b) (6) ; McQuaid, Nicholas (CRM) (b) (6)
Cc: Heinzelman, Kate (OAG) (b) (6)
Subject: RE: state and local partners

No flags from ODAG.

From: Klapper, Matthew B. (OAG) (b) (6) >
Sent: Monday, October 4, 2021 11:46 AM
To: Chambers, Kevin (ODAG) (b) (6) ; Matthews-Johnson, Tamarra D. (OAG) (b) (6) ; Stamper, Gwendolyn (CRM) (b) (6) McQuaid, Nicholas (CRM) (b) (6)
Cc: Heinzelman, Kate (OAG) (b) (6)
Subject: RE: state and local partners

Given the scope is expanded to include threats to teachers (and even without that), I have to believe that the issue exists or on tribal lands and in the territories. Going to include mention of both unless flags are raised.

From: Chambers, Kevin (ODAG) (b) (6)
Sent: Monday, October 4, 2021 11:38 AM
To: Matthews-Johnson, Tamarra D. (OAG) (b) (6) ; Stamper, Gwendolyn (CRM) (b) (6) >; McQuaid, Nicholas (CRM) (b) (6)
Cc: Klapper, Matthew B. (OAG) (b) (6) >; Heinzelman, Kate (OAG) (b) (6)
Subject: RE: state and local partners

There was not. Earlier drafts (which only I may have seen) contained S, L, Tr., but reduced down to S, L. The letter makes reference only to S/L, and I don't know how widely this is an issue on tribal land or in territories, but there was no conscious decision on my part to include/exclude Tr. and T.

Thanks,
Kevin

From: Matthews-Johnson, Tamarra D. (OAG) (b) (6)
Sent: Monday, October 4, 2021 11:32 AM
To: Chambers, Kevin (ODAG) (b) (6) ; Stamper, Gwendolyn (CRM) (b) (6) >; McQuaid, Nicholas (CRM) (b) (6)
Cc: Klapper, Matthew B. (OAG) (b) (6) >; Heinzelman, Kate (OAG) (b) (6)
Subject: state and local partners

Hi -
For the school board memo, was there a conscious decision on how we list our partners
State and local
As opposed to
State, local, and tribal
Or
State, local, tribal, and territorial

Tamarra Matthews Johnson
she/her/hers
Counsel
Office of the Attorney General
U.S. Department of Justice
Mobile: (b) (6)

From: Rossi, Rachel (OASG)
Subject: RE: Bios & Materials
To: Visser, Tim (OAG)
Sent: October 4, 2021 10:40 AM (UTC-04:00)

Totally your call! Just flagging this as a big announcement that may come today on an overlapping topic. But I have little visibility.

From: Visser, Tim (OAG) (b) (6)
Sent: Monday, October 4, 2021 10:32 AM
To: Rossi, Rachel (OASG) (b) (6)
Subject: RE: Bios & Materials

I spoke to Matt about the HHS event tomorrow and he did not say a peep about this – only asked that we keep tomorrow as simple as humanly possible. I will discuss with him later but I'm inclined to leave this as is.

From: Rossi, Rachel (OASG) (b) (6)
Sent: Monday, October 4, 2021 10:24 AM
To: Visser, Tim (OAG) (b) (6)
Subject: RE: Bios & Materials

The AG is issuing a statement or memo of some kind today about the Department's full resources on combatting hate in schools – if the AG or OAG want to bring the topic up tomorrow I think that's really your decision. We've decided to (1) not change the questions we're asking for tomorrow and to (2) not invite any new groups to expand the focus tomorrow, but the AG may still want to mention this because it is somewhat connected. I would imagine he may want to at minimum say "I issued x yesterday…"

I don't know the latest plan on what he's going to issue either. Maybe Tamarra knows?

From: Visser, Tim (OAG) (b) (6)
Sent: Monday, October 4, 2021 10:10 AM
To: Rossi, Rachel (OASG) (b) (6)
Subject: RE: Bios & Materials

I thought the decision was *not* to include that anymore… I am very, very confused on that issue.

From: Rossi, Rachel (OASG) (b) (6)
Sent: Monday, October 4, 2021 10:10 AM
To: Visser, Tim (OAG) (b) (6)
Subject: RE: Bios & Materials

Yes, oh! I forgot to figure out if/how we may want to mention the school threats issue. Sounds like an AG statement may come out today listing the Department's resources to combat hate/threats. So I would defer to you on adding anything in his remarks?

From: Visser, Tim (OAG) (b) (6)
Sent: Monday, October 4, 2021 10:00 AM
To: Rossi, Rachel (OASG) (b) (6)
Subject: RE: Bios & Materials

Indeed! Maybe he can draft it? Haha. Let me know when you get the speaker bios.

From: Rossi, Rachel (OASG) (b) (6)

Sent: Monday, October 4, 2021 12:47 AM
To: Visser, Tim (OAG) (b) (6)
Subject: Re: Bios & Materials

Looks great! Also did you know Becerra in his former role, actually did some guidance on hate during the pandemic? Interesting, https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-guidance-law-enforcement-hate-crimes-during

Good night!

Sent from my iPhone

> On Oct 3, 2021, at 11:21 PM, Visser, Tim (OAG) (b) (6) wrote:
>
> Thanks! Looks good. These are still very much works in progress – and as you've seen the AG routinely cuts down these draft remarks significantly – but here is where I am heading at the moment for the AG materials. I will plan on finalizing these and getting them to the AG by tomorrow afternoon. Let me know if you have any concerns.
>
> ---
>
> **From:** Rossi, Rachel (OASG) (b) (6)
> **Sent:** Sunday, October 3, 2021 10:55 PM
> **To:** Visser, Tim (OAG) (b) (6)
> **Subject:** RE: Bios & Materials
>
> Sending the draft so far, I imagine this will still be fine-tuned, especially as we connect with HHS tomorrow to finalize. VG also tends to edit. Note that we planned about 10-15 minutes leeway throughout.
>
> ---
>
> **From:** Visser, Tim (OAG) (b) (6) >
> **Sent:** Sunday, October 3, 2021 10:16 PM
> **To:** Rossi, Rachel (OASG) (b) (6)
> **Subject:** RE: Bios & Materials
>
> This background section is very helpful. Thank you!
>
> ---
>
> **From:** Rossi, Rachel (OASG) (b) (6)
> **Sent:** Sunday, October 3, 2021 9:24 PM
> **To:** Visser, Tim (OAG) (b) (6) >
> **Subject:** RE: Bios & Materials
>
> Sending this draft to you so you have it ASAP, but still editing.
>
> Note, I thought we agreed that the AG and Secretary would provide some concluding remarks, right? I asked Krystal to confirm so that we can update the agenda. If so, content from VG's closing will need to be transferred into her opener and shortened.
>
> ---
>
> **From:** Visser, Tim (OAG) (b) (6) >
> **Sent:** Sunday, October 3, 2021 7:46 PM
> **To:** Rossi, Rachel (OASG) (b) (6)
> **Subject:** RE: Bios & Materials
>
> Thanks for the heads up. FWIW, I am nearly certain you, me, ASG, and AG will all be in the same room on

the same link.

From: Rossi, Rachel (OASG) (b) (6) >
Sent: Sunday, October 3, 2021 7:40 PM
To: Visser, Tim (OAG) (b) (6)
Subject: RE: Bios & Materials

Of course. Also, flagging that you, me, and 2 staffers from HHS will have "panelist" links. We'll get them emailed to us tomorrow. We will all have our cameras and mics off, but will be on in case Principals need us or if we need to step in for any reason. All other attendees will not be visible and the chat feature will be disabled.

From: Visser, Tim (OAG) (b) (6)
Sent: Sunday, October 3, 2021 7:37 PM
To: Rossi, Rachel (OASG) (b) (6)
Subject: RE: Bios & Materials

Thanks!

From: Rossi, Rachel (OASG) (b) (6) >
Sent: Sunday, October 3, 2021 7:35 PM
To: Visser, Tim (OAG) (b) (6) >
Subject: RE: Bios & Materials

I don't think I ever got her final draft – Kristen had some edits. But here is the most final version I had. Also, let me forward you something Sparkle just sent, some of the data on prosecutions is different.

From: Visser, Tim (OAG) (b) (6)
Sent: Sunday, October 3, 2021 7:32 PM
To: Rossi, Rachel (OASG) (b) (6) >
Subject: RE: Bios & Materials

Thanks. Would you mind passing along your full TPs and Kristen's full TPs from the WH session you did? I don't think I ended up ever seeing those.

From: Rossi, Rachel (OASG) (b) (6) >
Sent: Sunday, October 3, 2021 7:25 PM
To: Visser, Tim (OAG) (b) (6) >
Subject: RE: Bios & Materials

Krystal is going to send them all the bios to us! She said by tonight/this evening, so I can reach out again. But she's preparing photos and bios of all speakers. I'll have Vanita's talking points done at some point tonight, not sure how late though. I'll try to get the opener to you at least – but she may have edits.

How much detail do you think the AG would like to have? The main pieces of info that I might provide (or include some data from) are (1) the FY2020 hate crimes statistics high level points (I think good to show anti-Black hate went up too, and that it is still the largest threat); and (2) the Stop AAPI Hate data (which we expect them to raise when they speak).

Also, just as a flag to be aware of because the Secretary is often focused on Latino issues and this may come up – there was what appeared to be a lynching of a Mexican man at the border, and Joaquin Castro tweeted about it today.

Here are some TPs from Kristen Clark on the 2020 Hate Crimes data, that may be helpful to curb:

- The FBI 2020 Hate Crime Statistics released on August 30 confirm what we have seen and heard from communities, advocates, and law enforcement agencies around the country.

- Hate crimes rose in 2020 to their highest levels in more than a decade. And the majority, over 60%, were motivated by race and ethnicity. And of those, more than a third targeted African Americans. We also saw a sharp rise in reported attacks on people of Asian descent this year, including multiple terrible attacks on elderly people and women.

- Here are some specifics.

    - The rise of anti-Asian hate was sharp (+70%) and represents the highest total in more than a decade.

    - There was another sharp rise (+25%) in incidents based on the gender identity of the victim (236), a category that has risen steadily every year since the FBI began tracking this category in 2013.

- There is another sobering statistic that we need to talk about today. For the third year in a row, the number of police agencies participating in the FBI's annual report declined, with thousands of departments either not reporting any data to the FBI or reporting zero hate crimes. Over 12,000 law enforcement agencies affirmatively reported zero (0) hate crimes – including 65 agencies in cities with populations over 100,000 people.

- Unfortunately, non-reporting of hate crimes by law enforcement has been a longstanding issue. And that's partly due to the fact that law enforcement agencies are not required by law to report hate crime data to the FBI.

From: Visser, Tim (OAG) (b) (6) >
Sent: Sunday, October 3, 2021 7:00 PM
To: Rossi, Rachel (OASG) (b) (6)
Subject: RE: Bios & Materials

Sorry for the inevitable pester on the below – particularly given how much you have going on. How's this coming along?

From: Rossi, Rachel (OASG) (b) (6) >
Sent: Friday, October 1, 2021 6:41 PM
To: Visser, Tim (OAG) (b) (6) >
Subject: RE: Bios & Materials

Not annoying, and I can aim to have this by then. Hoping Krystal will have speaker bios at least already done.

From: Visser, Tim (OAG) (b) (6) >
Sent: Friday, October 1, 2021 6:40 PM

To: Rossi, Rachel (OASG) (b) (6)
Subject: Bios & Materials

Hi, Rachel –

Sorry if this is annoying, but by ~6pm on Sunday, can you get me all confirmed speaker bios, a draft intro for Vanita, and any other pre-read materials that you think the AG should have? I will of course give him the text of the legislation and run of show, but welcome your thoughts on anything else he should see.

I will likely need to finish up his remarks and event memo by Sunday night.

-TV
<Draft AG Remarks_10.5 Listening Session with HHS.docx>
<10.5_ HHS COVID-19 Hate Crimes_Event Memo.doc>

From: Singh, Anita M. (ODAG)
Subject: Re: Threats to school boards
To: Klapper, Matthew B. (OAG)
Cc: Chambers, Kevin (ODAG); Carlin, John P. (ODAG)
Sent: October 3, 2021 10:23 AM (UTC-04:00)

Thanks!

Anita M. Singh
Chief of Staff
Office of the Deputy Attorney General
U.S. Department of Justice

C: (b) (6)
O: (b) (6)

On Oct 3, 2021, at 9:25 AM, Klapper, Matthew B. (OAG) (b) (6) wrote:

Thanks Anita. Will likely be Monday late or Tuesday am for issuance due to AG's calendar. OAG will review this morning and ship to him in the event we can get eyes on sooner for review.

Sent from my iPhone

On Oct 3, 2021, at 9:13 AM, Chambers, Kevin (ODAG) (b) (6) wrote:

Thanks, Anita.
CRM is aware of the new approach on memo. I will update remaining components.

From: Singh, Anita M. (ODAG) (b) (6)
Sent: Sunday, October 3, 2021 7:55 AM
To: Klapper, Matthew B. (OAG) (b) (6)
Cc: Chambers, Kevin (ODAG) (b) (6) ; Carlin, John P. (ODAG) (b) (6)
Subject: Threats to school boards

From: Klapper, Matthew B. (OAG)
Subject: Fwd: Threats to school boards
To: Matthews-Johnson, Tamarra D. (OAG)
Cc: Heinzelman, Kate (OAG)
Sent: October 3, 2021 9:30 AM (UTC-04:00)
Attached: NSBA Letter to President Biden Concerning Threats to Public Schools and School Board Members.pdf, DRAFT AG MEMO TO USAOs AND SACs (10.3.21) (SCHOOL BOARDS ONLY).docx

Would like to ship this to AG by noon if possible. Please engage directly with Kevin if you have questions or edits (Kate and I are happy to discuss too, of course). The attached has component and ODAG sign off. We'll obviously have to run it through again once AG offers edits. Note that issuance is NLT Tuesday morning, but we'll aim for tomorrow.

Sent from my iPhone

Begin forwarded message:

From: "Singh, Anita M. (ODAG)" (b) (6)
Date: October 3, 2021 at 7:54:43 AM EDT
To: "Klapper, Matthew B. (OAG)" (b) (6)
Cc: "Chambers, Kevin (ODAG)" (b) (6) , "Carlin, John P. (ODAG)" (b) (6)
Subject: Threats to school boards

From: Carlin, John P. (ODAG)
Subject: Re: Drafts for DAG Review
To: Klapper, Matthew B. (OAG)
Sent: October 3, 2021 9:28 AM (UTC-04:00)

Will do

On Oct 3, 2021, at 9:23 AM, Klapper, Matthew B. (OAG) (b) (6) wrote:

Thanks. Call when can.

Sent from my iPhone

On Oct 2, 2021, at 9:02 PM, Carlin, John P. (ODAG) (b) (6) wrote:

Bootleg for review, will explain

Begin forwarded message:

From: "Chambers, Kevin (ODAG)" (b) (6)
Date: October 2, 2021 at 8:01:29 PM EDT
To: "Carlin, John P. (ODAG)" (b) (6)
Subject: Drafts for DAG Review

John,

Attached are the following documents:

1. DRAFT AG memo covering both election and school board threats
2. DRAFT AG memo covering school board threats only
3. Strategy document for school board threats response

Can discuss at your convenience.

Kevin

From: Carlin, John P. (ODAG) (b) (6)
Sent: Saturday, October 2, 2021 7:20 PM
To: Chambers, Kevin (ODAG) (b) (6)
Subject: Re: CRM

Many thanks

On Oct 2, 2021, at 7:00 PM, Chambers, Kevin (ODAG) (b) (6) wrote:

Ok. Will prepare an SB only version and send to you for DAG review. No other comments so far.

Sent from my iPhone

> On Oct 2, 2021, at 6:24 PM, Carlin, John P. (ODAG) (b) (6) wrote:
>
> Spoke to nick, he will call you: we can try option of just school board threats and hold election threats for later
>
> > On Oct 2, 2021, at 6:03 PM, Chambers, Kevin (ODAG) (b) (6) wrote:
> >
> > Spoke to CRM, which has significant concerns about including directives about convening Election Threats- and School Board-related meetings in the same AG communication. Concern is that including latter will severely undermine efforts on former as two will be conflated, despite our efforts to distinguish. Recommend that we discuss this evening to keep trains moving.

<DRAFT AG MEMO TO USAOs AND SACs (10.2.21) (SCHOOL BOARDS ONLY).docx>
<DRAFT AG MEMO TO USAOs AND SACs (10.2.21).docx>
<Draft School Board Threats Response Strategy (10.2.21).docx>
<NSBA Letter to President Biden Concerning Threats to Public Schools and School Board Members.pdf>

From: Sooknanan, Sparkle (OASG)
Subject: RE: school board threats - CRT role, for public statement today?
To: Colangelo, Matthew (OASG)
Cc: Gupta, Vanita (OASG); Hyun, Peter (OASG)
Sent: October 2, 2021 5:30 PM (UTC-04:00)

More from EOS. Nothing yet from CRM.

<<No, there's nothing specific or public I can share. We've followed the school board meetings in Davis, for example, but that's not some to we would discuss publicly. And that's for the purpose of assessing a hostile environment for students, not for staff or school board members. A good example is how Gavin Grimm was targeted at the Gloucester County school board meetings.>>

From: Colangelo, Matthew (OASG) (b) (6)
Sent: Saturday, October 2, 2021 4:37 PM
To: Sooknanan, Sparkle (OASG) (b) (6)
Cc: Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6)
Subject: Re: school board threats - CRT role, for public statement today?

Thanks - yes, CRS has prepared something and ODAG is working with the CRM Div and FBI

> On Oct 2, 2021, at 4:34 PM, Sooknanan, Sparkle (OASG) (b) (6) wrote:
>
> Still waiting for more. But EOS confirmed that threats or violence by private citizens against school board officials would not fall within its civil authorities.
>
> I assume that ODAG is working with the FBI/ CRM? Also wondering whether CRS has a role (through its mediation program)?
>
> ---
>
> **From:** Sooknanan, Sparkle (OASG)
> **Sent:** Saturday, October 2, 2021 12:07 PM
> **To:** Colangelo, Matthew (OASG) (b) (6)
> **Cc:** Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6)
> **Subject:** RE: school board threats - CRT role, for public statement today?
>
> Waiting for more from EOS. Nothing yet from CRM.
>
> ---
>
> **From:** Colangelo, Matthew (OASG) (b) (6)
> **Sent:** Saturday, October 2, 2021 11:27 AM
> **To:** Sooknanan, Sparkle (OASG) (b) (6)
> **Cc:** Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6)
> **Subject:** RE: school board threats - CRT role, for public statement today?
>
> Thanks very much. Anything more specific EOS can say about the disruptions they do think they have jurisdiction to examine? Are there particular school districts or incidents they are investigating or examining that they can identify or specify for us today? Thank you
> (and I take it no info from CRM yet on 241 or 245?)
>
> ---
>
> **From:** Sooknanan, Sparkle (OASG) (b) (6)
> **Sent:** Saturday, October 2, 2021 10:59 AM
> **To:** Colangelo, Matthew (OASG) (b) (6)

Cc: Gupta, Vanita (OASG) (b) (6) >; Hyun, Peter (OASG) (b) (6)
Subject: RE: school board threats - CRT role, for public statement today?

From EOS:
EOS is looking at disruptions of school board meetings in a few limited contexts where the disruptions may be relevant to evaluating the existence of a hostile environment for students based on a protected characteristic. We are not looking at the disruptions or statements regarding COVID protocols and think those would likely fall outside our jurisdiction.

As for ED-OCR:
Suzanne Goldberg from ED-OCR is also looking at this issue, and she is connected with Myesha.

From: Sooknanan, Sparkle (OASG)
Sent: Saturday, October 2, 2021 8:09 AM
To: Colangelo, Matthew (OASG) (b) (6)
Cc: Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6)
Subject: RE: school board threats - CRT role, for public statement today?

Yes, I'll reach out to them now.

From: Colangelo, Matthew (OASG) (b) (6)
Sent: Saturday, October 2, 2021 7:42 AM
To: Sooknanan, Sparkle (OASG) (b) (6)
Cc: Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6) >
Subject: school board threats - CRT role, for public statement today?
Importance: High

Sparkle – re: the letter to the President on threats against school board members (link and accompanying reporting below) – I gather ODAG may have reached out to CRT yesterday to see if there were any authorities CRT enforces that could help address this issue. Can you check with CRT (this is a Saturday ask, apologies) to see if they have identified anything that they could consider doing to investigate or address this issue?

For CRM matters, does Robert think any of this conduct would be actionable under 241 or 245(b)(1)(F)? And is there any civil authority that EOS enforces (or that ED OCR might enforce) that we think could apply? The Department may need to say something publicly today about its response to these threats, so unfortunately this is a quick-turn request. Thank you - Matthew

https://nsba.org/-/media/NSBA/File/nsba-letter-to-president-biden-concerning-threats-to-public-schools-and-school-board-members-92921.pdf

https://www.npr.org/sections/back-to-school-live-updates/2021/09/30/1041870027/school-boards-federal-help-threats-violence

https://apnews.com/article/coronavirus-pandemic-joe-biden-health-education-school-boards-940da42fac771366929fc2150c8acf4d

https://www.cnn.com/2021/09/30/us/school-board-threats-violence/index.html

From: Colangelo, Matthew (OASG)
Subject: RE: school board threats - CRT role, for public statement today?
To: Sooknanan, Sparkle (OASG)
Cc: Gupta, Vanita (OASG); Hyun, Peter (OASG)
Sent: October 2, 2021 12:11 PM (UTC-04:00)

thanks

From: Sooknanan, Sparkle (OASG) (b) (6) >
Sent: Saturday, October 2, 2021 12:07 PM
To: Colangelo, Matthew (OASG) (b) (6) >
Cc: Gupta, Vanita (OASG) (b) (6) ; Hyun, Peter (OASG) (b) (6)
Subject: RE: school board threats - CRT role, for public statement today?

Duplicative Material, Document ID: 0.7.1451.8528

From: Hyun, Peter (OASG)
Subject: Question about OLA Incoming re: Threats to School Boards
To: Gaeta, Joseph (OLA); Helaine A. Greenfeld (OLA) (b) (6) ; Christina M. Calce (OLA) (b) (6))
Cc: Rossi, Rachel (OASG)
Sent: October 2, 2021 10:12 AM (UTC-04:00)

Helaine/Joe/Christina:

Flagging for you that these items have come to our attention re: attacks/threats to school boards. Just wanted to touch base to see if OLA has received any incoming about this as well? Thanks!

https://www.npr.org/sections/back-to-school-live-updates/2021/09/30/1041870027/school-boards-federal-help-threats-violence

https://nsba.org/-/media/NSBA/File/nsba-letter-to-president-biden-concerning-threats-to-public-schools-and-school-board-members-92921.pdf

https://apnews.com/article/coronavirus-pandemic-joe-biden-health-education-school-boards-940da42fac771366929fc2150c8acf4d

https://www.cnn.com/2021/09/30/us/school-board-threats-violence/index.html

Peter S. Hyun | Chief of Staff
Office of the Associate Attorney General
(b) (6)
Desk: (b) (6)
Cell: (b) (6)

From:
Subject: FW: DRAFT Memorandum from AG to USAOs and SACs: convenings election official and workers
To: Klapper, Matthew B. (OAG)
Sent: October 3, 2021 12:23 PM (UTC-04:00)
Attached: DRAFT AG MEMO TO USAOs AND SACs (10.3.21) (SCHOOL BOARDS ONLY) tmj edits.docx

Matt –

I'm not sure about all of the conversations that have been had on this – but a few points I don't want to lose:

1. I support having these be separate for different reasons than those stated by CRIM. Happy to discuss. Have shared my thinking with Tamarra.
2.

From: Matthews-Johnson, Tamarra D. (OAG) (b) (6)
Sent: Sunday, October 3, 2021 11:52 AM
To: Chambers, Kevin (ODAG) (b) (6)
Cc: Heinzelman, Kate (OAG) (b) (6) ; Klapper, Matthew B. (OAG) (b) (6)
Subject: Re: DRAFT Memorandum from AG to USAOs and SACs: convenings election official and workers

HOUSE JUDICIARY COMMITTEE HEARING OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

MARCH 29, 2022

WITNESSES:

- BRYAN A. VORNDRAN, ASSISTANT DIRECTOR, CYBER DIVISION, FBI

NADLER: The House Committee on the Judiciary will come to order. Without objection, the chair is authorized to declare recesses of the community at any time.

We welcome everyone to this morning's hearing on oversight of the FBI Cyber Division. Before we begin, I'd like to remind members that we have established an e-mail address and distribution list dedicated to circulating exhibits, motions or other written materials that members might want to offer as part of our hearing today. If you'd like to submit materials, please send them to the e-mail address that has previously been distributed to your offices and we will circulate the materials to members and staff as quickly as we can.

I will now recognize myself for an opening statement.

This hearing could not be more appropriately timed. Americans today live at a critical juncture in the history of cybersecurity. Our schools, our businesses, our public safety, our local government, our federal government, our public utilities and our critical infrastructure all exist at a nexus of threats from cyber criminals. In the last year, we've experienced attacks that shut down a gas pipeline along the Eastern Corridor, infiltrated government e-mail systems and froze hospital networks during their time of greatest need. To tritely describe the threat of cyber attacks against the United States as simply great or high as we often do minimizes the danger we face as a nation.

Ransomware attacks in which a hacker encrypts a victim's data and withholds a decryption key in exchange for a ransom have skyrocketed in recent years, with an estimated 105 percent increase worldwide in 2021. American businesses, healthcare institutions and local government entities have borne the brunt of ransomware attacks in the United States. An estimated 37 percent of businesses and over 2,300 schools, local governments and health organizations were hit by ransomware attacks in 2021.

Ransom attacks -- ransomware attacks against software companies such as in the attack against Kaseya affect thousands of small business clients who often feel the most pain from the destruction of data, loss of business and damage to customer trust. The attack against software company Blackbaud, for example, compromised thousands of downstreet clients -- downstream clients -- like Christ Hospital in Cincinnati and the Children's Hospital of Pittsburgh.

Local government entities such as schools, county elections offices and police departments are often underfunded and under-resourced. For many educators, the decision between patching software systems and acquiring new textbooks is just one of the many painful decisions they have to make in what is often a thankless job. In these cases, a -- a grant for new technology can mean updating systems and increasing accessibility, but also increasing risks with more opportunities for hackers to exploit system vulnerabilities.

The Biden administration has acted to turn the tide on the ransomware cyber attack threat, and the FBI has played a central role in assuring of our defensive position. It has even begun recovering ransom payments from cyber criminals, as in the case of Colonial Pipeline.

But these successes have not been without controversy. After the -- after the attack on Kaseya, the FBI withheld for weeks the -- the decryption key it had recovered, which left many downstream businesses without the tools they needed to operate and cost those businesses many millions of dollars that could have been avoided had the FBI provided it immediately.

Many people also raised privacy concerns in the wake of the attack on Microsoft Exchange. After the FBI discovered that the individual networks of private companies had been compromised by the Microsoft Exchange intrusion, it obtained warrants to alter victims' systems without their knowledge or permission.

No sector needs more protection than our critical infrastructure. In 2021, ransomware was used to attack 14 out of 16 critical infrastructure sectors, including agriculture, financial services, energy, dams and other often unseen but crucial industries that buttress American lives and businesses.

In February of 2021, an attacker attempted to poison the water in Oldsmar, Florida. In 2017, Russian government-affiliated cyber attackers hacked a third-party contractor and used the company's e-mail to gain access to part of the American electrical grid. And in April, 2021, Chinese state-affiliated hackers breached New York's Metropolitan Transit Authority network, potentially exposing data and showcasing just how vulnerable our transit operational systems could be to attack.

These are real threats. Blackouts and loss of electrical service could cripple our country's economy and paralyze our ability to respond to an attack. Without significant investment in I.T. systems and training these industries will remain vulnerable.

But the threat does not end there. State-affiliated cyber threat actors from Russia, Iran and China have engaged in cyber espionage against our government and political systems, accessing critical data and loitering on our servers. American businesses have suffered breaches by cyber criminals looking for personal data, as well -- looking for personal data to sell, I should say. While the Russian invasion of Ukraine has not yet spilled over into cyber attacks that affect governments and businesses in the United States, President Biden has warned all Americans of evolving intelligence that Russia may soon launch cyber attacks against the United States.

Our ability as a country to respond to such an attack rests in the hands of the FBI and its partner agencies. The Biden administration has encouraged businesses large and small to adopt a shields-up posture to defend against cyber threats. Because it is the security of private companies, those that keep our lights on, provide lifesaving healthcare and teach our children that will determine the fallout from an attack, we must all evolve to better protect our networks. This means strengthening our cybersecurity systems by patching vulnerabilities, training users how to recognize phishing attacks and increasing network cybersecurity protocols. When we invest in our schools, local governments and healthcare systems' cybersecurity we contribute to a safer country.

We live in a technologically-advanced nation of early adopters with private networks and the freedom to maintain our networks however we choose. There is no easy way to mitigate all cyber

vulnerabilities in the United States, but by engaging in meaningful oversight of our nation's cybersecurity defenses this committee can ensure we are ready to meet any threat head-on.

NADLER: I look forward to hearing from Assistant Director Vorndran on what he and his colleagues at the FBI's Cyber Division are doing to keep our country safe and to engaging in an important discussion about the threats our networks face.

I now recognize the Ranking Member of the Judiciary Committee, the gentleman from Ohio, Mr. Jordan for his opening statement.

JORDAN: Thank you, Mr. Chairman. Last week, the President said a cyberattack from Russia is coming. And what's the Biden administration been doing? They released Alexei Burkov, a notorious Russian cyber criminal.

Here's what -- here's what has been said about Mr. Burkov -- "he's an asset of supreme importance, one of the most connected and skilled malicious hackers ever apprehended by U.S. authorities," and what did the Biden administration do six months ago? Put him on a plane headed to Moscow.

"A cyberattack from Russia is coming," the President said, and what's our Justice Department been doing? We know they've been spying on Carter Page and not following the FISA rules. How do we know that? Cause Inspector General Horowitz has done two different audits, two different reports that he's given to us.

400 errors in 29 randomly selected FISA applications -- 400 errors in 29 of them. In four of those 29 applications, there wasn't even a Woods File, which is the file you keep that has the underlying supporting evidence for the claims made in the application itself.

"A cyberattack from Russia is coming," the President said, and what's our Justice Department been doing? Not only ignoring the FISA rules, they don't even follow their own rules. We know that from a story two weeks ago, where in sensitive investigative matters, special cases dealing with First Amendment concerns, concerns when they're investigating religious groups, investigating candidates, investigating government officials or the press, 353 cases, 747 errors in those cases.

Not only are they not following the FISA rules, they don't even follow their own darn rules. It's why we sent a letter asking for the internal audit. We hope that that will be given to the Judiciary Committee, Mr. Chairman, so we can look at that.

"A cyberattack from Russia is coming," the President said a week ago, and what's been going over on -- on -- over at the Justice Department? Well, we know this from Mr. Durham, they were spying on President Trump's campaign. Mr. Durham just told the court that last month. Tech executive number one spying on not only the President Trump's campaign, looks like spying on him went during the transition period and potentially even while he was President of the United States.

"A cyberattack from Russia is coming," and of course, we learned just four months ago what was our Justice Department doing, what are they still doing? Spying on parents, treating moms and dads as domestic terrorists. We had the Attorney General in front of this committee back in October and he misled this committee and he said it wasn't going on, but we've now had a whistleblower come forward and tell us it is -- is -- is in fact going on, so much so that there's a -- there was an e-mail sent to FBI

agents with a threat tag designation that you're supposed to put on parents who are simply showing up to school board meetings voicing their concerns about what's being taught to their children.

President Biden says a cyberattack from Russia is eminent, it's coming, and what were 51 former intel officials doing just a year and a half ago? They were telling us the whole Hunter Biden story was false, they told us it was Russian disinformation. The disinformation is what they told us, something we need to check out. How did 51 of them, in -- in the days before a presidential election, tell us a story that the New York Times has now said was absolutely true, the laptop was true, the eyewitness was real and the e-mails and evidence and documents were real, as well?

So I look forward to today's hearing, hearing from our witness, but I think a fundamental question we've got to ask is how do you trust the Department of Justice to protect us from cyberattacks when they've been spying on presidential campaigns, spying on parents, telling us Hunter Biden was Russian disinformation, and releasing the most notorious Russian cyber criminal we've ever had?

The simple question I'm going to have for our witness is why did we let him go? What did we get for that? What kind of trade -- what kind of a rail -- what happened there?

So Mr. Chairman, I hope we can get answers to these key questions and I hope, again -- we've -- we've -- we've talked about this now for months. We hope we can get the Attorney General back here to answer some questions about this whole school boards issue and some of the other things I raised in my opening statement.

With that, I yield back.

NADLER: The -- the gentleman yields back. Thank you, Mr. Jordan. Without objection, all other opening statements will be included in the record.

I will now introduce today's witness. Bryan Vorndran has served as Assistant Director of the Cyber Division of the FBI since March 2021. He joined the FBI as a special agent in the Washington Field Office in -- in -- in 2003 and has held a variety of positions since then, including part -- including serving as part of an -- of the International Contract Corruption Task Force in Afghanistan, Unit Chief in the Counter-Terrorism Division at FBI Headquarters, and leading the Washington Field Office's Joint Terrorism Task Force.

Mr. Vorndran also served as Assistant Special Agent in Charge of the Cyber and Counter-Intelligence Programs at the Baltimore Field Office, Chief of the Strategic Operations Section of the Counter-Terrorism Division Headquarters, and later as a Deputy Assistant Director of the Criminal Investigative Division.

Prior to assuming his current position, Mr. Vorndran served as a Special Agent in Charge of the New Orleans Field Office. Before joining the bureau, Mr. Vorndran was an engineer for the Procter & Gamble Company and for Merck and Company.

He earned a Bachelor's Degree in Civil Engineering from Lafayette College and a Master of Business Administration from the Law School of Business at the University of Michigan. We welcome our distinguished witness and we thank you for participating today.

I'll begin by swearing you in. I ask that you please rise and raise your right hand. Do you swear or affirm under penalty of perjury that the testimony you're about to give is true and correct to the best of your knowledge, information or belief, so help you God? Let the record show that the witness has answered in the affirmative. Thank you and please be seated.

Please note that your test -- written testimony -- statement will be entered into the record in its entirety. Recording (ph) -- that I ask that you summarize your testimony in five minutes. To help you stay within that time limit, there is a timing light on your table. When the light switches from green to yellow, you have one minute to conclude your testimony. When the light turns red, it signals your five minutes have expired.

Mr. Vorndran, you may begin.

VORNDRAN: Chairman Nadler, Ranking Member Jordan and members of this committee, thank you for providing me this opportunity to speak to you today about FBI cyber. Although the FBI investigates a wide range of threats, we're here today to talk specifically about the cyber threats facing our nation, the FBI's place in U.S. cybersecurity ecosystem and the FBI's valuable role in identifying, disrupting and imposing costs on America's cyber adversaries.

The FBI Cyber Division turns 20 years old this year, and over that time, the American public has invested heavily to ensure the FBI has staff where it is needed most. Today, we have more than 1,000 cyber-trained personnel spread across 56 field offices and more than 350 sub-offices, and we can now put a cyber-trained agent on nearly any doorstep in this country within one hour of an attack.

We have agents located in more than 70 countries, working with our global law enforcement and intelligence counterparts. Some of these agents are dedicated to countering the cyber threat full time while others stand ready to support our cyber mission.

VORNDRAN: Today, as you know, we're putting the FBI's decades of expertise countering foreign intelligence and investigating cyber threats in the United States to work against malicious Russian cyber activity. But we do not do it alone.

Our emphasis on disrupting cyber adversaries, including through sharing information and enabling our partner and our partners enabling us, is part of the FBI's continued move away from indictments and arrest first mentality toward a playbook where we work with the government and industry partners around the world to execute joint sequenced operations that impose the greatest possible cost on our adversaries.

As this committee knows more than any other, sometimes an arrest and prosecution is the most decisive disruption, like earlier this month when we were able to bring cyber criminal Yaroslav Vasinskyi to the inside of a U.S. federal courtroom for his role in the Kaseya attack; and the willingness of the Justice Department and the FBI to publicly attribute and expose damaging cyber intrusions by Russia, China, Iran and North Korea has undermined those government's denials and created a platform for U.S. allies to condemn destabilizing cyber activity while also undermining our adversary's operations.

Our focus, though, is investigating based on information we obtain from all sources, victims, foreign intelligence services, human sources and our surveillance of adversary infrastructure, and then pushing it whoever can do the most good for victims here and cause the most harm to hackers abroad.

At the risk of making some enemies on this committee I'll draw a comparison between the FBI's role in the cyber ecosystem and an event I attended 30 years ago yesterday when Duke beat Kentucky in the 1992 NCAA Men's Eastern Regional Final. Sometimes we're Grant Hill throwing the pass and sometimes we're Christian Laettner taking the shot.

Having said that, for the FBI to continue supporting our partners in executing successful operations ourselves we need your support -- even the Kentucky and North Carolina fans amongst you. As one of our key oversight committees and allies, your backing is crucial for our continued growth of authorities and resources.

First, we appreciate Congress' action to pass a mandatory cyber incident reporting law and we're looking forward to working with CISA and others to implement this legislation in a way that enables law enforcement to use incident reports to disrupt our cyber adversaries.

At the same time, we need to be postured to continue hiring and retaining the right people to achieve our goals. At the FBI we have been working hard to identify ways to better attract, train and retain talented tech minds. Although we promote our mission to the greatest of extent possible, the calling to protect American people and uphold the Constitution does not equate to paying off weighty student loans or entitle someone to a salary competitive with what's available in the private sector. We have found our struggles to pay those minds market value; even federal government market value is often a deal breaker.

We will continue to work with DOJ, excuse me, DOJ, OPM, the administration and Congress to ensure we're able to properly pay and incentivize our cyber workforce.

While we're trying to fill these seats with talent, passion and patriotism, we're seeing the cyber threat grow exponentially. It now touches every program at the FBI. Cyberspace is where nation-states go to learn our country's secrets, it's where criminals are extorting billions of dollars and it's where wars are being waged.

We are now at a critical juncture. We must keep pace with the expansion of the tools at our adversary's disposal, and we need to see the same sense of urgency reflected in funding these programs through increases in our base budget.

Yes, the people in technology, the FBI Cyber Division, needs to keep pace with these adversaries are expensive. But they're essential investments because cybersecurity equates to national security.

I look forward to working with this committee on these topics and several other issues important to the success of the FBI and other U.S. government cyber programs.

Chairman Nadler, Ranking Member Jordan and members of this committee, thank you, again, for inviting me here today. I look forward to your questions.

NADLER: Thank you for your testimony. We'll now proceed under the five-minute rule with questions and I will recognize myself for five minutes to start off. Mr. Vorndran, in September of last year Howard University was forced to shut down much of its web services after a suspected ransomware attack took over its systems.

K-12 schools are also enduring an increase in cyberattacks against their systems. Ransomware attacks in particular surged last year and continued in January. On average, education victims pay over $100,000 in ransom payments to decrypt their data and regain network access.

Why are schools and higher education institutions a growing target? And who are the most common perpetrators of cyberattacks on schools?

VORNDRAN: Sir, I'm sorry, what was the second part of your question?

NADLER: Who are the most common perpetrators of cyberattacks on schools?

VORNDRAN: OK. Sir, what -- what we've found is that institutions or organizations with low cybersecurity budgets, and I think public schools for the most part would fall into that space, not because they're not trying but the resources that are available to a K-12 school may be different than the resources available to a multi-national company.

It is hard to keep up with all the patching requirements, all the new operating systems. And so what we see is cybercriminals really preying on targets of opportunity. We see these criminals looking for opportunities more than precision attacks against one specific entity, or one specific sector.

And so, when they -- those criminals find a vulnerability in a traditional sector, they will continue to exploit it in hopes that they can make a lot of money off of it. In terms of who the most common perpetrators are, the bottom line is the most common perpetrators are cybercriminals, they are global, but the most heavy concentration is through Russia and surrounding countries in the Russian territory.

NADLER: Thank you. In 2016, Russia attacked Ukraine's Ukrenergo, I hope I pronounced that right, electrical network succeeding in causing a blackout but failing to destroy the system. This attack was noteworthy because it was a case where the perpetrator attempted to use software to permanently damage hardware.

Can you describe for us how software could be capable of destroying a hardware system and we know how many entities have developed or are seeking to develop this capacity?

VORNDRAN: One of the questions we typically ask is, is there bleed over between what we would define as the IT and the OT system. Essentially, the information technology and the operational element of a company of an organization of an entity.

And so, firmware and hardware, different than software still has a potential to have a lot of vulnerabilities that can be exploited by cyber adversaries. So the software bleed over would really be a question of can this software being exploited actually affect the operational component?

To your second part, it's really, really challenging question to answer what the scope and scale of those are. We just would point back to the fact that undoubtedly cybercriminals are going to work to find vulnerabilities where they can have the biggest impact, cause the biggest disruption or make the most money off those vulnerabilities being exploited.

NADLER: It's been widely reported that on March 18th the FBI warned the federal government of Russian hackers scanning the systems of five U.S. energy companies as well as other critical infrastructure.

What's the significance of a foreign power scanning networks in our energy sector? And have instances of Russian scanning increased in the last month?

VORNDRAN: So sir, instances of Russian scanning have increased. The significance of that is I would draw a comparison to traditional crime. In order for a criminal to conduct a bank robbery, it's undoubtedly true that that criminal is going to likely conduct reconnaissance, surveillance to understand when the bank may be open, when the bank may be closed, what the security posture looks like.

In the scanning of those, the scanning as you described it, really is a reconnaissance phase to understand what the net defense side of that company would look like. And whether there are vulnerabilities that can or cannot be exploited. It's an extremely important part of the overall attack cycle.

NADLER: Thank you. And my final question, can you explain for us the different ways that the FBI is expanding its responses to cyber threats? And how it can better serve victims of cyberattacks?

VORNDRAN: Sure. We always encourage a couple of key things. The first is to build a relationship with your FBI field office we are all over this country and international as well.

But for companies in this country or organizations, K-12 schools would be included there, we encourage those entities to build a proactive relationship with their FBI cyber squad in their area.

Would also encourage them to build a proactive relationship with their CISA rep in their area because CISA is going to be very helpful as well, and has some helpful resources. Independently of the government, all of those organizations need to have a defined incident response plan.

They need to know who they're going to call in the moment they become a victim, they need to know who their insurance company is, who their attorney is, who they're going to call at the FBI, who they're going to call at CISA.

We recommend that those -- those are exercised every 90 days, not that they're drafted by a general council and put on the shelf and never thought of again. And then the third thing we say is if you do become a victim we would ask that you report. You can report to CISA, you can report to the Bureau.

It doesn't much matter to us, we'll synchronize on the backside to make sure that those companies have the weight of the U.S. government. In terms of things that we can do, Sir, the -- the list is potentially endless. We've been asked to help with the media before, we're willing to do that.

We've been asked to help with victims' services if somebody's not going to get a paycheck we're willing to do that. We've been asked to help take servers offline, we're willing to do that.

We've been asked to simply take the indicators of compromise that are provided by that organization's third-party incident response firm, and then move onto our investigation we're happy to do that. It really is a menu of options that we can provide in that moment.

NADLER: Thank you. My time has expired. Mr. Chabot.

CHABOT: Thank you, Mr. Chairman.

It's estimated that the FBI's Internet Crime Complaint Center received nearly 2,500 complaints in 2020, which represented a 20 percent increase over the previous year. And over that same time, there was a 225 percent increase in ransom payoffs from nearly 9 million in 2019 to nearly 30 million in 2020.

But it actually may be a lot worse than that because my understanding is if the payoffs that were reported were $30 million, there's another -- there's a number of experts who believe it could be 10 times that amount. So we're looking at $300/350 million.

So in other words, only, you know, one out of 10 of the incidences are even reported yet nine out of 10 actually payoff the criminals. That same report estimated that cybercrimes whether it's phishing or extortion or identity theft or data breaches of botnets or -- that they all collectively cost the American businesses, and after all small businesses especially employed by half the people in this country, about $4 billion with a B.

CHABOT: And again, the chairman mentioned the Colonial Pipeline attack, which my understanding is, was one of the most devastating ransomware attacks in -- in U.S. history. And eventually, to contain that attack, the Colonial Pipeline made the decision to pay over $4 million to the criminals, and it turned out the decryption tool that was sent back to them in return for the payment wasn't particularly helpful in restoring the functionality to their networks, which is my understanding oftentimes the case.

The good news, of course, is that the Department of Justice was able to track and to seize roughly, my understanding, about half of the payment that was made to the Russian-based hackers. But that still left about $2 million to the criminals to be used against future victims of -- of malware crimes, and it's likely that the figures I've just mentioned only represent the tip of the iceberg of this ever-growing problem.

Cybersecurity experts estimate that ransomware victims made an average payment of about $300,000 in 2020. They further suggest that when a company made a ransom payment, less than one out of 10 of them actually regained access in a reasonable amount of time to their hijacked data. Undoubtedly, cyber attacks are becoming more frequent, they're having larger impacts and many, unsurprisingly, are connected to the governments, as has been mentioned, of both Russia and -- and China.

So Mr. Vorndran, let me get to my questions. First, do you agree that of their ill-gotten gains, the payoffs, basically, that are made to these criminals, some significant portion of that is likely to go towards targeting the next victim or victims; that they're not doning (ph) this money, they're not donating it to the Red Cross or the American Cancer Society or the Little Sisters of the Poor. It's more people, the public or businesses that are going to be targeted. Would you agree with that?

VORNDRAN: Yes, sir.

CHABOT: And -- and -- and that's what I'd like to focus on. We've got to make cybercrime, particularly the use of malware extortion, less lucrative, less profitable to these Internet thugs. How about making it

illegal to pay them off? After all, giving them money, which we know they'll use to go after the next victim, is sort of like aiding and abetting the next crime in -- in some ways. Would you agree with that?

VORNDRAN: So sir, if you're asking me if I think it's right to make the paying of ransoms illegal, I don't think that's a good decision.

CHABOT: OK.

VORNDRAN: And the reason is, is because it creates a triple extortion model.

And so in our current system, ransomware actors, cyber criminals can attack a company and hold an extortion for payment to get a decryption key. They can also extort that company or that organization to threaten to leak information, PII, of company employees or other sensitive information. That's the second of the three extortions. If you make the paying of ransoms illegal you're creating a third extortion, which means that if a company chooses to pay and they have now broken the law, then a -- then a cyber adversary has the ability to hold them accountable for that in the public's eye and threaten them even more with a higher extortion.

So we would actually recommend that that's not the best decision, but that's certainly just an FBI perspective.

CHABOT: OK, well, I think it's something that certainly ought to be considered, because what we're doing right now certainly has not worked. They're still doing it. They're getting more money than ever. Companies are actually allowed to write off on their taxes a payoff. Is that -- is that correct?

VORNDRAN: I -- sir, I don't know the answer to that question. I apologize.

CHABOT: Well, they are. They -- they can do it, and I would argue that it's against public policy to allow that to occur.

And then finally, some insurance companies, I understand, actually advise their clients that paying off the blackmailer is the cheapest course of action. Would you understand, or have heard that?

VORNDRAN: So I think that...

NADLER: The gentleman's time has expired. The witness may answer the question.

VORNDRAN: You want me to answer?

NADLER: Yeah.

CHABOT: Yeah.

VORNDRAN: Sir, in terms of advisement of an insurance company to a -- a -- a victim, we think -- what we hear is that companies are put in a position to simply make a business decision. So when I go back to my position before I joined the FBI at Procter & Gamble and we made a very large-scale manufacturing, I was told, "Hey, Bryan, listen, an hour of downtime on this manufacturing line equates to this much revenue." And I think the business equation for any business that becomes a victim is

simply that. If we're looking at restoring from backups taking 24 hours or 48 hours or 72 hours, and that equates to $4 million in lost revenue, and we can pay a ransom for $3 million, from a business decision it's actually cheaper to pay the ransom.

Now, to your first point, that just fuels the fire and that just causes the criminal enterprise to grow stronger, so it is very much a vicious cycle.

CHABOT: Thank you.

I yield back, Mr. Chairman.

NADLER: The gentleman yields back.

Ms. Lofgren?

LOFGREN: Thank you, Mr. Chairman, and thank you, Mr. Vorndran, for your testimony and for your appearance before the committee today.

You know, most computer systems and transactions with sensitive information are encrypted in one way or another. I'm sure you would agree that encryption is important to defending against cyber threats, and that cyber defenses without effective end-to-end encryption are problematic. Now historically, the FBI has called for legally-mandated backdoors to allow law enforcement access to encrypted communications. Is this still the FBI's position? And how does that squared so with the importance of encryption to effective cyber defense and the risks of legally-mandated backdoors?

VORNDRAN: Ma'am, thanks for the question. I -- I am not an expert on lawful access as we define what you're describing, but I'll do my best with your question.

When we talk about backdoors, we're really talking about, should federal law enforcement have the authorities, through court-approved warrants, to see evidence on a device that is critical to a criminal prosecution or an investigation?

LOFGREN: Well, I understand that, but the question is, do we want to build in vulnerabilities to encryption to allow that court order to be effective? But we understand -- we're the Judiciary Committee. We understand court orders.

VORNDRAN: Yeah, I -- I -- I do think that it's important that law enforcement has access to that data through official court process.

LOFGREN: Let me ask this: In ransomware attacks, you know, and hackers have law companies and institutions out of their own data, and systems. Now, in at least one instance, according to the House Oversight Committee testimony, the FBI reportedly got a decryption key on its own that could unlock a certain ransomware, but didn't provide the key to the victim, and according to the testimony that I think you provided, the FBI repeatedly tested the decryptor in different environments -- and this -- a quote of your testimony -- "in -- in order to avoid introducing new vulnerabilities and backdoors into U.S. infrastructures." Can you explain this? How might a decryption key create new vulnerabilities?

VORNDRAN: Yes, ma'am. That's my testimony from Oversight and Reform, I believe in December, with National Cyber Director Chris Inglis.

So that specific decryption key that you're referencing, which is an open source, is related to Kesaya. When we were able to obtain that, we obviously don't go to Best Buy and purchase that and have a trusted supply chain. And so, the way we're able to obtain that is littered with potential points of vulnerability and criminal access to it.

So, when we were able to pull that it's extremely important that we put that through a testing environment to make sure that it doesn't have any additional malware or create any additional backdoors, as you describe it, or vulnerabilities, as we implement it not just in CASA but in their downstream environment.

LOFGREN: Let me ask another question and it really goes to something that the European Union has just done, which is to require technology platforms to interoperate with other apps and services.

For example, WhatsApp to connect and communicate with other chat and messaging systems. That's allocable (ph) goal I think that everybody on the committee shares. A concern has been expressed in some areas about the impact on cybersecurity.

Alex Stamos, who is at the Stafford Internet Observatory, one of the leading cyber research facilities in the United States, said this, "There is no way to allow for end-to-end encryption without trusting every provider to handle the identity managing if the goal is for all of the messaging systems to treat each other's users exactly the same then this is a privacy and security nightmare.

Now, I'm not asking you to comment on legislation you may not be familiar with, but generally speaking, do you agree that requiring private companies to connect and interoperate with other entities could create new cybersecurity vulnerabilities, especially if it reduces or eliminates end-to-end encryption or other security measures that are in place?

VORNDRAN: Yes, ma'am.

LOFGREN: What's the -- the answer is yes?

VORNDRAN: Yes.

LOFGREN: OK, I see that my time has expired, Mr. Chairman. And so, I yield back. Thank you.

NADLER: The gentlelady yields back. Mr. Buck?

BUCK: Thank you, Mr. Chairman. And thank you for being here, Mr. Vorndran. I am trying to figure something out. What is the purpose of these cyberattacks on Colonial Pipeline, JBS, Solar Winds, et cetera? In a -- in a short summary.

VORNDRAN: Sure. Two different points. So on Solar Winds -- I'm sorry, on JBS and on Colonial it's a pure financial gain for a criminal element. On Solar Winds, you know, the best answer I can provide you, it's obviously Russia state-backed activity to see what that software as a service and supply chain attack could get them access too. That would be of interest to them.

So, perhaps, U.S. government information where Solar Winds is a software platform in any number one of the departments. But, it would be an access point so that they could actual trade or find information that's of interest to them.

BUCK: So, there have also been attacks, cyber-attacks on OPM, on government agencies, gathering data about United States citizens and former government employees or for other purposes. I assume that some of the cyber-attacks on banks, other institutions, give the cyber attackers the ability to gain information about U.S. citizens.

VORNDRAN: Yes, sir.

BUCK: And I'm also assuming that at a time of war that could be used to destabilize our country.

VORNDRAN: I -- certainly that's one of the potential uses, yes.

BUCK: And so, we really have sort of two categories, if I'm not mistaken and I appreciate Mr. Chabot's questions about how this money can be used to further the enterprise, when Procter & Gamble makes toothpaste they sell it and they're going to be able to make more toothpaste.

When these folks receive money they're going to be able to invest in maybe more intricate equipment or more people and continue their activities. But, there's also this national security implication where U.S. citizens are vulnerable as a result of all of these -- not all of these, but some of these attacks.

VORNDRAN: Yes, I think that when we look at Russia, specifically, and their targeting. But if you're OK with it I'll expand it to China as well. When we look at their targeting of what I'll call personally identifiable information that is something that they're going to take back and utilize to craft a more overarching campaign. It's very hard for me to say what those are here in this moment, not because it's classified or unclassified, we just don't know how they're going to potentially use that information.

You know, I could come up with a use case in my mind that says perhaps the Chinese are using it in the criminal underground to generate income off of U.S. PII, right? I mean, there's any number of use cases. So, I think your terminology of destabilizing is absolutely fair. But, it's very hard for me to be precise about exactly what they're going to do with that information.

BUCK: Well, here's the issue, I guess. We know that part of future war would be attacking the infrastructure of another country. And so, if Russia had the capability to shut down our electric grid or our airports or whatever it is, our banking system, they -- if there in fact a war, we're -- and obviously we all pray there never is such a thing, but if there was that could be.

But, it could also be to make sure that Thomas Massie, for example, wouldn't have access to his bank account. There's a lot of money in that bank account I understand, and so, if there is that type of -- and what I'm wondering is, is there that type of individual capability to not just take out an infrastructure system, but also affect individuals whether they're in leadership positions in this country or not?

VORNDRAN: Yes, so we have seen leadership individuals targeted precisely, right. We have seen the primary, you know, you can name them, Russian, China, Iran, North Korea, take precision action to

compromise and e-mail account, to compromise primarily an e-mail account as I'm working through it in my head, of all -- people that we all know the names of this country.

But for the average American, what we see, both the state actor side and the criminal side, is overarching campaigns to have the most disruptive capacity that they're capable of. Not really precision targeting of Mr. Massie's bank account.

BUCK: OK.

VORNDRAN: Independent of the amount of money that may be in there.

BUCK: Well, I'm sure he finds that comforting. I guess, my last question is what can Americans do -- obviously, these major companies have staffs and they take care of themselves or maybe not, but what can Americans do to protect themselves from an attack like this?

VORNDRAN: Yes, I mean two basic things, right. Ensure that your operating system on your home computer is upgraded to the most current operating system, whether that's traditional Microsoft or Apple. And number two is, two-factor authentication on all your accounts. Never use the same e-mail -- or the same password on any accounts.

And like think about it this way, right, if people did open-source research on me they would understand where I grew up, probably could get my wife's name, probably could get my brother's name, probably could understand where I -- where I've lived, where I've worked. Well, that's largely what people use for their passwords.

And so, if you do life-based profiling around that you can really narrow down how to break a password. So, really obscure passwords and long passwords is very good advice.

BUCK: Thank you for being here.

Mr. Chairman, I yield back.

NADLER: The gentle -- the gentleman yields back. Ms. Jackson Lee?

JACKSON LEE: Thank you, Mr. Chairman. And Mr. Vorndran, thank you so very much. I've got a bunch of pithy questions -- I hope and -- you will help me get it within the time frame that I have.

First of all, I've introduced legislation H.R. 2980, which is the Cybersecurity Vulnerability Remediation Act, which has passed the House, which gives your counterpart, DHS, working with you, of course, and the FBI, just the opportunity to be able to mitigate against cybersecurity vulnerabilities and to know more about ransomware attacks and ransom payments, something I think all of our agencies should ramp up, but we look to the FBI, we look to the Department of Defense and Homeland Security to really be our front line.

And so as you answer your question, I just -- I'd like your comment as to the importance of that kind of efforts in various agencies that you partner with. I'm giving you an answer to answer (ph) but if you would -- if you would share that in your answer as we come forward.

This is a question of vulnerabilities and so my question -- and I have a series of them -- is to what extent the FBI can provide early warnings of perceived vulnerabilities and/or incursions? And why don't I let you do that and then have -- try to get in a bunch before my time.

VORNDRAN: I'll be quick. So at -- what you're describing is can the FBI or anyone else in the U.S. government actually provide what we could consider tactical warning of an imminent cyberattack? That's a very, very, very hard threshold to meet.

What we consider currently in the -- the current ecosystem is we have absolute strategic warning that Russia plans to hit us. We will do our best amongst our interagency partners to provide more real-time updates, as we already have through specific sectors, but providing what I would call "tactical warning."

"This is imminent" is going to be very, very hard because it assumes that we see everything, and we don't.

JACKSON LEE: But can you get in the ballpark sometimes?

VORNDRAN: We have been in the ballpark in the last three weeks, yes.

JACKSON LEE: And the vulnerability question that I had and agencies getting abilities to know more about ransomware vulnerabilities? That a good -- good thing that they should be focused on?

VORNDRAN: We're -- anything that makes us stronger through legislation, in terms of information sharing, transparency, understanding vulnerabilities, we're absolutely support of and willing to look at.

JACKSON LEE: What do you think about an infirmative (sic) act or affirmative responsibility, maybe legally, for the companies that have been attacked to notice the FBI? I knew that was a problem with Colonial, I was really shocked how long they waited or they hesitated. Obviously it was a new timeframe. What do you think about that?

VORNDRAN: So I think that through the legislation that just passed Congress and the Senate in the last couple of weeks through HSGAC, with CISA specifically, that we're able to get real-time access to the reports that CISA had, is going to have access to through law, and so we hope that we're able to accomplish that in the near term.

JACKSON LEE: One of the bottom rock (ph) infrastructure -- bottom rock (ph) part of the infrastructure of democracy is voting. In 2021, U.S. Cyber Command acknowledged that in 2020, it launched an operation against the software TrickBot, which posed a danger to U.S. voting systems.

Are U.S. voting systems in continued danger from malware, unlike other representations of individuals, like TrickBot, and what is the scope of the malware threat going into the 2022 election season? Where is the FBI in this effort of prevention?

VORNDRAN: Yeah, absolutely. So I want to be really clear -- for victims of what we would call cyber interference operations targeting election infrastructure, candidates and campaigns, and other election-related victims, the FBI is lead on the threat response side, through PPD-41. We have two primary functions there -- victim and witness assistance and attribution.

In terms of vulnerabilities going into 2022, all I can say is that it's something that we started talking about over a year ago. And when I say "we," at the interagency level, to include the agency that you referenced, and we are meeting routinely on a regular basis to ensure that 2022 is a secure election.

JACKSON LEE: I would look forward to maybe a briefing that is separate and distinct, that focuses squarely on that because that is the bedrock of democracy.

VORNDRAN: Sure.

JACKSON LEE: And we've already heard some accusations that are -- are far away from -- from the truth but still speak to the issue of violations dealing with voting. So thank you.

Let -- let me just -- you're not the Department of Defense but can Russia win a war with cyberattacks? Obviously, having just listened this morning to Ukrainian Parliamentarian women, talked about the -- just the sheer brutality and bloodshed and butchering that's going on, can Russia now just move to cyber efforts?

VORNDRAN: Ma'am, that's a really hard question for me to answer, not because I don't want to but I just don't know the answer.

JACKSON LEE: In your involvement with them...

(CROSSTALK)

JACKSON LEE: ... capacity?

VORNDRAN: They are -- Russia is one of the two most capable cyber adversaries we face globally. Whether they have the ability to completely destabilize our country and win a war is a whole different conversation but they are a formidable foe.

JACKSON LEE: Thank you. Mr. Chairman, I just want to introduce into the record four articles dealing with cybersecurity, which maybe I'll get a chance to talk about -- the rockets, Memorial Hospital, medical provider UMCC, hospitals, as I indicated, cybersecurity -- I think there are one, two, three, four, five that I ask unanimous consent to submit into the record on cyberattacks in Texas and in Houston.

NADLER: Without objection. Mr. Biggs?

BIGGS: Thank you, Mr. Chairman. Sir, thank you for being here today. I'm over here -- way over here.

JACKSON LEE: Thank you.

BIGGS: I -- I don't know if you know anything about this, but on March 21st, myself and several of my colleagues sent a letter to -- to Director Wray with regard to various issues. And I'm wondering if you've come prepared to answer questions on his behalf, since he's chosen not to answer our questions?

VORNDRAN: Sir, I'm sorry, I didn't hear the last part.

BIGGS: Have -- have -- have you come prepared to today to answer any questions that any of my colleagues -- that we -- we've sent Director Wray three -- three letters in the -- within the last three weeks.

VORNDRAN: If you're referring to the -- just on my prep notes, I have a March 21st letter on the sensitive investigative matter audit. Is that the one you're...

BIGGS: Yes. Are you prepared to answer questions on that?

VORNDRAN: I am not, sir.

BIGGS: OK. But you are aware of that? Will you take -- will you take back to Director Wray that we expect an answer soon?

VORNDRAN: Yes, sir.

BIGGS: Appreciate that. Last June, President Biden gave President Vladimir -- Vladimir Putin a list of 16 critical infrastructure entities that are off-limits to a Russian cyberattack. And then a week ago, President Biden warned that a cyberattack is coming and is imminent. The entities that he described in June were -- were listed as critical infrastructure entities.

According to CISA, 16 entities included commercial facilities, chemical, communications, critical manufacturing, dams, energy, Defense Industrial Base, emergency services, financial, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactor -- reactors, materials and waste, transportation systems and water, and waste water systems, but I think you're probably aware of -- of that list that he provided cause it was in your documentation as well.

BIGGS: So giving a list of entities that are off-limits implies that all other entities are fair game for cyberattacks or maybe it is that we haven't (ph) inadequately protected other sectors, but as former DNI Ratcliffe suggested in a -- in a -- a story that was -- included his comments about it, it was that you might accidentally be suggesting that we have vulnerabilities in these areas.

Can you -- can you tell me what the President has done? What he's directed you guys to do to protect these sectors or any other area, for that matter, from cybersecurity threats?

VORNDRAN: Sir, I'll do my best with your question. I mean the President doesn't tell us anything, what we should or shouldn't do. What we've agreed upon internally within the FBI and interagency partners and the interagency partners that I think are notable are Cyber Command...

BIGGS: Hold on, before you get there. It just occurs to me that if he doesn't tell you anything to do, did you know that he was going to give that list of sensitive sectors to Vladimir Putin?

VORNDRAN: No, sir, I did not.

BIGGS: Did anybody on your team know?

VORNDRAN: I don't know that answer.

BIGGS: So there was no communication, no briefing from the White House that he was going to share that list of vulnerabilities?

VORNDRAN: Not -- sir, not that made it to me.

BIGGS: OK. OK and so if you can give me a brief response then, previously as you were -- as you were giving?

VORNDRAN: Sure. When we look at our primary interagency partners; state, treasury, the folks at the forts (ph), CIA, et cetera, we all have a very, very good working plan related to the current threat streams about what our priority goals are. And so there is extremely strong operational coordination based on strategic and tactical intelligence. That I think if any of them were sitting here today in front of you separate from me that would speak with confidence about what we're prioritizing.

BIGGS: In those -- in those 16 areas that President Biden listed off to Vladimir Putin, has there been cybersecurity attacks or breaches in any of those 16 areas since he's given those -- that list to Putin?

VORNDRAN: Sir, I don't know the answer to your question. I apologize, I can certainly take that back and get that answer for you. I just don't know in this moment.

BIGGS: OK, I wish you would let us know. And then -- and then also if you can identify, since you don't know that you probably can't answer the next question, which was have any of those come from Russia? And so if you can identify the -- whether they're national actors or other actors, if you can identify where those threats have come from and those attacks have come from.

Are you aware of any other cyber attacks to any other entities outside the 16 sensitive areas that the President listed and gave to Vladimir Putin?

VORNDRAN: Yes, sir.

BIGGS: Can you describe those, please?

VORNDRAN: Well just off the top of my head, certainly we have software companies that have been targeted. I'm just trying to go through my head over the past couple weeks. We certainly have -- sir, as I'm working through this in my head in real-time, there are compromises against some of those 16 critical infrastructure sectors that you mentioned.

I can't speak specifically to which ones.

BIGGS: And you can -- you can provide that to...

NADLER: Your time, gentleman, has expired.

BIGGS: Mr. Chairman, can I just -- I've got some submissions for the record.

NADLER: Yes.

BIGGS: Thank you. An article dated September 29th, says U.S. deports high profile hacker to Russia before prison sentence ends. A series of CISA articles and notifications and memos as well as a piece by Leah Barcas (ph) entitled "Biden Actually Gave Putin a List of Critical Infrastructure Not to Carry Out Cyber Attacks on in The U.S." Another piece entitled "Ratcliffe Says Biden Handed Putin the Wrong List, It Should Have Been a List of our Targets in Russia".

Another one, on "The Sun: from June 18, 2021, "Biden Gave Putin Greenlight to Cyber Attack U.S. When He Listed 16 Off-Limit Targets, Experts Say". Another one says -- entitled "Biden's Off-Limits List for Russian Cyber Attacks Criticized as Green Light to Target Everything Else". Another piece entitled, "Russia May Target U.S. Business With Cyber Attacks, Biden Warns". Another piece entitled, "Biden Warns Russian Cyber Attacks are Coming".

Another -- the official statement by the White House and then a series of memos from -- that our joint cyber...

NADLER: Without objection to everything you're submitting.

BIGGS: OK, got a whole bunch more. Thank you, Mr. Chairman.

NADLER: Without objection. Mr. Johnson.

H. JOHNSON: Thank you, Mr. Chairman. Ransomware attacks stripped the City of Atlanta in March of 2018 causing a disruption to municipal functions and affecting critical sectors including the drinking water system, the police department, the judicial system and other critical departments. That attack cost taxpayers nearly $2.7 million in emergency contracts to recovery.

And Mayor Keisha Lance Bottoms -- then Major Keisha Lance Bottoms later called on the federal government to quote "Expand programs that share real-time threat information which is often critical in avoiding and mitigating threats.", end quote.

Now there are reports, Mr. Vorndran, that the federal government's response to the Atlanta cybersecurity attack was incredibly lack luster and prompted needed change. How has the role of the FBI in responding to a municipal government ransomware attack changed since 2018?

VORNDRAN: Sure, sir, just my records do not indicate that it was lack luster. In fact the City of Atlanta engaged the FBI and the U.S. Secret Service almost immediately. There was actually a leaked ransomware note, certainly not by the FBI, that actually prevented the City of Atlanta from being able to pay a ransom. I would note that we have indicted two Iranians for that activity.

But to your core question, listen, we strive for perfection. I'm not saying we're always there but we strive for perfection. Our goal in that moment is to provide any and all available resources that a company in this case a victim or in this case a municipality city, is in need of. As I have described that could include taking a server off-line. That could include victim service support. That could include support with the media or any number of other things.

To your question about sharing indicators, I think the velocity of which we share indicators has definitely improved and that's not just an FBI statement that's a U.S. government interagency statement. And certainly a goal of ours is to improve velocity even more.

But those are some of the foundational goals that we have when we respond to a victim.

H. JOHNSON: Thank you, sir. And if Atlanta were to happen again today what would the FBI do differently than what it did in response to the Atlanta attack?

VORNDRAN: Sure, sir.

So I obviously was not in Atlanta when that happened so I'm not familiar with the inner workings of that incident response. But in today's world, if the FBI received the call first, we would first contact CISA and between CISA and the FBI, perhaps Secret Service as well, we would go meet with the victim and to the best of the victim's ability -- in this case -- use case, Atlanta, ask them what is going on, and then how we can help. And we, again, as the U.S. government, there are certain recommendations that we would have for anybody in this position that Atlanta was in. Probably the most notable one is to specifically identify a point of ingress and egress into and out of the organization by the federal government. So that could be CISA, that could be the FBI, that could be Secret Service, but that will help synthesize the flow of information, in this use case, with Atlanta and the U.S. government.

H. JOHNSON: Thank you. What role, if any, is there for the private sector, when it comes to attacks against governmental entities like municipalities or government agencies? Is there any -- is there room for the private sector? Is there a need for the private sector?

VORNDRAN: Absolutely. I -- the private sector is going to see the threats almost -- let's just -- let's just say nine times out of 10, the private sector is likely to see the manifestation of the threat before the U.S. government. Because remember, when you have these major multinational companies out there that are all U.S.-based -- I don't want to name them in public testimony -- but they see -- they are the infrastructure that all of us ride on for our networking needs. And "all of us" means Americans at the household level all the way up to the multinational corporation level. And so they're going to be able to see activity very, very quickly, and so they have an absolutely enormous role, and I think being part of the ecosystem in the last year has shown that they have been willing to step very formidably into that space to benefit the U.S. government and to benefit victims.

H. JOHNSON: OK, I thank you for your responses. My time has wound down, and I yield back.

NADLER: The gentleman yields back.

Mr. Massie?

MASSIE: Thank you, Mr. Chairman.

I would tell the witness that I wasn't going to ask any questions today until he brought up the Duke versus U.K. ballgame from -- from ancient history. But I do have some questions that I want to ask now.

First of all, are -- are you aware of a piece of software named Pegasus? It's provided by NSO Group, Israeli software company.

VORNDRAN: Yes, sir.

MASSIE: Does the FBI use this program? It looks like they had a license to it for $5 million.

VORNDRAN: Yeah, so -- so the FBI has not and did not ever use the NSO products operationally or in any investigation. We did buy a limited license for testing and evaluation. Those limited licenses are part of our normal exploratory process to understand what other technologies are out there. But again, we have never purchased it for use operationally or in an ongoing investigation.

MASSIE: So your -- your division hasn't used this spyware domestically?

VORNDRAN: No, sir.

MASSIE: Have you detected the use of this software domestically?

VORNDRAN: Sir, there's reporting in the media about Apple filing a lawsuit against NSO, and there's a lot of information in that article. I can't comment further on your question truly due to classification, but if that is of interest to you, we could consider a -- a background briefing.

MASSIE: I would appreciate that very much. Thank you.

Executive Order 14028 called "Improving the Nation's Cybersecurity" requires agencies to adopt a zero-trust architecture and to achieve certain goals by the end of fiscal year 2024. The FireEye's pack was possible because everybody trusted that software. And so I -- I think the zero-trust architecture has merit. Can you tell us if the cybercrime -- or Cyber Division is taking any steps toward that executive order in adopting zero-trust architecture or promoting that?

VORNDRAN: Sure, so I -- I mean, when we look at 14028, which is really tailored towards DHS and CISA's role in the cybersecurity ecosystem, you know, CISA would be responsible for multifactor authentication recommendation zero-trust. We are absolutely supportive of all those top line requests because they do move us to a better security posture.

From a bureau perspective, we're focused on is that that executive order should lead to more transparency between government and private sector's standard operating procedures for incident response alignment between the bureau and CISA on what incident response is and how to do it effectively.

MASSIE: One of the sort of catch-22s or oxymorons that I see in cybersecurity is in order to be most secure, some platforms and operating systems require real-time updates, and that's a -- that -- in other words, the argument is that if you detect some kind of vulnerability you could push out the fix immediately to those platforms, but the problem is hackers use that as -- as a vulnerability in itself. And so, you know, how do you view that trade-off? You mentioned before, everybody should have the most recent operating system, and I think that's good advice. But you know, should we promote, allow, encourage or should we discourage operating systems that do their own updates without user involvement, without a -- sort of a two-factor authentification (sic), without some user sitting there saying, "OK, I'll accept this update"?

VORNDRAN: Sure, I mean, what you're describing is exactly how SolarWinds was utilized to catalyze a downstream attack in terms of a forced update. What I would simply is perhaps a third recommendation for people in America, but for corporations to have daily backups so that if that forced O.S. update or

another update compromises the system, you or your company has a within-24-hour backup that would allow you to restore fairly efficiently with the most relevant data.

MASSIE: My final question: When it comes to security audits, it's -- it seems like it's not such a great idea to let the same vendors that are selling the software do the audits. And do you think there's any merit into making sure that these audits are legitimate audits instead of sort of scripts that the vendor provides -- the software vendor provides, and then the user -- end user runs the script, and then feels secure because now they think they've audited it, but they really don't know what's going on?

VORNDRAN: Yeah, I just think...

NADLER: The time of the gentleman's expired. The witness may answer the question.

VORNDRAN: Sure. I just think due diligence of vendors and understanding your risk profile as an organization is extremely important. That's based on your own variabilities. Same conversation we have for doing business in China. There's going to be risk. What is your risk tolerance, and what is your due diligence to put your organization in the best position possible?

MASSIE: Thank you.

I yield back.

NADLER: The gentleman yields back.

Mr. Cicilline?

CICILLINE: Thank you, Mr. Chairman, for this hearing, and thank you to our witness for being here.

In recent years, we've seen an alarming number of cyber attacks on our nation's infrastructure, including election systems, police departments, local governments and hospitals, and in fact, a healthcare company in Rhode Island was affected this year when a contractor of Care New England faced a cyber attack that disrupted their payroll system, requiring Care to independently pay its (ph) approximately 7,500 (ph) employees manually.

So Mr. Vorndran, my first question is what is it about healthcare providers that the FBI and CISA, back in October of 2020, did an advisory warning of an increase in imminent cyber (inaudible) to the healthcare and public health sectors? So why is the healthcare industry such a lucrative target for ransomware attackers and what is the FBI doing to help healthcare providers protect against this vulnerability?

VORNDRAN: Sure. I appreciate the question and I say that sincerely, sir, because it's -- it's an area that touches all of us and people in our families and in our circles of friends.

What we would say is that we saw criminals, ransomware actors shamelessly trying to exploit the COVID-19 pandemic by attempting to extract high payouts from target (inaudible) like you said, such as hospitals.

That can mean disruptions to patient care are fully on the table to motivate a victim into paying a ransom for their information or system access. The reason is because obviously those hospitals are life safety related and hospitals in that scenario, faced with that set of circumstances, are likely going to be more willing to pay a ransom more quickly. And so it becomes a very, very target rich environment for a financially-motivated criminal.

You know, last June, even on the nation state side, hackers sponsored by the Iranian government compromised a children's hospital. You know, there is -- there is just endless lists of potential impact to hospitals that causes deep, deep concern.

And we have a very, very strong relationship with the American Hospital Association and with the Health ISAC, which is the Information Sharing and Analysis Center for the health industry and the health sector. We're very engaged with them, in terms of pushing out indicators of compromise that are specific or vulnerabilities that are specific to software applications or supply chain software that's meaningful to the healthcare industry.

So sir, I hope that provides a -- a -- a good response to your question.

CICILLINE: Thank you, it does.

And Director, now I want to just turn to election security. Director Wray testified back in September of 2020 about his concern about what he called "smaller cyber intrusions and the steady drumbeat of misinformation and its ability to undermine America's confidence in our elections."

So, you know, has the FBI seen indications of cyber misinformation campaigns in the lead up to the 2022 midterm elections? And what is the FBI doing to prepare for misinformation campaigns, whether from foreign powers or from within the United States?

VORNDRAN: Sure, sir. I'll -- I'll answer your question in -- in two phases. One is about election security and one is about foreign influence.

So I'm -- I'm previously on the record here today but I -- I'm happy to repeat it. On election security, from the FBI perspective, it's all about cyber interference operations targeting election infrastructure, candidates and campaigns, and other election-related victims.

From an FBI-centric perspective, the FBI would have threat response lead through PPD-41, which means that we would provide assistance to the victims and the witnesses and we would be squarely focused on attribution.

More largely on foreign influence, you know, the FBI has really specific responsibilities and authorities. By design and necessity, the FBI is just one part of the foreign influence team. We follow the actor and the activity, and I think that's really, really important to mention.

The problem is when an actor masquerades as someone he or she is not and amplifies disinformation through a coordinated campaign. You know, over the past years, we've worked really, really hard to understand how we can best provide information to our private sector partners so they can take appropriate action in terms of terms of service violations.

And I just want to foundationally say this last point, I think it's really important -- like, one -- the -- the primary goal we have in -- in -- in foreign influence is ensuring the respectful rights of U.S. persons. We -- as Americans, we have very broad rights to consume, create, spread information, and that's an underpinning of our democracy, that's very, very important to keep intact.

Leading into the 2022 midterms, sir, we have already started interagency conversations, they've been underway for perhaps as much six or seven months at this point, to ensure that we're properly prepared if we face any types of threats to the 2022 midterms.

CICILLINE: Thank you very much. I -- I yield back, Mr. Chairman.

NADLER: The gentleman expired -- the gentleman's time has expired.

(LAUGHTER)

God forbid the gentleman expired.

CICILLINE: I hope that wasn't a Freudian slip, Mr. Chairman.

(LAUGHTER)

NADLER: The gentleman's -- the gentleman's time only has expired. Mr. Issa?

ISSA: Thank you, Mr. Chairman. I want to stipulate for the record the gentleman has not expired.

Director Vorndran, a couple of things. One of them that I think is timely -- recently, the New York Times reversed its position on the Hunter Biden laptop being fake or -- and Russian misinformation. Do you have any reason to believe that's inaccurate or would you support that that appears to be an authentic -- I know you have investigation going -- but that -- that -- that the laptop itself appears to be authentic, it always was?

VORNDRAN: Sir, I have no background on that investigation and I'm here to talk about the cyber program.

ISSA: I -- I just asked if you had any knowledge of -- of it -- of -- that would cause us to believe that it was not authentic? If -- if -- if the answer is no, that's fine.

VORNDRAN: No, sir.

ISSA: Thank you.

VORNDRAN: Sir, let me go back. I mean, just parsing words, if you're asking me if I have any information on the investigation, the answer is...

ISSA: No, I got -- I got the answer I wanted. To be honest, you know, after 50 well-organized intelligence people, including former CIA directors, national security people, all said it was fake, and now the -- we now know that it's true, I just wondered if that was -- you know, since that did affect an election, it was worth asking.

VORNDRAN: Sir, I -- I want to be really clear. My answer to your question is, from my perspective, do I have any knowledge of that investigation...

ISSA: Right, you said "no."

VORNDRAN: No, sir.

ISSA: Thank you.

VORNDRAN: Yep.

ISSA: So moving on -- when Russia hacked Viasat early in this conflict, they hacked into what I would believe would -- would have been the infrastructure that would have been on the President's list of 16. As we all here mostly know, Viasat also controls -- Air Force is one and other related asset communications out of the same area and facility that was hacked.

Would you agree to give us a -- a appropriately classified briefing on the level of penetration and the remediation that's been done since that time to protect not only assets that were hacked but other assets that would be vulnerable potentially?

VORNDRAN: Yes, sir, I'd be happy to do that.

ISSA: Thank you. Last -- this next -- the President gave a list of 16 items that were off limits. Can you give us at least one item that was not on that list that you believe should be off limits to Russia hacking?

VORNDRAN: Sir, I mean, the -- the -- the 16 critical infrastructure sectors are very, very broad and almost all-encompassing. I would have to spend some time thinking about what is actually not on that list...

ISSA: Would -- would it be fair to say, maybe turning it around, that it is -- that the list should be "You may not hack the United States of America, period"?

VORNDRAN: Sir, I'm not going to get into a conversation about what the administration...

ISSA: No, no, no, I'm asking what the standard should be in accepting Russian hacking and disruption of - of any of our systems. Is the standard supposed to be they don't do it?

VORNDRAN: Our role in this ecosystem is to investigate when foreign adversaries, criminal or nation states, compromise U.S. networks, infrastructure, et cetera. That's my specific role ...

ISSA: OK.

VORNDRAN: ... this ecosystem.

ISSA: As of today, currently, in the last 31 days, has Russia-based organization hacked or tried to interfere with any U.S. assets to your knowledge?

VORNDRAN: Sir, can I consult with someone about what is and isn't classified?

ISSA: I - well, I just want to know whether there's an existence of any activity by Russia that seems to be broad enough that it would fall outside of classified.

VORNDRAN: Sir, the threat from Russia, at the - in the criminal sense, in the nation state sense, is very, very real.

ISSA: And current?

VORNDRAN: Yes, sir.

ISSA: Thank you. That's - that's all I needed for today, was the - the, quote "current."

VORNDRAN: Yes.

ISSA: The last question is - is maybe beyond your scope but it's important, I think, to everyone. Historically, when ransomware has occurred from Russia, with some regularity, there have been payoffs. Under current sanctions, wouldn't it in fact be a payment to a Russian entity prohibited under U.S. sanctions and therefore any payment would - would now be something that the U.S. - U.S. person should not be able to do?

VORNDRAN: So sir, that's a complicated question. Let me do my best with it. When we talk about sanction entities, there are a lot of cyber criminal entities in and around Russia that are not currently sanctioned. So a U.S. government - or a U.S. victim, person or company or organization, that chooses to pay someone affiliated with the Lapsus$ ...

ISSA: So - so for the record, persons or entities - criminal enemy - entities we may not know much about, that may or may not be connected to the Soviet Union - or the Russia, could in fact be getting payments as we speak, based on those attacks and that could end up going to the same Russia that is murdering people in Ukraine?

NADLER: The gentleman's time has expired. The witness may answer the question.

VORNDRAN: So the first part of your question, sir, is yes, there are people being paid over there right now. Whether that money flows through to the regime, I'm not in a position to talk about that. I just don't have that information.

ISSA: Could you give that to us for the record if you can find it?

VORNDRAN: Yes, sir.

ISSA: Thank you. Thank you, Mr. Chairman. I yield back.

NADLER: The gentleman yields back. Mr. Lieu?

LIEU: I thank you, Chairman Nadler, for holding this important hearing. Thank you, Assistant Director Vorndran, for your public service and for answering questions today.

A few years ago, hackers in Germany listened in on my cell phone conversations and they tracked my movements from California all the way to the House of Representatives. Now, the good news is I had a heads up that this might happen and as part of an investigative report by 60 Minutes on mobile security.

The bad news is that this problem has not been fixed. It's known as the security system number seven (sic) flaw, also known as SS7 for short. And as (inaudible) number seven, and it allows foreign governments and hackers to access your cell phone data, exploiting a loophole in our wireless systems.

This past November, a telecomm executive did a whistleblower complaint saying that the NSO Group, a spyware firm, offered to exchange bags of cash in order to access wireless systems to spy on people. We sent the criminal referral to FBI. I know that you cannot comment directly on individual cases. I'm going to ask you some general questions.

In the last five years, has the FBI investigated cases where the SS7 flaw was exploited to access cell phone contents?

VORNDRAN: Sir, all of our information in the FBI holdings on SS7 is at a higher classification. I'd be happy to have a conversation with you in the right forum with that information.

LIEU: Does the FBI itself exploit the SS7 flaw to access cell phone contents?

VORNDRAN: Sir, I'm not in a position to answer that question. I don't know the answer.

LIEU: Previously, Congress member Massey asked you about a briefing and I just want to make sure - will you commit to a bipartisan briefing classified on Pegasus and the NSO Group and the SS7 issue?

VORNDRAN: Sir - and I - yes, and if I can expand, I mean, it's very important for me personally as a representative for the cyber program at the FBI to keep that as an open invitation in both directions, between all of you and me and from me to all of you, that whatever information that you would want access to, we would try to facilitate that.

LIEU: Thank you. I'm going to ask you a series of questions, and if you could answer yes or no and then you can expound on it afterwards - it's about infrastructure.

So is it possible for hackers to take control of a dam and do an uncontrolled release of water?

VORNDRAN: Yes, sir.

LIEU: Is it possible for hackers to take over a chemical plant system and do a release of toxic gas?

VORNDRAN: Sir, just as a blanket statement, anything is in the realm of possible if they have - if the adversary has the right access.

LIEU: All right. Is it possible for a foreign government or hackers to access a transit system, disrupt railway signals and cause trains to crash into each other?

VORNDRAN: I - I would imagine so, sir.

LIEU: Is it possible for a foreign government or hackers to access an air traffic control tower or airplane guidance systems and cause planes to crash?

VORNDRAN: I don't know that answer, sir.

LIEU: OK. Is it possible for a - foreign governments and hackers to access a waste waster treatment facility and cause a release of harmful chemicals into the water?

VORNDRAN: To the best of my knowledge, yes, sir.

LIEU: OK, all right. Does the FBI only investigate these incidents if it were to happen after the fact or does it take actions to tell these different infrastructure places how to harden their systems?

VORNDRAN: So when you look at the evolution of the U.S. government in this space since mid-2018, when CISA, in its current form, came into what we know it today, I would divide it into two - two tiers.

When you look at the FBI role as defined in PPD-41, it's largely what we would call threat response. That's the term used in the - in the documentation. What that means is response to an incident, bilateral information, intelligence sharing with the affected entity, organization, company, school, you know, dam. It doesn't matter.

CISA would be there primarily to deal with the net defense remediation side, and that's what's termed in PPD-41 as "asset response." So I would look it as what is on the operational investigative side - that's the FBI - what is on the net defense asset recovery side - that's CISA's responsibility - but the information sharing and what investigatively can inform that defense or what on the net defense side can inform investigation is very synonymous.

LIEU: For the actual hardening of our infrastructure against cyberattacks, is that something that the Department of Homeland Security would be doing or is it the Department of Defense or ...

VORNDRAN: So the answer is both, depending on the critical infrastructure sector. So obviously, within the Defense Industrial Base, DOD would have a very, very significant role in that, but within the traditional 15 critical infrastructure sectors as defined in CISA's mission statement, they would largely be on point for the hardening, what we would call resiliency net defense.

LIEU: Thank you, and I yield back.

VORNDRAN: Sure.

NADLER: The gentleman yields back.

Mr. Gaetz?

GAETZ: So where is it? The laptop?

VORNDRAN: Sir, I'm not here to talk about the laptop. I'm here to talk about the FBI's cyber program.

GAETZ: You are the assistant director of FBI cyber. I want to know where Hunter Biden's laptop is. Where is it?

VORNDRAN: Sir, I don't know that answer.

GAETZ: That is astonishing to me. Is -- has -- has FBI Cyber assessed whether or not Hunter Biden's laptop could be a point of vulnerability, allowing America's enemies to hurt our country?

VORNDRAN: Sir, the FBI's cyber program is based off of what's codified in Title 18 -- or Title 18, Section 1030, a code which talks about computer intrusions by using nefarious-intent networks (inaudible)...

GAETZ: But you've talked about passwords here. I mean, Hunter Biden's password on his laptop was Hunter02. He drops it off at a repair store. I'm holding the receipt from Mac's (ph) Computer Repair, where in December 2019, they turned over this laptop to the FBI, and what now you're telling me right here is that as the assistant director of FBI Cyber, you don't know where this is after it was turned over to you three years ago.

VORNDRAN: Yes, sir, that's an accurate statement.

GAETZ: How are Americans supposed to trust that you can protect us from the next Colonial Pipeline if it seems that you can't locate a laptop that was given to you three years ago from the first family, potentially creating vulnerabilities for our country?

VORNDRAN: Sir, it's -- it's not in the purview my investigative responsibilities.

GAETZ: But -- but that is shocking, that -- that you wouldn't, as the assistant director of cyber, know whether or not there are international business deals, kickbacks, shakedowns that are on this laptop that would make the first family suspect to -- to some sort of compromise. Mr. Assistant Director, have you assessed whether not the first family is compromised as a result of the Hunter Biden laptop?

VORNDRAN: Sir, as a representative of the FBI cyber program it is not in the realm of my responsibilities to deal with the questions that you're asking me.

GAETZ: Has -- has anyone at FBI Cyber been asked to make assessments whether not the laptop creates a point of vulnerability?

VORNDRAN: Sir, we have multiple lines of investigative responsibility in the FBI. They're all available on public sources.

GAETZ: Well, I would think you'd know this one. I mean, I would think that if the president's son, who does international business deals referencing the now-president with the Chinese, with Ukrainians -- I mean, have you assessed whether or not the Hunter Biden laptop gives Russia the ability to harm our country?

VORNDRAN: Sir, again, we can do this back-and-forth for the next couple of minutes. I don't have any information about the Hunter Biden laptop or the investigation.

GAETZ: Well, should you? I mean, you're the assistant director of FBI Cyber.

VORNDRAN: I am -- my -- by the block-and-line chart (ph), no, sir, I should not.

GAETZ: Who should -- who should we put in that chair to ask questions about this laptop that FBI has had for three years?

VORNDRAN: Sir, I'm not -- I'm -- I'm not in a position to make a recommendation of who should sit in this...

GAETZ: So you don't have it. You don't know who has it. You don't know where it is. You're the assistant director. You know, earlier, you talked about whether or not you were the Grant Hill (ph) or the Christian Laettner (ph). It sounds like you're the Chris Webber (ph) trying to call a timeout when you don't have one.

So I mean, who is it? Do you even know who has it? Do you know who we should put that chair to ask these questions to?

VORNDRAN: No, sir, I don't know who has it.

GAETZ: Well, it -- could you find out and tell us? You're going to have to give us briefings, thanks to Mr. Lieu and Mr. Massie's question about whether or not the FBI was taking a $5 million test drive on the Pegasus system that was being used to target people in politics, people in government, people in the media, people in American life. So will you commit to give us a briefing, as the assistant director of FBI Cyber, as to where the laptop is, whether or not it's a point of vulnerability, whether not the American people should wonder whether or not the first family is compromised?

VORNDRAN: Sir, I'd be happy to take your request back to our office.

GAETZ: Gosh, that -- I mean, will you advocate for that briefing as a...?

VORNDRAN: (inaudible).

GAETZ: You -- you will?

VORNDRAN: I will be happy to take your request back to the FBI headquarters.

GAETZ: Well, will you -- do you believe that that is a briefing that the Congress is -- is worthy of having, I guess?

VORNDRAN: Sir, I'm -- I am -- I'm not going to answer that question. I'm -- I'm here to talk -- the invitation...

GAETZ: (inaudible) time out.

VORNDRAN: The invitation says, "Oversight of the FBI's Cyber Division". It does not say anything about (inaudible)...

GAETZ: Well -- well, right, but I mean, this is -- this is a cyber asset.

VORNDRAN: This is not a cyber asset.

GAETZ: This is a point of vulnerability if there are passwords, if there are business deals, if there are references to things that could harm our country. Like, you can't even sit here right now and say that you know that there's not a point of vulnerability. Maybe there are other crimes. Maybe there are tax issues or whatever. But as it relates to our -- I mean, it -- is the first family sufficient cyber infrastructure to protect? You don't even know if they're compromised.

Tell you what, Mr. Chairman. I seek unanimous consent to enter into the record of this committee the contents of Hunter Biden's laptop, which I am in possession of.

NADLER: I'm not...

(UNKNOWN): There's no objection to that.

(CROSSTALK)

NADLER: (inaudible) So I -- I can't say (inaudible) objection.

(UNKNOWN): Just say (inaudible).

(CROSSTALK)

GAETZ: I've -- I've never had to (inaudible)...

NADLER: We will object pending further investigation.

GAETZ: What -- what's the basis of that objection?

NADLER: It's a unanimous consent request, and I object under (inaudible)...

GAETZ: Well, I have a subsequent question.

NADLER: (inaudible)...

GAETZ: Mr. Chairman, I seek unanimous consent to enter into the record the receipt...

NADLER: It may very well be entered...

GAETZ: ... of the Mac shop...

NADLER: It may very well be entered into the record after we look at it further.

GAETZ: Very -- well, Mr. -- I have a subsequent unanimous consent...

NADLER: Ms. Deming's now recognized.

(CROSSTALK)

JORDAN: He's got a second unanimous (inaudible).

NADLER: Oh, I'm sorry.

GAETZ: Mr. Chairman, I seek unanimous consent to enter into the record the receipt from the Department of Justice...

DEMINGS: Mr. Chairman, this is (inaudible) Demings. Am I next, or -- am I next, or...?

NADLER: Without -- without -- without -- without objection.

Now, Ms. Demings?

DEMINGS: Thank you so much, Mr. Chairman, and -- and thank you, Assistant Director Vorndran, for your patience, your endurance, and most of all, for your service to our nation.

In a February 9th advisory, FBI and partner agencies warned about the continued prevalence of phishing emails, remote desktop protocols exploitation and exploitation of software vulnerabilities as attackers' strategies for gaining access to systems. Assistant Director, could you tell me why these strategies have been so effective -- are -- are so effective?

VORNDRAN: Ma'am, could you restate that question? I missed a part towards the end. I just want to make sure I'm crisp on the answer.

DEMINGS: Yes, yes. Regarding the phishing emails, remote desktop protocol exploitation, exploitation of software vulnerabilities as attackers' strategies for gaining access to systems, could you please tell us why these strategies have been so effective?

VORNDRAN: Sure. Because remote desktop protocol is going to give any adversary direct access to essentially command-and-control of a server or of a -- of a user end computer, and that will give them the rights, the administrative rights to arguably do whatever they need to do to meet the intent of their -- their attack.

DEMINGS: Which tactic, phishing emails versus software exploitation, is most commonly used by cyber attackers?

VORNDRAN: Ma'am, it's -- it's any of the above based on what is going to work. So attackers will often look for broad vulnerabilities and deploy multiple different tools or vectors of attack to achieve their goals. So it's - it's very, very challenging to say statistically which one is more prevalent. The better question is how have we, as a collective at the American level but also the corporation level, armed ourselves to defend against them?

DEMINGS: OK. And could you answer that question?

VORNDRAN: Sure. I mean, it's all about, you know, hygiene for information security. I mentioned a few of these, right - multi-factor authentication, two factor authentication for all of us at home on general accounts, complicated passwords, having active backups, those types of standard, what I would call hygiene operating system, routine operating system maintenance is very, very important.

DEMINGS: What level of cooperation have you seen from the private sector in terms of arming their systems and working with you to do just that?

VORNDRAN: Yeah, I mean, we have very, very strong relationships with the private sector that cross-cut, you know, pretty much every industry in this country. And so they - I mentioned this earlier in my testimony - I think the private sector has really answered the - the bell here in the last year about coming and being part of solutions because they own a lot of the infrastructure that we all use to have our daily access to the Internet. And so they're seeing adversary activity very, very quickly and they've been a tremendous part of the solution in the - in the distant past but really in the recent past.

DEMINGS: What other - excuse me - type of cyberattacks or - we talked about the phishing emails, we talked about the software exploitation. What other types of strategies did you see in 2021?

VORNDRAN: Well, we - we look at it - there's ransomware, botnets. I mean, the list goes on and on. Spear phishing is a very, very important targeting tool that all of the adversaries use. It's not as simple to say that 80 percent of all cyber intrusions occur because of spear phishing. I know that statistic is out there. But there's a lot of interdependencies once an adversary has access to a system.

But, you know, really arming an organization or institution with understanding what spear phishing looks like, a very, very helpful step for any organization.

DEMINGS: Thank you. Mr. Chairman, I yield back.

NADLER: The gentlelady yields back. Mr. Jordan?

JORDAN: Thank you, Mr. Chairman. Mr. Vorndran, why did the Biden administration release Burkov?

VORNDRAN: Sir, Mr. Burkov was investigated by the U.S. Secret Service, not by the FBI. I don't know specifics. What I do know is that there was no swap or concession and it's my understanding that his release ...

JORDAN: So we didn't get anything for it?

VORNDRAN: Sir, to the best of my knowledge, there were no swap or concessions.

JORDAN: Well, why do you think we did - I mean, you've said Russia - your - your statements today - "a formidable foe," "foremost adversary," and "the threat is current." Mr. Burkov has been described as "an asset of supreme importance, one of the most connected, skilled malicious hackers ever apprehended by U.S. authorities" and you don't know why we let him go?

VORNDRAN: No, sir. It's a Department of Justice question.

JORDAN: But you're the Director of Cyber at the FBI and the Department of Justice. It's part of the Department of Justice, right?

VORNDRAN: Sir - yes, sir, it is, but obviously we're our own agency ...

JORDAN: Now look, I - I read your bio, and - and other than the degree from Michigan, it's pretty impressive. You've worked at - you've worked at the FBI for ...

(LAUGHTER)

You've worked at the FBI for, like, 20 years, right? You've held all kinds of positions, you're the Director of Cyber and you can't tell me why we let the most notorious Russian hacker go and you don't know what we got for it?

VORNDRAN: No, sir.

JORDAN: Were you consulted?

VORNDRAN: It's not an FBI investigation.

JORDAN: But you're the cyber man. Just - Mr. Gaetz just talked about - you're - you're the key guy - you're the guy the administration sent here today to talk about cyber in the - in lieu of the - in - in - in light of the fact that the last week, President Biden said "the threat from Russia is imminent," you've confirmed that today, you said "it is current, it is as we speak," and you can't answer if it was a good idea or not whether you were consulted?

VORNDRAN: Sir, I don't actually - no, I - to your question, I was not consulted.

JORDAN: You were not consulted. OK. Do you - do you think it was a good idea?

VORNDRAN: Sir, I'm not in a position to comment on that.

JORDAN: The head of Cyber is not in a position to comment, the guy in front of the Judiciary Committee, at a time when the most formidable foe, our number one enemy when it comes to cyberattacks, with the threat that's imminent and current - what - can't answer whether it was a good idea or not to release the most notorious Russian hacker we've ever caught.

VORNDRAN: Sir, it was a Department of Justice decision, through the U.S. courts process, right? I would refer all of the questions on Mr. Burkov ...

JORDAN: Mr. Vorndran, why did you come? So - so far today, you've not - you've not been able to answer questions about Pegasus, you've - can't answer questions about sensitive investigative matters. Mr. Gaetz just went through the whole thing on Hunter Biden - Biden's laptop, you couldn't answer any questions about that.

Can you answer questions about anything today? Can you answer questions about the school board situation, the spying on parents? Do you know anything about that?

VORNDRAN: Just to correct the record, sir, I actually did answer the questions to two representatives about NSO and Pegasus.

To your point, I have not answered questions about the Hunter Biden laptop or about the ...

JORDAN: Or the sensitive investigative matters.

VORNDRAN: I was just going to say that if you'd let me finish (inaudible) about the sensitive investigative matter audit.

JORDAN: You know how many threat tags are on parents, how many - how many of the threat tags that say "EDU official have been assigned," how many cases have - now have that threat tag designation? Do you know any - any - anything about that?

VORNDRAN: Sir, no. All those questions should be referred to the Department of Justice.

JORDAN: Last week, when - in Mr. Biden speech, he said this - I mean, just to emphasize the - I - I - I can't figure this out - he said when he's talking to business leaders, "the magnitude of Russia's cyber capacity is fairly consequential and it's coming," as we've talked about before and as you've - you've said as well - "we'll help you" - saying to the business leaders "we'll help you in any way to deal with cyberattacks."

Do you think it helps the businesses who the President is asking to do everything you can to shore up your - your systems - do you think it helps to release the most notorious Russian hacker we've ever apprehended?

VORNDRAN: Sir, I'm not going to answer any questions on Mr. Burkov. Secret Service case. As I said, the decision was made, through my understanding, through the ordinary course of action by the U.S. courts.

JORDAN: Well, you - you've - you've agreed to give us briefings on - on other issues. Do you think there's someone at the FBI who could brief us on the Burkov situation?

VORNDRAN: Probably not because it's not our case.

JORDAN: Do you think there's a chance Mr. Burkov's name was on the Hunter Biden laptop?

VORNDRAN: Sir, I have no idea.

JORDAN: No idea, and that - that says it all - that says it all cause we - we - we want someone in front of the committee - as Mr. Gaetz alluded to earlier, we want someone here who can answer these questions about - about the - the - our constituents come up to me and talk to me about the school board situation, they come up and talk to me about the Hunter Biden laptop, they talk to me about all this.

They - they're concerned with the - the - the fact that we had an FBI that has abused the FISA process, looks like they've abused this sensitive investigative matter process - and we've sent letters on it, not to get a response - and by the way, we did send a letter to - to - to the Biden administration on the Burkov

situation, asked them to respond by 5:00 yesterday, got no response from them, and then the guy we send today - or the guy who comes in front of the committee today can't answer any questions about that either.

Seems to me that's the most - that - that'd be the most important question that we'd want the witness, Mr. Chairman, to be able to answer is the whole why did the United States of America let go Alexei Burkov, why did we release him, put him on a plane back to Moscow when - when this is the biggest cyber threat we face, is from - from Russia?

With that, Mr. Chairman, I would - I would yield back.

NADLER: The gentleman yields back. Ms. Scanlon?

SCANLON: Thank you. Over here. Since 2015, we've seen foreign adversaries try to manipulate our elections and national politics with false and misleading information being shared online, and sometimes we've seen domestic politicians amplify that disinformation and media hosts. Using a mix of bots and organic posts on social media, Russia, China and Iran have spread or amplified disinformation in a coordinated attempt to influence the outcome of both local and federal elections.

Can you talk to us a little bit about why disinformation campaigns are so difficult to identify and take down? And how does the FBI work with public and private partners to neutralize disinformation campaigns?

VORNDRAN: Sure. So, what you're primarily talking about is what we term foreign influence. And, you know, I'm on the record already saying this, but I'm happy to go through it again. The FBI has very specific responsibilities and authorities by design and necessity the FBI is just one part of the solution amongst many other U.S. government partners. Important to note, that we follow the actor and the activity.

The problem is when an actor masquerades as someone he or she is not and amplifies disinformation through obviously a coordinated campaign. And we've worked really hard over the past couple years to build relationships with private sector partners so that we can transparently and in a timely fashion take appropriate action and allow those companies to take appropriate action inline with their corporate terms of service. And we do all that, what we consider very mindfully, legal process as appropriate.

And, you know, I think just underscoring all this is ensuring we're respecting the rights of possible U.S. persons, as Americans have had very broad rights to consume, create and spread information. So, that is our position on foreign influence as an organization.

SCANLON: OK, yes. And, of course, there's a First Amendment Right to consume and spread information. But, of course, we wish that our people in leadership positions would not spread disinformation quite so freely.

I want to turn to something that's impacted some of the retirees in my community. Cyber fraud that has impacted some of our seniors. On couple in particular in my district was targeted by a cryptocurrency scam that ultimately defrauded them of almost $1 million in retirement funds.

So, it's a nationwide problem according to the 2020 Elder Fraud Report. Of the 791,790 complaints reported to the FBI Internet Crime Complaints Center in 2020 about 28 percent of the total fraud losses were sustained by victims over the age of 60, resulting in approximately $1 billion in losses to seniors. So, this is, you know, folks who've worked hard all their lives and tried to save for retirement.

Can you tell us a little bit about how the FBI is working to protect seniors from internet scams and what we could do to help you in that quest?

VORNDRAN: Sure. I mean, the Department of Justice, for as long as I can remember, has had a very, very keen focus on what we would call elder care fraud and elder care abuse. And that's something that the FBI takes very, very seriously because they are amongst, like children, our most vulnerable.

The fraud schemes that are run against that population are very, very vast, very complicated and unfortunately very lucrative for the -- for the criminals. So, we have dedicated FBI agents, dedicated analysts, Department of Justice's dedicated prosecutors dedicated to this problem. And only this problem throughout the entirety of the country.

In terms of what you can do to help us, it's all about awareness, right. And I think that, you know, all of us who have elderly people in our -- in our lives that may not understand the current trend of technology and the vulnerabilities that poses are very, very important from a messaging perspective.

SCANLON: Thank you. In 2020, one of the countries that I represent was targeted by a ransomware attack. And the attackers extorted, I think, it was $25,000 in ransom and it took months of staff time and resources for the county government to recover from the attack. So, we've seen these attacks against local governments and obviously they have personal information of folks that could be at risk.

But one of the wrinkles that we ran into was trying to get insurance coverage back. And I was wondering if they FBI has any information about working with these private insurance companies or whatever.

There was a -- you know -- questions about whether the FBI had negotiated with the ransom attackers and I understand that's not the position of the FBI. And some insurance companies are requiring that their -- they appoint a negotiator. So, I was wondering if you had any recommendations with respect to that.

VORNDRAN: No, the -- I don't, unfortunately. The insurance industry is a -- is a -- is a difficult conversation for the Bureau and certainly from a cyber perspective. And so, those relationships that really exist, exist between generally routine council, a third party instant response (ph) room (ph) and then the insurance company.

This is why exercising instant response plans are so important to companies, so that they know what their insurance company is or is not going to be looking for in that moment and they can plan for that effectively. But, to look back on, as 2020 hindsight and offer a recommendation, I really don't have one.

SCANLON: OK, thank you for that information. I yield back.

NADLER: The gentlelady yields back. What purpose does Mr. Gaetz seek recognition?

GAETZ: For a unanimous consent request.

NADLER: The gentleman is recognized.

GAETZ: Thank you, Mr. Chairman. After a consultation with Majority staff, I seek unanimous consent to enter into the record of this committee content from, files from and copies from the Hunter Biden laptop.

NADLER: Without objection.

GAETZ: Thank you. I yield back.

NADLER: The gentleman yields back. Mr. Johnson of Louisiana.

M. JOHNSON: Thank you, Mr. Chairman. Thank you for being here Mr. Vorndran. On page 6 of written statement today you concluded this quote, "The most significant nation state threats we face are those from China, Russia, Iran and North Korea. They're coming at us using every element of their national power and these adversaries are becoming more sophisticated and stealthier," unquote. That sounds pretty ominous.

And I know that you agree -- I assume you agree, we are in a very dangerous time. I think it's difficult to overstate it, because we have very serious and fiercely committed foreign adversaries, right?

VORNDRAN: Yes, sir.

M. JOHNSON: And President Biden said several days ago, Ranking Member Jordan noted earlier, that a cyber attack from Russia is coming, right?

VORNDRAN: Yes, sir. I believe that was his statement.

M. JOHNSON: So, here's the problem. Here's one of the things that have concerned us and this is why the questions keep coming back to one of the issues that has not yet been adequately addressed today.

In spite of all that, according to the records we now have, a significant amount of DOJ time, attention and resources are being used to monitor and, we'll say, intimidate the parents of American school children who had the audacity to express concern over their local school board's decisions.

On October 4, of last year, Attorney General Merrick Garland issued a memorandum, now infamous memo, directing the FBI and the U.S. Attorney's Offices to investigate those concerned parents. And since then we've had more and more information that's come to light about that directive, such as the fact that the National School Board Association worked in conjunction with the White House to write the letter that spurred Attorney General Garland's memorandum.

The NSBA's letter has led many state school board association to call its leadership into question. Many have since removed their affiliation, including my home state and the one where you spend a lot of time, Louisiana, they dropped out.

Unlike the national association, those local state associations understand that parents can and should have a say in their children's education. They have a right to closely monitor school curricula. They have a right to try to influence those choices as best they can. That's our system. That's the beauty of it. It is not the government's job to raise our children, it's the parents' job.

So let me ask you a couple of general questions, because I know what (inaudible) your responses -- I anticipate what some of your initial responses would be here. But let me ask you just out of the gates, do you think it's appropriate for any White House to commission outside groups to make false or misleading claims about its political adversaries?

VORNDRAN: Sir, I'm not here to...

M. JOHNSON: I know. I know you're going to say you're not here -- I'm not asking you in your official capacity, I'm asking you under oath, in your personal opinion as a general notion, is it OK for the White House to do that?

VORNDRAN: Sir, I am here in a personal and professional capacity under oath because of my job.

M. JOHNSON: Right.

VORNDRAN: OK? So I am not in -- I'm not going to comment on anything related to the school board or anything related to the administration.

M. JOHNSON: Let me ask you about your job. Do you think it's appropriate for the Department of Justice, where you work, to be influenced by a White House's actions in a case like that?

VORNDRAN: Sir, the memo was issued by the attorney general, and I would defer all of your questions back to him on this topic.

M. JOHNSON: Oh, we'd love to get him back here, but he won't -- he won't be called by the Democrats in charge. An FBI whistleblower revealed that counterterrorism division is using threat tags against concerned parents they were labeled by some of the parties involved as domestic terrorists, or at least analogized to them.

They've categorized them into the FBI system, so their so-called crimes could easily be pulled up for investigation. That was the supposed justification for it. In general, does the FBI's cyber division, your division, engage in the practice of using threat tags?

VORNDRAN: Sir, when we talk about threat tags from a cyber perspective, we could use the current system of Russia activity and perhaps there would be a tag for that so that we could find anything that's relevant. But I can't honestly answer the question right now about whether we're currently using them or not.

M. JOHNSON: Why not?

VORNDRAN: Sir, we have thousands of investigations in the cyber ecosystem. I just don't know the answer.

M. JOHNSON: But the threat tag is a tool that you use in your division, right?

VORNDRAN: Sir, I don't know that answer, if I'm being very honest with you. I don't know if we use them in our division or not.

M. JOHNSON: How many active or closed investigations does the FBI's cyber division have regarding any parents who've voiced concerns at school board meetings, or via social media about their children's education?

VORNDRAN: Sir, how many active or closed investigations does FBI's cyber division have on school board matters?

M. JOHNSON: On parents. Parents who have come up on the threat assessment somehow for expressing their views about their children's education in social media or at school boards.

VORNDRAN: Sir, I don't know that answer.

M. JOHNSON: Who would know that answer? You don't -- there's a lot of answers you don't have for us today and you're the Assistant Director of the Cyber Division. Who has that information?

VORNDRAN: I mean, organizationally we probably have that information. But I mean, again, all these questions need to be directed back to DOJ.

M. JOHNSON: I wish somebody from DOJ would send the appropriate party here. I yield back.

NADLER: The gentleman's -- the gentleman yields back.

Mr. Swalwell.

SWALWELL: Thank you, Chairman. Thank you, Director. We have a very capable adversary in Russia with capable cyber and nuclear abilities. Europe has seen the largest invasion since World War II. Millions of refugees are on the run. And Russia could move farther west.

And I'm sorry that despite the serious job you have, the serious background that you bring, that you have been treated to unserious questioning by some of my colleagues. It's like a greatest hit channel on Sirius Radio of Hilary's e-mails, Hunter Biden's laptop, and school board meetings.

But I want to talk to you about our private sector vulnerabilities right now, and in light of what the president said about Russia. What letter grade would you give America's private sector readiness as far as a cyber attack that Russia could bring?

VORNDRAN: That's a really tough question to answer, but I think that the dialogue between the U.S. government and the private sector especially what we would consider higher vulnerability sectors -- finance, energy these type of sectors, I would score them very high in terms of preparedness.

That is never going to guarantee absolute 100 percent success. But to say that they're engaged with the current threat picture, that they understand the current threat picture, and that they're trying to be

helpful to the United States and their fellow companies and their fellow citizens is an accurate statement.

SWALWELL: Do you agree with former CISCO CEO John Chambers who predicted that the year 2022 would bring approximately 120,000 private sector and public sector ransomware attacks to the tune of $60,000 for each attack as far as the cost to the public and private sector?

VORNDRAN: When was that statement made?

SWALWELL: It was made in the fall of 2021.

VORNDRAN: The current ransom -- I believe are numbered (ph). So our data is only about 20 to 25 percent complete because of the number of complaint referrals that we receive. But I think based off of that data, the current ransom payment is actually higher than that threshold already. The number of victims is hard to say one way or the other, but I think that's within the realm of possibility for sure.

SWALWELL: Because right now there's no requirement that a victim actually notify you that they've been hit.

VORNDRAN: Right, right.

SWALWELL: Now, it's pretty clear in what we've seen from Russian ransomware attackers is that they want to make it clear when they're seeking a high ransom that they are not associated with the Russian government, because they know that if there is any link then that prohibits the private sector's ability to pay because the Russian government, many of them are on the sanctions list.

As we continue to cripple the Russian economy though, what are we going to do as more and more Russian actors who are unable to support themselves and their families resort to ransomware as a means to try and make money? How are we going to make sure that our private sector is not inadvertently paying a ransom that violates the sanctions? I just worry that we could be a victim of our own success in that realm and then put the private sector in a tough position.

VORNDRAN: Sure. I mean, when you look at OFAC's guidance it specifically says one of the most important mitigation criteria is whether the victim, the company, has engaged federal law enforcement prior to paying the ransom. The reason for that is that we can very much help that entity who's having a bad day understand who they're paying and whether that is a sanctioned entity. And that as you've looked at (ph) as a very, very significant point of mitigation from a Treasury perspective.

So that really just draws me back to the need to report is not just so that the FBI in my world has the information. There are specific things we can do to better position a company, an organization who's a victim in that moment to ensure, in this case and your question, that they're not paying a sanctioned entity.

SWALWELL: And Director Wray at the House Intelligence Committee hearing recently said that within about, I think he said an hour or less, if you report a ransomware attack you could have an agent there to assist you. Could you just kind of describe what that agent would do?

And also maybe, address some fears that the Bureau would be looking at -- other non-ransomware parts of the business that may -- a business may be uncomfortable with the Bureau looking around. I mean, we want our businesses to report and have the benefit of your resources. But can you just talk about what that looks like when you get a call?

VORNDRAN: Sure. So I mean, when we -- when we show at a doorstep, you know, a lot of the conversation is about what the victim company is seeing. When the initial compromise occurred, do they have indicators of compromise, are they seen in tactics, techniques, procedures, malware signatures, these types of information.

Are there life safety matters that have been compromised in the case of a hospital? And then it really becomes an information-sharing proposition and what services we can or cannot provide. What it is not in anyway is asking us to sit behind a keyboard with administrative access to say give us unfiltered access to your system so we can do what we want to do.

I look at it as a bilateral exchange in a moment of need, and that moment of need has benefits to the organization, the victim that having us engaged early can definitely help in the short-term and long-term. But if a company wants to bring us in and say, hey, can you just walk through this journey with us?

And then in a day or in two days, we'll give you the evidence that our third-party incident response firm has obtained, we're absolutely fine with that. So I very much look at it as a malleable engagement to serve multiple priorities.

SWALWELL: Great, thank you. I yield back.

NADLER: The gentleman yields back. Mr. Steube.

STEUBE: Thank you, Mr. Chairman. While much has been said about cyberattacks coming from Russia and China today, Mexico is also a growing cyber threat. Mexican cartels have increased their involvement in cyber crimes, for instance, the Bandidos Revolutions Team stole nearly $15 million from financial institutions in 2018.

Drug cartels are increasingly buying synthetic opioids using the dark web. Do you agree yes or no, the Mexican cybercriminal organizations are a growing threat?

VORNDRAN: I -- I would just say the Mexican cyber or Mexican criminal cartels have always been a threat, and will use whatever means they need to financially grow, and so, yes.

STEUBE: And to make matters worse these Mexican criminal organizations can gain physical access to the United States, we've had over 2 million illegal crossings since Joe Biden has been president. We had 160,000 illegal crossings last month, and we're on pace to get 200,000 illegal crossings in the southern border.

The ongoing border crisis is putting America at risk in countless ways including cybersecurity. Month after month we've seen increased illegal border crossings since Biden took office. Do you agree yes or not that the ability of the Mexican cybercriminals to physically enter the United States make them an increased threat?

VORNDRAN: Sir, I'm not here to talk about southwest border crossings by the cartels. I'm here to specifically talk about computer intrusions using network architecture to catalyze a cyber attack.

STEUBE: Yeah, but you just said that, and correct me if I'm wrong, that Mexican cartels are a cyber threat, correct?

VORNDRAN: Mexican cartels to the best of my understanding, right, and this is not my area of expertise at all, right, but specifically to the dark web, which you referenced, there is in my investigative portfolio activity on -- investigative activity on the dark web.

And yes, there are synthetic opioids, and other drugs sold on there, which undoubtedly come back to the cartels.

STEUBE: And so, wouldn't you agree as a law enforcement official that if you have those individuals illegally operating in your country that's more a threat to the union that it would be if they were operating in Mexico?

VORNDRAN: Sure, I mean, cartel activity in the United States is -- is, obviously, not helpful in any way.

STEUBE: So the more cartels and illegals and folks that come across the border that are operating in the dark web doing this type of things as it relates to drug activity is, obviously, not helping the United States and hindering law enforcement efforts, and increasing the amount of fentanyl criminal activity that would occur in our country?

VORNDRAN: Sir, again, I -- I'm here to talk about the cyber program, right, and like, if you want to talk about...

STEUBE: Well this -- we're talking about cybercrimes and related...

VORNDRAN: If you want to talk about the dark web specifically, right, there is activity on the dark web related to opioids and every other illegal narcotic, illegal drug that's consumed in this country.

That -- those drugs that are provided on the dark web are sourced to the best of my knowledge both domestically and, you know, internationally, right. And so some of them come back to the cartels? I would presume yes.

STEUBE: How -- how long have you been in law enforcement?

VORNDRAN: Nineteen years.

STEUBE: So in your 19 years of law enforcement experience if you have a bad guy operating in a different country on the internet versus operating here in this country domestically, again, we're talking cyber knowing what the things are going on in Texas, knowing what's happening in the United States, knowing what -- what is going on here in our country, don't you think that it is a increased threat to the safety and security of the American people versus them being in Mexico and not coming into our country domestically?

VORNDRAN: Yeah, they are, but in the traditional drug world, right, that you're describing, they are distribution channels to users here in the country. So yes, they are a mandatory -- they are a necessary element of the supply chain.

STEUBE: All right. Switching subjects quickly, big tech as has been discussed today, cybercrimes are growing at an alarming rate in a wide variety of activities. While some take place entirely on the dark web or involve sophisticated hacking operations, many occur on common online platforms like Facebook and Twitter.

Such crimes can involve the exploitations of children, communication and coordination between terrorists or cartels, and even the organization of smash and grab thefts. If an online brick or mortar business openly serves as a meeting space for criminal organization that business and its owners may face criminal liability.

At what point do online platforms like Facebook and Twitter face criminal liability for opening -- allowing criminal conduct on their platforms?

VORNDRAN: (OFF MIC).

STEUBE: Your mic's not on.

VORNDRAN: I apologize, Sir. I don't know the answer to that question. I have to apologize, I truly don't know the answer to that question.

STEUBE: So can you get us -- so you're the head -- aren't you the head of cybersecurity for the FBI?

VORNDRAN: Not for cybersecurity, Sir, no.

STEUBE: So what is your position title exactly?

VORNDRAN: Investigations on the cyber system and...

STEUBE: Investigations on the cyber system and you don't know...

VORNDRAN: If you want...

STEUBE: ...crimes committed on online platforms say child porn, child exploitation, that there's no liability on behalf of the platforms that allow that activity to occur?

VORNDRAN: Sir, the reason I...

NADLER: Time is expired, the witness may answer.

VORNDRAN: ...the reason I...

NADLER: The gentlemen's time is expired; the witness may answer the question.

VORNDRAN: Sir, the reason I'm saying I don't know is because I don't know where the line of civil liability and criminal liability starts and stops in the example that you're providing me.

So it -- Facebook, as you mentioned, right, do they have liability for conveying child sexually exploited material? The answer is likely yes but I don't know where the civil and the criminal bleed over and I would need to get a better answer on that.

NADLER: The gentleman's time is expired. Ms. -- Ms. Garcia.

GARCIA: Thank you, Mr. Chairman, and thank you for convening this very urgent hearing on our nation's cyber resiliency. Cyberattacks are at an unprecedented high levels, our small businesses, and our critical infrastructure around the country are under relentless siege.

The consequences of ransomware ramifies throughout our economy, public health infrastructure, and national security. Making things worse, of course, is that ransomware has -- has and continues to be increasingly become a multi-dollar criminal history -- industry.

In 2020 more than 2,300 U.S.-based entities were affected by ransomware and including billions of dollars of economic damage. So I want to focus on a few of those, sir, and I know you said you're here to talk about intrusion so lets talk about a few of those, getting back to the topic.

Several of these events have happened in my district. One that comes to mind is a cyber attack on the Port of Houston. The Port of Houston of course is a critical piece of infrastructure in my district and is important to the national security of our country.

It was subject to a cyber attack by a foreign nation state. They were able to resist the attack. How often does something like this happen where it's a major piece of infrastructure like a - like a port?

VORNDRAN: So we don't know because there are no mandatory reporting requirements from victims. So I'm very, very familiar with the incident that you're describing and would credit the CISO and associated with the Port of Houston for being a tremendously productive and transparent partner in that moment.

And I do believe that if you spoke to that CISO he would be very complimentary of the U.S. government's role in helping them gain restoration of the situation they face.

What we see though is when an adversary finds a vulnerability, as zero day vulnerability in a specific piece of software and that software may be consumed or used routinely by the same industry. So I the case that you're providing, if there was a piece of software in the Port of Houston compromise that you're describing that's used in other ports it's likely that the foreign adversary would go after them in the immediate aftermath.

We generally lack some understanding about why the adversary may be interested in that target. But that would be the best answer I could give you today in terms of how these things stack up and sequentially evolve.

GARCIA: Right. Then I had a school, a high school, that a superintendent - I mean the district's offices hi-jacked. And this is not a big major school district, I mean this was in an unincorporated area which is

semi-rural outside of Houston, less than 10,000 students and they were hacked. And they had to spend, I think it was $207,000 and Bitcoin was the ransom.

How often and why are schools under such attack?

VORNDRAN: Ma'am, what I would say is that the criminal adversaries that we face, the criminals that we face that are going to specifically - are going to specifically look at financial motivations which is the example that you're providing. They are going to go after targets who are the most vulnerable.

And so school districts, perhaps some other entities at the municipality level, it's very important for them to keep their budget requirements where they need to be to maintain operating systems that are current to ensure that patches are passed for operating systems or for other vulnerabilities. To ensure that their employees do understand what spear phishing is and is not.

But what we see criminals do is where can they get the most - the most ease of access to guarantee some generation of money back. And so I'm not saying that it is a resource issue. But it - they are going to go after the areas that -

GARCIA: So it's not just the big banks, it's not just the big companies --

VORNDRAN: It's everyone.

GARCIA: -- it's happening everywhere. I mean like again -

VORNDRAN: It's everywhere.

GARCIA: -- this school district is a small school district. The $207,000 may not sound like a lot -

VORNDRAN: It's a lot of money.

GARCIA: -- but for them it is. And then they wanted it in Bitcoin which I think - from what my reading is that that is a current trend where they're using cryptocurrency for ransom.

VORNDRAN: That's correct. Yes, it is - it is industry organization agnostic, right. The criminals will go and find vulnerabilities where they can, where they believe people are going to pay.

GARCIA: Right. I do have a couple of other questions that I'll submit for the record, Mr. Chairman, because I see my time is gone. But I do want to submit for the record three articles. One, "Port of Houston Target of Suspected -

NADLER: Without objection.

GARCIA: -- (inaudible) Nation State Hack". And the second one is "Sheldon ISD Forced to Pay Nearly $207,000 After Hackers Attacked". And the last one is, "Information for Over 6,000 Memorial Hermann Hospital System Patients Accessed in Security Breach".

NADLER: Without objection.

GARCIA: Thank you.

NADLER: Mr. Bishop.

BISHOP: Thank you, Mr. Chairman. Director Vorndran, has the FBI taken new steps since 2017 to ensure that private government contractors do not abuse access to sensitive U.S. government data stores for self-serving purposes including political purposes?

VORNDRAN: Sir, I'm not familiar with the background of your question. Can you -

BISHOP: Well, the DOJ claims in court that Rodney Jaffe, a.k.a. Tech Executive 1 exploited sensitive DNS data reflecting internet traffic to and from Trump Tower, to and from Donald Trump's personal residential apartment building and the executive office of the President.

He allegedly affiliated with Clinton campaign officials including Michael Sussmann, who had been a cyber lawyer at DOJ and tech researchers are Georgia Tech to fabricate plausible sounding but false allegations about connections between Trump and a Russian bank before the election in 2016 and then after the election about the use of a Russian made phone.

Both of these were scams. Mr. Sussmann fed them to the FBI at the highest levels while concealing his political motives. So that's the background. And the question is, has the FBI taken new steps since 2017 to see that these awesome stores of sensitive data the U.S. has are not being exploited for political purposes by private contractors?

VORNDRAN: Sir, I mean compliance is obviously important to us and just taking a little bit of a broader view, we've obviously taken a lot of reform steps over the past couple of years. Many of them have been in the public whether it's FISA Woods702. So I can't speak specifically to your question, I don't know the answer.

But the bureau has taken a lot of reform steps through that time period that all have been discussed in public forums such as this and in the media.

BISHOP: You mentioned FISA Woods 702 so I think you're talking about the Woods file abuse in FISA applications. I don't think I'm asking about that. Can you think of any reforms that have been taken specifically to see to it that this kind of private contractor abuse of these data stores can't happen?

VORNDRAN: Sir, not at this moment I can not.

BISHOP: What are the cybersecurity implications of a private company being able to intercept internet traffic to and from the White House?

VORNDRAN: Sir, I'm not here to talk about those matters.

BISHOP: Look, you said what you're here not to talk about. I'm a member of Congress asking you for something within your knowledge is a question you're bond to answer, sir. Do you know what the cybersecurity implications are of data being intercepted into and out of the White House?

VORNDRAN: Do I know what the cybersecurity implications are? If you're asking me if I know what the policy is that backs up when we can and cannot -

BISHOP: That's not what I'm asking you. I'm asking you what the implications are, the national security implications of intercepting data in and out of the White House and a private company having access to that?

VORNDRAN: Yes, in general terms, yes.

BISHOP: There are exposures from that wouldn't you agree?

VORNDRAN: Yes, sir.

BISHOP: This article from "The Wall Street Journal" entitled, "Durham Probe Reveals Government Access to Unregulated Data Streams", February 26, 2022, have you seen that article?

VORNDRAN: No, sir, I have not.

BISHOP: It relates -- that the latest developments in the high -- high-profile criminal probe by Special Counsel John Durham show the extent to which the world's Internet traffic is being monitored by a coterie of network researchers and security experts inside and outside of government. There are concerns, obviously, about the privacy implications of private cybersecurity companies being able to tap into the web traffic and then give that data to government at any particular level without warrants or court orders. In what ways does the FBI rely on this kind of data in their investigations?

VORNDRAN: Sir, as I've said earlier today, the -- when you look at private sector broadly defined, but when you look at private sector a little bit more narrowly-defined about who provides infrastructure for network servers, computers, et cetera, those network providers obviously see a lot of traffic. They see my personal traffic. They see your personal traffic on a very routine basis. We have subpoena processes that we go through to request that information when it's relevant to an investigation, so that is how we interact with those companies on a routine basis from an investigative perspective.

BISHOP: Well, my time's about to expire. What this article relates is that a lot of that information can be accessed without warrant, and that's exactly the problem I'm talking about. You've spoken two times to the priority given to the FBI at the highest level to the imperative of protecting the rights of Americans, particularly First Amendment rights, Fourth Amendment rights. And I'm looking for some indication that those are more than empty words, more than just a platitude. I'm stunned that above all the things we've talked about today that you can't even speak to something that -- an abuse that is out in public based on allegations of the -- of the Department of Justice involving the use of cyber data. Is there anything that you can offer to the American people to improve their confidence that the FBI is, indeed, protecting their rights beyond just platitudes?

NADLER: The time is expired. The gentleman -- the witness may answer the question.

VORNDRAN: Sir, you're very familiar with the legal process that we have to go through to obtain information from any number of companies. or even from victims in certain cases. That is our baseline protocol of how we do business. I'm unfamiliar with the article, so I cannot speak to what it actually says in there.

BISHOP: Mr. Chairman, ask unanimous consent to submit for the record the article from the Wall Street Journal entitled "Durham Probe Reveals Government Access to Unregulated Data Streams."

NADLER: Without objection.

Mr. Jeffries?

JEFFRIES: Well, thank you very much, Mr. Chairman, and to the witness, thank you so much for your presence, for the work that you and the FBI do. I'm sorry that you've been subjected to somewhat pro-Putin, pro-insurrection, pro-conspiracy rhetoric as if Donald Trump is a victim, not the perpetrator of perhaps the most significant ongoing crime spree in the history of the American presidency, from Russia's interference in the election explicitly designed to artificially place him in 1600 Pennsylvania Avenue, to his corrupt abuse of power when he pressured a foreign government, Ukraine, to target an American citizen, Joe Biden, by withholding $391 million in military aid to a country, Ukraine, under Russian threat in order to try to extract phony political dirt as part of his scheme to artificially interfere in the 2020 election. And then, to cap it off, he incited a violent insurrection and attack on the United States Capitol to try to halt the peaceful transfer of government.

Donald Trump is not a victim, despite what some of my colleagues from the other side of the aisle have endeavored to project. He is a perpetrator, a one-man walking crime spree. I'm sorry you've been subjected to this.

And let me ask a question or two that relates to everyday Americans. According to a recent report by the FBI Internet Crime Complaint Center, I guess in 2020 alone, approximately 30 percent of fraud losses reported to the FBI was sustained by victims aged 60 or over. Is that correct?

VORNDRAN: Sir, I don't have the exact number in front of me, but that number sounds appropriate based on both the 2020 and 2021 annual report.

JEFFRIES: Is it fair to say that we've seen an increased trend of cyber criminals targeting older Americans?

VORNDRAN: Sir, the -- what we would call eldercare fraud has been a priority of the bureau for many, many years. We have dedicated analyst agents, prosecutors and the Department of Justice that work just this, so it's a very important threat and a very important victim set for us to protect. So whether there has or has not been an increase, I don't know the specific answer, but I think what I would say perhaps more meaningfully is that it's at unacceptable levels even if it's decreasing because it's targeting some of our country's most vulnerable.

JEFFRIES: And what are some of the steps that the FBI is contemplating taking or that you are taking sort of to deal with what you describe as this unacceptable threat that appears to have intensified as we've been navigating our way through this once-in-a-century deadly pandemic?

VORNDRAN: Sir, I'm not sure I understood your question. Did you say what is the FBI specifically doing?

JEFFRIES: Right. What steps are you contemplating? It appears to be intensifying. You've indicated that it obviously is unacceptable and troubling.

VORNDRAN: Yeah.

JEFFRIES: And so just trying to get a sense of what -- what you're doing.

VORNDRAN: Sure. Again, we've -- we've dedicated agents investigating these type of crimes across the country, a lot of them tied to international criminals, and working with our international law enforcement partners, we have FBI agents in 70 countries and very, very good relationships in many of those 70 countries that allow us to get closer to these criminals. But then the second piece of it is public awareness campaigns for those who are elderly and who may not understand the current threats that pose -- or face them in terms of technology. So it's a multifaceted approach and something that's very, very important to us today; no different than it was in the past.

JEFFRIES: Now, you have public education campaigns that, you know, are designed in part to be preventative, and of course, you know, proactive FBI action to kind of take down these cyber criminals. But once, you know, you've sort of uncovered criminality, prosecuted it successfully in partnership with the DOJ, could you comment a little bit in the time that I have remaining on your restitution efforts? Have you been successful, or is part of the FBI's work designed to recover money that has been stolen so that these older Americans who are adversely impacted can -- can gain back some semblance of what was taken away from them?

VORNDRAN: Sure. Of -- of course, recovering money is always important to us, and that restitution back to victims, quite frankly, is what drives many of us to come to work every day and drove many of us to apply to this organization. But it's very, very challenging, especially in the international landscape of how money is transferred. I'll just give you some statistics that may not relate specifically to eldercare fraud, but does relate to business email compromise.

In terms of business email compromise, when -- when we receive reports of BEC fraud, we do have a 75 percent success rate when those transfers are domestic. And so I think if you know you've become a victim of a fraud, independent of what time, that reporting timeline is extremely, extremely important. And many of these frauds hit individual Americans, and I think that makes it more -- even more relevant for the audience.

NADLER: The time of the gentleman has expired.

JEFFRIES: Thank you, sir.

NADLER: Mr. Tiffany?

TIFFANY: Thank you, Mr. Chairman. First of all, sir, thank you for being here. And I'm sorry you were subject to two scurrilous comments about the previous President who gave us a peace through strength - gave us a peace through strength, kept us out of wars, who took crime seriously, who gave us energy independence, which we've given up in just a little over one year, and had kept illegal border crossings down to a level that we had not seen in a long time, and we wish for those days to come back, when we had a strong America.

I think Mr. Bishop's testimony showed that - I would say to the Chairman that it is time to bring the Director back in. There's a lot of questions to be answered. As we heard from the witness here, there's things that he could not answer. I would hope that the FBI Director would be able to answer some of those questions that we'd like to have answers to.

As you follow social media and efforts to facilitate illegal immigration, does it raise concern for you when you have people like the Vice President of Facebook who openly admits they facilitate illegal immigration, FBI is in the business of stopping illegal activities, breaking the law here in the United States? Does that raise concern for you?

VORNDRAN: Sir, again, I'm not familiar with that post or what you're referring to. I mean, any violations of U.S. law, we are interested in exploring, right? And those referrals should come into the bureau. They can either come to the local field office - but if there is a violation of U.S. law, that is obviously what we're here to do.

TIFFANY: So if I show those to you, will the Cybersecurity Division follow up on them?

VORNDRAN: It - it's not going to be a cybersecurity responsibility. The - what you're describing is going to largely fall in the Criminal Investigative Division, but if that's what you want to do, you want to make a referral to the bureau, then we can get it to the right people.

TIFFANY: So it should be a criminal investigation, if they're posting things that facilitate illegal immigration? Is that what you're saying?

VORNDRAN: Sir, I don't know what the post says. What I'm saying is that if there is a criminal - a violation of U.S. law, criminal allegation that you think warrants investigation, then we'd be happy to take a look at it.

TIFFANY: Absolutely. Spread the word at FBI, it needs to be done. And by the way, it wasn't a post, it's numerous posts, and as you know how social media works, it spreads like wildfire and that's what's happening down on the southern border, where the Big Tech companies are helping facilitate illegal immigration.

In February 22 (ph), the Biden administration, just recently, last month, decided to scuttle its China initiative, a program launched by the Justice Department during the Trump administration to protect America from national security threats posed by the PRC.

I'm troubled that that's going away. What comments do you have? Isn't that something that is important to protect Americans and American interests?

VORNDRAN: It - what I would say about China is, from a cyber perspective, they are the top overall cyber threat that we face as a country. That poses both security and economic ...

TIFFANY: So in other words, when we hear from the other side "Russia, Russia, Russia, Russia," it's actually China is the biggest threat, is that correct? Not - not diminishing that we should pay attention to Russia also but you just said China is the biggest threat. Is that right?

VORNDRAN: So we have a big four, right? China, Russia, Iran and North Korea. They're all formidable adversaries. From a cyber perspective, we would assess that China is our most formidable adversary.

TIFFANY: Does the Biden administration scuttling the China initiative bring you any concern?

VORNDRAN: Sir, we operate fairly autonomously, independent of what the Biden administration did or didn't say. Our investigative posture on cyber threats posed by China has not diminished in any way and we have the largest percentages of our organization dedicated to those types of investigations.

TIFFANY: I thank you for that answer.

It was recently reviewed at the start of the Russia-Ukraine conflict that information that President Biden passed on to General Secretary Xi in China, that it was compromised, that information was sent on to Russia, do you know if any of our foreign assets and/or infrastructure was compromised?

VORNDRAN: Sir, I don't know that answer.

TIFFANY: Who do I go to to get that answer?

VORNDRAN: I - I - what I would say is let me take that back and - and we'll get that answer for you. I don't know that answer in the moment.

TIFFANY: Yeah. Deeply concerning, Mr. Chairman, that we're seeing information just simply passed on to our number one adversary, China, and the Russians are able to use it. And just another thing where it seems this administration, the Biden administration, is giving away the keys to the castle here in the United States. I yield back.

NADLER: The time of - the gentleman yields back. Ms. McBath?

MCBATH: Thank you, Mr. Chairman, and good afternoon, Assistant Director Vorndran. Thank you so much for coming before us today.

As has been mentioned by my colleagues earlier, you know, the nation's cybersecurity is just likely one of the most important security trunks (ph) that our nation actually faces but it's also quickly becoming a major threat at the individual level for everyday Americans.

My district - I represent Georgia's sixth congressional district. It's the headquarters to the Colonial Pipeline and that's one of the largest pipeline systems for refined oil products in the United States. And it was victim to one of the most - one of the worst ransomware attacks that our nation's energy sector has seen.

And so this attack really affected not only just Georgians, my constituents, but it affected Americans throughout the country. Americans, they were racing to fill up their tanks at the gas stations before they ran out of fuel and Americans that are relying on their vehicles to perform their jobs and also, you know, there are many people that are ride share drivers and delivery drivers. They wondered whether or not they were actually going to be able to get to work the next day. And this was just not too - not - you know, this happened just fairly recently.

You know - but these cyberattacks aren't just restrict - restricted to large corporations. And the city of Dunwoody, Georgia, which is also in my district, which is - was subject actually to ransomware on Christmas Eve of 2019, and this forced a shutdown of all department networks for several days and it was just really preventing the most important work, necessary work that needed to be done in our Atlanta suburbs.

Additionally, my local school district, Cobb County, Georgia, was also subject to a cyberattack on its emergency alert system, which placed all 112 of its schools - of my - our schools in lockdown.

So I know that we've really - as - as - as has been - been expressed, we really have to make sure that we're doing all that we can to - within our powers to keep America's towns and our businesses secure and just really making sure again that we're allowing America - America to keep running.

But Assistant Director Vorndran, my first question for you is this - how is the FBI's Cyber Division ensuring that America's towns and cities, like my city Dunwoody in Georgia, have the tools and the resources that they need to quickly and appropriately respond to these cyberattacks? Because I'm assuming that, you know, this will continue to happen. So what do we do to assure that they are prepared?

VORNDRAN: Sure. Well, a couple of things. Number one, we would recommend that all those municipalities have active relationships in the U.S. government to the best of their ability that would cross-cut the FBI, U.S. Secret Service, and CISA as well, because FBI and/or U.S. Secret Service can fill the threat response side of PPD-41, and CISA can fill the asset response side. CISA specifically to the net defense resiliency piece has a lot of online resources available for those towns and municipalities to ensure that they're aware of the latest vulnerabilities. And by mission design and I believe but E.O., I believe that is CISA's core responsibility -- one of CISA's core responsibilities is to maintain those vulnerability lists, to ensure that those entities, like you describe, have access to that information about how to ensure resiliency of their systems.

A few other points I would make are, you know, it is important that these municipalities have incident response plans built and that they are in a position to exercise those so that if they do become a victim that they can call people they know and engage in meaningful dialogue with the bureau, with Secret Service, or with CISA to ensure that the latest information is in their hands. You know, as I've described here already today, there is a whole host of things that the U.S. government can do leading up to and at compromise and on the backside of becoming a victim. But probably most important is to ensure that the U.S. government inter-agency level, that would be inclusive of, certainly, the FBI, Secret Service, CISA, NSA, to name a few, that we are disseminating information about indicators of compromise, known vulnerabilities in a timely fashion. And I think that's an area that collectively as the inter-agency we've made tremendous progress in the past year.

MCBATH: Thank you so much. And I know -- quickly, I know I'm out of time, but September 24th of last year, Ciox Health, which is also in my district, it's health care information management company, they discovered that they had an authorized individual -- an unauthorized individual also had access to sensitive patient information. You know, what are ways in which the FBI Cyber Division is ensuring that patient data posted by various health information management companies is also protected?

NADLER: The time of he gentlelady has expired. The witness may answer the question.

VORNDRAN: Sure, sir.

Ma'am, that's a fairly complicated question because from an FBI perspective, you know, our role is asset recovery in terms of if something has been lost, in this case data. So in these scenarios that you described such as Ciox Health, we're actively engaged to try and prevent that data from being pushed out or being used for other nefarious purposes. And I believe that was the exact reason Ciox engaged us. But, again, I would point back to like what is the U.S. government doing? It's really a focus on the resiliency net defense training side to make sure that operating systems are updated, that there is active backups for all of these corporations, all of these things that are very, very much within CISA's roles and responsibilities by mission and E.O., very much relevant on their website, are things that they should pay -- they being the entities in your district should pay attention to.

NADLER: The gentlelady's time has expired.

Ms. Fischbach.

FISCHBACH: Thank you, Mr. Chair.

And, Assistant Director, thank you for being here. I'm just going to ask some questions about -- that have to do with rural areas. And -- and my district is very rural and has large amounts of farmland, very big. It goes from half of Minnesota, from Canada to almost to Iowa, but you - does the FBI categorize these cyberattacks or the cyber threats by geographic location?

VORNDRAN: So we - the answer is yes but not in a - in a way that we use it to drive resourcing. So when we look at the threats, we're looking really at who is conducting the activity that's causing people in your district problems.

Obviously, almost entirely - I mean, I'll throw a figure out there - close to 100 percent are outside of the U.S. that are - that are adversaries (inaudible) in the cyberspace. But in your example, whenever there is a compromise, we will have the FBI engage with the organization or the entity or the company, and because of that, we certainly have information that indicates how many victims have been relevant in a district or in a state.

FISCHBACH: Do you think that it should be categorized, I mean, so that - so the people in - in rural areas understand that they are at risk too? I mean, because obviously - do we know if there's more in big cities? I mean, that's kind of what I'm asking about and ...

VORNDRAN: I don't know the answer. I mean, it's an interesting question. I mean, what we see is that a lot of these attacks will be indiscriminate, in terms of who they're going after, just to find access points or vulnerabilities and then to see what values there - and like we've talked about here today, on the ransomware side specifically, the bottom dollar is the bottom dollar, right? If they can get money out of a victim, they're going to continue to go back to that industry.

You know, you described farmland. We know that certain industries within ag have been targeted through known vulnerabilities - I don't believe in Minnesota but perhaps more in the Midwest, where we have seen a trend of specific ag industries being targeted.

As we've talked about here today, that usually happens because those industries or those companies are using the same software packages that have the same vulnerability in them.

FISCHBACH: OK. So maybe that - it - it was going to be a follow up but - so you kind of answered cause I was going to ask if you understand how much of a threat cyber crime and cyberattacks are to agricultural businesses, big or small. So I - it sounds like you are addressing those?

VORNDRAN: Absolutely.

FISCHBACH: OK.

VORNDRAN: Absolutely. And by "we," it's not just the FBI, it's - it's the interagency of the U.S. government that has roles and responsibilities in this space, but certainly FBI is a big part of that.

FISCHBACH: Do you think that there is any way, Assistant Director, to get the information about it being, you know, either rural or metro? Because I know that there was a hospital in - a small hospital in - in my district that - that was - I believe it was ransomware.

VORNDRAN: Yeah.

FISCHBACH: And so I'm just - I'm wondering if there is a way to determine that.

VORNDRAN: So I'd be happy to take that back to our - to our team and to see what we can come up with that could answer - answer that request for you. That's not a problem.

FISCHBACH: OK. Well, thank you very much, I appreciate that.

And then just one last - one last question - you know, the FBI maintains the Internet Crime Complaint Center for reporting cyber crime. Unfortunately, it's online. Is that correct, it's only online?

VORNDRAN: Correct.

FISCHBACH: In my district, Internet signals can be weak, and we have been working on, you know, deploying broadband, but it does make it difficult for victims to always report cyberattacks or seek help from the FBI. And I - is there something that the FBI can do differently or take into consideration to do to mitigate this, so is there an option to - if they don't have Internet - good Internet available?

VORNDRAN: Yeah, I mean, they can simply call our field office or the local resident agency to report that. That's not a problem.

FISCHBACH: Is that generally something that would be - I mean, if you see something that says, you know, "report it here, ww.whatever (sic)" - would then a - a phone number be in a - with that same information or is it something that should be added?

VORNDRAN: You know, IC3 is a very, very valuable resource ...

NEGUSE: The gentlelady ...

VORNDRAN: ... just looking at some statistics here. But what I would say is our focus - and - and it's been very, very core of our message, is we actually rather have a personal relationship with a company, an organization, a municipality than we would receive a random report through an Internet portal, right?

So yes, IC3 is available but please know, like, that personal relationship is extremely important to us. And if there's anything I can do to facilitate that or if you think we're missing out on important data because we're only offering an Internet portal, I'd be more than happy to have that conversation about how to improve that.

FISCHBACH: Well - and just one more - I - I was just - I'm just concerned that when there are those attacks, whether it be in agriculture or a small hospital, that they are able to reach out immediately ...

VORNDRAN: Sure.

FISCHBACH: ... so that's - and that they know where to reach out to. So - but thank you very much, I appreciate that.

VORNDRAN: Of course.

DEAN: The gentlelady's time has expired.

FISCHBACH: Mr. Chair, I yield back.

NEGUSE: The gentlelady yields back. Recognize myself for five minutes of questions.

Director Vorndran, thank you for attending this hearing today, for helping us understand how we may better address this serious issue. In my home state of Colorado, local government entities have been hit hard by ransomware attacks, as have large organizations, like the University of Colorado, which is in my district.

One of my biggest concerns is the link between some of these attacks and hostile foreign entities. The University of Colorado, for instance, was affected by an attack on Accellion, a third party vendor used by the university in 2021. The university refused to pay the ransom request and over 300,000 records containing personal information was ultimately released on the dark web.

And it turns out the hackers, at least as we understand it, were part of a ransomware consortium known as Cl0p. They were arrested in Ukraine, as you know, and the Ukrainian authorities believe the group may have caused half a billion dollars in financial damages around the world.

I wonder if you might be able to share some additional information on this particular organization and what the potential links are between groups like this one and the Russian government?

VORNDRAN: OK. So Cl0p is one - is a very well - in my world, Cl0p is a very well known ransomware variant. We've heard them referred to as ransomware gangs. I personally don't like that, that terminology, because it infers that you have a dedicated group of people under the banner of one variant.

We know that's not true. We know that many of these actors, many of who are in Russia or the surrounding region, are affiliated with multiple variants because when we look at it, it - really, the ecosystem breaks down this way - you have key services, you have malware and delivery, you have infrastructure, you have communications and you have financial, right? Those five key services are paramount to catalyze and bring home any cyberattack.

So actors cross-cut those services. So there may be an actor who's great on the financial side. That individual may decide to service four or five or six or even more of the ransomware variants. The ransomware variants are simply a brand name.

But to your core question, sir, Cl0p is a very, very well known ransomware variant that the entire interagency and the U.S. government has been aware of, as well as technology researchers and cyber - cyber threat intel companies know (ph).

NEGUSE: I do think that the point - you - thank you for your answer - and - and the point you make is a salient one, with respect to the cross-currency of these variants, right, and the fact that they may be operating under multiple different banners.

I guess I wonder - more of an open-ended question - I reviewed your written testimony and appreciated a lot of the exchanges that you've had today - this is clearly a pervasive issue across the country, certainly in Colorado. Across our state, we have had attacks on Children's Hospital in Colorado, which was attacked in 2017; exposed the personal data of more than 3,000 patient families, the Fort Collins Loveland Water District, of course, the Colorado Department of Transportation, the University of Colorado, as I've mentioned; entity after entity impacted by these cyber attacks.

Congress has proposed a series of solutions. We have a bill, a bill that I introduced last year, the State and Local Government Cybersecurity Act that would expand DHS responsibilities to provide education and assistance to state and local, tribal and territorial governments along the lines of what you've described today, as well as the general public, right, on cyber threat indicators and on defensive measures that they can take, right, to better kind of determine their own vulnerabilities and their incident response, which you referenced in response to a question from one of my colleagues. I don't know if you would care to opine on that particular bill. It's passed the United States Senate. We're trying to get it through the House. But also on a more open-ended question, what other tools you might recommend the Congress legislate...

VORNDRAN: Yeah.

NEGUSE: ... and new statutes that you might recommend that we consider.

VORNDRAN: Sir, I appreciate the question and the opportunity. Certainly, on the proposed legislation that you mentioned, would be more than happy to have a look at it and offer you more refined thoughts.

In terms of your question about what legislation would be helpful, you know, first would be to give prosecutors stronger stakes to prosecute using RICO charges for cyber criminals, enhanced punishments for damaging critical infrastructure. Second would be equipping courts and law enforcement with more tools to disrupt a large-scale cybercrime. So criminalizing selling infrastructure access to botnets, injunctions to stop ongoing or imminent mass cybercrime, and last would be to improve DOJ's forfeiture

authorities so that we increase our ability to authorities to seize cyber crime critical -- or infrastructure, network infrastructure, that is. So those are just a few thoughts that I think are very relevant.

NEGUSE: Thank you, Director, for you, your service, or for your hard work, to your team for the work that you're doing each and every day to protect our country, our states, our local governments from these pernicious attacks, and we'll certainly take your recommendations under advisement.

And with that, the chair now recognizes the gentleman from Oregon, Mr. Bentz, for five minutes.

BENTZ: Thank you, Mr. Chair, and thank you, Mr. Vorndran, for your patience. So it would have -- it would have helped me had there been a definition of cybercrime at the very onset of the hearing because it appears that the definition I quickly looked up here in the dictionary which says "cybercrime: criminal activity carried out by means of computer or the Internet" is a far broader definition than that which your portion of the FBI is dealing with. Do I have that right?

VORNDRAN: Yes, sir. When we look at cyber within the FBI, I would -- I would split it as computer-enabled crime and cyber. Cyber, we would define specifically as network intrusions, where computer-enabled crimes, things -- child exploitation on the Internet, you know, eldercare fraud facilitated by the Internet, these types of things. Those are in different investigative programs within the FBI.

BENTZ: This is still within the FBI because you're the lead agency, are you not, when it comes to all the other sub-agencies we've heard about today. So one way or the other, the FBI is in charge, and I guess, so you would -- you would carve yourself out from responsibility for some of the things we've heard about today. The one that comes most readily to my mind is the situation on the border, where we see and heard from the Border Patrol that the Internet is being used to attract thousands of folks to the border, and we know it's being done illegally, but yet, nothing's being done about it. But that's outside the scope of what you believe your portion of the agency is dealing with.

VORNDRAN: That is an accurate statement.

BENTZ: OK, so...

VORNDRAN: As I mentioned to, I believe, Mr. Tiffany, if there is a belief that there is a violation of U.S. law, then that referral should be made. I'm not specifically familiar with the issue you're talking about. Certainly not saying it's not out there.

BENTZ: Oh, it's out there, and -- and it has been referred and is being ignored, and that's -- but that's not your, apparently, scope of -- of -- of purpose.

So let's shift instead to what you do do, and it sounds to me like what -- if we looked at this cyber situation as a continuum and -- and the -- the cyber event occurs in the middle, your primary focus in prevention would be to point out those who are in the business of writing software in the private sector to try to head off attacks of malware and other things, as opposed to you, because you're -- the FBI isn't writing that software. Or am I wrong? Are you -- do you have your own division that's trying to write software that's going to head off some of these things?

VORNDRAN: Not to my knowledge, no.

BENTZ: OK, so going back to my continuum, what we have is a situation where the FBI is saying it -- alerting people. "Hey, we've had an attack over here. Get ready. It could happen. Go buy some new protective software." And then the event happens, and then you come in afterwards and say, "Hey, look what just happened. We'll try to help you clean up the mess and we'll try to find whoever did it and prosecute." Have I summarized the nature of your department appropriately?

VORNDRAN: Yes, but in my opening statement, I gave some -- I think some really important notes, that we're not an arrest first/indictments first organization when it comes to our cyber ecosystem role. We're very much interested in understanding who in the inner agency has the most impactful operational play to impose the most significant costs on the adversary. At times, that may be an arrest, an -- an indictment and arrests and extradition, but at times, that may be degrading the infrastructure that these adversaries are riding (inaudible)...

BENTZ: Right, and I understand that you have tools, and you have different ones you might use after the event.

Now I want to go to a -- a question of great interest to me, and that is your assessment of the quality and ability of our private sector to head off that which is happening in China. So tell me, how good a job are we doing in that private sector? Are you seeing an increase in attacks? Are you seeing the private sector doing a good or a bad job?

VORNDRAN: So -- and I want to try to be consistent, and I've answered this question twice, so I'll try to be really consistent. My interactions and our organizational interactions in cyber relative to the private sector have been very positive in the last year that I've been here. It's hard for me to speak to the time before that. I was in New Orleans. But in the last year, these infrastructure providers, these major server providers, they have been very, very good partners. And if you go and do some research, you'll see they're actually writing their own blogs and disseminating their own products to the American public largely before, sometimes, anyone else outing adversarial activity. So I think they've been tremendously transparent and tremendously proactive in that space in terms of (inaudible)...

BENTZ: And that's all very good, but I haven't heard you tell me if -- how well we're doing when it comes to keeping up with China.

VORNDRAN: Sir, the -- my statement covers China. It covers Russia because they -- the -- the private sector sees a lot of the activity from all of those countries.

BENTZ: So then you're saying we're doing just fine.

VORNDRAN: Sir, there's always room for improvement, undoubtedly. What I'm saying is the private sector is very proactively engaged and -- and been a very good partner in that space to us.

BENTZ: Thank you.

I yield back.

DEAN: The gentleman yields back.

The gentleman from Arizona, Mr. Stanton, is recognized for five minutes.

STANTON: Madam Chair, thank you very much. Thank you to Mr. Orfragen (sic) for your service at the FBI and for testifying at today's very important hearing.

In recent years we have witnessed cyber threats and cyber attacks as they become more sophisticated, more targeted, and more harmful.

These attacks not only are directed at strategic national security operations but also essential infrastructure, educational institutions, and local governments. For instance, in my home state of Arizona, one of our local community colleges was forced to cancel classes when a cyber threat was detected in their network.

Luckily, they were prepared, they took preventative measures, and they safeguarded their students' and their employees' information. But these smaller incidents don't always get the national attention like the bigger attacks on Colonial or JBS. But the threats are no less real, and neither are the disruptions they cause to our daily lives.

So, Mr. Vorndran, I want to ask you about these lower-profile attacks. In February of 2022, the Cybersecurity and Infrastructure Security Agency published an alert that the FBI had observed some ransomware groups shifting away from so-called big game hunting in the United States, and instead increasingly targeting smaller victims to avoid scrutiny from the federal government.

Do you believe that this change was due to the administration's crackdown on ransomware attackers?

VORNDRAN: No, sir. I just think that we are seeing an evolution of the criminal enterprise that instigates and catalyzes ransomware attacks. And they are going to go where they can find the most routine financial gain on a routine basis. So they are going to go where the money is and that's the bottom line.

STANTON: Why are small to mid-size victims a safer bet for ransomware groups?

VORNDRAN: Sir, my opinion on that question is that smaller entities are not as well resourced as some of these larger entities. Resourcing really covers the resiliency and net defense side whether that's patching, multi-factor authentications, zero-trust architecture.

Whether that's training for spear phishing, keeping your operating systems patched and updated. Any number of these things that tie back to resources. My assessment personally would be that these type of organizations, entities, municipalities are not as well resourced as some of your major multi-national companies.

And because of that, they're likely potentially more vulnerable.

STANTON: Are you concerned that by cracking down on the hackers of bigger, wealthier companies that the FBI has sent a message that smaller targets will be met with less force?

VORNDRAN: The way we work our investigations, Sir, we -- we look at the -- the -- the conglomerate of all the victims that, unfortunately, become victims and tie them back to the adversarial activity that's perpetrated by -- by groups of people almost all of which are overseas.

And so, the ability for us to investigate or for the inner agency to include the Bureau to run offensive operations really isn't impacted in any way. So it would be hard for me to -- to see a scenario where we're encouraging smaller targets to be hit. Because it's just not tied to our investigative or inner agency operational calculus.

STANTON: How will the FBI adjust its attack plan to better ensure that small and medium-sized businesses are protected as they are with some of the larger entities?

VORNDRAN: Yeah, Sir, so, the FBI's always available for these entities. And we would encourage those relationships to start if they're not present. But this exact question is why CISA was stood up. And it's, you know, codified in the executive orders. They are there for the purpose of improving what we would define as resiliency in net defense.

And they have these resources in their mission statement or as part of their mission and available for the exact type of groups that you're talking about. And so, they are in the U.S. government the best entity for those small businesses to really work with to improve their net defense plans.

The FBI and CISA have a tremendously strong operational day-to-day, week-to-week relationship. What we can do is we're sharing indicators of compromise, latest intelligence that can better inform the net defense side that CISA carries forward.

STANTON: I appreciate your testimony today. And I will yield back.

DEAN: The gentleman yields back. And now the gentleman from Wisconsin, Mr. Fitzgerald is recognized for five minutes.

FITZGERALD: Thank you, Madam Chair. On -- Mr. Vorndran, on February 23, 2022, Department of Justice announced the end of the China Initiative despite an internal review finding no indication of racial bias.

Mr. Vorndran, what is your division doing to absorb all the activities that were part of that China Initiative that was, you know, we all thought was being very successful in countering national security threats posed by China?

VORNDRAN: Sir, our workload in terms of cyber division has not changed as a result of that -- that initiative that you referenced. You know, as I've said already on the record here today, you know, we do consider China our top overall cyber threat to the United States and to our allies.

We have an enormous amount of our workforce dedicated to that cyber threat. That has not changed in the last six months, the last 12 months, the last 18 months. The problem with China is that they're very indiscriminate about who they target.

It's not that it's the U.S. government, I just have a few notes here, think tanks, academia, CDCs, journalists, medical, COVID-19, the list goes on, they're very indiscriminate. And so, we would say that

they are the biggest national security and economic threat. But to your question has my workload changed, it has not.

We've had a lot of people dedicated to that problem over the -- certainly over the past year.

FITZGERALD: So in relationship to the initiative there had to be some items that I would assume would have to be picked up in some form by your division, is that -- but you're saying that did not happen?

VORNDRAN: No, Sir, that didn't happen for me. And again, this -- this gets into some of the Bureau structure, counterintelligence division, you know, they may have a different answer to that question I'm unsure. But for me personally, you know, under oath, my workload has not changed or been altered in any way as a result of that.

FITZGERALD: There was some discussion earlier by other members about Alexei Burkov and the cybercriminal now that he's kind of out there. And we're not sure exactly I guess, and it would difficult I think for you to tell us how -- how you're tracking that.

Can you tell us today that you're confident that there aren't currently cyberattacks that are being coordinated or launched as a result of his release?

VORNDRAN: I don't have any information that would indicate that's happening. That's as -- that's as much of a refined answer I can provide to you.

FITZGERALD: OK. REvil, a Russian-based criminal -- cybercriminal group claimed responsibility for one of the biggest ransomware attacks on the information, technology, management, and security software company Kaseya, which I'm sure you're aware of.

Reportedly victims, including schools and hospitals, many lost millions of dollars in recovery. Is it accurate that the FBI withheld a digital decryptor tool that could have unlocked the system subject to the ransomware attack in the case of CSAM?

VORNDRAN: Sure it is. And among myself and National Cyber Director Chris Inglis, sir, in open testimony in December in Oversight and Reform where we're on the record about this exact topic. So yes, that is an accurate statement. I'd be happy to explain our decision on that if that would be helpful right now.

FITZGERALD: Let me just tell you, is it also accurate that goal of withholding this tool was to disrupt the hackers, the Russian hackers, without alerting them? Was that what the goal was?

VORNDRAN: There were multiple derivative elements to the operational plan that were being evaluated during that time period to include the validity of the decrypter tool and ensuring that it didn't have malware or introduce other vulnerabilities into the supply chain.

FITZGERALD: Is it fair to say that the mission overall was not successful?

VORNDRAN: Sir, my pause is because I'm trying to remember specifically on that operation.

FITZGERALD: Did -- let me ask you this, did you or anyone in the FBI caution against withholding the decrypter?

VORNDRAN: Did we caution against withholding the decrypter? We had a series of variables that were under consideration in that moment that ranged from providing the decrypter key immediately to letting an operational plan play out in infinite time period. Once we had indications that that operational opportunity -- the opportunities were not going to be valid we immediately moved towards deploying the decrypter.

In parallel, from the moment this started we were testing the decrypter to ensure that it didn't have any malware, because I had already described, we don't go buy this from Best Buy, right. This is touched by many, many criminals, developed by criminals and many hands in the supply chain.

So in order to get that we obviously have to put it through a testing environment knowing that CASA is going to deploy it in a supply chain environment and we don't want them to introduce vulnerabilities downstream.

FITZGERALD: I'm out of time, but I'm going to follow-up with a letter trying to dig into this a little bit deeper. So, thank you Madam Chair.

DEAN: The gentleman yields back. And now the gentlewoman from Washington State, Ms. Jayapal is recognized for five minutes.

JAYAPAL: Thank you Madam Chair. Mr. Vorndran, thank you so much for your commitment to ensure our security in light of new and evolving cyber threats.

I wanted to focus my five minutes on the data breeches of critical infrastructure, namely our hospital systems. Hospital attacks against healthcare facilities are becoming more frequent as the pandemic and workforce shortages created new vulnerabilities.

Just this past June, Sea Mar Community Health Centers, a non-profit community-based provider in my district, learned that the sensitive personal health data of nearly 700,000 patients were compromised. Names, addresses and social security numbers were stolen from its internal network.

The FBI has stated its deep concern about the increase in ransomware attacks on hospitals and other critical infrastructure. Can you elaborate on why these attacks on healthcare systems have become so frequent?

VORNDRAN: Sure. Give me one second here. So, we have seen excessive targeting of the healthcare industry during the COVID-19 pandemic. We would assess that the reason for that more than anything else is because adversaries, criminals know those hospitals, healthcare providers are in a very, very vulnerable position in terms of continuing to provide care. And as a result of that are likely to potentially pay an extortion payment or a ransom more quickly.

And so, it's really a sad state of affairs when criminals really are looking to disrupt patient care and that's actually on the table of viable options for them as criminals and how they're going to effect us here in the United States.

So, that would be the primary reason that we would assess that there's been an escalation. The other point that I would really highlight, I've talked about this several times today, what we see is industries, hospitals in this use case, it could be any industry though, have common software platforms that they all generally use.

And when an actor finds a vulnerability in one of those software platforms that is obviously likely to be pervasive or potentially pervasive across other hospitals. So, you may see a surge of activity against a traditional or a specific sector until that is closed. I hope that answers your question.

JAYAPAL: It does. And, you know, what's really terrible, and you referenced it, is that these attacks are just leaving patients so vulnerable and delay first responder from responding to emergencies or prevent hospitals from accessing life-saving equipment. In fact, 22 percent of healthcare organizations that suffered a ransomware attack this year experienced increased patient mortality after the attack.

So, what is your -- what are your best thoughts on how hospital systems that are suffering from cyber attacks can mitigate negative patient outcomes?

VORNDRAN: Yes, so again when we look at the cyber ecosystem, or what you're describing specifically as cyber security, within the U.S. government CISA is on point for those recommendations. Largely what you hear from them is cyber hygiene is really important.

That includes a multi-factor authentication, implementing zero-trust architecture that includes making sure that your patch management is where it needs to be, updated operating systems, et cetera. It also includes strong passwords, but also strong discipline of users, specifically administrators. All of that information is available on CISA's websites. And that's a really good one-stop-shop for hospitals, like you're describing, to kind of get to a best of checklist.

JAYAPAL: But is the FBI launching your own special initiative to make sure that hospitals that are struggling with access to sufficient cyber security defenses, because they have low budgets or staffing restraints, what are the ways that the FBI can help elevate this for healthcare providers to kind of reinforce their defenses against ransomware attacks?

VORNDRAN: I appreciate that opportunity to answer that question. We have very, very strong relationships with the American Hospital Association and with the Health-ISAC. ISAC is the Information Sharing and Analysis Center. We do very routine podcasts with the American Hospital Association and their director and some of our personnel on both the analytical and the operational side to try and reemphasis this message.

We're very much prioritizing the investigations that hit critical infrastructure overall to include hospitals. So, I hope those few additional items help. The only other thing I would say is, in order for CISA to do its job well, all of on the investigative side have to do our job well, because we're seeing new indicators compromised, new malware signatures, new tactics, techniques and procedures, all of which reinforce and inform the net defense side. So, that's how we would plug into it and what we've been doing to amplify it.

JAYAPAL: Thank you, sir, for elevating that. I really appreciate it. Madam Chair, I yield back.

DEAN: The gentlewoman yields back. I now recognized the gentleman from Texas, Mr. Gohmert, for five minutes.

GOHMERT: Thank you, Madam Chair. And appreciate your being here. Looks like we may be the last. There may be somebody else to ask questions. But there was an internal review done at the FBI in 2019 to gauge compliance with FBI rules for handling high-profile delicate cases known sensitive investigative matters S.I.M.s, general involved activities of domestic public officials, political candidates, religious organizations.

And the FBI's audit turns out found that in auditing 353 cases there were 747 compliance errors in violation of FBI rules. To your knowledge were aspects of those 353 cases handled by the cyber division?

VORNDRAN: Sir, to the best of my knowledge there were a handful of cyber cases that were a part of that audit.

GOHMERT: Well I know Jamie, members of Congress, Jamie Raskin and Nancy Mace has requested a review of the FBI's domestic operation. Will the cyber division comply with that request?

VORNDRAN: Sir, are you referring to the DIOG, the Domestic Operations Guide? I'm not sure.

GOHMERT: Well they had made a request to review domestic operations so -

VORNDRAN: Any request that's supported by the department and by the director of the FBI I obviously will support.

GOHMERT: Well then I guess that's the question. Are they supporting - the question is, would you support them to the director?

VORNDRAN: Sir, I'd be happy to take back you request. I am actually not familiar with what you're referring to.

GOHMERT: OK. And I'm not asking for any specifics, just numbers, but how many cyber cases have been - have involved warrants for surveillance of any American citizens from the FISA court?

VORNDRAN: Sir, I couldn't even hazard a guess, I apologize.

GOHMERT: So there would be a lot?

VORNDRAN: Of U.S. citizens?

GOHMERT: Right.

VORNDRAN: Sir, I don't know that answer off the top of my head. I apologize.

GOHMERT: Well how about generally speaking, more than 1,000?

VORNDRAN: No, sir.

GOHMERT: Less than 1,000?

VORNDRAN: My best guess would be absolutely the latter.

GOHMERT: Do you know if there's been any internal review like that one that we just found out about from 2019. Has there been any internal audit for 2020 or 2021?

VORNDRAN: Not that I'm aware of, sir.

GOHMERT: The cyber crime website on FBI.gov says the FBI is the lead agency for investigating cyber attacks and intrusions and the decision collects and shares intelligence and engages with victims while working to unmask those committing malicious cyber activities.

According to a Department of Justice audit in 2017, the FBI disrupted or dismantled 262 high level criminal operations targeting global U.S. interest. In 2014 we know that the cyber crimes disrupted - you division disrupted 2,492 but in 2017 just 262. Has the track record improved since 2017? What was the reason for having so few compared to what your division's done before that?

VORNDRAN: Yes, I'm unsure about the 2014 number and what that is or isn't referencing.

GOHMERT: More concerned about 2017 when you didn't disrupt too many.

VORNDRAN: Yes, I guess - I guess my point though would be like I'm unsure of how the metrics were pulled in 2014 on that website.

GOHMERT: OK. If you don't know, but I would sure like to find out and I'd like give the rest of my time to Mr. Jordan.

JORDAN: I thank the gentleman for yielding. Mr. Vorndran, where you involved in the original indictment and prosecution of Alexi Brookhoff (ph)?

VORNDRAN: No, sir.

JORDAN: OK, thank you. I yield - well I yield back to the gentleman.

GOHMERT: OK. Just quickly, does the cyber crime division pay informants as part of cybersecurity investigations?

VORNDRAN: Sir, I'm not going to go into specifics about our source operational activity.

GOHMERT: Well I just asked a general question.

VORNDRAN: I understand.

GOHMERT: Do you/

VORNDRAN: I understand. That is always an option that we would consider if the circumstances are appropriate.

GOHMERT: OK. My time's expired.

DEAN: The gentleman yields back. I now recognize myself, the member from Pennsylvania, for five minutes. And Director Vorndran, I'm very thankful to you for your service at such an important critical time in our country.

I'd like to turn to voting. There is a concerning level of apathy among American voters. Citizens on both sides of the aisle believe more and more that their vote doesn't matter. And of course I couldn't disagree more. So restoring our faith in the voting system, in our democracy requires greater investigation into the ways to protect the integrity of our voting system.

And protect it against misinformation, cyber attacks they've become a tenement of the American voting system. I believe America deserves better. We deserve better.

Director, what are disinformation campaigns so difficult to identify and take down? And what does that process look like?

VORNDRAN: I mean they're so difficult to identify and take down because the rights of U.S.-- people in the United States are very, very broad in terms of their rights to consume, create and spread information even disinformation. And so it's a very, very - very, very nuance conversation.

To you question about how we handle this, the FBI has very specific responsibilities and authorities but it's important to note that we're just one part of the U.S. government team that looks at that.

Specifically we follow the actor and the activity more so than identifying a piece of disinformation. We don't do that. We really are following the actor and the activity. The problem is when an actor masquerades as someone he or she is not and understanding the amplification, the disinformation campaign and to deal with the coordination of that from an adversarial prospective proves to be pretty challenging.

We work really hard to understand how our private sector partners like to receive information from us and other partners in the U.S. government so that they can take appropriate actions that lines with their terms of service violations. But I think we do it all very mindfully. We use court (ph) process when appropriate. But I cannot underscore more that like the underlying principle is respecting the rights of U.S. people, right.

And we all know that their rights to consume, create, et cetera, are very, very broad from a (inaudible) perspective.

DEAN: Absolutely. I know that is the challenge. It's part of the beauty of our democracy but also the challenge. Is the FBI doing processes to combat misinformation campaigns? Not just domestically but also foreign?

VORNDRAN: Are we doing a campaign?

DEAN: To combat - disinformation campaigns foreign, please (ph).

VORNDRAN: When you say campaign to me I think of media, so not to my knowledge. We are doing a lot of work in this space to investigate actors and activity, to deal with that appropriately through what we would consider foreign influence. That work is done in complete collaboration with our interagency partners who have very specific responsibilities and authorities in that space as well.

DEAN: And in a room full of politicians, I probably shouldn't use the word "campaign" because I think of something else.

I'm a former teacher. I was a professor for 10 years before I came to public service. I was surprised to learn that schools, K-12 schools, are some of the most common targets of ransomware attacks. I have a school district in my suburban Philadelphia area, Souderton, PA, and in September of 2019, they suffered a - a cyberware attack.

I don't think we even know - and maybe you could offline get back to me if there's anything more you would know about the Souderton, PA cyber attack - why - why schools? And are they particularly easier to attack?

VORNDRAN: I - I do think - my personal assessment, based on where I sit on a daily basis - there are very mature cybersecurity organizations in this country. There are also - and I don't use this term maliciously at all - cyber immature organizations. They may not have the resources, they may not have the funding, they may not have a culture of cybersecurity in place.

Those second batch of companies, organizations, entities, municipalities, school districts become very, very vulnerable. And the best practices are really on the net defense resiliency side, ensuring that the - the employees of Souderton High School, which I'm familiar with, by the way, is - are - are well prepared in terms of identifying spear phishing campaigns. Very, very important.

But we see these targets becoming targets generally because they're immature from a cyber perspective. And again, with all due respect to school districts, municipalities, they're just not as well resourced as a multinational bank when it comes to cybersecurity.

DEAN: I see my time is expiring but maybe we could connect offline and allow me to learn what we can learn. Thank you for your answers. I yield back.

For what purpose does Ms. Jackson Lee seek recognition?

JACKSON LEE: I thank you so very much and I would like to engage the FBI offline on - it's what - I'm going to just read headlines into the record please. And thank you so very much for your testimony, and as well, your very keen effort in trying to answer our questions of substance.

Let me just read - "information for over 6,000 Memorial Hermann patients accessed in security breach" - these are all Houston and Texas. This goes to the question of healthcare - "medical provider waited months to send patient letters about ransomware." Of course, this goes to the seeming intimidation that our firms have about letting people know what has happened to them.

"NBA's Houston Rockets face a cyberattack by ransomware group." And I would argue that - that this had some impact. They would've been in the Finals had - had they not had that ransomware attack.

"Already in the midst of a crisis, Houston hospital was attacked by ransomware." This was during the midst of the pandemic COVID-19.

"Cyberattack briefly shuts down Humble ISD on their first day of remote learning." That was really devastating during the pandemic. And then "restaurant Landry (sic) warns customers of potential data breach." That's all of the credit cards and things of that sort.

So it is pervasive and I - I look forward to some further discussions but I wanted Houston's impact to be in the record and let them know that we're fighting to (inaudible) this kind of - these kinds of attacks. And I thank you so very much. Again, I thank you for your service and yield back.

DEAN: Without objection, they shall become part of the record.

And mindful of the Chair that - that is - is here, this concludes today's hearing. We thank you, Director Vorndran, for participating, for all of the time that you have given us. Without objection, all members will have five legislative days to submit additional written questions for the witness or additional materials for the record.

Without objection, the hearing is adjourned.

END

SPEAKERS:

REP. JERROLD NADLER, D-N.Y., CHAIRMAN

REP. ZOE LOFGREN, D-CALIF.

REP. SHEILA JACKSON LEE, D-TEXAS

REP. STEVE COHEN, D-TENN.

REP. HANK JOHNSON, D-GA.

REP. TED DEUTCH, D-FLA.

REP. KAREN BASS, D-CALIF.

REP. HAKEEM JEFFRIES, D-N.Y.

REP. DAVID CICILLINE, D-R.I.

REP. PRAMILA JAYAPAL, D-WASH.

REP. TED LIEU, D-CALIF.

REP. JAMIE RASKIN, D-MD.

REP. ERIC SWALWELL, D-CALIF.

REP. VAL B. DEMINGS, D-FLA.

REP. LOU CORREA, D-CALIF.

REP. MADELEINE DEAN, D-PA.

REP. VERONICA ESCOBAR, D-TEXAS

REP. SYLVIA GARCIA, D-TEXAS

REP. LUCY MCBATH, D-GA.

REP. JOE NEGUSE, D-COLO.

REP. MARY GAY SCANLON, D-PA.

REP. GREG STANTON, D-ARIZ.

REP. CORI BUSH, D-MO.

REP. MONDAIRE JONES, D-N.Y.

REP. DEBORAH ROSS, D-N.C.

REP. JIM JORDAN, R-OHIO, RANKING MEMBER

REP. LOUIE GOHMERT, R-TEXAS

REP. STEVE CHABOT, R-OHIO

REP. DARRELL ISSA, R-CALIF.

REP. KEN BUCK, R-COLO.

REP. MIKE JOHNSON, R-LA.

REP. ANDY BIGGS, R-ARIZ.

REP. MATT GAETZ, R-FLA.

REP. TOM MCCLINTOCK, R-CALIF.

REP. GREGORY STEUBE, R-FLA.

REP. TOM TIFFANY, R-WIS.

REP. THOMAS MASSIE, R-KY.

REP. CHIP ROY, R-TEXAS

REP. VICTORIA SPARTZ, R-IND.

REP. DAN BISHOP, R-N.C.

REP. MICHELLE FISCHBACH, R-MINN.

REP. SCOTT FITZGERALD, R-WIS.

REP. CLIFF BENTZ, R-ORE.

REP. BURGESS OWENS, R-UTAH

Mar 29, 2022 15:02 ET .EOF

Provider ID: 20fk0s02

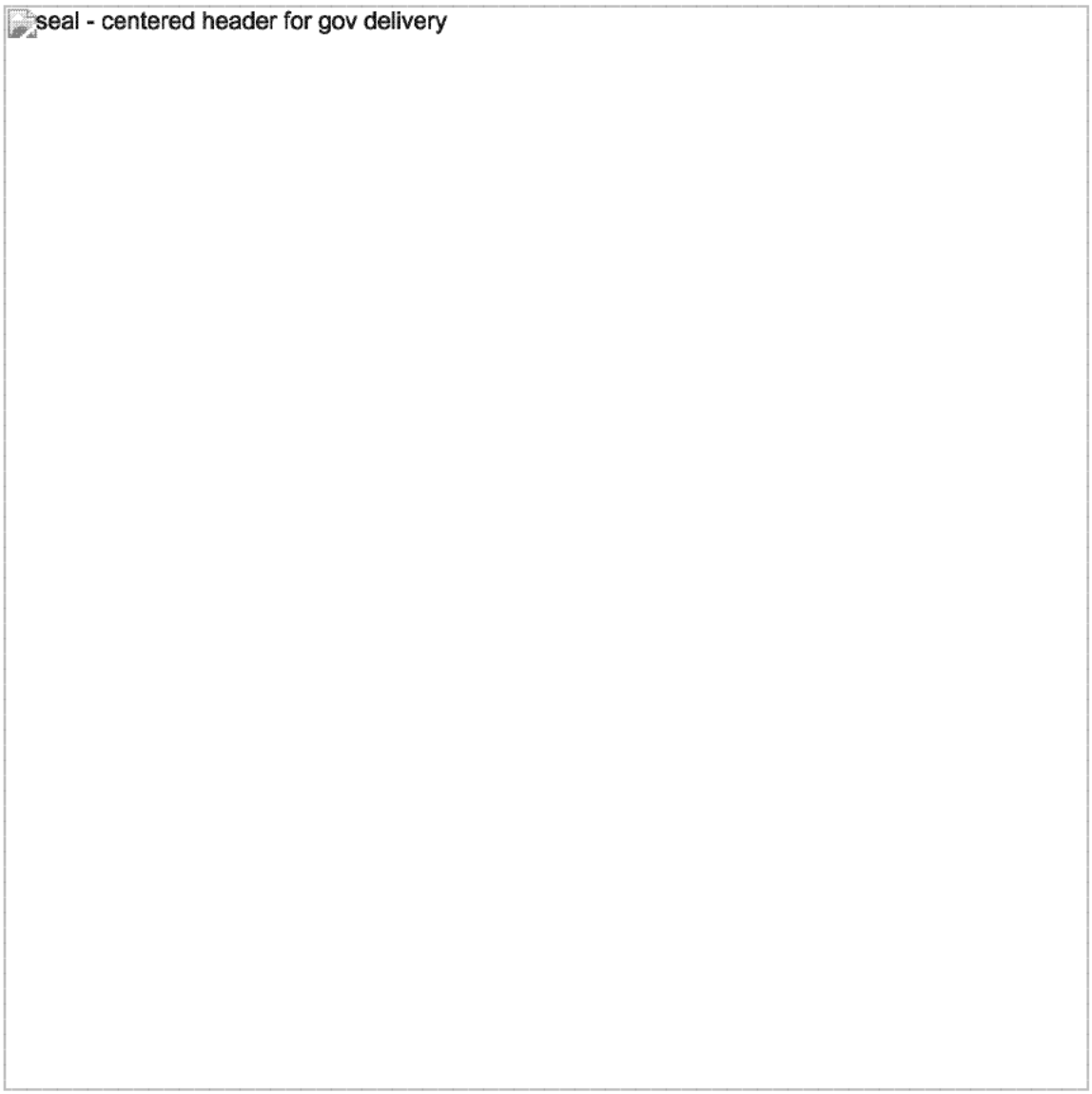
-0- Mar/29/2022 19:02 GMT

[No Subject]

From: "polite, kenneth (crm)"
Date: Mon, 20 Dec 2021 20:09:54 +0000
Attachments: Fwd_ FOR REVIEW_ Draft Documents Re_ School Board Threats.msg (80.38 kB); Re_ proposed response to draft response to school board threats.msg (71.68 kB); proposed response to draft response to school board threats.msg (71.17 kB); Fwd_ FOR REVIEW_ Draft Documents Re_ School Board Threats.msg (306.69 kB)

[EXTERNAL] Justice Department Addresses Violent Threats Against School Officials and Teachers

From: USDOJ-Office of Public Affairs <usdoj-officeofpublicaffairs@public.govdelivery.com>
To: "McQuaid, Nicholas (CRM)" (b) (6) [redacted]
Date: Mon, 04 Oct 2021 22:08:10 +0000



The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

October 4, 2021

Note: Read the Attorney General's memorandum here.

Justice Department Addresses Violent Threats Against School Officials and Teachers

WASHINGTON – Citing an increase in harassment, intimidation and threats of violence against school board members, teachers and workers in our nation's public schools, today Attorney General Merrick B. Garland directed the FBI and U.S. Attorneys' Offices to meet in the next 30 days with federal, state, tribal, territorial and local law enforcement leaders to discuss strategies for addressing this disturbing trend. These sessions will open dedicated lines of communication for threat reporting, assessment and response by law enforcement.

"Threats against public servants are not only illegal, they run counter to our nation's core values," wrote Attorney General Garland. "Those who dedicate their time and energy to ensuring that our children receive a proper education in a safe environment deserve to be able to do their work without fear for their safety."

According to the Attorney General's memorandum, the Justice Department will launch a series of additional efforts in the coming days designed to address the rise in criminal conduct directed toward school personnel. Those efforts are expected to include the creation of a task force, consisting of representatives from the department's Criminal Division, National Security Division, Civil Rights Division, the Executive Office for U.S. Attorneys, the FBI, the Community Relations Service and the Office of Justice Programs, to determine how federal enforcement tools can be used to prosecute these crimes, and ways to assist state, Tribal, territorial and local law enforcement where threats of violence may not constitute federal crimes.

The Justice Department will also create specialized training and guidance for local school boards and school administrators. This training will help school board members and other potential victims understand the type of behavior that constitutes threats, how to report threatening conduct to the appropriate law enforcement agencies, and how to capture and preserve evidence of threatening conduct to aid in the investigation and prosecution of these crimes.

Threats of violence against school board members, officials, and workers in our nation's public schools can be reported by the public to the FBI's National Threat Operations Center (NTOC) via its national tip line (1-800-CALL-FBI) and online through the FBI website (http://fbi.gov/tips). To ensure that threats are communicated to the appropriate authorities, NTOC will direct credible threats to FBI field offices, for coordination with the U.S. Attorney's Office and law enforcement partners as appropriate. Reporting threats of violence through NTOC will help the federal government identify increased threats in specific jurisdictions as well as coordinated widespread efforts to intimidate educators and education workers.

###

OAG

21-960

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.

Follow us: T F Y In

RE: pre-meet (threats)

From: "Matthews-Johnson, Tamarra D. (OAG)" (b) (6)
To: "McQuaid, Nicholas (CRM)" (b) (6); "Driscoll, Kevin (CRM)" (b) (6)
Cc: "Chambers, Kevin (ODAG)" (b) (6); "Folk, Anders (ODAG)" (b) (6); "Keller, John (CRM)" (b) (6)
Date: Thu, 13 Jan 2022 19:59:11 +0000
Attachments: AG Threats Briefing 1 13 2022 (DRAFT) .docx (22.91 kB)

Outline attached – thanks! T

From: McQuaid, Nicholas (CRM) (b) (6)
Sent: Thursday, January 13, 2022 9:41 AM
To: Driscoll, Kevin (CRM) (b) (6)
Cc: Chambers, Kevin (ODAG) (b) (6); Folk, Anders (ODAG) (b) (6); Matthews-Johnson, Tamarra D. (OAG) (b) (6); Keller, John (CRM) (b) (6)
Subject: Re: pre-meet (threats)

I cant do 11. I could do 1:30 or you all could proceed without me at 11.

On Jan 13, 2022, at 9:27 AM, Driscoll, Kevin (CRM) (b) (6) wrote:

Could do 11.

On Jan 13, 2022, at 9:15 AM, Chambers, Kevin (ODAG) (b) (6) wrote:

Hey all. TMJ has an unexpected conflict. Are you all available at 10, 11, or between 1:30 and 3p?

-----Original Appointment-----
From: Chambers, Kevin (ODAG)
Sent: Wednesday, January 12, 2022 5:45 PM
To: Chambers, Kevin (ODAG); McQuaid, Nicholas (CRM); Folk, Anders (ODAG); Matthews-Johnson, Tamarra D. (OAG)
Cc: Driscoll, Kevin (CRM); Keller, John (CRM)
Subject: pre-meet (threats)
When: Thursday, January 13, 2022 10:30 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: Microsoft Teams Meeting

Join Microsoft Teams Meeting

(b) (6) (Toll)

Conference ID: (b) (6)

Local numbers | Reset PIN | Learn more about Teams

MEMORANDUM FOR THE ATTORNEY GENERAL

FROM: TAMARRA MATTHEWS JOHNSON

SUBJECT: Briefing on Department Efforts to Address Threats of Violence

DATE: January 13, 2022

PROPOSED TIMELINE: This briefing is scheduled for 1.5 hours on Friday, January 14, 2022

DISCUSSION:

On Friday, you will receive a briefing on Department efforts to address violence and threats of violence in our civic and public spaces against election officials and workers, flight crews and airport staff, school personnel, members of Congress, and federal agents, prosecutors, and judges. The briefing will be conducted virtually. Attendees will participate in their portion of the briefing and then depart.

Outline for the Briefing:

Scoped Out Per Agreement

IV. Threats Against School Personnel and School Board Members
(estimated time: 2:20 - 2:30 pm)
Presenters: Kevin Chambers (ADAG – ODAG)
Monty Wilkinson (Director, EOUSA)
Norm Wong (EOUSA) (possibly)

The presenters will provide an update on the work stemming from your October 2021 memorandum directing USAOs and the FBI to partner and communicate with state and local law enforcement agencies concerning threats of violence against school board members, administrators, teachers, and personnel. The presentation will include updates on the current threat picture and the status of matters that have entered the investigation and prosecution phase, as appropriate.

FW: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

From: "Driscoll, Kevin (CRM)" (b) (6)
To: "Amundson, Corey (CRM)" (b) (6); "Keller, John (CRM)" (b) (6)
Date: Mon, 04 Oct 2021 21:08:57 +0000
Attachments: Final.AG MEMO TO USAOs AND SACs (10.4.21).docx (22.07 kB); DRAFT PRESS RELEASE - Threats Against School Workers (version to components).docx (17.68 kB)

Kevin Driscoll
Deputy Assistant Attorney General
Criminal Division, United States Department of Justice
Desk: (b) (6)
Mobile: (b) (6)

From: Chambers, Kevin (ODAG) (b) (6)
Sent: Monday, October 4, 2021 3:00 PM
To: Jensen, Steven J. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; McQuaid, Nicholas (CRM) (b) (6); Moossy, Robert (CRT) (b) (6); Wilkinson, Monty (USAEO) (b)(6), (b)(7)(C) per EOUSA; Toscas, George (NSD) (b) (6); Darke Schmitt, Katherine (OJP/OVC) (b) (6); Tarasca, James A. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Blue, Matt (NSD) (b) (6); Langan, Timothy R. Jr. (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; (b)(6), (b)(7)(C) per FBI (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Vorndran, Kevin (CTD) (FBI) (b)(6); (b)(7)(E) per FBI; Lesko, Mark (NSD) (b) (6); Wiegmann, Brad (NSD) (b) (6); Driscoll, Kevin (CRM) (b) (6); Rossi, Rachel (OASG) (b) (6); Monroe, Becky (OASG) (b) (6); Wong, Norman (USAEO) (b)(6), (b)(7)(C) per EOUSA
Cc: Braden, Myesha (ODAG) (b) (6); Newman, David A. (ODAG) (b) (6); Lan, Iris (ODAG) (b) (6)
Subject: FOR IMMEDIATE REVIEW: Draft AG Memo Re: School Board Threats and Draft Press Release

Re: FOR REVIEW: Draft Documents Re: School Board Threats

From: Jay Greenberg (b)(6); (b)(7)(E) per FBI
To: "Driscoll, Kevin (CRM)" (b) (6)
Date: Sat, 02 Oct 2021 22:48:22 +0000

Copy. Tracking. If there is a possibility, we would request a delay in messaging until we can all discuss early this week. Not sure if we have that capability at this point?

From: Driscoll, Kevin (CRM) (b) (6)
Sent: Saturday, October 2, 2021 4:45:19 PM
To: Greenberg, Jay (CID) (FBI) (b)(6); (b)(7)(E) per FBI
Subject: [EXTERNAL EMAIL] - Fwd: FOR REVIEW: Draft Documents Re: School Board Threats

Want to make sure you're tracking.

Kevin Driscoll
Deputy Assistant Attorney General
Criminal Division, Department of Justice
Desk: (b) (6)
Mobile: (b) (6)

Begin forwarded message:

From: "Chambers, Kevin (ODAG)" (b) (6)
Date: October 2, 2021 at 4:02:33 PM EDT
To: "Jensen, Steven J. (CTD) (FBI)" (b)(6); (b)(7)(E) per FBI, "McQuaid, Nicholas (CRM)" (b) (6)
"Moossy, Robert (CRT)" (b) (6), "Wilkinson, Monty (USAEO)" (b)(6), (b)(7)(C) per EOUSA, "Toscas, George (NSD)" (b) (6), "Darke Schmitt, Katherine (OJP/OVC)"
(b) (6), "Tarasca, James A. (CTD) (FBI)" (b)(6); (b)(7)(E) per FBI, "Blue, Matt (NSD)"
(b) (6), "Langan, Timothy R. Jr. (CTD) (FBI)" (b)(6); (b)(7)(E) per FBI, (b)(6), (b)(7)(C) per FBI (CTD) (FBI)"
(b)(6); (b)(7)(E) per FBI, (b)(6), (b)(7)(C) per FBI (CTD) (FBI)" (b)(6); (b)(7)(E) per FBI, "Vorndran, Kevin (CTD) (FBI)"
(b)(6); (b)(7)(E) per FBI, "Lesko, Mark (NSD)" (b) (6), "Wiegmann, Brad (NSD)"
(b) (6), "Driscoll, Kevin (CRM)" (b) (6), "Rossi, Rachel (OASG)"
(b) (6), "Monroe, Becky (OASG)" (b) (6), "Wong, Norman (USAEO)"
(b)(6), (b)(7)(C) per EOUSA
Cc: "Carlin, John P. (ODAG)" (b) (6), "Braden, Myesha (ODAG)" (b) (6),
"Newman, David A. (ODAG)" (b) (6), "Lan, Iris (ODAG)" (b) (6)
Subject: FOR REVIEW: Draft Documents Re: School Board Threats