From: Collins, Jimmie L

To: BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; [redacted]; Shawn Acosta ([redacted]); [redacted]; Ray Andrade ([redacted]); [redacted]; Adam Arluke ([redacted]); [redacted]; Baggs, Kevin L; Dax Bajema ([redacted]); Christopher Ballog ([redacted]); [redacted]; [redacted]; Cory S. Brailsford ([redacted]); Craig Burns ([redacted]); Christopher Butch ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro ([redacted]); [redacted]; Robert Caulfield ([redacted]); [redacted]; Cullen Chong ([redacted]); Christopher Church ([redacted]); Randy Clark ([redacted]); [redacted]; Coronel, Romel M; [redacted]; [redacted]; Fred Edwards ([redacted]); [redacted]; [redacted]; [redacted]; Daniel Ford ([redacted]); Jon Franquez ([redacted]); Charles (Chaz) Frye ([redacted]); Robin (Chris) Grant ([redacted]); Jonathon Grems ([redacted]); [redacted]; Isra Harahap ([redacted]); Scott Higbee ([redacted]); [redacted]; [redacted]; Nic Iannarone ([redacted]); [redacted]; [redacted]; Kenn Ishida ([redacted]); Sarah Jacob ([redacted]); [redacted]; Weldon James ([redacted]); Diego Jarrin ([redacted]); [redacted]; [redacted]; Brian Keith ([redacted]); Scott Klein ([redacted]); [redacted]; Brandon Kumalae ([redacted]); [redacted]; [redacted]; Kerry Looby ([redacted]); Kendall Lopez ([redacted]); Marciel, Bryan D; Lisa McGahan ([redacted]); Humberto Antonio (Mac) Mclaren Jr ([redacted]); Eric Mitsuyoshi ([redacted]); Erik Modisett ([redacted]); Nahale, Sean S; [redacted]; Trevor Ohnstad ([redacted]); [redacted]; [redacted]; Pace, Frank J; Brent Parks ([redacted]); Giovan Patalano ([redacted]); Craig Petersen ([redacted]); [redacted]; [redacted]; Shane Reagan ([redacted]); Jordan Reigel ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles ([redacted]); [redacted]; [redacted]; Eric Shimodoi ([redacted]); [redacted]; Joh Strandhagen ([redacted]); Bennett Strobel ([redacted]); [redacted]; Gen Tamura ([redacted]); Dustin Truax ([redacted]); John Udani ([redacted]); [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government ([redacted]); John Woodruff - US Federal Government ([redacted]); [redacted]; [redacted]; Jeremy Young ([redacted]); Lee Zawacki ([redacted])

Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; Wilson, John D IV CTR USARMY USARPAC (USA); Jarin, Michael S PO1 USN NAVIOCOM OAHU HI (USA); Spencer, Daniel Wesli JR CIV USARMY USAG (USA); Forthofer, Molly; EASTON, KRISHNA; Clifford Ramson ([redacted])

Subject: RE: C-UAS Working Group

Date: Tuesday, April 22, 2025 9:32:00 AM

Attachments: EXTERNAL Feature Article Detecting and Mitigating Drones on the Border.msg
image001.png

Aloha All

Sharing a recent article regarding detecting and mitigating drones. See attached.

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816

[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

-----Original Appointment-----
From: Collins, Jimmie L
Sent: Friday, October 4, 2024 2:38 PM
To: Collins, Jimmie L; BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; [redacted]; Shawn Acosta ([redacted]); [redacted]; Ray Andrade ([redacted]); [redacted]; Adam Arluke ([redacted]); [redacted]; Baggs, Kevin L; Dax Bajema ([redacted]); Christopher Ballog ([redacted]); [redacted]; [redacted]; Cory S. Brailsford ([redacted]); Craig Burns ([redacted]); Christopher Butch ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro ([redacted]); [redacted]; Robert Caulfield ([redacted]); [redacted]; Cullen Chong ([redacted]); Christopher Church ([redacted]); Randy Clark ([redacted]); Jimmie Collins ([redacted]); [redacted]; Coronel, Romel M; [redacted]; [redacted]; Fred Edwards ([redacted]); [redacted]; [redacted]; [redacted]; Daniel Ford ([redacted]); Jon Franquez ([redacted]); Charles (Chaz) Frye ([redacted]); Robin (Chris) Grant ([redacted]); Jonathon Grems ([redacted]); [redacted]; Isra Harahap ([redacted]); Scott Higbee ([redacted]); [redacted]; [redacted]; Nic Iannarone ([redacted]); [redacted]; [redacted]; Kenn Ishida ([redacted]); Sarah Jacob ([redacted]); [redacted]; Weldon James ([redacted]); Diego Jarrin ([redacted]); [redacted]; [redacted]; Brian Keith ([redacted]); Scott Klein ([redacted]); Brandon Kumalae ([redacted]); [redacted]; [redacted]; Kerry Looby ([redacted]); Kendall Lopez ([redacted]); Marciel, Bryan D; Lisa McGahan ([redacted]); Humberto Antonio (Mac) Mclaren Jr ([redacted]); Eric Mitsuyoshi ([redacted]); Erik Modisett ([redacted]); Nahale, Sean S; [redacted]; Trevor Ohnstad

([redacted]); [redacted];
[redacted]; Frank Pace ([redacted]); Brent Parks
([redacted]); Giovan Patalano ([redacted]); Craig
Petersen ([redacted]); [redacted];
[redacted]; Shane Reagan ([redacted]); Jordan Reigel
([redacted]); [redacted]; [redacted];
[redacted]; [redacted]; [redacted]; Jason
Scoles ([redacted]); [redacted]; [redacted]; Eric
Shimodoi ([redacted]); [redacted]; Joh Strandhagen
([redacted]); Bennett Strobel ([redacted]);
[redacted]; Gen Tamura ([redacted]); Dustin Truax
([redacted]); John Udani ([redacted]); [redacted];
[redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US
Federal Government ([redacted]); John Woodruff - US Federal Government
([redacted]); [redacted]; [redacted]; Jeremy Young
([redacted]); Lee Zawacki
Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; Wilson, John D IV CTR USARMY USARPAC (USA); Jarin, Michael S PO1 USN NAVIOCOM OAHU HI (USA); Spencer, Daniel Wesli JR CIV USARMY USAG (USA); Forthofer, Molly; EASTON, KRISHNA; Clifford Ramson ([redacted])
Subject: C-UAS Working Group
When: Thursday, April 17, 2025 9:00 AM-11:00 AM (UTC-10:00) Hawaii.
Where: Rm [redacted]; / Teams; LAW – OHS Conference Rm

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room (in the location block above) – if you intend to join us **in person** please let me know directly so I can monitor our capacity.

Notional Agenda (pending speaker confirmations):

- Guest speaker(s):
  - [tentative] DHS/CISA HQ
  - [tentative] John Abbey – SafeFlight update
  - [tentative] FBI
- Incident reporting: Reference attached.
- Events/Training:
- Policy: Prior to our meeting I will reach out to working group members to solicit interested parties for further development of the below lines of effort from previous meeting and will save space here for dialogue on agreeable path forward to pursue
  - Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
  - Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?

- Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?
- News:
- Other/Open Discussion:
- Conclusion:

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

Microsoft Teams Need help?

Join the meeting now

Meeting ID: [redacted]
Passcode: [redacted]

Dial in by phone

+1 808-829-4853, [redacted] United States, Honolulu
Find a local number
Phone conference ID: [redacted]

For organizers: Meeting options | Reset dial-in PIN

From: U.S. Department of Homeland Security
To: Collins, Jimmie L
Subject: [EXTERNAL] Feature Article: Detecting and Mitigating Drones on the Border
Date: Tuesday, April 22, 2025 6:41:53 AM

S&T Header with logo

Feature Article: Detecting and Mitigating Drones on the Border

The ability to locate and deal with drones operating in unauthorized areas is vital to maintaining secure borders and protecting assets. The Science and Technology Directorate (S&T) and Canadian partners are testing and deploying the latest technology to address these challenges.

In early autumn near Buffalo, New York, the weather was comfortable and warm, with a touch of color in the trees marking the change of seasons. As locals went about their business and tourists enjoyed the changing leaves, several nondescript vehicles traveled alongside them on the scenic byways along the Niagara River. Inside these trucks and vans were S&T technicians watching screens, tracking the movements of small Unmanned Aerial Systems (sUAS) flying across the U.S.-Canada border.

S&T carried out the exercise in coordination with U.S. Border Patrol (USBP) Buffalo Sector and Canadian government counterparts. The goal was to practice locating and intercepting UAS flying near or crossing the Niagara River, which marks the international border. UAS are often used to move drugs and other contraband back and forth across the border. As technology advances, some have become large and powerful enough to potentially transport a person.

“We're only able to see our side of the border, and because the UAS move so fast, we don't have enough time to do an intercept,” said Tony Hammerquist, Deputy Program Manager in S&T’s C-UAS Program. “If we're able to see from the Canadian side, then we're able to prepare an intercept, if required, and the same thing goes for the Canadians on their side.”

One of the target drones being tracked across the international border. Photo credit: S&T.

READ THE FULL STORY →

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; [redacted]; Ray Andrade [redacted]; [redacted]; Adam Arluke [redacted]; [redacted]; Baggs, Kevin L; Dax Bajema [redacted]; Christopher Ballog [redacted]; [redacted]; [redacted]; Cory S. Brailsford [redacted]; Brandon, John; Craig Burns [redacted]; Christopher Butch [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro [redacted]; [redacted]; Robert Caulfield [redacted]; [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Collins, Jimmie L; [redacted]; Coronel, Romel M; [redacted]; [redacted]; EASTON, KRISHNA; Fred Edwards [redacted]; [redacted]; [redacted]; [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Joseph Doyle [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; [redacted]; [redacted]; [redacted]; Nic Iannarone [redacted]; [redacted]; [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; [redacted]; Weldon James [redacted]; [redacted]; Diego Jarrin [redacted]; [redacted]; [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; [redacted]; [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; Trevor Ohnstad [redacted]; [redacted]; Pace, Frank J; [redacted]; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; [redacted]; [redacted]; Clifford Ramson [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles [redacted]; [redacted]; Eric Shimodoi [redacted]; [redacted]; Jason Scoles [redacted]; Joh Strandhagen [redacted]; Bennett Strobel [redacted]; [redacted]; Gen Tamura - US Federal Government [redacted]; Dustin Truax [redacted]; John Udani [redacted]; [redacted]; Judy Van Nguyen [redacted]; Wade, Kathleen N; [redacted]; [redacted]; [redacted]; Woodruff, John; [redacted]; [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]

Subject: C-UAS Working Group - 17 April Meeting Minutes

Date: Thursday, April 17, 2025 3:03:48 PM

Attachments: Minutes.docx
image001.png

Aloha All

Mahalo for your participation, for those that were able to join us today. Attached please find minutes from our discussions. Please provide your feedback if there were any errors or omissions.

Have a wonderful Easter weekend!

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer

CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

-----Original Appointment-----
From: Collins, Jimmie L
Sent: Friday, October 4, 2024 2:38 PM
To: Collins, Jimmie L; BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; [redacted]; Shawn Acosta ([redacted]); [redacted]; Ray Andrade ([redacted]); [redacted]; Adam Arluke ([redacted]); [redacted]; Baggs, Kevin L; Dax Bajema ([redacted]); Christopher Ballog ([redacted]); [redacted]; [redacted]; Cory S. Brailsford ([redacted]); Craig Burns ([redacted]); Christopher Butch ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro ([redacted]); [redacted]; Robert Caulfield ([redacted]); [redacted]; Cullen Chong ([redacted]); Christopher Church ([redacted]); Randy Clark ([redacted]); Jimmie Collins ([redacted]); [redacted]; Coronel, Romel M; [redacted]; [redacted]; Fred Edwards ([redacted]); [redacted]; [redacted]; [redacted]; Daniel Ford ([redacted]); Jon Franquez ([redacted]); Charles (Chaz) Frye ([redacted]); Robin (Chris) Grant ([redacted]); Jonathon Grems ([redacted]); [redacted]; Isra Harahap ([redacted]); Scott Higbee ([redacted]); [redacted]; [redacted]; Nic Iannarone ([redacted]); [redacted]; [redacted]; Kenn Ishida ([redacted]); Sarah Jacob ([redacted]); [redacted]; Weldon James ([redacted]); Diego Jarrin ([redacted]); [redacted]; [redacted]; Brian Keith ([redacted]); Scott Klein ([redacted]); Brandon Kumalae ([redacted]); [redacted]; [redacted]; Kerry Looby ([redacted]); Kendall Lopez ([redacted]); Marciel, Bryan D; Lisa

McGahan ( ); Humberto Antonio (Mac) Mclaren Jr ( ); Eric Mitsuyoshi ( ); Erik Modisett ( ); Nahale, Sean S; ; Trevor Ohnstad ( ); ; ; Frank Pace ( ); Brent Parks ( ); Giovan Patalano ( ); Craig Petersen ( ); ; ; Shane Reagan ( ); Jordan Reigel ( ); ; ; ; ; ; Jason Scoles ( ); ; ; Eric Shimodoi ( ); ; Joh Strandhagen ( ); Bennett Strobel ( ); ; Gen Tamura ( ); Dustin Truax ( ); John Udani ( ); ; ; Wade, Kathleen N; ; Giovanni Williams - US Federal Government ( ); John Woodruff - US Federal Government ( ); ; ; Jeremy Young ( ); Lee Zawacki

Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; Wilson, John D IV CTR USARMY USARPAC (USA); Jarin, Michael S PO1 USN NAVIOCOM OAHU HI (USA); Spencer, Daniel Wesli JR CIV USARMY USAG (USA); Forthofer, Molly; EASTON, KRISHNA; Clifford Ramson ( )

Subject: C-UAS Working Group

When: Thursday, April 17, 2025 9:00 AM-11:00 AM (UTC-10:00) Hawaii.

Where: Rm ; / Teams; LAW – OHS Conference Rm

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room (in the location block above) – if you intend to join us **in person** please let me know directly so I can monitor our capacity.

Notional Agenda (pending speaker confirmations):

- Guest speaker(s):
  - [tentative] DHS/CISA HQ
  - [tentative] John Abbey – SafeFlight update
  - [tentative] FBI
- Incident reporting: Reference attached.
- Events/Training:
- Policy: Prior to our meeting I will reach out to working group members to solicit interested parties for further development of the below lines of effort from previous meeting and will save space here for dialogue on agreeable path forward to pursue
  - Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
  - Reporting/investigations: what actions/activities will increase air domain awareness, what

mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
    - Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?
- News:
- Other/Open Discussion:
- Conclusion:

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

Microsoft Teams Need help?

Join the meeting now

Meeting ID: [redacted]
Passcode: [redacted]

Dial in by phone

+1 808-829-4853,, [redacted] United States, Honolulu
Find a local number

Phone conference ID: [redacted]

For organizers: Meeting options | Reset dial-in PIN

---

17 Apr 25/09-1100 (3rd Thursday, quarterly)

Location:

[redacted]

and

Microsoft Teams,

Meeting ID: [redacted],

Passcode: [redacted]

+1 808-829-4853,, [redacted]

Minutes:

1. Guest speaker(s):

2. John Abbey; SafeFlight update: Although not required under the current contract, the end product will be a ConOps document (estimated 1 Jun 25) to support the statewide project that outlines:
   - A problem statement outlining the risk trends and Hawai'i-specific vulnerabilities;
   - The "protected entities," including all civilian passenger airports and all military/USCG air facilities in the first phase of implementation, with detailed detection technologies and response protocols in place and anticipated future. (starting with O'ahu and outer islands thereafter).
   - Based on the scope of response, determined by the number of responding agencies and number of licensed responders, the apportioned percentage of resources will be proposed for future contractual support costs;
   - The "responder entities," including civilian law enforcement agencies, civilian military law enforcement (first phase HPD and HI Sheriff), security forces, and garrison military police, and their staffing numbers and deployment factors;
   - The "recipient entities," including FAA (Flight Standards District Office, Law Enforcement Assistance Program, and real time notifications), TSA, FBI, Secret Service, and other federal agencies, HI DLE (Office of Homeland Security, Hawai'i State Fusion Center, and other appropriate recipients), HPD Real Time Crime Center and the Hawai'i Garrison and other military POC's;
   - Existing policies and Standard Operating Procedures for all stakeholders;
   - The outline of jurisdictional and joint response agreements or proposed MOU's where multiple agencies have responsibility (e.g. military base intrusion- controlled from civilian jurisdiction, civilan on-base violations, and other reported use cases); and
   - Solution outline, including proposed unified protocols and software support

3. Incident reporting:

   - FBI's SSA Bryan Oakley ([redacted]) shared the FBI's Law Enforcement Drone Incident Guide. It contains a trove of pertinent information from a UAS Incident Report outline, and examples of Certificates/Licenses, to suspicious drone indicators, and more. It is Law Enforcement Sensitive, so I will defer to Bryan to provide to those who did not receive the chat attachment provided at the meeting.

4. Events/Training: The Drone Assessment and Response Tactics (DART) Training was mentioned. Lee Zawacki ([redacted]) mentioned that he was coordinating with [redacted] for

their DART training in [redacted] at the end of July and again in [redacted] the beginning of August. Please contact him if you know anyone interested in attending.

5. Project Subgroups: In an email (14 April 25), as well as at this working group meeting, OHS solicited interested Working Group members to participate in one or more of the following subgroups for further development of each of these lines of effort. Contact me with your feedback should you want to participate – below is the short list of participants identified thus far. In anticipation of the ConOps development as part of the SafeFlight project, OHS will be launching planning activities in these focus areas in order to carry forward and compliment the technological approach championed through SafeFlight's efforts.
    a. Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
    b. Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
    c. Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

Last	First	Title	Organization	Policy	Reporting / Investigations	Response Planning
Collins	Jimmie	Chief, Planning and Operations	Hawaii OHS	X	X	X
Ruic	Devin	Special Agent – Office of Special Projects	NCIS	X	X	X
Spencer	Daniel	Protection Chief	US Army Garrison	X	X	X

6. News: NSTR

7. Other/Open Discussion: SA Devin Ruic ([redacted]) of NCIS' Office of Special Projects introduced himself as one of our latest working group additions.

8. Conclusion

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; Ray Andrade [redacted]; Adam Arluke [redacted]; Baggs, Kevin L; Dax Bajema [redacted]; Christopher Ballog [redacted]; Cory S. Brailsford [redacted]; Brandon, John; Craig Burns [redacted]; Christopher Butch [redacted]; Daniel Carreiro [redacted]; Robert Caulfield [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Collins, Jimmie L; Coronel, Romel M; [redacted]; Fred Edwards [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Joseph Doyle [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; Nic Iannarone [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; Weldon James [redacted]; Diego Jarrin [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; Trevor Ohnstad [redacted]; Pace, Frank J; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; Clifford Ramson [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; Jason Scoles [redacted]; Eric Shimodoi [redacted]; Jason Scoles [redacted]; Joh Strandhagen [redacted]; Bennett Strobel [redacted]; Gen Tamura - US Federal Government [redacted]; Dustin Truax [redacted]; John Udani [redacted]; Judy Van Nguyen [redacted]; Wade, Kathleen N; [redacted]; John Woodruff - US Federal Government [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]

Subject: C-UAS Working Group - 17 April Meeting Minutes

Date: Thursday, April 17, 2025 3:03:00 PM

Attachments: Minutes.docx
image001.png

Aloha All

Mahalo for your participation, for those that were able to join us today. Attached please find minutes from our discussions. Please provide your feedback if there were any errors or omissions.

Have a wonderful Easter weekend!

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer

CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

-----Original Appointment-----
From: Collins, Jimmie L
Sent: Friday, October 4, 2024 2:38 PM
To: Collins, Jimmie L; BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; [redacted]; Shawn Acosta ([redacted]); [redacted]; Ray Andrade ([redacted]); [redacted]; Adam Arluke ([redacted]); [redacted]; Baggs, Kevin L; Dax Bajema ([redacted]); Christopher Ballog ([redacted]); [redacted]; [redacted]; Cory S. Brailsford ([redacted]); Craig Burns ([redacted]); Christopher Butch ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro ([redacted]); [redacted]; Robert Caulfield ([redacted]); [redacted]; Cullen Chong ([redacted]); Christopher Church ([redacted]); Randy Clark ([redacted]); Jimmie Collins ([redacted]); [redacted]; Coronel, Romel M; [redacted]; [redacted]; Fred Edwards ([redacted]); [redacted]; [redacted]; [redacted]; Daniel Ford ([redacted]); Jon Franquez ([redacted]); Charles (Chaz) Frye ([redacted]); Robin (Chris) Grant ([redacted]); Jonathon Grems ([redacted]); [redacted]; Isra Harahap ([redacted]); Scott Higbee ([redacted]); [redacted]; [redacted]; Nic Iannarone ([redacted]); [redacted]; [redacted]; Kenn Ishida ([redacted]); Sarah Jacob ([redacted]); [redacted]; Weldon James ([redacted]); Diego Jarrin ([redacted]); [redacted]; [redacted]; Brian Keith ([redacted]); Scott Klein ([redacted]); Brandon Kumalae ([redacted]); [redacted]; [redacted]; Kerry Looby ([redacted]); Kendall Lopez ([redacted]); Marciel, Bryan D; Lisa

McGahan ( ); Humberto Antonio (Mac) Mclaren Jr ( ); Eric Mitsuyoshi ( ); Erik Modisett ( ); Nahale, Sean S; ; Trevor Ohnstad ( ); ; ; Frank Pace ( ); Brent Parks ( ); Giovan Patalano ( ); Craig Petersen ( ); ; ; Shane Reagan ( ); Jordan Reigel ( ); ; ; ; ; ; Jason Scoles ( ); ; ; Eric Shimodoi ( ); ; Joh Strandhagen ( ); Bennett Strobel ( ); ; Gen Tamura ( ); Dustin Truax ( ); John Udani ( ); ; ; Wade, Kathleen N; ; Giovanni Williams - US Federal Government ( ); John Woodruff - US Federal Government ( ); ; ; Jeremy Young ( ); Lee Zawacki

Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; Wilson, John D IV CTR USARMY USARPAC (USA); Jarin, Michael S PO1 USN NAVIOCOM OAHU HI (USA); Spencer, Daniel Wesli JR CIV USARMY USAG (USA); Forthofer, Molly; EASTON, KRISHNA; Clifford Ramson ( )

Subject: C-UAS Working Group

When: Thursday, April 17, 2025 9:00 AM-11:00 AM (UTC-10:00) Hawaii.

Where: / Teams; LAW – OHS Conference Rm

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room (in the location block above) – if you intend to join us **in person** please let me know directly so I can monitor our capacity.

Notional Agenda (pending speaker confirmations):

- Guest speaker(s):
  - [tentative] DHS/CISA HQ
  - [tentative] John Abbey – SafeFlight update
  - [tentative] FBI
- Incident reporting: Reference attached.
- Events/Training:
- Policy: Prior to our meeting I will reach out to working group members to solicit interested parties for further development of the below lines of effort from previous meeting and will save space here for dialogue on agreeable path forward to pursue
  - Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
  - Reporting/investigations: what actions/activities will increase air domain awareness, what

mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
    - Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?
- News:
- Other/Open Discussion:
- Conclusion:

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

Microsoft Teams Need help?

Join the meeting now

Meeting ID: [redacted]
Passcode: [redacted]

Dial in by phone

+1 808-829-4853,, [redacted] United States, Honolulu
Find a local number

Phone conference ID: [redacted]

For organizers: Meeting options | Reset dial-in PIN

---

17 Apr 25/09-1100 (3rd Thursday, quarterly)

Location:

[redacted]

and

Microsoft Teams,

Meeting ID: [redacted],

Passcode: [redacted]

+1 808-829-4853,, [redacted]

Minutes:

1. Guest speaker(s):

2. John Abbey; SafeFlight update: Although not required under the current contract, the end product will be a ConOps document (estimated 1 Jun 25) to support the statewide project that outlines:
   - A problem statement outlining the risk trends and Hawai'i-specific vulnerabilities;
   - The "protected entities," including all civilian passenger airports and all military/USCG air facilities in the first phase of implementation, with detailed detection technologies and response protocols in place and anticipated future. (starting with O'ahu and outer islands thereafter).
   - Based on the scope of response, determined by the number of responding agencies and number of licensed responders, the apportioned percentage of resources will be proposed for future contractual support costs;
   - The "responder entities," including civilian law enforcement agencies, civilian military law enforcement (first phase HPD and HI Sheriff), security forces, and garrison military police, and their staffing numbers and deployment factors;
   - The "recipient entities," including FAA (Flight Standards District Office, Law Enforcement Assistance Program, and real time notifications), TSA, FBI, Secret Service, and other federal agencies, HI DLE (Office of Homeland Security, Hawai'i State Fusion Center, and other appropriate recipients), HPD Real Time Crime Center and the Hawai'i Garrison and other military POC's;
   - Existing policies and Standard Operating Procedures for all stakeholders;
   - The outline of jurisdictional and joint response agreements or proposed MOU's where multiple agencies have responsibility (e.g. military base intrusion- controlled from civilian jurisdiction, civilan on-base violations, and other reported use cases); and
   - Solution outline, including proposed unified protocols and software support

3. Incident reporting:

   - FBI's SSA Bryan Oakley ([redacted]) shared the FBI's Law Enforcement Drone Incident Guide. It contains a trove of pertinent information from a UAS Incident Report outline, and examples of Certificates/Licenses, to suspicious drone indicators, and more. It is Law Enforcement Sensitive, so I will defer to Bryan to provide to those who did not receive the chat attachment provided at the meeting.

4. Events/Training: The Drone Assessment and Response Tactics (DART) Training was mentioned. Lee Zawacki ([redacted]) mentioned that he was coordinating with New Mexico Tech for

their DART training in American Samoa at the end of July and again in Maui the beginning of August. Please contact him if you know anyone interested in attending.

5. Project Subgroups: In an email (14 April 25), as well as at this working group meeting, OHS solicited interested Working Group members to participate in one or more of the following subgroups for further development of each of these lines of effort. Contact me with your feedback should you want to participate – below is the short list of participants identified thus far. In anticipation of the ConOps development as part of the SafeFlight project, OHS will be launching planning activities in these focus areas in order to carry forward and compliment the technological approach championed through SafeFlight's efforts.
    a. Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
    b. Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
    c. Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

Last	First	Title	Organization	Policy	Reporting / Investigations	Response Planning
Collins	Jimmie	Chief, Planning and Operations	Hawaii OHS	X	X	X
Ruic	Devin	Special Agent – Office of Special Projects	NCIS	X	X	X
Spencer	Daniel	Protection Chief	US Army Garrison	X	X	X

6. News: NSTR

7. Other/Open Discussion: SA Devin Ruic ([redacted]) of NCIS' Office of Special Projects introduced himself as one of our latest working group additions.

8. Conclusion

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; [redacted]; Ray Andrade [redacted]; Adam Arluke [redacted]; Baggs, Kevin L; Keolani Bailey [redacted]; Dax Bajema [redacted]; Christopher Ballog [redacted]; [redacted]; Cory S. Brailsford [redacted]; Craig Burns [redacted]; Christopher Butch [redacted]; [redacted]; Daniel Carreiro [redacted]; Robert Caulfield [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Coronel, Romel M; [redacted]; Joseph Doyle [redacted]; Fred Edwards [redacted]; [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; [redacted]; Nic Iannarone [redacted]; [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; [redacted]; Weldon James [redacted]; Diego Jarrin [redacted]; [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; [redacted]; Trevor Ohnstad [redacted]; [redacted]; Pace, Frank J; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles [redacted]; [redacted]; Eric Shimodoi [redacted]; [redacted]; Joh Strandhagen [redacted]; Bennett Strobel [redacted]; [redacted]; Gen Tamura [redacted]; Dustin Truax [redacted]; John Udani [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government [redacted]; John Woodruff - US Federal Government [redacted]; [redacted]; [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]

Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; Wilson, John D IV CTR USARMY USARPAC (USA)

Subject: RE: C-UAS Working Group - request for feedback ahead of this Thursday"s meeting

Date: Monday, April 14, 2025 11:12:00 AM

Attachments: image001.png

Aloha All

As promised in the invitation for this week's working group meeting, I am looking to devote some time during that meeting to dive into a more detailed discussion of the topical areas we initiated dialogue on in our las meeting – see below for my notes on those:

1. Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
2. Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
3. Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

Initially, my intent is to flesh out these topics into developed action plans with objectives that our

collective can tackle in the coming months. As an example, an objective for the Response Planning focal area may be development of a protocol for communicating incursion incidents.

For those that cannot participate in this week's meeting – it would be helpful if those that would like to participate in these breakout group(s) notify me and include which group(s) are of interest and what your preference is for meeting timings/frequency for each of the topical areas of interest to you.

For those who will be attending – I can gather this information from you during it.

I envision using the quarterly working group meetings to share progress from each of these three breakout groups and polling the larger group for broad feedback on any draft recommendations they come up with.

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

-----Original Appointment-----
From: Collins, Jimmie L
Sent: Friday, October 4, 2024 2:38 PM
To: Collins, Jimmie L; [redacted]; Shawn Acosta ([redacted]); [redacted]; Ray Andrade ([redacted]); [redacted]; Adam Arluke ([redacted]); [redacted]; Baggs, Kevin L; Keolani Bailey ([redacted]); Dax Bajema ([redacted]); Christopher Ballog ([redacted]);

[redacted]; [redacted]; Cory S. Brailsford ([redacted]); Craig Burns ([redacted]); Christopher Butch ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro ([redacted]); [redacted]; Robert Caulfield ([redacted]); [redacted]; Cullen Chong ([redacted]); Christopher Church ([redacted]); Randy Clark ([redacted]); Jimmie Collins ([redacted]); [redacted]; Coronel, Romel M; [redacted]; [redacted]; Joseph Doyle ([redacted]); Fred Edwards ([redacted]); [redacted]; [redacted]; [redacted]; Daniel Ford ([redacted]); Jon Franquez ([redacted]); Charles (Chaz) Frye ([redacted]); Robin (Chris) Grant ([redacted]); Jonathon Grems ([redacted]); [redacted]; Isra Harahap ([redacted]); Scott Higbee ([redacted]); [redacted]; [redacted]; Nic Iannarone ([redacted]); [redacted]; [redacted]; Kenn Ishida ([redacted]); Sarah Jacob ([redacted]); [redacted]; Weldon James ([redacted]); Diego Jarrin ([redacted]); [redacted]; [redacted]; Brian Keith ([redacted]); Scott Klein ([redacted]); Brandon Kumalae ([redacted]); [redacted]; [redacted]; Kerry Looby ([redacted]); Kendall Lopez ([redacted]); Marciel, Bryan D; Lisa McGahan ([redacted]); Humberto Antonio (Mac) Mclaren Jr ([redacted]); Eric Mitsuyoshi ([redacted]); Erik Modisett ([redacted]); Nahale, Sean S; [redacted]; Trevor Ohnstad ([redacted]); [redacted]; [redacted]; Frank Pace ([redacted]); Brent Parks ([redacted]); Giovan Patalano ([redacted]); Craig Petersen ([redacted]); [redacted]; [redacted]; Shane Reagan ([redacted]); Jordan Reigel ([redacted]); [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles ([redacted]); [redacted]; [redacted]; Eric Shimodoi ([redacted]); [redacted]; Joh Strandhagen ([redacted]); Bennett Strobel ([redacted]); [redacted]; Gen Tamura ([redacted]); Dustin Truax ([redacted]); John Udani ([redacted]); [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government ([redacted]); John Woodruff - US Federal Government ([redacted]); [redacted]; [redacted]; Jeremy Young ([redacted]); Lee Zawacki

Cc: Felix, Ivan S CIV USN JBPHH PEARL HI (USA); John Abbey; McGregor, Shannon L CWO-3 USCG D14 (USA); Brandon, John; BARNER, NEILS C Col USAF PACAF PACAF/PADS/CC; Wilson, John D IV CTR USARMY USARPAC (USA)

Subject: C-UAS Working Group

When: Thursday, April 17, 2025 9:00 AM-11:00 AM (UTC-10:00) Hawaii.
Where: [redacted]

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room (in the location block above) – if you intend to join us **in person** please let me know directly so I can monitor our capacity.

Notional Agenda (pending speaker confirmations):

- Guest speaker(s):
  - [tentative] DHS/CISA HQ
  - [tentative] John Abbey – SafeFlight update
  - [tentative] FBI
- Incident reporting: Reference attached.
- Events/Training:
- Policy: Prior to our meeting I will reach out to working group members to solicit interested parties for further development of the below lines of effort from previous meeting and will save space here for dialogue on agreeable path forward to pursue
  - Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
  - Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
  - Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?
- News:
- Other/Open Discussion:
- Conclusion:

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

Microsoft Teams Need help?

Join the meeting now

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-4853, [redacted] United States, Honolulu

Find a local number

Phone conference ID: [redacted]

For organizers: Meeting options | Reset dial-in PIN

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; [redacted]; Ray Andrade [redacted]; [redacted]; Adam Arluke [redacted]; Baggs, Kevin L; Keolani Bailey [redacted]; Dax Bajema [redacted]; Christopher Ballog [redacted]; [redacted]; Cory Brailsford; Craig Burns [redacted]; Christopher Butch [redacted]; [redacted]; [redacted]; Daniel Carreiro [redacted]; [redacted]; Robert Caulfield [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Collins, Jimmie L; [redacted]; Coronel, Romel M; [redacted]; James Cruz [redacted]; Joseph Doyle [redacted]; Fred Edwards [redacted]; [redacted]; [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Joseph Doyle [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; [redacted]; Nic Iannarone [redacted]; [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; Weldon James [redacted]; Diego Jarrin [redacted]; [redacted]; [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; [redacted]; [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; [redacted]; Trevor Ohnstad [redacted]; [redacted]; [redacted]; Pace, Frank J; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; [redacted]; [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles [redacted]; [redacted]; [redacted]; Eric Shimodoi [redacted]; [redacted]; Jason Scoles [redacted]; Jon Strandhagen [redacted]; Bennett Strobel [redacted]; [redacted]; Gen Tamura [redacted]; Dustin Truax [redacted]; John Udani [redacted]; [redacted]; Judy Van Nguyen [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government [redacted]; Woodruff, John; [redacted]; [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]

Subject: C-UAS WG, 16 Jan 25 - Minutes and membership

Date: Friday, January 17, 2025 5:25:41 PM

Attachments: image001.png
2025 01 16 Minutes.docx
RSVP-Attendance List.xlsx
Interagency Legal Advisory on UAS Detection and Mitigation Technologies.pdf

---

Aloha All

My sincere appreciation to all of those that were able to join us for the great discussions and information sharing!

As one of our colleagues noted, “this workgroup enhances comms and coordination among federal, state, and local agencies regarding various deployed detection systems; response and investigations of breaches of security; and authority and jurisdiction (or lack thereof).”

We are only able to do that due to the dedication and energy of our membership and your willingness to dig into this challenging mission space.

Our intent at OHS is to facilitate this collaboration – and drive improvements where they are needed most. To that end, you will see a tight group of action items in the attached minutes that I will be championing in the year to come and look forward to engaging with those willing and able to participate in those undertakings.

I have a couple follow on communications for the group, so I will keep this one short.

My last topic here is our distribution list. There was great desire to have that roster shared and I have included what details I have at hand, but I need your assistance to improve the roster. I have updated the roster I had based on feedback from this meeting.

1. Please add any information that may be missing from your information (mostly that is titles and organizations) and return the spreadsheet back to me with your feedback.
2. Help me identify those individuals that joined but did not note their titles and organizations – I do not have their email addresses as they were not on my initial invitation roster.
3. Let me know if you prefer NOT to share your contact information so I can annotate that appropriately.

For those that could use a refresher or that are new to the topic, Parker Corts (FAA) reshared the attached Legal Advisory – a really good primer.

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

Counter-UAS Working Group
16 January 2025
RSVP-Attendance List (002)

Last	First	Email	Title	Organization	Response	On-Line/ In Person	Present
Abbey	John	[redacted]			Accepted	In Person	X
Acosta	Shawn	[redacted]			None	Virtual	X
Adams	Sara	[redacted]			None		
Andrade	Ray	[redacted]			Accepted	Virtual	X
Arias	Adrien	[redacted]			None		
Arluke	Adam	[redacted]			None		
Baggs	Kevin	[redacted]			Accepted	In Person	X
Bailey	Keolani (KO)	[redacted]		PADS/CC	None	Virtual	X
Bajema	Dax	[redacted]	MAJ	HING	None	Virtual	X
Ballog	Christopher	[redacted]			None		
Blanchard	Aaron	[redacted]			None	In Person	X
Blankinship	Lisa	[redacted]			None		
Brailsford	Cory	[redacted]			Accepted	In Person	X
Burns	Craig	[redacted]			Accepted		
Butch	Christopher	[redacted]			None		
Butler	Rhett	[redacted]			None		
Carpenter	Jason	[redacted]			None		
Carreiro	Daniel	[redacted]			None		
Carter	Scott	[redacted]			Declined		
Castillo			MAJ		None	Virtual	X
Caulfield	Robert	[redacted]			None		
Chong	Cullen	[redacted]			None		
Church	Christopher	[redacted]			None		
Clark	Randy	[redacted]			Accepted		
Collins	Jimmie	[redacted]	Chief, Planning and Operations	Hawaii OHS	Accepted	In Person	X
Comisky	Brian	[redacted]			None		
Coronel	Romel	[redacted]			None		
Corts	Parker	[redacted]	HQ Senior Representative to USINDOPACOM and PACAF, AJR-25 Special Operations	FAA	None	Virtual	X
Crotts	Ray	[redacted]		FAA	None		
Cruz	James	[redacted]			Accepted		
Doyle	Joseph	[redacted]			None		
Edwards	Fred	[redacted]			None		
Felix	Ivan	[redacted]			None		
Ferguson	Patrick	[redacted]			None		
Flynn	Sheldon	[redacted]		FAA	None		
Ford	Daniel	[redacted]			None		
Franquez	Jon	[redacted]			None	Virtual	X
Frye	Charles (Chaz)	[redacted]			None		
Fuerst	Dennis	[redacted]			None		
Grant	Robin (Chris)	[redacted]			Accepted		
Gregory	Diana		Col	298 ADG/CC	None	Virtual	X
Grems	Jonathon	[redacted]			None		
Haley	Talwyn	[redacted]		FAA	None		
Harahap	Isra	[redacted]			None		
Higbee	Scott	[redacted]			None		
Hook	Sean	[redacted]		FAA	None	Virtual	X
Iannarone	Nic	[redacted]			Tentative		
Ibanez	Sandra	[redacted]			None		
Ishida	Kenn	[redacted]			None		
Jacob	Sarah	[redacted]			None		
James	Weldon	[redacted]			None		
Jarrin	Diego	[redacted]	Senior Federal Air Marshal, CUAS Lead agent	LA Field Office	None	Virtual	X
Jones	Mars	[redacted]			Accepted		
Kaonohi	Lance	[redacted]			None		
Keith	Brian	[redacted]			None	Virtual	X
Klein	Scott	[redacted]			None		
Kumalae	Brandon	[redacted]			None		
Lee	Norreal	[redacted]			Accepted	In Person	X
Lindsey	Bradley	[redacted]	CPO	USCG	None	Virtual	X
Looby	Kerry	[redacted]			None		
Lopez	Kendall	[redacted]			None		

Counter-UAS Working Group
16 January 2025
RSVP-Attendance List (002)

Last	First	Email	Title	Organization	Response	On-Line/ In Person	Present
Marciel	Bryan	[redacted]			None		
McGahan	Lisa	[redacted]			Tentative		
Mclaren	Humberto (Mac)	[redacted]	Maritime Cybersecurity Specialist	USCG	Accepted	Virtual	X
Merrill					None	Virtual	X
Mindo	Rei				None	Virtual	X
Mitsuyoshi	Eric	[redacted]			Accepted	Virtual	X
Modisett	Erik	[redacted]	Supervisory Agent	DHS/CBP/CAMDEx: Center for Air and Marine Drone Exploitation	Accepted	Virtual	X
Nahale	Sean	[redacted]			None		
Oakley	Bryan	[redacted]			None		
Ohnstad	Trevor	[redacted]			None		
Okagawa	Jensen	[redacted]			None		
O'Keefe	Garrett	[redacted]			None		
Pace	Frank	[redacted]			Accepted	In Person	X
Parks	Brent	[redacted]			None		
Partin	James		Physical Security Program Manager	IMCOM Pacific	None	Virtual	X
Patalano	Giovan	[redacted]			None		
Petersen	Craig	[redacted]			Accepted	In Person	X
Piazza	Vincent	[redacted]			Accepted	In Person	X
Priestly	Christopher	[redacted]			None	Virtual	X
Ramirez			CW2	25th CEMA	None	Virtual	X
Reagan	Shane	[redacted]			None		
Reigel	Jordan	[redacted]			None	Virtual	X
Russell	Patrick	[redacted]			None		
Sagun	Arnold	[redacted]			None		
Sanders	Paul	[redacted]	Sr. Chemical Security Inspector	DHS/CISA	Accepted	Virtual	X
Scoles	Jason	[redacted]			None		
Shaha	Daniel	[redacted]			Accepted	In Person	X
Shaw	Keith	[redacted]			None		
Shimodoi	Eric	[redacted]			None		
Song	Douglas	[redacted]			None	In Person	X
Stanco	Marc	[redacted]			None		
Strandhagen	Joh	[redacted]	Protective Security Advisor	DHS/CISA	Accepted	Virtual	X
Strobel	Bennett	[redacted]			None		
Takahashi	Rodney	[redacted]			Accepted	In Person	X
Tamura	Gen	[redacted]	Protective Security Advisor	DHS/CISA	Accepted	Virtual	X
Truax	Dustin	[redacted]			None		
Udani	John	[redacted]			None		
Valoroso	Deric	[redacted]			None		
Van Nguyen	Judy	[redacted]	Intelligence Analyst	FBI	Accepted	Virtual	X
Villegas	Julio Alvarado	[redacted]		FBI	None		
Wade	Kathleen	[redacted]			Declined		
Waller	Joshua	[redacted]		FBI	None		
Williams	Giovanni	[redacted]			Accepted	In Person	X
Woodruff	John	[redacted]			None	Virtual	X
Wright	Alvin	[redacted]			None	In Person	X
Young	Andrea	[redacted]	FAMS AFSD-LE HNL	DHS/TSA	Accepted	Virtual	X
Young	Jeremy	[redacted]			Declined		
Zawacki	Lee	[redacted]			None	In Person	X

Counter-Unmanned Aerial Systems Working Group

16 Jan 25/09-1100 (HST)
Minutes

Location: [redacted]
and
Microsoft Teams
Meeting ID: [redacted]
Passcode: [redacted]
+1 808-829-4853,, [redacted]

1. Attendees (see RSVP-Attendance List attached to distribution email)
2. Guest Speakers:
    a. Rodney Takahashi, C-sUAS Program Manager, USINDOPACOM: DOD Announces Strategy for Countering Unmanned Systems
        i. Rodney discussed his initial thoughts regarding the recent designation of the Commanders of NORTHCOM and INDOPACOM as the lead synchronizers for operations to counter-UAS in the homeland. He talked about the three 'lines of effort' and generated a good bit of discussion amongst the grup regarding:
            1. Policy: What topics should be included in intergovernmental leadership dialogue, what leaders should be engaged, what policies are needed
            2. Reporting/investigations: air domain awareness, developing 'the' threat picture, information sharing. PADS representative (KO Bailey) indicated their tactical arrangement with Guard and Active forces that could increase air domain awareness and also briefly described a recent Oahu-based proof-of-concept event using the Ukrainian Sky Fortress. CBP/CAMDEx representative, Erik Modisett talked briefly about the friction between DoD (fence line) versus CBP (wide) detection authorities.
            3. Response Planning: who are key stakeholders in response, who can action, concept of operations
    b. John Abbey, SafeFlight: Hawai'i UAS Response, Enforcement, and Reporting; Air Force Phase I Contract
        i. The SafeFlight proposal for a 90-day Phase I scoping effort was funded and John is looking to launch that effort with Office of Homeland Security support in connecting with stakeholder organizations actioning data gathering activities necessary to approach Phase II funding. Those activities include:
            1. Identify the "protected sites" (airports, air bases, sports/ entertainment venues, and critical infrastructure), "responder agencies" (state and county law enforcement and military security forces), and "supporting agencies" (Fusion Center, 911 PSAP's, and BDOC's),
            2. Identify and develop output data specifications for all military and domestic C-UAS detention systems,
            3. Work individually and collectively with all stakeholder groups to identify and catalog all low altitude airspace ISR and mitigation and enforcement policies,

4. Work with management and user groups to draft Dual Use, universal protocols and adapt the software specifications developed with the Air Force Accelerator and cleared by the FAA for all US airports,
5. Reach consensus with all stakeholders for final protocols, joint operations/ mutual-aid agreements, detailed statewide software solution specifications and a detailed implementation plan.

ii. OHS (Jimmie Collins) will send a separate query to the working group membership to solicit appropriate organizational contacts to support John's data gathering.

3. Incident reporting: Nothing to add from meeting agenda in invitation.
4. Events: Nothing to add from meeting agenda in invitation.
5. Policy: Nothing to add from meeting agenda in invitation.
6. News:
    a. The group discussed the reported drone 'strike' that was in the news recently. Cory Brailsford, HPD, added to the discussion by doing an overview of several recent operational experiences, including drones flying over an active response (New Years Eve explosion response) and issues relating air operations incidental to and operationally supporting a major event. He mentioned his desire to pursue legislation for [redacted]. Cory also provided some details regarding his C-UAS approach within his organization:
        i. Education/awareness training for recruits
        ii. Documentation to expand available data to scope the response need and the capacity and capability building needs
        iii. Response-enabling processes that tackle issues like TFR-breaching, utility of TFR versus NOTAM
7. Other/Open Discussion:
    a. Training: Erik Modisett spoke briefly about specialized C-UAS training his organization conducts.
8. Conclusion:
    a. Jimmie closed the meeting with an overview of actionable items from the discussion that she will facilitate:
        i. Initiate outreach to working group members to solicit organizational representation to support data gathering for the SafeFlight: Hawai'i UAS Response, Enforcement, and Reporting project.
        ii. Initiate outreach to working group members to solicit interested parties for further development of these working group lines of effort (notes here are not intended to be all inclusive, just initial ideas):
            1. Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
            2. Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
            3. Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

b. Follow-ons: Because our members are overachieving, collaborative, communicating types, there were items dropped in the chat and provided to me afterwards to share onwards:
    i. Firmware Update Removes Geofencing From DJI Drones - AVweb
    ii. Basic Law Enforcement Response Drone Card
    iii. FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan
c. Next Working Group meeting: 17 Apr 25, 09-1100 (HST), same location. Invitation to follow.

Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems

August 2020

The Federal Aviation Administration (FAA), Department of Justice (DOJ), Federal Communications Commission (FCC), and Department of Homeland Security (DHS) are issuing an advisory guidance document to assist non-federal public and private entities interested in using technical tools, systems, and capabilities to detect and mitigate Unmanned Aircraft Systems (UAS). The advisory is intended to provide an overview of potentially applicable federal laws and regulations, as well as some factors relevant to whether those laws may apply to particular actions or systems.

Specifically, this advisory addresses two categories of federal laws that may apply to UAS detection and mitigation capabilities: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does *not* address state and local laws, which UAS detection and mitigation capabilities may also implicate. Neither does it cover potential civil liability flowing from the use of UAS detection and mitigation technologies (*e.g.*, the potential liability from causing physical damage to persons or property as a result of mitigating a UAS threat, or civil liability and recovery for an unlawful interception of wire, oral, or electronic communications under 18 U.S.C. § 2520).

This advisory is provided for informational purposes only. It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. As part of that analysis, entities should closely evaluate and consider whether the use of UAS detection and mitigation capabilities might impact the public's privacy, civil rights, and civil liberties. This is particularly important because potential legal prohibitions, as discussed below, are not based on broad classifications of systems (*e.g.*, active versus passive, detection versus mitigation), but instead are based on the functionality of each system and the specific ways in which a system operates and is used. A thorough understanding of both applicable law and the systems' functionality will ensure important technologies designed to protect public safety, by detecting and/or mitigating UAS threats, are used effectively, responsibly, and legally.

I. Federal Criminal Laws

Congress has exclusively authorized the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities to counter UAS presenting a credible threat to covered facilities or assets, notwithstanding certain otherwise potentially applicable federal criminal laws, including various laws relating to surveillance.[1] In addition, the FAA has been expressly authorized to engage in limited testing activities notwithstanding certain federal criminal surveillance laws.[2]

Because no other entities have been granted that authority, it is important that state, local, tribal and territorial (SLTT) and private sector entities without such statutory authority (including SLTT law enforcement organizations, SLTT governments, and owners and operators of critical infrastructure, stadiums, outdoor entertainment venues, airports, and other key sites) understand that federal laws may prevent, limit, or penalize the sale, possession, or use of UAS detection and mitigation capabilities.[3] Capabilities for detecting and mitigating UAS may implicate federal criminal laws relating to surveillance, accessing or damaging computers, and damage to an aircraft. Below, the advisory sets out separately how detection and mitigation capabilities may implicate these laws.

A. Detection Capabilities

Systems that detect, monitor, or track UAS often rely on radio-frequency (RF), radar, electro-optical (EO), infrared (IR), or acoustic capabilities, or a combination thereof. These capabilities detect the physical presence of UAS or signals sent to or from the UAS. In general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, depends on whether it captures, records, decodes, or intercepts, in whole or in part, electronic communications transmitted to and from a UAS and/or controller, and the type of communications involved. Detection systems that emit electromagnetic waves or pulses of sound or light that are reflected off an object and back to the detection system—such as radar, EO/IR, and acoustic systems—are less likely to pose concerns under federal criminal surveillance statutes. Such technology senses the sound or electromagnetic waves produced by or reflected from the UAS and does not capture, record, decode, or intercept electronic communications. However, the use of such systems must also comply with laws and regulations administered by the FCC and FAA, as discussed below.

By contrast, systems using RF capabilities to detect and track UAS by monitoring the communications passed between a UAS and its ground control station may implicate the Pen/Trap Statute and Wiretap Act.

- The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127, criminalizes the "use" or "installation" of a "device" or "process" that "records," "decodes," or "captures" non-content[4] dialing, routing, addressing, or signaling ("DRAS") information. DRAS information is non-content information used to transmit or process communications; depending on the system, this could include device serial numbers, cell site information, media access control (MAC) addresses, the international mobile equipment identity (IMEI), or the international mobile subscriber identity (IMSI). Use or installation of a pen register or trap and

[1] *See* 10 U.S.C. § 130i, 50 U.S.C. § 2661, and 6 U.S.C. § 124n.

[2] *See* 49 U.S.C. § 44810(g).

[3] This advisory does not address the general authorities of public safety agencies, or specific actions they might take consistent with governing law, to protect the public in exigent circumstances.

[4] While non-content is not defined, content is defined in footnote 7, *infra*.

trace device is prohibited, unless conducted pursuant to a court order or when a statutory exception applies.[5] With respect to the Pen/Trap Statute, the exceptions state that they are limited only to providers of wire or electronic communication services.

- *Questions to consider:*
  - What information is the technology collecting (*e.g.*, UAS type, manufacturer, model, protocol, unique identifier, telemetry)?
  - Is the information DRAS or content?
  - Do any Pen/Trap exceptions apply?

- The Wiretap Act (also known as Title III), 18 U.S.C. §§ 2510 *et seq.*, prohibits, among other things, "intentionally intercept[ing]" the content of "any . . . electronic communication[,]" unless it is conducted pursuant to a court order or a statutory exception applies.[6] An "electronic communication" is defined, with certain exceptions, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12).

[5] Law enforcement may use such devices with a court order, but can only obtain such an order in furtherance of an ongoing criminal investigation, *see* 18 U.S.C. § 3122(b)(2), and must use reasonably available technology that prevents the interception of the content of a communication. *See* 18 U.S.C. § 3121(c). Private actors are unable to obtain a court order under the Pen/Trap Statute and, therefore, must operate pursuant to one of the statute's exceptions. The Pen/Trap Statute and Wiretap Act do not contain identical exceptions. For example, while the Pen/Trap Statute includes an exception for use of a pen register or trap and trace device with the consent of a "user," it does not provide an exception based on the consent of a "party to the communication." *Compare* 18 U.S.C. § 3121(b)(3), *with* 18 U.S.C. § 2511(2)(c). In addition, the Pen/Trap Statute does not include an analogue to the Wiretap Act's exception allowing interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i).

[6] The Wiretap Act contains several exceptions to the blanket prohibition, including for operators and service providers, for uses "in the normal course of employment" that are a necessary incident to the rendition of services; for surveillance authorized under the Foreign Intelligence Surveillance Act of 1978; and where a party to the communication has given prior consent to such interception. *See*, e.g., 18 U.S.C. § 2511(2)(a)(i), (d) & (e). Law enforcement may also intercept communications without a court order in certain emergency situations, provided an application for an order is made within 48 hours of the interception. *Id.* § 2518(7).

- The Wiretap Act has an exception for the interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i). Section 2510(16) defines which radio communications do not fall into the foregoing exception. The Wiretap Act also has an exception for the interception of any radio communications that are transmitted "by any . . . aeronautical communications system." *Id.* § 2511(2)(g)(ii)(IV). UAS RF control systems may be considered "aeronautical communications systems" under the Act. However, existing case law raises questions as to the scope of both exceptions.[7]

- *Questions to consider:*
  - Are electronic communications being acquired?
  - Are any acquired communications transmitted by a system that affects interstate or foreign commerce (*e.g.*, a system that is connected to the Internet or a mobile network)?
  - Are any portions of the communications acquired by the technology "content?"[8]
  - Do any of the Wiretap Act's exceptions apply (*e.g.*, is the person intercepting the communications a party to the communication under 18 U.S.C. § 2511(2)(d))?

- 18 U.S.C. § 2512 generally prohibits the manufacture, assembly, possession, sale, advertisement, and distribution of devices that are "primarily useful for the surreptitious interception of wire, oral, or electronic communications."[9] Section 2513 provides that any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of § 2512 may be seized and forfeited to the United States.

B. Mitigation Capabilities

Mitigation capabilities fall into two general categories: non-kinetic and kinetic. Non-kinetic solutions use non-physical measures to disrupt or disable UAS, including RF, WiFi, or Global Positioning System (GPS) jamming; spoofing; hacking techniques; and non-destructive directed energy weapons. Kinetic solutions may employ a variety of measures capable of physically disrupting or disabling a UAS, including nets, projectiles, and lasers. The use of non-kinetic or kinetic solutions may implicate federal criminal prohibitions against, among other things, intercepting and interfering with communications, damaging a "protected computer,"[10] and damaging an "aircraft." The term "aircraft" refers to "a civil, military or public contrivance invented, used, or designed to navigate, fly, or travel in the air." 18 U.S.C. § 31(a)(1). This definition is consistent with the meaning of "aircraft" in 49 U.S.C. § 40102(a)(6). In the FAA Reauthorization Act of 2018, Congress codified the term "unmanned aircraft" as "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft." 49 U.S.C. § 44801(11).

---

[7] *See Joffe v. Google Inc.*, 746 F.3d 920, 928-29 (9th Cir. 2013) (panel rehearing), *cert. denied*, 134 S. Ct. 2877 (2014).

[8] Content is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Importantly, machine-to-machine communications and data transfers between devices can be considered "content."

[9] The statute exempts "officer[s], agent[s], or employee[s] of, or [] person[s] under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof." 18 U.S.C. § 2512(2)(b).

[10] The term "protected computer" includes any computer that is used in or affecting interstate or foreign commerce or communication, or that is used by or for a financial institution or the United States government. 18 U.S.C. §§ 1030(e)(1) & (2).

Jamming technologies are designed to block or interfere with authorized radio communications.[11] Examples of jamming include transmitting RF signals from a jammer at a higher "signal strength" than the RF signals being used to navigate or control the aircraft; preventing a cellular, WiFi, or Bluetooth-enabled device from connecting to a network (such as a cellular system or the Internet); or preventing a GPS unit from receiving positioning signals from a satellite. Spoofing technologies can replicate and replace or modify signals, and can lead to loss of control over the UAS's navigation and communications link (*e.g.*, its link to its ground controller). Hacking techniques generally focus on the UAS's communications link and/or the onboard computer processors.

Jamming, spoofing, and hacking technologies should be evaluated under the federal criminal statutes below (including the aircraft sabotage and aircraft piracy provisions), in addition to the laws discussed above with regard to detection. Because jamming and spoofing are also likely to implicate laws relating to the RF spectrum, parties should carefully review the information in Section II, below, as well.

- The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, among other things, prohibits intentionally accessing a "protected computer" without authorization and thereby obtaining information, or intentionally damaging a protected computer without authorization, including by transmitting a program, information, code, or command that causes such damage.[12] The CFAA broadly defines the term "protected computer"[13] in a manner that could include UAS control systems.

- Interference with the Operation of a Satellite, 18 U.S.C. § 1367, generally prohibits "obstruct[ing] or hinder[ing] any satellite transmission."[14] Jamming, spoofing, degrading or otherwise interfering with GPS signals to a UAS or ground control station could be prohibited under this section, as well as jamming or interfering with any control signals sent to a UAS directly from a satellite.

- Communication Lines, Stations, or Systems, 18 U.S.C. § 1362, prohibits "willfully or maliciously injur[ing] or destroy[ing] . . . means of communication operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States," as well as by "hinder[ing] or delay[ing] the transmission of any communication" over such means of communication. This statute could apply if UAS detection and/or mitigation operations willfully or maliciously degrade or otherwise hinder any frequency or transmissions, including cellular or WiFi signals, with a demonstrable use or intended use by the military or by SLTT law enforcement or emergency personnel engaged in civil defense functions.

Finally, it is possible for mitigation capabilities that destroy, seize, or exercise control of a UAS to implicate federal criminal laws that otherwise apply to "aircraft," as that term is statutorily defined. While all kinetic solutions will likely have one or more of these capabilities implicating those laws, non-kinetic solutions should also be evaluated for compliance.

---

[11] Authorized radio communications include radio communications operating pursuant to federal authorizations or FCC licenses and those operating without a license but pursuant to FCC rules.

[12] The statute exempts the "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State." 18 U.S.C. § 1030(f).

[13] *See id.* § 1030(e)(1), (2).

[14] The statute exempts "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States." *Id.* § 1367(b).

- The Aircraft Sabotage Act, 18 U.S.C. § 32(a), criminalizes certain destructive actions with respect to "aircraft," including damaging, destroying, or disabling those aircraft.

- The Aircraft Piracy Act, 49 U.S.C. § 46502, criminalizes the act of seizing or exercising control of an "aircraft" with "wrongful intent." An intent to seize or exercise control of an aircraft without the legal authorization to do so could involve wrongful intent.

II. Additional Federal Laws Relating to Aviation and Spectrum

In addition to implicating federal criminal laws, the acquisition, installation, testing, and use of UAS detection or mitigation technologies may implicate laws and regulations administered by the FAA and the FCC relating to aviation and RF spectrum. UAS response measures may also implicate existing aviation security laws and regulations administered by the Transportation Security Administration (TSA).

A. Laws Relating to Aviation Safety and Efficiency[15]

Non-federal entities should evaluate UAS detection activities for compliance with laws and regulations administered by the FAA, including but not limited to the following:

[15] This subsection is limited to the discussion of UAS detection systems because, as previously indicated, only certain federal agencies have been expressly authorized by Congress to mitigate UAS notwithstanding certain federal laws. The FAA does not support the use of mitigation systems by any entities that do not have express authority from Congress.

- Use of Airspace. 49 U.S.C. § 40103 establishes a public right of transit through the navigable airspace and vests the FAA with authority to ensure the safety of aircraft and the efficient use of airspace. This includes ensuring that compliant aircraft (including UAS) may move through the airspace without improper interference. For example, detection systems may lead to the identification of both legitimate airspace users as well as unlawful activity. Additional analysis is necessary to identify whether an operation identified by a detection system is in violation of FAA regulation before engaging in an operational response. This also includes identifying and working to address any potential collateral impacts of detection technology or systems on the safe and efficient operation of the National Airspace System.

- Airport Operating Certificates. 49 U.S.C. § 44706, as implemented by 14 CFR Part 139, prescribes the rules governing the certification and operation of airports in the United States. Holders of Airport Operating Certificates issued under 14 CFR Part 139 must protect navigational aids. *See* 14 CFR § 139.333. Commercial service airport operators may also need to update the contents of their airport certification manuals to include operating procedures for the use of a UAS detection system. *See id.* § 139.203. Moreover, the installation or use of UAS detection systems by sponsors of commercial service airports may also implicate other regulatory requirements under CFR Title 14. The FAA has provided extensive information to airport sponsors, which can be accessed at: https://www.faa.gov/airports/airport_safety/#SafetyGuidance.

- Structures Interfering with Air Commerce. 49 U.S.C. § 44718, as implemented in 14 CFR Part 77, requires entities proposing construction or alteration of existing structures in the vicinity of an airport to provide the FAA with notice. *See also* FAA Order 7400.2M, Procedures for Handling Airspace Matters (Feb. 28, 2019). The required notice allows the FAA to conduct an aeronautical study of the potential for the proposed structure and any electromagnetic broadcast signals to create a hazard to air navigation, including interference with aircraft and navigational aids.[16] Entities seeking to install or use equipment for UAS detection activities should also evaluate whether 14 CFR Part 77 requires them to provide the FAA with advance notice of proposed construction or alteration.

- Project Grant Application Approval Conditioned on Assurances About Airport Operations. 49 U.S.C. § 47107 establishes obligations for recipients of grant funds for an airport development project to maintain and operate airport facilities safely and efficiently and in accordance with specified conditions. Airports subject to such conditions may need to ensure that the installation or use of a UAS detection system does not introduce a hazard that cannot be mitigated, consistent with applicable grant assurance obligations, such as Grant Assurance 20, Hazard Removal and Mitigation. In addition, such airports may need to ensure that UAS detection systems and associated structures are accurately reflected in the Airport Layout Plan consistent with Grant Assurance 29, Airport Layout Plan.

For additional information concerning these laws, please contact the Office of National Security Programs and Incident Response at the FAA.

[16] Non-federal entities are encouraged to independently validate the performance and characteristics of UAS detection systems being considered. Significant deviations between vendor claims and real world operation, including the potential for RF emissions and interference, have been observed by the FAA.

B. Laws Relating to Transportation/Airport Security

Through its broad authorities, the TSA oversees the implementation and ensures the adequacy "of security measures at airports and other transportation facilities." 49 U.S.C. § 114(f)(11). TSA may also take appropriate action to address threats, including coordination of security measures with other agencies and to impose requirements on transportation stakeholders, through regulations, security directives, emergency amendments, and security programs. *See* 49 U.S.C. § 114(f)(4) & (l)(1)-(2); 49 U.S.C. § 44932; 49 CFR § 1542.105(d), 1542.303, 1544.305, 1544.105(d), 1546.105(d).

Airports seeking to deploy, buy, or purchase UAS detection or mitigation systems should consider laws, regulations, and security requirements related to local aviation security response. For example, TSA regulations require each operator of an airport regularly serving air carriers to establish an air transportation security program (ASP). *See* 49 U.S.C. §§ 114 and 44903; 49 CFR Part 1542. Among other requirements, the ASP must provide law enforcement personnel in the number and manner adequate to support the program. 49 CFR § 1542.215. In addition, TSA's enforcement authorities include the ability of the Administrator, in consultation with the airport operator and law enforcement authorities, to order the deployment of personnel at any secure area of the airport to counter threats to aircraft and aircraft operations or to address national security concerns, such as those posed by UAS. 49 U.S.C. § 44903(h)(1).

For additional information or coordination, please contact your local TSA Federal Security Director.

C. Laws Relating to the Radiofrequency Spectrum

Any systems that involve emission of radio waves, including radar, must be evaluated for compliance with laws and regulations administered by the FCC, including but not limited to the following:

- Authorizations for Use of Spectrum. Authorized non-federal radio communications include unlicensed operations and operations on frequencies requiring individual licenses.
    - Transmissions on frequencies authorized for unlicensed operations, such as common WiFi and Bluetooth frequencies, do not require a license but may nevertheless implicate statutory or regulatory prohibitions against harmful interference as well as other requirements.
    - Operating on a frequency allocated for licensed private-sector use (such as on the bands used by mobile phones) is subject to licensing requirements and other regulation at the federal level. *See* 47 U.S.C. § 301.
        - For example, use of radar to detect UAS requires a Radiolocation Service license from the FCC. General guidance regarding how to prepare and file an application is available at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/industrial-business/industrial-business-licensing. The application must identify the locations and frequencies where the applicant proposes to operate as well as provide other technical information. Equipment vendors may be able to assist with gathering this information. No prior frequency coordination is required, but if the applicant proposes to operate near a U.S. Government facility, it may wish to consult with appropriate Federal officials before applying in order to avoid having the application rejected when the FCC conducts its Federal coordination.

- Marketing, Sale, or Operation of Jammers. 47 U.S.C. § 302a prohibits most non-federal entities from manufacturing, importing, shipping, selling, or using devices that fail to comply with FCC regulations regarding devices that can interfere with radio reception, including transmitters designed to block, jam, or interfere with wireless communications. 47 U.S.C. § 302a(b).

- Interference with Radio Communications. 47 U.S.C. § 333 prohibits "willfully or maliciously interfer[ing] with or caus[ing] interference to any radio communications of any station licensed or authorized by [the FCC] or operated by the United States Government."

Guidance disclaimer: This advisory is provided for informational purposes only. Guidance documents, like this document, are not binding and lack the force and effect of law, unless expressly authorized by statute or expressly incorporated into a contract, grant, or cooperative agreement. Consistent with Executive Order 13891 and the Office of Management and Budget implementing memoranda, the issuing Departments will not cite, use, or rely on any guidance document that is not accessible through the issuing Departments' guidance portals, or similar guidance portals for other Executive Branch departments and agencies, except to establish historical facts. To the extent any guidance document sets out voluntary standards (*e.g.*, recommended practices), compliance with those standards is voluntary, and noncompliance will not result in enforcement action. Guidance documents may be rescinded or modified in the issuing Departments' complete discretion, consistent with applicable laws.

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; [redacted]; Ray Andrade [redacted]; Adam Arluke [redacted]; Baggs, Kevin L; Keolani Bailey [redacted]; Dax Bajema [redacted]; Christopher Ballog [redacted]; [redacted]; Cory S. Brailsford [redacted]; Craig Burns [redacted]; Christopher Butch [redacted]; [redacted]; Daniel Carreiro [redacted]; [redacted]; Robert Caulfield [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Collins, Jimmie L; [redacted]; Coronel, Romel M; [redacted]; James Cruz [redacted]; Joseph Doyle [redacted]; Fred Edwards [redacted]; [redacted]; [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Joseph Doyle [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; [redacted]; Nic Iannarone [redacted]; [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; Weldon James [redacted]; Diego Jarrin [redacted]; [redacted]; [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; [redacted]; [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; [redacted]; Trevor Ohnstad [redacted]; [redacted]; [redacted]; Pace, Frank J; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; [redacted]; [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles [redacted]; [redacted]; [redacted]; Eric Shimodoi [redacted]; [redacted]; Jason Scoles [redacted]; Joh Strandhagen [redacted]; Bennett Strobel [redacted]; [redacted]; Gen Tamura [redacted]; Dustin Truax [redacted]; John Udani [redacted]; [redacted]; Judy Van Nguyen [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government [redacted]; John Woodruff - US Federal Government [redacted]; [redacted]; [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]

Subject: C-UAS WG, 16 Jan 25 - Minutes and membership

Date: Friday, January 17, 2025 5:25:00 PM

Attachments: image001.png
2025 01 16 Minutes.docx
RSVP-Attendance List.xlsx
Interagency Legal Advisory on UAS Detection and Mitigation Technologies.pdf

---

Aloha All

My sincere appreciation to all of those that were able to join us for the great discussions and information sharing!

As one of our colleagues noted, “this workgroup enhances comms and coordination among federal, state, and local agencies regarding various deployed detection systems; response and investigations of breaches of security; and authority and jurisdiction (or lack thereof).”

We are only able to do that due to the dedication and energy of our membership and your willingness to dig into this challenging mission space.

Our intent at OHS is to facilitate this collaboration – and drive improvements where they are needed most. To that end, you will see a tight group of action items in the attached minutes that I will be championing in the year to come and look forward to engaging with those willing and able to

participate in those undertakings.

I have a couple follow on communications for the group, so I will keep this one short.

My last topic here is our distribution list. There was great desire to have that roster shared and I have included what details I have at hand, but I need your assistance to improve the roster. I have updated the roster I had based on feedback from this meeting.

1. Please add any information that may be missing from your information (mostly that is titles and organizations) and return the spreadsheet back to me with your feedback.
2. Help me identify those individuals that joined but did not note their titles and organizations – I do not have their email addresses as they were not on my initial invitation roster.
3. Let me know if you prefer NOT to share your contact information so I can annotate that appropriately.

For those that could use a refresher or that are new to the topic, Parker Corts (FAA) reshared the attached Legal Advisory – a really good primer.

v/r
jc

Ms. Jimmie L Collins
Chief, Planning and Operations
State Security Clearance POC
Protected Critical Infrastructure Information (PCII) Officer
CISA Gateway Administrator - Hawai'i
Hawai'i Office of Homeland Security
3949 Diamond Head Road, Honolulu HI 96816
[redacted]
office: [redacted]
cell: [redacted]
Office of Homeland Security (hawaii.gov)

Counter-Unmanned Aerial Systems Working Group

16 Jan 25/09-1100 (HST)
Minutes

Location: [redacted]
and
Microsoft Teams
Meeting ID: [redacted]
Passcode: [redacted]
+1 808-829-4853,, [redacted]

1. Attendees (see RSVP-Attendance List attached to distribution email)
2. Guest Speakers:
    a. Rodney Takahashi, C-sUAS Program Manager, USINDOPACOM: DOD Announces Strategy for Countering Unmanned Systems
        i. Rodney discussed his initial thoughts regarding the recent designation of the Commanders of NORTHCOM and INDOPACOM as the lead synchronizers for operations to counter-UAS in the homeland. He talked about the three 'lines of effort' and generated a good bit of discussion amongst the grup regarding:
            1. Policy: What topics should be included in intergovernmental leadership dialogue, what leaders should be engaged, what policies are needed
            2. Reporting/investigations: air domain awareness, developing 'the' threat picture, information sharing. PADS representative (KO Bailey) indicated their tactical arrangement with Guard and Active forces that could increase air domain awareness and also briefly described a recent Oahu-based proof-of-concept event using the Ukrainian Sky Fortress. CBP/CAMDEx representative, Erik Modisett talked briefly about the friction between DoD (fence line) versus CBP (wide) detection authorities.
            3. Response Planning: who are key stakeholders in response, who can action, concept of operations
    b. John Abbey, SafeFlight: Hawai'i UAS Response, Enforcement, and Reporting; Air Force Phase I Contract
        i. The SafeFlight proposal for a 90-day Phase I scoping effort was funded and John is looking to launch that effort with Office of Homeland Security support in connecting with stakeholder organizations actioning data gathering activities necessary to approach Phase II funding. Those activities include:
            1. Identify the "protected sites" (airports, air bases, sports/ entertainment venues, and critical infrastructure), "responder agencies" (state and county law enforcement and military security forces), and "supporting agencies" (Fusion Center, 911 PSAP's, and BDOC's),
            2. Identify and develop output data specifications for all military and domestic C-UAS detention systems,
            3. Work individually and collectively with all stakeholder groups to identify and catalog all low altitude airspace ISR and mitigation and enforcement policies,

4. Work with management and user groups to draft Dual Use, universal protocols and adapt the software specifications developed with the Air Force Accelerator and cleared by the FAA for all US airports,
5. Reach consensus with all stakeholders for final protocols, joint operations/ mutual-aid agreements, detailed statewide software solution specifications and a detailed implementation plan.

ii. OHS (Jimmie Collins) will send a separate query to the working group membership to solicit appropriate organizational contacts to support John's data gathering.

3. Incident reporting: Nothing to add from meeting agenda in invitation.
4. Events: Nothing to add from meeting agenda in invitation.
5. Policy: Nothing to add from meeting agenda in invitation.
6. News:
    a. The group discussed the reported drone 'strike' that was in the news recently. Cory Brailsford, HPD, added to the discussion by doing an overview of several recent operational experiences, including drones flying over an active response (New Years Eve explosion response) and issues relating air operations incidental to and operationally supporting a major event. He mentioned his desire to pursue legislation for [redacted]. Cory also provided some details regarding his C-UAS approach within his organization:
        i. Education/awareness training for recruits
        ii. Documentation to expand available data to scope the response need and the capacity and capability building needs
        iii. Response-enabling processes that tackle issues like TFR-breaching, utility of TFR versus NOTAM
7. Other/Open Discussion:
    a. Training: Erik Modisett spoke briefly about specialized C-UAS training his organization conducts.
8. Conclusion:
    a. Jimmie closed the meeting with an overview of actionable items from the discussion that she will facilitate:
        i. Initiate outreach to working group members to solicit organizational representation to support data gathering for the SafeFlight: Hawai'i UAS Response, Enforcement, and Reporting project.
        ii. Initiate outreach to working group members to solicit interested parties for further development of these working group lines of effort (notes here are not intended to be all inclusive, just initial ideas):
            1. Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
            2. Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
            3. Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

b. Follow-ons: Because our members are overachieving, collaborative, communicating types, there were items dropped in the chat and provided to me afterwards to share onwards:
    i. Firmware Update Removes Geofencing From DJI Drones - AVweb
    ii. Basic Law Enforcement Response Drone Card
    iii. FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan
c. Next Working Group meeting: 17 Apr 25, 09-1100 (HST), same location. Invitation to follow.

Counter-UAS Working Group
16 January 2025
RSVP-Attendance List (002)

Last	First	Email	Title	Organization	Response	On-Line/ In Person	Present
Abbey	John	[redacted]			Accepted	In Person	X
Acosta	Shawn	[redacted]			None	Virtual	X
Adams	Sara	[redacted]			None		
Andrade	Ray	[redacted]			Accepted	Virtual	X
Arias	Adrien	[redacted]			None		
Arluke	Adam	[redacted]			None		
Baggs	Kevin	[redacted]			Accepted	In Person	X
Bailey	Keolani (KO)	[redacted]		PADS/CC	None	Virtual	X
Bajema	Dax	[redacted]	MAJ	HING	None	Virtual	X
Ballog	Christopher	[redacted]			None		
Blanchard	Aaron	[redacted]			None	In Person	X
Blankinship	Lisa	[redacted]			None		
Brailsford	Cory	[redacted]			Accepted	In Person	X
Burns	Craig	[redacted]			Accepted		
Butch	Christopher	[redacted]			None		
Butler	Rhett	[redacted]			None		
Carpenter	Jason	[redacted]			None		
Carreiro	Daniel	[redacted]			None		
Carter	Scott	[redacted]			Declined		
Castillo			MAJ		None	Virtual	X
Caulfield	Robert	[redacted]			None		
Chong	Cullen	[redacted]			None		
Church	Christopher	[redacted]			None		
Clark	Randy	[redacted]			Accepted		
Collins	Jimmie	[redacted]	Chief, Planning and Operations	Hawaii OHS	Accepted	In Person	X
Comisky	Brian	[redacted]			None		
Coronel	Romel	[redacted]			None		
Corts	Parker	[redacted]	HQ Senior Representative to USINDOPACOM and PACAF, AJR-25 Special Operations	FAA	None	Virtual	X
Crotts	Ray	[redacted]		FAA	None		
Cruz	James	[redacted]			Accepted		
Doyle	Joseph	[redacted]			None		
Edwards	Fred	[redacted]			None		
Felix	Ivan	[redacted]			None		
Ferguson	Patrick	[redacted]			None		
Flynn	Sheldon	[redacted]		FAA	None		
Ford	Daniel	[redacted]			None		
Franquez	Jon	[redacted]			None	Virtual	X
Frye	Charles (Chaz)	[redacted]			None		
Fuerst	Dennis	[redacted]			None		
Grant	Robin (Chris)	[redacted]			Accepted		
Gregory	Diana		Col	298 ADG/CC	None	Virtual	X
Grems	Jonathon	[redacted]			None		
Haley	Talwyn	[redacted]		FAA	None		
Harahap	Isra	[redacted]			None		
Higbee	Scott	[redacted]			None		
Hook	Sean	[redacted]		FAA	None	Virtual	X
Iannarone	Nic	[redacted]			Tentative		
Ibanez	Sandra	[redacted]			None		
Ishida	Kenn	[redacted]			None		
Jacob	Sarah	[redacted]			None		
James	Weldon	[redacted]			None		
Jarrin	Diego	[redacted]	Senior Federal Air Marshal, CUAS Lead agent	LA Field Office	None	Virtual	X
Jones	Mars	[redacted]			Accepted		
Kaonohi	Lance	[redacted]			None		
Keith	Brian	[redacted]			None	Virtual	X
Klein	Scott	[redacted]			None		
Kumalae	Brandon	[redacted]			None		
Lee	Norreal	[redacted]			Accepted	In Person	X
Lindsey	Bradley	[redacted]	CPO	USCG	None	Virtual	X
Looby	Kerry	[redacted]			None		
Lopez	Kendall	[redacted]			None		

Counter-UAS Working Group
16 January 2025
RSVP-Attendance List (002)

Last	First	Email	Title	Organization	Response	On-Line/ In Person	Present
Marciel	Bryan	[redacted]			None		
McGahan	Lisa	[redacted]			Tentative		
Mclaren	Humberto (Mac)	[redacted]	Maritime Cybersecurity Specialist	USCG	Accepted	Virtual	X
Merrill					None	Virtual	X
Mindo	Rei				None	Virtual	X
Mitsuyoshi	Eric	[redacted]			Accepted	Virtual	X
Modisett	Erik	[redacted]	Supervisory Agent	DHS/CBP/CAMDEx: Center for Air and Marine Drone Exploitation	Accepted	Virtual	X
Nahale	Sean	[redacted]			None		
Oakley	Bryan	[redacted]			None		
Ohnstad	Trevor	[redacted]			None		
Okagawa	Jensen	[redacted]			None		
O'Keefe	Garrett	[redacted]			None		
Pace	Frank	[redacted]			Accepted	In Person	X
Parks	Brent	[redacted]			None		
Partin	James		Physical Security Program Manager	IMCOM Pacific	None	Virtual	X
Patalano	Giovan	[redacted]			None		
Petersen	Craig	[redacted]			Accepted	In Person	X
Piazza	Vincent	[redacted]			Accepted	In Person	X
Priestly	Christopher	[redacted]			None	Virtual	X
Ramirez			CW2	25th CEMA	None	Virtual	X
Reagan	Shane	[redacted]			None		
Reigel	Jordan	[redacted]			None	Virtual	X
Russell	Patrick	[redacted]			None		
Sagun	Arnold	[redacted]			None		
Sanders	Paul	[redacted]	Sr. Chemical Security Inspector	DHS/CISA	Accepted	Virtual	X
Scoles	Jason	[redacted]			None		
Shaha	Daniel	[redacted]			Accepted	In Person	X
Shaw	Keith	[redacted]			None		
Shimodoi	Eric	[redacted]			None		
Song	Douglas	[redacted]			None	In Person	X
Stanco	Marc	[redacted]			None		
Strandhagen	Joh	[redacted]	Protective Security Advisor	DHS/CISA	Accepted	Virtual	X
Strobel	Bennett	[redacted]			None		
Takahashi	Rodney	[redacted]			Accepted	In Person	X
Tamura	Gen	[redacted]	Protective Security Advisor	DHS/CISA	Accepted	Virtual	X
Truax	Dustin	[redacted]			None		
Udani	John	[redacted]			None		
Valoroso	Deric	[redacted]			None		
Van Nguyen	Judy	[redacted]	Intelligence Analyst	FBI	Accepted	Virtual	X
Villegas	Julio Alvarado	[redacted]		FBI	None		
Wade	Kathleen	[redacted]			Declined		
Waller	Joshua	[redacted]		FBI	None		
Williams	Giovanni	[redacted]			Accepted	In Person	X
Woodruff	John	[redacted]			None	Virtual	X
Wright	Alvin	[redacted]			None	In Person	X
Young	Andrea	[redacted]	FAMS AFSD-LE HNL	DHS/TSA	Accepted	Virtual	X
Young	Jeremy	[redacted]			Declined		
Zawacki	Lee	[redacted]			None	In Person	X

Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems

August 2020

The Federal Aviation Administration (FAA), Department of Justice (DOJ), Federal Communications Commission (FCC), and Department of Homeland Security (DHS) are issuing an advisory guidance document to assist non-federal public and private entities interested in using technical tools, systems, and capabilities to detect and mitigate Unmanned Aircraft Systems (UAS). The advisory is intended to provide an overview of potentially applicable federal laws and regulations, as well as some factors relevant to whether those laws may apply to particular actions or systems.

Specifically, this advisory addresses two categories of federal laws that may apply to UAS detection and mitigation capabilities: (1) various provisions of the U.S. criminal code enforced by DOJ; and (2) federal laws and regulations administered by the FAA, DHS, and the FCC. The advisory does *not* address state and local laws, which UAS detection and mitigation capabilities may also implicate. Neither does it cover potential civil liability flowing from the use of UAS detection and mitigation technologies (*e.g.*, the potential liability from causing physical damage to persons or property as a result of mitigating a UAS threat, or civil liability and recovery for an unlawful interception of wire, oral, or electronic communications under 18 U.S.C. § 2520).

This advisory is provided for informational purposes only. It is strongly recommended that, prior to the testing, acquisition, installation, or use of UAS detection and/or mitigation systems, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws. Entities should conduct their own legal and technical analysis of each UAS detection and/or mitigation system and should not rely solely on vendors' representations of the systems' legality or functionality. As part of that analysis, entities should closely evaluate and consider whether the use of UAS detection and mitigation capabilities might impact the public's privacy, civil rights, and civil liberties. This is particularly important because potential legal prohibitions, as discussed below, are not based on broad classifications of systems (*e.g.*, active versus passive, detection versus mitigation), but instead are based on the functionality of each system and the specific ways in which a system operates and is used. A thorough understanding of both applicable law and the systems' functionality will ensure important technologies designed to protect public safety, by detecting and/or mitigating UAS threats, are used effectively, responsibly, and legally.

I. Federal Criminal Laws

Congress has exclusively authorized the Departments of Defense, Energy, Justice, and Homeland Security to engage in limited UAS detection and mitigation activities to counter UAS presenting a credible threat to covered facilities or assets, notwithstanding certain otherwise potentially applicable federal criminal laws, including various laws relating to surveillance.[1] In addition, the FAA has been expressly authorized to engage in limited testing activities notwithstanding certain federal criminal surveillance laws.[2]

Because no other entities have been granted that authority, it is important that state, local, tribal and territorial (SLTT) and private sector entities without such statutory authority (including SLTT law enforcement organizations, SLTT governments, and owners and operators of critical infrastructure, stadiums, outdoor entertainment venues, airports, and other key sites) understand that federal laws may prevent, limit, or penalize the sale, possession, or use of UAS detection and mitigation capabilities.[3] Capabilities for detecting and mitigating UAS may implicate federal criminal laws relating to surveillance, accessing or damaging computers, and damage to an aircraft. Below, the advisory sets out separately how detection and mitigation capabilities may implicate these laws.

A. Detection Capabilities

Systems that detect, monitor, or track UAS often rely on radio-frequency (RF), radar, electro-optical (EO), infrared (IR), or acoustic capabilities, or a combination thereof. These capabilities detect the physical presence of UAS or signals sent to or from the UAS. In general, whether a detection or tracking system implicates federal criminal surveillance laws, such as the Pen/Trap Statute and the Wiretap Act, depends on whether it captures, records, decodes, or intercepts, in whole or in part, electronic communications transmitted to and from a UAS and/or controller, and the type of communications involved. Detection systems that emit electromagnetic waves or pulses of sound or light that are reflected off an object and back to the detection system—such as radar, EO/IR, and acoustic systems—are less likely to pose concerns under federal criminal surveillance statutes. Such technology senses the sound or electromagnetic waves produced by or reflected from the UAS and does not capture, record, decode, or intercept electronic communications. However, the use of such systems must also comply with laws and regulations administered by the FCC and FAA, as discussed below.

By contrast, systems using RF capabilities to detect and track UAS by monitoring the communications passed between a UAS and its ground control station may implicate the Pen/Trap Statute and Wiretap Act.

- The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127, criminalizes the "use" or "installation" of a "device" or "process" that "records," "decodes," or "captures" non-content[4] dialing, routing, addressing, or signaling ("DRAS") information. DRAS information is non-content information used to transmit or process communications; depending on the system, this could include device serial numbers, cell site information, media access control (MAC) addresses, the international mobile equipment identity (IMEI), or the international mobile subscriber identity (IMSI). Use or installation of a pen register or trap and

[1] *See* 10 U.S.C. § 130i, 50 U.S.C. § 2661, and 6 U.S.C. § 124n.

[2] *See* 49 U.S.C. § 44810(g).

[3] This advisory does not address the general authorities of public safety agencies, or specific actions they might take consistent with governing law, to protect the public in exigent circumstances.

[4] While non-content is not defined, content is defined in footnote 7, *infra*.

trace device is prohibited, unless conducted pursuant to a court order or when a statutory exception applies.[5] With respect to the Pen/Trap Statute, the exceptions state that they are limited only to providers of wire or electronic communication services.

- *Questions to consider:*
  - What information is the technology collecting (*e.g.*, UAS type, manufacturer, model, protocol, unique identifier, telemetry)?
  - Is the information DRAS or content?
  - Do any Pen/Trap exceptions apply?

- The Wiretap Act (also known as Title III), 18 U.S.C. §§ 2510 *et seq.*, prohibits, among other things, "intentionally intercept[ing]" the content of "any . . . electronic communication[,]" unless it is conducted pursuant to a court order or a statutory exception applies.[6] An "electronic communication" is defined, with certain exceptions, as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *Id.* § 2510(12).

[5] Law enforcement may use such devices with a court order, but can only obtain such an order in furtherance of an ongoing criminal investigation, *see* 18 U.S.C. § 3122(b)(2), and must use reasonably available technology that prevents the interception of the content of a communication. *See* 18 U.S.C. § 3121(c). Private actors are unable to obtain a court order under the Pen/Trap Statute and, therefore, must operate pursuant to one of the statute's exceptions. The Pen/Trap Statute and Wiretap Act do not contain identical exceptions. For example, while the Pen/Trap Statute includes an exception for use of a pen register or trap and trace device with the consent of a "user," it does not provide an exception based on the consent of a "party to the communication." *Compare* 18 U.S.C. § 3121(b)(3), *with* 18 U.S.C. § 2511(2)(c). In addition, the Pen/Trap Statute does not include an analogue to the Wiretap Act's exception allowing interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i).

[6] The Wiretap Act contains several exceptions to the blanket prohibition, including for operators and service providers, for uses "in the normal course of employment" that are a necessary incident to the rendition of services; for surveillance authorized under the Foreign Intelligence Surveillance Act of 1978; and where a party to the communication has given prior consent to such interception. *See*, e.g., 18 U.S.C. § 2511(2)(a)(i), (d) & (e). Law enforcement may also intercept communications without a court order in certain emergency situations, provided an application for an order is made within 48 hours of the interception. *Id.* § 2518(7).

- The Wiretap Act has an exception for the interception of electronic communications that are "readily accessible to the general public." *Id.* § 2511(2)(g)(i). Section 2510(16) defines which radio communications do not fall into the foregoing exception. The Wiretap Act also has an exception for the interception of any radio communications that are transmitted "by any . . . aeronautical communications system." *Id.* § 2511(2)(g)(ii)(IV). UAS RF control systems may be considered "aeronautical communications systems" under the Act. However, existing case law raises questions as to the scope of both exceptions.[7]

- *Questions to consider:*
  - Are electronic communications being acquired?
  - Are any acquired communications transmitted by a system that affects interstate or foreign commerce (*e.g.*, a system that is connected to the Internet or a mobile network)?
  - Are any portions of the communications acquired by the technology "content?"[8]
  - Do any of the Wiretap Act's exceptions apply (*e.g.*, is the person intercepting the communications a party to the communication under 18 U.S.C. § 2511(2)(d))?

- 18 U.S.C. § 2512 generally prohibits the manufacture, assembly, possession, sale, advertisement, and distribution of devices that are "primarily useful for the surreptitious interception of wire, oral, or electronic communications."[9] Section 2513 provides that any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of § 2512 may be seized and forfeited to the United States.

B. Mitigation Capabilities

Mitigation capabilities fall into two general categories: non-kinetic and kinetic. Non-kinetic solutions use non-physical measures to disrupt or disable UAS, including RF, WiFi, or Global Positioning System (GPS) jamming; spoofing; hacking techniques; and non-destructive directed energy weapons. Kinetic solutions may employ a variety of measures capable of physically disrupting or disabling a UAS, including nets, projectiles, and lasers. The use of non-kinetic or kinetic solutions may implicate federal criminal prohibitions against, among other things, intercepting and interfering with communications, damaging a "protected computer,"[10] and damaging an "aircraft." The term "aircraft" refers to "a civil, military or public contrivance invented, used, or designed to navigate, fly, or travel in the air." 18 U.S.C. § 31(a)(1). This definition is consistent with the meaning of "aircraft" in 49 U.S.C. § 40102(a)(6). In the FAA Reauthorization Act of 2018, Congress codified the term "unmanned aircraft" as "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft." 49 U.S.C. § 44801(11).

---

[7] *See Joffe v. Google Inc.*, 746 F.3d 920, 928-29 (9th Cir. 2013) (panel rehearing), *cert. denied*, 134 S. Ct. 2877 (2014).

[8] Content is "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Importantly, machine-to-machine communications and data transfers between devices can be considered "content."

[9] The statute exempts "officer[s], agent[s], or employee[s] of, or [] person[s] under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof." 18 U.S.C. § 2512(2)(b).

[10] The term "protected computer" includes any computer that is used in or affecting interstate or foreign commerce or communication, or that is used by or for a financial institution or the United States government. 18 U.S.C. §§ 1030(e)(1) & (2).

Jamming technologies are designed to block or interfere with authorized radio communications.[11] Examples of jamming include transmitting RF signals from a jammer at a higher "signal strength" than the RF signals being used to navigate or control the aircraft; preventing a cellular, WiFi, or Bluetooth-enabled device from connecting to a network (such as a cellular system or the Internet); or preventing a GPS unit from receiving positioning signals from a satellite. Spoofing technologies can replicate and replace or modify signals, and can lead to loss of control over the UAS's navigation and communications link (*e.g.*, its link to its ground controller). Hacking techniques generally focus on the UAS's communications link and/or the onboard computer processors.

Jamming, spoofing, and hacking technologies should be evaluated under the federal criminal statutes below (including the aircraft sabotage and aircraft piracy provisions), in addition to the laws discussed above with regard to detection. Because jamming and spoofing are also likely to implicate laws relating to the RF spectrum, parties should carefully review the information in Section II, below, as well.

- The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, among other things, prohibits intentionally accessing a "protected computer" without authorization and thereby obtaining information, or intentionally damaging a protected computer without authorization, including by transmitting a program, information, code, or command that causes such damage.[12] The CFAA broadly defines the term "protected computer"[13] in a manner that could include UAS control systems.

- Interference with the Operation of a Satellite, 18 U.S.C. § 1367, generally prohibits "obstruct[ing] or hinder[ing] any satellite transmission."[14] Jamming, spoofing, degrading or otherwise interfering with GPS signals to a UAS or ground control station could be prohibited under this section, as well as jamming or interfering with any control signals sent to a UAS directly from a satellite.

- Communication Lines, Stations, or Systems, 18 U.S.C. § 1362, prohibits "willfully or maliciously injur[ing] or destroy[ing] . . . means of communication operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States," as well as by "hinder[ing] or delay[ing] the transmission of any communication" over such means of communication. This statute could apply if UAS detection and/or mitigation operations willfully or maliciously degrade or otherwise hinder any frequency or transmissions, including cellular or WiFi signals, with a demonstrable use or intended use by the military or by SLTT law enforcement or emergency personnel engaged in civil defense functions.

Finally, it is possible for mitigation capabilities that destroy, seize, or exercise control of a UAS to implicate federal criminal laws that otherwise apply to "aircraft," as that term is statutorily defined. While all kinetic solutions will likely have one or more of these capabilities implicating those laws, non-kinetic solutions should also be evaluated for compliance.

---

[11] Authorized radio communications include radio communications operating pursuant to federal authorizations or FCC licenses and those operating without a license but pursuant to FCC rules.

[12] The statute exempts the "lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State." 18 U.S.C. § 1030(f).

[13] *See id.* § 1030(e)(1), (2).

[14] The statute exempts "any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or of an intelligence agency of the United States." *Id.* § 1367(b).

- The Aircraft Sabotage Act, 18 U.S.C. § 32(a), criminalizes certain destructive actions with respect to "aircraft," including damaging, destroying, or disabling those aircraft.

- The Aircraft Piracy Act, 49 U.S.C. § 46502, criminalizes the act of seizing or exercising control of an "aircraft" with "wrongful intent." An intent to seize or exercise control of an aircraft without the legal authorization to do so could involve wrongful intent.

II. Additional Federal Laws Relating to Aviation and Spectrum

In addition to implicating federal criminal laws, the acquisition, installation, testing, and use of UAS detection or mitigation technologies may implicate laws and regulations administered by the FAA and the FCC relating to aviation and RF spectrum. UAS response measures may also implicate existing aviation security laws and regulations administered by the Transportation Security Administration (TSA).

A. Laws Relating to Aviation Safety and Efficiency[15]

Non-federal entities should evaluate UAS detection activities for compliance with laws and regulations administered by the FAA, including but not limited to the following:

[15] This subsection is limited to the discussion of UAS detection systems because, as previously indicated, only certain federal agencies have been expressly authorized by Congress to mitigate UAS notwithstanding certain federal laws. The FAA does not support the use of mitigation systems by any entities that do not have express authority from Congress.

- Use of Airspace. 49 U.S.C. § 40103 establishes a public right of transit through the navigable airspace and vests the FAA with authority to ensure the safety of aircraft and the efficient use of airspace. This includes ensuring that compliant aircraft (including UAS) may move through the airspace without improper interference. For example, detection systems may lead to the identification of both legitimate airspace users as well as unlawful activity. Additional analysis is necessary to identify whether an operation identified by a detection system is in violation of FAA regulation before engaging in an operational response. This also includes identifying and working to address any potential collateral impacts of detection technology or systems on the safe and efficient operation of the National Airspace System.

- Airport Operating Certificates. 49 U.S.C. § 44706, as implemented by 14 CFR Part 139, prescribes the rules governing the certification and operation of airports in the United States. Holders of Airport Operating Certificates issued under 14 CFR Part 139 must protect navigational aids. *See* 14 CFR § 139.333. Commercial service airport operators may also need to update the contents of their airport certification manuals to include operating procedures for the use of a UAS detection system. *See id.* § 139.203. Moreover, the installation or use of UAS detection systems by sponsors of commercial service airports may also implicate other regulatory requirements under CFR Title 14. The FAA has provided extensive information to airport sponsors, which can be accessed at: https://www.faa.gov/airports/airport_safety/#SafetyGuidance.

- Structures Interfering with Air Commerce. 49 U.S.C. § 44718, as implemented in 14 CFR Part 77, requires entities proposing construction or alteration of existing structures in the vicinity of an airport to provide the FAA with notice. *See also* FAA Order 7400.2M, Procedures for Handling Airspace Matters (Feb. 28, 2019). The required notice allows the FAA to conduct an aeronautical study of the potential for the proposed structure and any electromagnetic broadcast signals to create a hazard to air navigation, including interference with aircraft and navigational aids.[16] Entities seeking to install or use equipment for UAS detection activities should also evaluate whether 14 CFR Part 77 requires them to provide the FAA with advance notice of proposed construction or alteration.

- Project Grant Application Approval Conditioned on Assurances About Airport Operations. 49 U.S.C. § 47107 establishes obligations for recipients of grant funds for an airport development project to maintain and operate airport facilities safely and efficiently and in accordance with specified conditions. Airports subject to such conditions may need to ensure that the installation or use of a UAS detection system does not introduce a hazard that cannot be mitigated, consistent with applicable grant assurance obligations, such as Grant Assurance 20, Hazard Removal and Mitigation. In addition, such airports may need to ensure that UAS detection systems and associated structures are accurately reflected in the Airport Layout Plan consistent with Grant Assurance 29, Airport Layout Plan.

For additional information concerning these laws, please contact the Office of National Security Programs and Incident Response at the FAA.

[16] Non-federal entities are encouraged to independently validate the performance and characteristics of UAS detection systems being considered. Significant deviations between vendor claims and real world operation, including the potential for RF emissions and interference, have been observed by the FAA.

B. Laws Relating to Transportation/Airport Security

Through its broad authorities, the TSA oversees the implementation and ensures the adequacy "of security measures at airports and other transportation facilities." 49 U.S.C. § 114(f)(11). TSA may also take appropriate action to address threats, including coordination of security measures with other agencies and to impose requirements on transportation stakeholders, through regulations, security directives, emergency amendments, and security programs. *See* 49 U.S.C. § 114(f)(4) & (l)(1)-(2); 49 U.S.C. § 44932; 49 CFR § 1542.105(d), 1542.303, 1544.305, 1544.105(d), 1546.105(d).

Airports seeking to deploy, buy, or purchase UAS detection or mitigation systems should consider laws, regulations, and security requirements related to local aviation security response. For example, TSA regulations require each operator of an airport regularly serving air carriers to establish an air transportation security program (ASP). *See* 49 U.S.C. §§ 114 and 44903; 49 CFR Part 1542. Among other requirements, the ASP must provide law enforcement personnel in the number and manner adequate to support the program. 49 CFR § 1542.215. In addition, TSA's enforcement authorities include the ability of the Administrator, in consultation with the airport operator and law enforcement authorities, to order the deployment of personnel at any secure area of the airport to counter threats to aircraft and aircraft operations or to address national security concerns, such as those posed by UAS. 49 U.S.C. § 44903(h)(1).

For additional information or coordination, please contact your local TSA Federal Security Director.

C. Laws Relating to the Radiofrequency Spectrum

Any systems that involve emission of radio waves, including radar, must be evaluated for compliance with laws and regulations administered by the FCC, including but not limited to the following:

- Authorizations for Use of Spectrum. Authorized non-federal radio communications include unlicensed operations and operations on frequencies requiring individual licenses.
    - Transmissions on frequencies authorized for unlicensed operations, such as common WiFi and Bluetooth frequencies, do not require a license but may nevertheless implicate statutory or regulatory prohibitions against harmful interference as well as other requirements.
    - Operating on a frequency allocated for licensed private-sector use (such as on the bands used by mobile phones) is subject to licensing requirements and other regulation at the federal level. *See* 47 U.S.C. § 301.
        - For example, use of radar to detect UAS requires a Radiolocation Service license from the FCC. General guidance regarding how to prepare and file an application is available at https://www.fcc.gov/wireless/bureau-divisions/mobility-division/industrial-business/industrial-business-licensing. The application must identify the locations and frequencies where the applicant proposes to operate as well as provide other technical information. Equipment vendors may be able to assist with gathering this information. No prior frequency coordination is required, but if the applicant proposes to operate near a U.S. Government facility, it may wish to consult with appropriate Federal officials before applying in order to avoid having the application rejected when the FCC conducts its Federal coordination.

- Marketing, Sale, or Operation of Jammers. 47 U.S.C. § 302a prohibits most non-federal entities from manufacturing, importing, shipping, selling, or using devices that fail to comply with FCC regulations regarding devices that can interfere with radio reception, including transmitters designed to block, jam, or interfere with wireless communications. 47 U.S.C. § 302a(b).

- Interference with Radio Communications. 47 U.S.C. § 333 prohibits "willfully or maliciously interfer[ing] with or caus[ing] interference to any radio communications of any station licensed or authorized by [the FCC] or operated by the United States Government."

Guidance disclaimer: This advisory is provided for informational purposes only. Guidance documents, like this document, are not binding and lack the force and effect of law, unless expressly authorized by statute or expressly incorporated into a contract, grant, or cooperative agreement. Consistent with Executive Order 13891 and the Office of Management and Budget implementing memoranda, the issuing Departments will not cite, use, or rely on any guidance document that is not accessible through the issuing Departments' guidance portals, or similar guidance portals for other Executive Branch departments and agencies, except to establish historical facts. To the extent any guidance document sets out voluntary standards (*e.g.*, recommended practices), compliance with those standards is voluntary, and noncompliance will not result in enforcement action. Guidance documents may be rescinded or modified in the issuing Departments' complete discretion, consistent with applicable laws.

From: Collins, Jimmie L

To: Adam Arkin; Ashley Doyle; Bennett Strobel; Brandon Kumalae; Brandon M Youngblood; Brent Parks; Brian Keith; Bryan D Marcial; Charles (Chan) Frye; Christopher Bubb; Christopher Church; Daniel Braithwaite; Daniel Ford; Dax Balonze; Dustin Miller; Frank Lopez; Gary Johnson; Gene Fujimoto; Gregory Mills; Jason Mesquinto; Jeff Shimooka; Jeremy Gilbert; Jesse Collins; Jessica Pouya; Joe Cotter; John Woodcock (JIC); Jonathan Hall; Jordan Bevan; Kelly Lockie; Kevin Ishii; Kimberly Bailey; Kyle Lee; Lance Ishikawa; Mark Ellis; Michael Hall; Mike H; Nathaniel Mendoza; Nicholas Ortiz; Paul Hoock; Sean Kim; Shane Hamamoto; Shawn Acosta; Steve Sheaks; Trevor Ohnesorge; Weldon Jensen; Giovanni Williams; Jeremy Hall; Patrick Paul

Cc: Collins, Jimmie L; Lay, Stephanie; NCON PACIFIC CUAS; Zerbe, Tiana

Subject: C-UAS Working Group

Attachments: OKNG CUAS Symposium 2025 MOI.pdf

Happy New Year!

I recently sent an email validation note to our membership (27 Dec 24). Please make sure to let me know if we need to take you off our roster – otherwise you are good to go.

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room – if you intend to join us please let me know directly so I can monitor our capacity.

Agenda

* Guest speaker Rodney Takahashi, C-sUAS Program Manager, USINDOPACOM

* DOD Announces Strategy for Countering Unmanned Systems In early December, Secretary of Defense Austin signed a classified Strategy for Countering Unmanned Systems. The strategy unifies the Department's approach to countering these systems that looks across domains, characteristics, and timeframes. The recent designation of the Commanders of NORTHCOM and INDOPACOM as the lead synchronizers for operations to counter-UAS in the homeland is also intended to ensure a cohesive approach. The press release can be found here <https://eur01.safelinks.protection.office365.us/?url=https%3A%2F%2Fwarfarefocus.com%2F=3%2F__https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3986597%2Fdod-announces-strategy-for-countering-unmanned-systems%2F__%3B!!LIYSdFfckKA!xmCmqBHdVaUGMkO9vzbV3cCFAYBbVCWDDZz0bcBswdDa1-a-I-mq2XKmZ2OiP-Hi-cF7wCJmdZ6O2SKxSMWTvFMe5k4jd%24&data=05%7C02%7Cmdney.y.takahashi.civ%40mc.navy.mil%7C31cae9b8bfeb41575dc208dd18a3afd1%7Cc3333c00c8774bf7b6ad45e942de1750%7C0%7C0%7C638693815506706452%7CUnknown%7CTWFpbGZsb3dEey J9IjoiMC4wLjAwMDAiLCJQIjoiV2inMzEiLCJBTiI6IkJhaWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=3n7ILPUhzSXnKX1Nhe1%2FN2vLSNnI7%2B0%2FmDmC9uY6g=%3D&reserved=0>

* Incident reporting

* Suspected Chinese underwater spy drone found by fishermen Officials said the drone was not armed, but the police report listed "potential national security implications" as one significance of its recovery. https //apple.news/Aew5m2y9KTj69OOpbiqUScg <https //urldefense.com/v3/__https /apple.news/Aew5m2y9KTj69OOpbiqUScg__;! LIYSdFfckKA!0Kr_37LxZ3vY24-QXcqk2QkZNevpRyJtXV0LHNDJjaVjr1hlliYZCjpr1Slq2EYRV3GlF2lkHpeyDB5xuugs4eYLrsT54S>

* Events

* The INTERPOL CUAS Exercise Report Can be found here https //www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf <https //urldefense.com/v3/__https /www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf__;! LIYSdFfckKA!yiloMWdGqMaBhAXAPvJQBYaFXiPoqmTiZmGiq5Bt54vOUDjSCI_KYjTPL6SSZqWcYIRtXVd-wyEGSI51MHm_Uvfid7oQS>
* The INTERPOL Red Hike Teaming Report (Qatar World Cup) https //www.interpol.int/en/content/download/20515/file/Guidelines%20for%20Evaluation%20in%20C-UAS%20Capabilities-October%202023.pdf <https //urldefense.com/v3/__https /www.interpol.int/en/content/download/20515/file/Guidelines*20for*20Evaluation*20in*20C-UAS*20Capabilities-October*202023.pdf__;JSUlSUlSUlU! LIYSdFfckKA!yiloMWdGqMaBhAXAPvJQBYaFXiPoqmTiZmGiq5Bt54vOUDjSCI_KYjTPL6SSZqWcYIRtXVd-wyEGSI51MHm_VHXqvPqQ>
* In 2025 INTERPOL will have a dedicated CUAS event is Europe (1/2nd Qtr. 2025) and in USA (3rd Qtr. 2025) with the INTERPOL Drone Expert Summit scheduled for Nov 2025
* National Guard ace <https //hawaiioimt.sharepoint.com/ b /r/teams/LAWOHS/Shared%20Documents/Planning/Goal%204%20Cmor%20Programs%20(CT-TVP-Cyber-CI-Emerging-COOP)/4.07%20Develop%20an%20emerging%20threats%20program/01-Unmanned%20Aerial%20Systems-UAS/2025%2001%2016%20CUAS%20WG/OKNG%20CUAS%20Symposium%202025%20MOI.pdf?csf=1&web=1&e=HuPguO> atch d

* Policy

* The INTERPOL Drone Forensics Framework https //www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf <https //urldefense.com/v3/__https /www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf__;! LIYSdFfckKA!yiloMWdGqMaBhAXAPvJQBYaFXiPoqmTiZmGiq5Bt54vOUDjSCI_KYjTPL6SSZqWcYIRtXVd-wyEGSI51MHm_W85Xuhw$>
* CUAS - Project Courageous created a standard for selecting testing and assessing CUAS for law enforcement use and this is now a voluntary standard https //standards.cencenelec.eu/dyn/www/f?p=CEN 110 0 FSP PROJECT,FSP ORG ID 80540,1321045&cs=1F5B9ABA977D16C970B42CB8F86055 01D <https //urldefense.com/v3/__https /standards.cencenelec.eu/dyn/www/f?p=CEN 110 0 FSP PROJECT,FSP ORG ID 80540,1321045&cs=1F5B9ABA977D16C970B42CB8F86055 01D__;! LIYSdFfckKA!yiloMWdGqMaBhAXAPvJQBYaFXiPoqmTiZmGiq5Bt54vOUDjSCI_KYjTPL6SSZqWcYIRtXVd-wyEGSI51MHm_X0eWtskQ$>

v/r

jc

Ms. Jimmie L Collins

Chief, Planning and Operations

State Security Clearance POC

Protected Critical Infrastructure Information (PCII) Officer

CISA Gateway Administrator - Hawai'i

Hawai'i Office of Homeland Security

3949 Diamond Head Road, Honolulu HI 96816

[redacted] <mailto:[redacted]>

office: [redacted]

cell: [redacted]

Office of Homeland Security (hawaii.gov) <https //law.hawaii.gov/oha/>

Microsoft Teams Need help? <https //aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now [redacted]

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-485[redacted] <tel +18088294485[redacted]> United States, Honolulu

Find a local number [redacted]>

Phone conference ID: [redacted]

For organizers Meeting options [redacted] > | Reset dial-in PIN <https //dialin.teams.microsoft.com/usp/pstnconferencing>

OKLAHOMA ARMY NATIONAL GUARD
JOINT FORCE HEADQUARTERS
3501 NE MILITARY CIRCLE
OKLAHOMA CITY, OK 73111

NGOK-DMS 21 November 2024

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Memorandum of Instruction, 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

1. General: The Oklahoma National Guard and the Oklahoma Aerospace Institute for Research and Education (OAIRE) host the Unmanned Aerial Systems / Launched Effects Symposium on 21-22 January 2025 in Oklahoma City, Oklahoma.

2. Objective: The Symposium will bring together Academic, Industry, Department of Defense and Interagency experts to discuss defense capabilities, challenges, and opportunities in the future of UAS and Launched Effects.

3. Agenda: The Symposium will take place over two days. Day One of the event will be held at Oklahoma State University Hamm Institute for American Energy (300 NE 9th St., Oklahoma City, OK 73104). Day Two will be held in a classified setting at the 137th Special Operations Air Wing (Will Rogers Air National Guard Base, 7100 Terminal Drive, Oklahoma City, OK 73159). *Security clearance will be required to attend Day Two.*

Day One (Tuesday, 21 January 2025)
0800: Doors Open
0845: Welcome, Orientation & Introduction
0900 to 1130: Morning Presentations & Discussions
1130 to 1300: Lunch
1300 to 1600: Afternoon Presentations
1600 to 1800: Networking Event

Day Two (Wednesday, 22 January 2025)
0800: Doors Open
0845: Welcome, Orientation & Introduction
0900 to 1145: Presentations & Discussions
1145 to 1200: Closing Comments

4. Security Clearance Verification**.** All Day Two participants should have their respective security professionals complete the following instructions: Day Two briefings will be held at the SECRET level. Please ensure that all the principal attendees have a valid “US Access” SECRET clearance and are properly indoctrinated. Additionally, please ensure that valid

NDA/NDS/Attestation dates are documented in the Defense Information System for Security (DISS).

Reason for Visit: UAS Symposium
Visit Access: Secret

First Day of Visit: 2025 01 22
Last Day of Visit: 2025 01 22

POC: Rian Keylon
POC Phone: [redacted]
SSO Email: [redacted]
Visited SMO: ANG 137 IP – INFO PROTECTION-ANG 137 IP-137
Additional Information: 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

For those outside the DoD:

Please include: "2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium" (in subject line)
Visit details:
Full name
Grade
Title
Social security number Organization name
Address
Security clearance type
Issue date
Visit details

Visit location: [redacted]

Purpose: 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

5. Transportation & Parking: Attendees are responsible for their travel from home station to lodging location, symposium venue, and any other necessary in/around travel.

6. Uniform and Dress:

a. Military attendees: Duty Uniform or Business Casual

b. Civilian attendees: Business Casual

7. Registration: To register for the Symposium please copy and paste the following into your browser. All interested attendees are welcome to attend Day One. If you have a Secret Clearance and are interested in attending the classified briefs on Day Two, please register for both days.

a. **Day One Registration**
Select the text link above or copy and paste the following URL:

https://www.eventbrite.com/e/2025-unmanned-aerial-systems-launched-effects-symposium-day-one-tickets-1082306149829

b. **Day Two Registration**
Select the text link above or copy and paste the following URL:

https://www.eventbrite.com/e/2025-unmanned-aerial-systems-launched-effects-symposium-day-two-tickets-1090024234829?aff=oddtdtcreator

8. Point of Contact for additional information is Mr. Adam Headrick (J5 Plans) at [redacted].

SHANE I. RILEY
COL, IN
Director, UAS / LE

From: Collins, Jimmie L

To: Adam Arkin; Ashley Doyle; Bennett Strobel; Brandon Kumalae; Brandon M Youngblood; Brent Parks; Brian Keith; Bryan D Marcial; Charles (Chan) Frye; Christopher Bulich; Christopher Church; Daniel Ford; Daniel Wrasse; Daniel Zimmerman; Eric Hiraoka; Erik Swenson; Fred Kamahele; Jake Kawabata; Jason Ellis; Jeremy Ellis; Jesse Kaiwi; John Woodruff; Jr; Kendall Lopez; Kerry Loshy; Kevin Clark; Kiley Andrade; Robert Ohnemus; Sarah Jones; Shane Reeder; Shawn Arita; Trevor Ohnstad; Weldon Jones; Jr; Sean Nahale

Subject: OKNG Working Group

Attachments: OKNG CUAS Symposium 2025 MOI.pdf

Happy New Year!

I recently sent an email validation note to our membership (27 Dec 24). Please make sure to let me know if we need to take you off our roster – otherwise you are good to go.

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room – if you intend to join us please let me know directly so I can monitor our capacity.

Agenda

* Guest speaker Rodney Takahashi, C-sUAS Program Manager, USINDOPACOM

* DOD Announces Strategy for Countering Unmanned Systems In early December, Secretary of Defense Austin signed a classified Strategy for Countering Unmanned Systems. The strategy unifies the Department's approach to countering these systems that looks across domains, characteristics, and timeframes. The recent designation of the Commanders of NORTHCOM and INDOPACOM as the lead synchronizers for operations to counter-UAS in the homeland is also intended to ensure a cohesive approach. The press release can be found here <https://usg01.safelinks.protection.office365.us/?url=https%3A%2F%2Fwarfidefense.com%2Fr=39%2F__https%3A%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3986597%2Flod-announces-strategy-for-countering-unmanned-systems%2F__%3Bl!!LIYSdFfckKA!zmCmqIHuIVuUGMdO5vcsAVs2CFaYB6YCWDDZzDbedIkwodDuU-a-I-zuq2XKm2ZOOP-H-cF7wC3mdZb5O25KcSbMWTeFMe3k4Uj9%24&data=05%7C02%7Ccodney.p.takahashi.civ%40us.navy.mil%7C313cee9b8bfe84157bdc208dd13a3a0f1%7Cc3333a4f0cf8774b87b6ad45e942de1750%7C0%7C0%7C638693815506706452%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C%7C&sdata=3u7ILPUbx8XdKX7bNrc1%2FN2zLSNnT%2B9%2FmEbmC9tgV0qc%3D&reserved=0> .

* Incident reporting

* Suspected Chinese underwater spy drone found by fishermen Officials said the drone was not armed, but the police report listed "potential national security implications" as one significance of its recovery. https://apple.news/Aew5m2y9KTj69OOpbiqUSzg <https://urldefense.com/v3/__https://apple.news/Aew5m2y9KTj69OOpbiqUSzg__;!!LIYSdFfckKA!0Ke_37LzZ3uY24-QXeqb2Q2Nzvp8yJ8XV9LHNDJipVjz0hhlYZC/pp1hlq2EYRVIGlF2lkHgoyDB5oauqp4eYLzuT54S>

* Events

* The INTERPOL CUAS Exercise Report Can be found here https://www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf <https://urldefense.com/v3/__https://www.interpol.int/content/download/17737/file/CUAS_Interpol_Low_Final.pdf__;!!LIYSdFfckKA!ylioMWdGipMaBhAXAPvJQBYaFXfPoqmTiIZmGq5Bl654v0UDjSCI_KYjTPL6SSDqWcYfRtkXVd-wyEGSI51MHm_Uvfld7oQS>
* The INTERPOL Red/Blue Teaming Report (Qatar World Cup) https://www.interpol.int/ar/content/download/20515/file/Guidelines%20for%20Testing%20and%20Evaluation%20of%20C-UAS%20Capabilities-October%202023.pdf <https://urldefense.com/v3/__https://www.interpol.int/ar/content/download/20515/file/Guidelines*20for*20Testing*20and*20Evaluation*20of*20C-UAS*20Capabilities-October*202023.pdf__;!!LIYSdFfckKA!ylioMWdGipMaBhAXAPvJQBYaFXfPoqmTiIZmGq5Bl654v0UDjSCI_KYjTPL6SSDqWcYfRtkXVd-wyEGSI51MHm_VHXqPbg$>
* In 2025 INTERPOL will have a dedicated CUAS event is Europe (1/2nd Qtr. 2025) and in USA (3rd Qtr. 2025) with the INTERPOL Drone Expert Summit scheduled for Nov 2025
* National Guard see <https://hawaiiontd.sharepoint.com/ b /s/teams/LAWOHS/Shared%20Documents/Planning/Goal%204%20-%20Cmn%20Programs%20(CT-TVP-Cyber-CI-Emerging-COOP)/4.07%20Develop%20an%20emerging%20threats%20program/01-Unmanned%20Aerial%20Systems-UAS/2025%2001%2016%20CUAS%20WG/OKNG%20CUAS%20Symposium%202025%20MOI.pdf?csf=1&web=1&e=HuPgoO> atch d

* Policy

* The INTERPOL Drone Forensics Framework https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf <https://urldefense.com/v3/__https://www.interpol.int/content/download/15298/file/DFL_DroneIncident_Final_EN.pdf__;!!LIYSdFfckKA!ylioMWdGipMaBhAXAPvJQBYaFXfPoqmTiIZmGq5Bl654v0UDjSCI_KYjTPL6SSDqWcYfRtkXVd-wyEGSI51MHm_W8SXuhwS>
* CUAS - Project Courageous created a standard for selecting testing and assessing CUAS for law enforcement use and this is now a voluntary standard https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:80540,3321045&cs=1F5B9ABA977D16C97#B42CB8F86055 01D <https://urldefense.com/v3/__https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:80540,3321045&cs=1F5B9ABA977D16C97#B42CB8F86055 01D__;!!LIYSdFfckKA!ylioMWdGipMaBhAXAPvJQBYaFXfPoqmTiIZmGq5Bl654v0UDjSCI_KYjTPL6SSDqWcYfRtkXVd-wyEGSI51MHm_X8o9vkrQS>

vir

jc

Ms. Jimmie L Collins

Chief, Planning and Operations

State Security Clearance POC

Protected Critical Infrastructure Information (PCII) Officer

CISA Gateway Administrator - Hawai'i

Hawai'i Office of Homeland Security

3949 Diamond Head Road, Honolulu HI 96816

[redacted] <mailto:[redacted]

office: [redacted]

cell: [redacted]

Office of Homeland Security (hawaii.gov) <https://law.hawaii.gov/oha/>

Microsoft Teams Need help? <https://aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now [redacted]

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-485[redacted] <tel:+18088294853,,[redacted] United States, Honolulu

Find a local number [redacted]

Phone conference ID: [redacted]

For organizers Meeting options [redacted] | Reset dial-in PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

OKLAHOMA ARMY NATIONAL GUARD
JOINT FORCE HEADQUARTERS
3501 NE MILITARY CIRCLE
OKLAHOMA CITY, OK 73111

NGOK-DMS 21 November 2024

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Memorandum of Instruction, 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

1. General: The Oklahoma National Guard and the Oklahoma Aerospace Institute for Research and Education (OAIRE) host the Unmanned Aerial Systems / Launched Effects Symposium on 21-22 January 2025 in Oklahoma City, Oklahoma.

2. Objective: The Symposium will bring together Academic, Industry, Department of Defense and Interagency experts to discuss defense capabilities, challenges, and opportunities in the future of UAS and Launched Effects.

3. Agenda: The Symposium will take place over two days. Day One of the event will be held at Oklahoma State University Hamm Institute for American Energy (300 NE 9th St., Oklahoma City, OK 73104). Day Two will be held in a classified setting at the 137th Special Operations Air Wing (Will Rogers Air National Guard Base, 7100 Terminal Drive, Oklahoma City, OK 73159). *Security clearance will be required to attend Day Two.*

Day One (Tuesday, 21 January 2025)
0800: Doors Open
0845: Welcome, Orientation & Introduction
0900 to 1130: Morning Presentations & Discussions
1130 to 1300: Lunch
1300 to 1600: Afternoon Presentations
1600 to 1800: Networking Event

Day Two (Wednesday, 22 January 2025)
0800: Doors Open
0845: Welcome, Orientation & Introduction
0900 to 1145: Presentations & Discussions
1145 to 1200: Closing Comments

4. Security Clearance Verification**.** All Day Two participants should have their respective security professionals complete the following instructions: Day Two briefings will be held at the SECRET level. Please ensure that all the principal attendees have a valid “US Access” SECRET clearance and are properly indoctrinated. Additionally, please ensure that valid

NDA/NDS/Attestation dates are documented in the Defense Information System for Security (DISS).

Reason for Visit: UAS Symposium
Visit Access: Secret

First Day of Visit: 2025 01 22
Last Day of Visit: 2025 01 22

POC: Rian Keylon
POC Phone: [redacted]
SSO Email: [redacted]
Visited SMO: ANG 137 IP – INFO PROTECTION-ANG 137 IP-137
Additional Information: 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

For those outside the DoD:

Please include: "2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium" (in subject line)
Visit details:
Full name
Grade
Title
Social security number Organization name
Address
Security clearance type
Issue date
Visit details

Visit location: [redacted]

Purpose: 2025 Oklahoma National Guard Unmanned Aerial Systems / Launched Effects Symposium

5. Transportation & Parking: Attendees are responsible for their travel from home station to lodging location, symposium venue, and any other necessary in/around travel.

6. Uniform and Dress:

a. Military attendees: Duty Uniform or Business Casual

b. Civilian attendees: Business Casual

7. Registration: To register for the Symposium please copy and paste the following into your browser. All interested attendees are welcome to attend Day One. If you have a Secret Clearance and are interested in attending the classified briefs on Day Two, please register for both days.

a. **Day One Registration**
Select the text link above or copy and paste the following URL:

https://www.eventbrite.com/e/2025-unmanned-aerial-systems-launched-effects-symposium-day-one-tickets-1082306149829

b. **Day Two Registration**
Select the text link above or copy and paste the following URL:

https://www.eventbrite.com/e/2025-unmanned-aerial-systems-launched-effects-symposium-day-two-tickets-1090024234829?aff=oddtdtcreator

8. Point of Contact for additional information is Mr. Adam Headrick (J5 Plans) at [redacted].

SHANE I. RILEY
COL, IN
Director, UAS / LE

From: Collins, Jimmie L

To: [redacted]; Shawn Acosta [redacted]; [redacted]; Ray Andrade [redacted]; [redacted]; Adam Arluke [redacted]; [redacted]; Baggs, Kevin L; Keolani Bailey [redacted]; Dax Bajema [redacted]; Christopher Ballog [redacted]; [redacted]; Cory S. Brailsford [redacted]; Craig Burns [redacted]; Christopher Butch [redacted]; [redacted]; [redacted]; [redacted]; Daniel Carreiro [redacted]; [redacted]; Robert Caulfield [redacted]; [redacted]; Cullen Chong [redacted]; Christopher Church [redacted]; Randy Clark [redacted]; Collins, Jimmie L; [redacted]; Coronel, Romel M; [redacted]; Joseph Doyle [redacted]; Fred Edwards [redacted]; [redacted]; [redacted]; Daniel Ford [redacted]; Jon Franquez [redacted]; Charles (Chaz) Frye [redacted]; Robin (Chris) Grant [redacted]; Jonathon Grems [redacted]; [redacted]; Isra Harahap [redacted]; Scott Higbee [redacted]; [redacted]; [redacted]; Nic Iannarone [redacted]; [redacted]; [redacted]; Kenn Ishida [redacted]; Sarah Jacob [redacted]; [redacted]; Weldon James [redacted]; Diego Jarrin [redacted]; [redacted]; [redacted]; Brian Keith [redacted]; Scott Klein [redacted]; Brandon Kumalae [redacted]; [redacted]; [redacted]; Kerry Looby [redacted]; Kendall Lopez [redacted]; Marciel, Bryan D; Lisa McGahan [redacted]; Humberto Antonio (Mac) Mclaren Jr [redacted]; Eric Mitsuyoshi [redacted]; Erik Modisett [redacted]; Nahale, Sean S; [redacted]; Trevor Ohnstad [redacted]; [redacted]; [redacted]; Pace, Frank J; Brent Parks [redacted]; Giovan Patalano [redacted]; Craig Petersen [redacted]; [redacted]; [redacted]; Shane Reagan [redacted]; Jordan Reigel [redacted]; [redacted]; [redacted]; [redacted]; [redacted]; Jason Scoles [redacted]; [redacted]; [redacted]; Eric Shimodoi [redacted]; [redacted]; Jon Strandhagen [redacted]; Bennett Strobel [redacted]; [redacted]; Gen Tamura [redacted]; Dustin Truax [redacted]; John Udani [redacted]; [redacted]; [redacted]; Wade, Kathleen N; [redacted]; Giovanni Williams - US Federal Government [redacted]; John Woodruff - US Federal Government [redacted]; [redacted]; [redacted]; [redacted]; Jeremy Young [redacted]; Lee Zawacki [redacted]; [redacted]

Subject: C-UAS Working Group

Attachments: Incident Brief - Recovery of sUAS Dropped Munitions Ocean Springs MS (002).pdf

---

For this upcoming quarterly, we have space to host 25 folks in-person at our conference room (in the location block above) – if you intend to join us in person please let me know directly so I can monitor our capacity.

Notional Agenda (pending speaker confirmations):

* Guest speaker(s):

 * [tentative] DHS/CISA HQ
 * [tentative] John Abbey – SafeFlight update
 * [tentative] FBI

* Incident reporting: Reference attached.
* Events/Training:
* Policy: Prior to our meeting I will reach out to working group members to solicit interested parties for further development of the below lines of effort from previous meeting and will save space here for dialogue on agreeable path forward to pursue

 * Policy: What topics require intergovernmental leadership dialogue, what leaders/organizations should be engaged, what policies/laws are needed?
 * Reporting/investigations: what actions/activities will increase air domain awareness, what mechanisms are in place or are needed to be put in place to facilitate compiling and sharing 'the' threat picture, what protocol(s) are needed, what public education can be mounted to diminish instances of 'nuisance' non-nefarious activities?
 * Response Planning: what are the key stakeholder agencies in response, who can action (and can action what/where), what is an appropriate concept of operations?

* News:
* Other/Open Discussion:
* Conclusion:

v/r

jc

Ms. Jimmie L Collins

Chief, Planning and Operations

State Security Clearance POC

Protected Critical Infrastructure Information (PCII) Officer

CISA Gateway Administrator - Hawai'i

Hawai'i Office of Homeland Security

3949 Diamond Head Road, Honolulu HI 96816

[redacted] <[redacted]>

office: [redacted]

cell: [redacted]

Office of Homeland Security (hawaii.gov) <https://law.hawaii.gov/ohs/>

Microsoft Teams Need help? <https://aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now [redacted]
[redacted]>

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-4853,[redacted] <tel:+18088294853,[redacted]> United States, Honolulu

Find a local number <[redacted]>

Phone conference ID: [redacted]

For organizers: Meeting options <[redacted]
[redacted] | Reset dial-in PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

From: Colafati, David
To: Baggs, Kevin L
Subject: [EXTERNAL] RE: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry
Date: Tuesday, May 13, 2025 2:01:19 PM
Attachments: image002.png
image003.png

Kevin,

HSI does not have an open investigation in reference to the below.

Please let me know if there is anything else you need.

Dave
David J. Colafati
Intelligence Group Supervisor
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: HSFC <hsfc@hawaii.gov>
Sent: Friday, February 28, 2025 11:40 AM
To: Colafati, David [redacted]>
Cc: HSFC <hsfc@hawaii.gov>; Baggs, Kevin L [redacted]>
Subject: Re: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Please use the Cofense Report Phishing button to report. If the button is not present, click here and follow instructions.

Acting Chief David Colafati

Good morning, sir,

Thank you for taking my call today. As we discussed, we are sharing the below tip regarding alleged financial fraud activity being observed in Honolulu.

The attachment is the flyer enclosed in the HSIN Exchange RFI:

[redacted] HSI BOLO - Project Red Hook

Export

LA-SAFE is disseminating the attached BOLO to Fusion Centers nationwide on behalf of HSI. Questions can be directed to Homeland Security Investigations (HSI) at GCFraud@hsi.dhs.gov or (800-973-2867) / 800-X-Sector.

I called the number above this morning and was directed to reach out to our local HSI Field Office for information/matters concerning the BOLO. The HSFC is interested in producing and distributing a Situation Awareness Bulletin for our LE and Private Sector stakeholders. We will wait for further information before doing so.

Very respectfully,

C. Dale Cites
Operations / Intelligence Analyst
Work Cell [redacted]

Hawaii State Fusion Center
hsfc@hawaii.gov
https://hsfc.hawaii.gov

"If you see something, Say something" TM

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

From: Baggs, Kevin L [redacted]>
Sent: Tuesday, February 25, 2025 4:57 PM
To: HSFC <hsfc@hawaii.gov>
Subject: FW: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry

Hi all,

See below as a local vendor reported the scam outlined below to the [redacted] who then passed it on to me.

Kevin

From: [redacted]
Sent: Monday, February 24, 2025 9:27 AM
To: Baggs, Kevin L [redacted]>
Subject: [EXTERNAL] FW: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry
Importance: High

Aloha, e Kevin,

Thank you for taking my call and helping us appropriately vet and share the concern from one of our tour operators [redacted] has said if you folks have any questions or one of the agencies need to follow up [redacted]s willing to help and its happened to more than one of their customers.

Mahalo,

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

From: [redacted]
Sent: Friday, February 21, 2025 6:56 PM
To: [redacted]
Subject: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry

Aloha e [redacted],

Have you heard more and more local businesses are complaining about fraudulent chargebacks? My name is [redacted], and I am a local business owner representing [redacted], the [redacted] in Hawaii, located on Oahu. I am reaching out to request [redacted] assistance in raising broader awareness about an increasingly sophisticated scam operation targeting Hawaii's tourism industry.

It is my kuleana to share with you my findings. Orchestrated through the Chinese social media platforms "Little Redbook" (小紅书) and "RedNotes," these fraudulent operations illegally sell heavily discounted tours and tickets—radically below market rates—for various attractions, including state park entries, Pearl Harbor, whale watching tours, snorkeling tours, scuba tours, and other activities on behalf of local Hawaiian tour operators and even state-operated visitor sites.

How the Scam Works:

1. **Bait & Payment:** Chinese consumers are lured by radically discounted tours and entry tickets advertised on the Little Redbook (小紅书) app and make payments directly to scammers via Chinese cash apps. They provide their legal name and contact information under the impression that they are securing a legitimate booking.
2. **Booking Process:** After receiving payment, the scammer books directly through a legitimate Hawaii tour operator's online booking system (e.g., FareHarbor).
3. **Name Manipulation & Payment Setup:**
   - Before making the online booking, the scammer adds the Chinese consumer as an authorized user on their credit card.
   - The scammer then completes the booking using their own credit card but in the Chinese consumer's legal name.
   - This ensures that the booking system records the Chinese consumer's name and the last four digits of the credit card, making the transaction appear legitimate.
4. **Confirmation & Service Delivery:** The Chinese consumer receives a real booking confirmation email with the tour operator's actual prices, making them believe they secured a great deal.
5. **Tour Participation:** The Chinese consumer checks in and completes the tour as if it were a standard booking.
6. **Post-Tour Chargeback Scam:**
   - After the tour is completed, the scammer removes the Chinese consumer as an authorized user on their credit card.
   - The scammer then files a fraudulent chargeback dispute with their Chinese credit card company, claiming the purchase was unauthorized.
7. **Financial Loss to Local Operators:**
   - Since the booking was made under the Chinese consumer's real name, tour operators have no way to detect the fraud beforehand.
   - In nearly all cases, the Chinese credit card companies side with the scammer, leaving Hawaii's local businesses responsible for chargeback losses.
   - In 2024 alone, [redacted] lost 12 disputes, despite providing clear evidence, contracts, and proof of service delivery.

It is also evident that online tutorials are being provided to Chinese consumers, instructing them on how to exploit this scam process effectively. These guides walk them through every step, from purchasing discounted tickets on the Little Redbook (小紅书) app to filing fraudulent chargeback claims after the tour is completed.

This organized scheme is not just an isolated scam but a systematic and well-documented fraud operation, actively teaching consumers how to cheat Hawaii's tourism businesses without consequences. This sophisticated scam operation is severely impacting Hawaii's tourism businesses. We need urgent action and awareness to protect local operators from these fraudulent schemes.

This scam not only undermines legitimate businesses but also poses significant risks to consumers who may unknowingly purchase invalid or unauthorized tickets. Given the increasing scale and sophistication of these fraudulent activities, I urge [redacted] to investigate and take appropriate measures to protect Hawaii's tourism industry and visitors from falling victim to these deceptive schemes.

Please let me know how we can collaborate to address this issue effectively. I appreciate your time and attention to this urgent matter. I have collected data, emails, screen shots and documents that fully sustain the claim and urgency. To protect the consumer privacy and who has supported the investigation, I am happy to provide all proof to the [redacted] upon further requests.

I have also reported this to the Hawaii local FBI office under IC3.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Happy Connecting on Linkedin

From: HSFC
To: [redacted]
Cc: [redacted]
Subject: Re: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry
Date: Friday, February 28, 2025 11:39:54 AM
Attachments: image.png
image.png
hsi-bolo-project-red-hook-2025-02-27.pdf

Acting Chief David Colafati

Good morning, sir,

Thank you for taking my call today. As we discussed, we are sharing the below tip regarding alleged financial fraud activity being observed in Honolulu.

The attachment is the flyer enclosed in the HSIN Exchange RFI:

[redacted] HSI BOLO - Project Red Hook

Export -

LA-SAFE is disseminating the attached BOLO to Fusion Centers nationwide on behalf of HSI. Questions can be directed to Homeland Security Investigations (HSI) at GCFraud@hsi.dhs.gov or (800-973-2867) / 800-X-Sector.

I called the number above this morning and was directed to reach out to our local HSI Field Office for information/matters concerning the BOLO. The HSFC is interested in producing and distributing a Situation Awareness Bulletin for our LE and Private Sector stakeholders. We will wait for further information before doing so.

Very respectfully,

C. Dale Clites
Operations / Intelligence Analyst
Work Cell [redacted]
[redacted]

Hawaii State Fusion Center
hsfc@hawaii.gov
https://hsfc.hawaii.gov

"If you see something, Say something" TM

From: Baggs, Kevin L <[redacted]>
Sent: Tuesday, February 25, 2025 4:57 PM
To: HSFC <hsfc@hawaii.gov>
Subject: FW: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry

Hi all,

See below as a local vendor reported the scam outlined below to the [redacted] who then passed it on to me.

Kevin

From [redacted]
Sent: Monday, February 24, 2025 9:27 AM
To: Baggs, Kevin L <[redacted]>
Subject: [EXTERNAL] FW: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry
Importance: High

Aloha, e Kevin,

Thank you for taking my call and helping us appropriately vet and share the concern from one of our tour operators. [redacted] has said if you folks have any questions or one of the agencies need to follow up she is willing to help and its happened to more than one of their customers.

Mahalo,

[redacted]

email [redacted]
tel [redacted] fax [redacted]

From: [redacted]
Sent: Friday, February 21, 2025 6:56 PM
To: [redacted]
Subject: Urgent Alert: Organized Chinese Social Network Scam Operation Targeting Hawaii's Tourism Industry

Aloha e [redacted],

Have you heard more and more local businesses are complaining about fraudulent chargebacks? My name is [redacted], and I am a **local business owner representing** [redacted], [redacted] **in Hawaii, located on Oahu.** I am reaching out to request [redacted] **assistance in raising broader awareness** about an increasingly **sophisticated scam operation** targeting Hawaii's tourism industry.

It is my kuleana to share with you my findings. Orchestrated through the **Chinese social media platforms "Little Redbook" (小红书) and "RedNotes," these** fraudulent operations **illegally sell heavily discounted tours and tickets**—radically below market rates—for various attractions, including **state park entries, Pearl Harbor, whale watching tours, snorkeling tours, scuba tours, and other activities** on behalf of local **Hawaiian tour operators** and even **state-operated visitor sites.**

How the Scam Works:

1. **Bait & Payment:** Chinese consumers are lured by **radically discounted tours and entry tickets** advertised on the **Little Redbook (小红书) app** and make payments directly to scammers via Chinese cash apps. They provide their **legal name and contact information** under the impression that they are securing a legitimate booking.
2. **Booking Process:** After receiving payment, the scammer **books directly** through a legitimate **Hawaii tour operator's online booking system** (e.g., FareHarbor).
3. **Name Manipulation & Payment Setup:**
    - Before making the online booking, the scammer **adds the Chinese consumer as an authorized user** on their credit card.
    - The scammer then completes the booking using their **own credit card** but **in the Chinese consumer's legal name.**
    - This ensures that the **booking system records the Chinese consumer's name and the last four digits of the credit card, making the transaction appear legitimate.**
4. **Confirmation & Service Delivery:** The Chinese consumer receives a **real booking confirmation email** with the tour operator's **actual prices**, making them believe they secured a great deal.
5. **Tour Participation:** The Chinese consumer **checks in and completes the tour** as if it were a standard booking.
6. **Post-Tour Chargeback Scam:**
    - After the tour is completed, the **scammer removes the Chinese consumer as an authorized user on their credit card.**
    - The scammer then **files a fraudulent chargeback dispute** with their Chinese credit card company, claiming the **purchase was unauthorized.**
7. **Financial Loss to Local Operators:**
    - Since the booking was made under the **Chinese consumer's real name**, tour operators have **no way to detect the fraud** beforehand.
    - In nearly all cases, the **Chinese credit card companies side with the scammer**, leaving Hawaii's **local businesses responsible for chargeback losses.**
    - In **2024 alone,** [redacted] **lost 12 disputes**, despite providing **clear evidence, contracts, and proof of service delivery.**

It is also evident that online tutorials are being provided to Chinese consumers, instructing them on **how to exploit this scam process** effectively. These guides **walk them through every step**, from purchasing discounted tickets on the **Little Redbook (小红书) app** to **filing fraudulent chargeback claims** after the tour is completed.
This organized scheme is not just an isolated scam but a **systematic and well-documented fraud operation**, actively **teaching** consumers how to **cheat Hawaii's tourism businesses** without consequences. This **sophisticated scam operation is severely impacting** Hawaii's tourism businesses. We need **urgent action and awareness** to protect local operators from these fraudulent schemes.
This scam not only **undermines legitimate businesses** but also poses significant risks to consumers who may unknowingly purchase invalid or unauthorized tickets. Given the increasing scale and sophistication of these fraudulent activities, I urge [redacted] to investigate and take appropriate measures to protect Hawaii's tourism industry and visitors from falling victim to these deceptive schemes.
Please let me know how we can collaborate to address this issue effectively. I appreciate your time and attention to this urgent matter. I have collected data, emails, screen shots and documents that fully sustain the claim and urgency. To protect the consumer privacy and who has supported the investigation, I am happy to provide all proof to the [redacted] upon further requests.
I have also reported this to the Hawaii local FBI office under IC3.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

Happy Connecting on [redacted]

HSI

HOMELAND SECURITY INVESTIGATIONS
is the principal investigative arm of the U.S. Department of Homeland Security, responsible for combating transnational criminal organizations that exploit the global infrastructure through which trade, travel, and finance move.

BOLO

Project Red Hook

An HSI-led, nationwide initiative targeting the abuse of retail gift cards by organized crime groups emanating from the People's Republic of China (PRC) to generate capital for illicit underground banking activities and black-market financial exchange.

Types of Gift Card Fraud

- **Card Tampering:** Criminals steals gift cards then manipulate gift card packaging to steal the card information before the card is sold.
- **Online Attacks:** Criminals gain access to online gift card accounts through phishing or hacking or tap to pay schemes.
- **Victim-Assisted Fraud:** This involves telemarketing groups tricking individuals via phone or online into purchasing gift cards and sharing the redemption codes with the criminals.

Recommended Actions & Procedures

- Ensure gift card fraud is a priority given the severity of the crime.
- Educate law enforcement teams about gift card fraud immediately.
- Coordinate investigation, arrest, and prosecution with retailers and brands.
- After an arrest occurs, share case information with HSI at **GCFraud@hsi.dhs.gov**.

Laken Riley Act

If you are involved in a gift card fraud case and believe the suspect in question is presently in the country illegally and has been charged with, arrested for, convicted of, or admits to having committed acts that constitute the essential elements of burglary, theft, larceny, or shoplifting, please make contact with your local HSI office at **1-800-X-Sector** and reference **Project Red Hook**.

Collaboration

Through collaboration, we can drastically disrupt and eliminate gift card fraud. For more information:

- Contact your local HSI field office
- Email **GCFraud@hsi.dhs.gov**
- Call **1-800-X-Sector** (24/7 assistance)

Scan to learn more about Project Red Hook

From: Colafati, David
To: Flores, David C; "Baggs, Kevin L" <[redacted]>; Beattie, Patricia A; "Bobbitt, Renae - GOV" <[redacted]>; Brehm, Kelly B; Butler, Rhett; Charley, Jay O; "[redacted]"; Dubrall, Jesse L; Fillmore, Mark W; "Gary Yabuta - Hawaii HIDTA ([redacted])"; "Gantt, Racquel A. - GOV" <[redacted]>; "[redacted]"; KIKKAWA, SCOTT K; "Hallstrom, David - GOV" <[redacted]>; "[redacted]"; Huerta, Jonathan (Jon) CIV USCG SEC HONOLULU (USA); LAU CHUNG-YAN; "[redacted]"; "[redacted]"; "Richard Witt" <[redacted]>; Robinson, Jennifer N LT USCG SEC HONOLULU (USA); "[redacted]"; Woodruff, John; Strandhagen, Joh; Nakamoto, Shannon K; Luevano, Eugene; "[redacted]"; Zawacki, Lee; Ganzorig, Togtokhbayar; Ammons, Christian J; Agustin, Heather R; Kaneko, John M (CTR); Ko, Christopher E; Arline III, Napoleon; Fejeran Jr, Robert J; Ward, James H; Beyer, John E; Musso, Erin E; Quintanilla, Meilani L; Duenas, Cristin S; Yoshinaga, Reyn A; Albert, Mary K P; Lansangan, Michael D; Dai, Laura L.V; Faulkner, Ryan K; Cabral-DeArmas, Lucia; Smith, Ryan T; Fujimoto, Kipp K; Waddell, Charles L; Albert, Mary K P; Beagle III, James R; Chambers, James A; Duenas, John S; Faulkner, Ryan K; Flores, Connie M; Harahap, Isra D; Quintanilla, Meilani L; Ramirez, Robert D; Steele, Isaac M; Yoshinaga, Reyn A; Young, Ivan K; Flores, Connie M; Tapia, Victoria A; Duenas, Cristin S; Lorenzo, Gracelyn M; Arzamendi, Mario
Subject: [EXTERNAL] RE: HSI Honolulu Quarterly Intel Brief - April 17, 2025
Date: Thursday, April 17, 2025 12:44:51 PM

Here is the MS Teams link.

HSI Honolulu Quarterly Intel Brief - April 17, 2025, 1430 (HST)

Join the meeting now

Dave
David J. Colafati
Intelligence Group Supervisor
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Colafati, David
Sent: Thursday, April 17, 2025 12:41 PM
To: Flores, David C <[redacted]>; 'Baggs, Kevin L' <[redacted]> <[redacted]>; Beattie, Patricia A <[redacted]>; 'Bobbitt, Renae - GOV' <[redacted]> <[redacted]>; Brehm, Kelly B <[redacted]>; Butler, Rhett <[redacted]>; Charley, Jay O <[redacted]>; [redacted]' <[redacted]>; Dubrall, Jesse L <[redacted]>; Fillmore, Mark W <[redacted]>; 'Gary Yabuta - Hawaii HIDTA ([redacted])' <[redacted]>; 'Gantt, Racquel A. - GOV' <[redacted]> <[redacted]>; [redacted]' <[redacted]>; KIKKAWA, SCOTT K <[redacted]>; 'Hallstrom, David - GOV' <[redacted]> <[redacted]>; [redacted]' <[redacted]>; Huerta, Jonathan (Jon) CIV USCG SEC HONOLULU (USA) <[redacted]>; LAU CHUNG-YAN <[redacted]>; [redacted]' <[redacted]>; '[redacted]' <[redacted]>; [redacted]' <[redacted]>; 'Richard Witt' <[redacted]> <[redacted]>; Robinson, Jennifer N LT USCG SEC HONOLULU

(USA) <[redacted]>; [redacted]'
<[redacted]>; Woodruff, John <[redacted]>; Strandhagen,
Joh <[redacted]>; Nakamoto, Shannon K <[redacted]>;
Luevano, Eugene <[redacted]>; [redacted]'
<[redacted]>; Zawacki, Lee <[redacted]>; Ganzorig, Togtokhbayar
<[redacted]>; Ammons, Christian J <[redacted]>;
Agustin, Heather R <[redacted]>; Kaneko, John M (CTR)
<[redacted]>; Ko, Christopher E <[redacted]>; Arline
III, Napoleon <[redacted]>; Fejeran Jr, Robert J <[redacted]>;
Ward, James H <[redacted]>; Beyer, John E <[redacted]>;
Musso, Erin E <[redacted]>; Quintanilla, Meilani L
<[redacted]>; Duenas, Cristin S <[redacted]>; Yoshinaga,
Reyn A <[redacted]>; Albert, Mary K P <[redacted]>;
Lansangan, Michael D <[redacted]>; Dai, Laura L.V; Faulkner, Ryan K
<[redacted]>; Cabral-DeArmas, Lucia <[redacted]>;
Smith, Ryan T <[redacted]>; Fujimoto, Kipp K
<[redacted]>; Waddell, Charles L <[redacted]>;
Albert, Mary K P <[redacted]>; Beagle III, James R <[redacted]>;
Chambers, James A <[redacted]>; Duenas, John S
<[redacted]>; Faulkner, Ryan K <[redacted]>; Flores, Connie M
<[redacted]>; Harahap, Isra D <[redacted]>; Quintanilla, Meilani
L <[redacted]>; Ramirez, Robert D <[redacted]>; Steele,
Isaac M <[redacted]>; Yoshinaga, Reyn A <[redacted]>; Young,
Ivan K <[redacted]>; Flores, Connie M <[redacted]>; Tapia,
Victoria A <[redacted]>; Duenas, Cristin S <[redacted]>;
Lorenzo, Gracelyn M <[redacted]>; Arzamendi, Mario
<[redacted]>
Subject: HSI Honolulu Quarterly Intel Brief - April 17, 2025

Reminder – The HSI Honolulu Quarterly Intel Brief is being held today via MS Teams at 1430 (HST). The entire brief is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Topics include:

- **Impact of Illegal Immigration on the HSI Honolulu AOR**
- **Signal App Communication Vulnerability**
- **Ransomware As A Service (RaaS) – Palau**
- **Critical Bottlenecks: Impact of Increased HSI Tip Line Volume**

If your schedule permits please join us. We look forward to seeing you there.

David J. Colafati

Intelligence Group Supervisor
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Colafati, David

To: Flores, David C; "Baggs, Kevin L" <[redacted]>; Beattie, Patricia A; "Bobbitt, Renae - GOV" <[redacted]>; Brehm, Kelly B; Butler, Rhett; Charley, Jay O; "[redacted]"; Dubrall, Jesse L; Fillmore, Mark W; "Gary Yabuta - Hawaii HIDTA ([redacted])"; "Gantt, Racquel A. - GOV" <[redacted]>; "[redacted]"; KIKKAWA, SCOTT K; "Hallstrom, David - GOV" <[redacted]>; "[redacted]"; Huerta, Jonathan (Jon) CIV USCG SEC HONOLULU (USA); LAU CHUNG-YAN; "[redacted]"; "[redacted]"; "Richard Witt" <[redacted]>; Robinson, Jennifer N LT USCG SEC HONOLULU (USA); "[redacted]"; Woodruff, John; Strandhagen, Joh; Nakamoto, Shannon K; Luevano, Eugene; "[redacted]"; Zawacki, Lee; Ganzorig, Togtokhbayar; Ammons, Christian J; Agustin, Heather R; Kaneko, John M (CTR); Ko, Christopher E; Arline III, Napoleon; Fejeran Jr, Robert J; Ward, James H; Beyer, John E; Musso, Erin E; Quintanilla, Meilani L; Duenas, Cristin S; Yoshinaga, Reyn A; Albert, Mary K P; Lansangan, Michael D; Dai, Laura L.V; Faulkner, Ryan K; Cabral-DeArmas, Lucia; Smith, Ryan T; Fujimoto, Kipp K; Waddell, Charles L; Albert, Mary K P; Beagle III, James R; Chambers, James A; Duenas, John S; Faulkner, Ryan K; Flores, Connie M; Harahap, Isra D; Quintanilla, Meilani L; Ramirez, Robert D; Steele, Isaac M; Yoshinaga, Reyn A; Young, Ivan K; Flores, Connie M; Tapia, Victoria A; Duenas, Cristin S; Lorenzo, Gracelyn M; Arzamendi, Mario

Subject: [EXTERNAL] HSI Honolulu Quarterly Intel Brief - April 17, 2025

Date: Thursday, April 17, 2025 12:41:11 PM

Reminder – The HSI Honolulu Quarterly Intel Brief is being held today via MS Teams at 1430 (HST). The entire brief is UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE. Topics include:

- **Impact of Illegal Immigration on the HSI Honolulu AOR**
- **Signal App Communication Vulnerability**
- **Ransomware As A Service (RaaS) – Palau**
- **Critical Bottlenecks: Impact of Increased HSI Tip Line Volume**

If your schedule permits please join us. We look forward to seeing you there.

David J. Colafati
Intelligence Group Supervisor
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: HSI, Honolulu Intel Notices
To: #ICE-HSI-INTEL_SIP- Honolulu; "Baggs, Kevin L"; Beattie, Patricia A; "Bobbitt, Renae - GOV"; Brehm, Kelly B; Butler, Rhett; Charley, Jay O; "[redacted]"; Dubrall, Jesse L; Fillmore, Mark W; "Gary Yabuta - Hawaii HIDTA ([redacted])"; "Gantt, Racquel A. - GOV"; "[redacted]"; KIKKAWA, SCOTT K; "Hallstrom, David - GOV"; "[redacted]"; Huerta, Jonathan (Jon) CIV USCG SEC HONOLULU (USA); LAU CHUNG-YAN; "[redacted]"; "[redacted]"; "Richard Witt"; Robinson, Jennifer N LT USCG SEC HONOLULU (USA); "[redacted]"; Woodruff, John; Strandhagen, Joh; Nakamoto, Shannon K; Luevano, Eugene; "[redacted]"; Zawacki, Lee; Ganzorig, Togtokhbayar; Ammons, Christian J
Subject: [EXTERNAL] Reminder --> HSI Quarterly Intel Brief this Thursday
Date: Tuesday, January 14, 2025 12:20:19 PM
Attachments: image002.png
image003.png
image004.png

A friendly reminder to please join us for our Quarterly Intelligence Brief, via Microsoft Teams on Thursday January 16th. The briefs are held the third Thursday, every 3 months, 2:30-3:30 PM. The briefings will be unclassified, and topics are announced a week prior.

This month's topics are:

- **Vehicle Threats:** Law enforcement awareness on the use of the vehicles for acts of terrorism.
- **Phone Porting/SIM Swap Scam:** An exploration of the scam, along with strategies to protect yourself.
- **Deed Fraud:** An examination of deed fraud trends and preventive measures.
- **Pink Cocaine**: A new street drug that has appeared in Hawaii in the recent months.
- **Salt Typhoon:** A state-sponsored Advanced Persistent Threat (APT) group likely operating under the direction of the Chinese Ministry of State Security (MSS).

If you ever have information you would like to share with the group during any of the briefs, please reach out and let me know and we can add you to that month's schedule to brief.

Thank you,

Paige V. Barry Chavez

Chief Intelligence Officer
Hawaii | Guam | CNMI
American Samoa | COFA Nations

Homeland Security Investigations | HSI Honolulu
595 Ala Moana BLVD | Honolulu, Hawaii 96813
[redacted] ☎ [redacted]
[redacted]
HSDN: [redacted]
C-LAN: [redacted]

From: HSI HONOLULU INTEL

Cc: #HSI Honolulu AOR-ALL; "Baggs, Kevin L" <[redacted]>; Beattie, Patricia A; "Bobbitt, Renae - GOV" <[redacted]>; Brehm, Kelly B; Butler, Rhett; Charley, Jay O; "[redacted]"; Dubrall, Jesse L; Fillmore, Mark W; "Gary Yabuta - Hawaii HIDTA ([redacted])"; "Gantt, Racquel A. - GOV" <[redacted]>; "[redacted]"; KIKKAWA, SCOTT K; "Hallstrom, David - GOV" <[redacted]>; "[redacted]"; Huerta, Jonathan (Jon) CIV USCG SEC HONOLULU (USA); LAU CHUNG-YAN; "[redacted]"; "[redacted]"; "[redacted]"; "Richard Witt" <[redacted]>; Robinson, Jennifer N LT USCG SEC HONOLULU (USA); "[redacted]"; Woodruff, John; Strandhagen, Joh; Nakamoto, Shannon K; Luevano, Eugene; "[redacted]"; Zawacki, Lee; Ganzorig, Togtokhbayar; Ammons, Christian J

Subject: HSI Honolulu Quarterly Intel Brief

Attachments: image001.png
image002.png
image003.png

I would like to invite you to please join us for our 2025 Quarterly Intelligence Briefs, via Microsoft Teams. They are held the third Thursday, every 3 months, 2:30-3:30 PM. The briefings will be unclassified, and topics are announced a week prior.

The 2025 dates are as follows:

January 16, 2025

April 17, 2025

July 17, 2025

October 16, 2025

If you ever have information you would like to share with the group during any of the briefs, please reach out and let me know and we can add you to that month's schedule to brief.

Thank you,

Paige V. Barry Chavez

Chief Intelligence Officer

Hawaii | Guam | CNMI

American Samoa | COFA Nations

Homeland Security Investigations |HSI Honolulu

595 Ala Moana BLVD | Honolulu, Hawaii 96813

[redacted] *|[redacted]

[redacted] <mailto[redacted]>

HSDN: [redacted] <mailto[redacted]>

C-LAN: [redacted] <mailto[redacted]>

Microsoft Teams Need help? <[redacted]

Join the meeting now <[redacted]>

Meeting ID: [redacted]

Passcode: [redacted]

For organizers: Meeting options [redacted]

From: Baggs, Kevin L
To: HSI HONOLULU INTEL
Subject: Accepted: HSI Honolulu Quarterly Intel Brief

From: Ward, James H
To: Baggs, Kevin L
Cc: Colafati, David
Subject: [EXTERNAL] RE: Greetings old friend
Date: Friday, February 21, 2025 3:57:06 PM
Attachments: GTO Hawaii Addresses.xlsx

Hi Kevin,

I've obtained the list of addresses.

The key question now is whether the data can be disclosed to your intended audience. Please refer to the BSA Warning statement below for guidance. If your briefing audience consists entirely of law enforcement personnel, there shouldn't be an issue. However, if you're presenting to private sector individuals, you will likely need to sanitize the information and discuss it in broader terms (e.g., no maps, specific addresses, etc.).

If the audience does not meet the below criteria, you can still discuss the information in general terms. In such cases, you would need to contact FinCEN through their help/contact us website to obtain their approval. I have done this in the past and received permission to present overview statistics without disclosing specific details of financial reports to non-law enforcement personnel.

> *(U//LES)* ***BSA Warning:*** *The enclosed information was collected and disseminated under provisions of the Bank Secrecy Act (BSA) and U.S. Department of the Treasury regulations implementing the BSA. See 31 U.S.C. 5311, et seq.; 31 CFR Chapter X. The information is sensitive in nature and is to be treated accordingly.* ***The information may be used only for a purpose consistent with a criminal, tax, or regulatory investigation or proceeding, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.*** *See 31 U.S.C. 5311. The information cannot be further released, disseminated, disclosed, or transmitted without prior approval of the Director of Financial Crimes Enforcement Network or his authorized delegate. Suspicious activity reports filed under the BSA must be treated with particular care given that they contain unsubstantiated allegations of possible criminal activity, akin to confidential informant tips. Unauthorized release of information collected under the BSA may result in criminal or civil sanctions.*

James H. Ward
Criminal Analyst
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Baggs, Kevin L <[redacted]>
Sent: Friday, February 21, 2025 2:36 PM
To: Ward, James H <[redacted]>
Subject: RE: Greetings old friend

Don't want to create work. Is there some open source reporting that you may have run across.. is just a side point to the how widespread the threats are and from all fronts even real estate..... My presentation is March 5th

From: Ward, James H <[redacted]>
Sent: Friday, February 21, 2025 2:33 PM
To: Baggs, Kevin L <[redacted]>
Cc: Colafati, David <[redacted]>
Subject: [EXTERNAL] RE: Greetings old friend

Hey Kevin!

I definitely miss my detail over at the fusion center. That was allot of fun.

I believe you're referring to my Real Estate Geographic Targeting Order (REGTO aka GTO) analysis.

I might be able to plot the Hawaii addresses on a map which you guys could then cross reference with a critical infostructure map with [redacted].

When would you need this product by?

James H. Ward
Criminal Analyst
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Baggs, Kevin L <[redacted]>
Sent: Friday, February 21, 2025 2:23 PM
To: Ward, James H <[redacted]>
Subject: Greetings old friend

James,

Hope all is well. We miss you at the fusion center! Come back and visit and perhaps some junpuu. Anyways I was wondering if I could ask a favor. You did a presentation on countries of concern purchasing land in US and even HI. Trying to remember if some of the concern was related to the land purchased being in proximity to critical infrastructure. I am doing a threat brief on March 5th on the threat landscape to critical infrastructure and thought I would include a bit on suspicious or concerning purchases of land near CI. Do you have anything open source you can share with me on this. If my memory of your presentation is off then I apologize for being old and clearly memory challenged. Ha

Kevin

From: Ward, James H
To: Baggs, Kevin L
Cc: Colafati, David
Subject: [EXTERNAL] RE: Greetings old friend
Date: Friday, February 21, 2025 2:33:12 PM

Hey Kevin!

I definitely miss my detail over at the fusion center. That was allot of fun.

I believe you're referring to my Real Estate Geographic Targeting Order (REGTO aka GTO) analysis.

I might be able to plot the Hawaii addresses on a map which you guys could then cross reference with a critical infostructure map with [redacted].

When would you need this product by?

James H. Ward
Criminal Analyst
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Baggs, Kevin L <[redacted]>
Sent: Friday, February 21, 2025 2:23 PM
To: Ward, James H <[redacted]>
Subject: Greetings old friend

James,

Hope all is well. We miss you at the fusion center! Come back and visit and perhaps some junpuu. Anyways I was wondering if I could ask a favor. You did a presentation on countries of concern purchasing land in US and even HI. Trying to remember if some of the concern was related to the land purchased being in proximity to critical infrastructure. I am doing a threat brief on March 5th on the threat landscape to critical infrastructure and thought I would include a bit on suspicious or concerning purchases of land near CI. Do you have anything open source you can share with me on this. If my memory of your presentation is off then I apologize for being old and clearly memory challenged. Ha

Kevin

From: Ward, James H
To: Baggs, Kevin L
Subject: [EXTERNAL] RE: Greetings old friend
Date: Friday, February 21, 2025 3:22:29 PM

I just tried calling [redacted].

Give me a buzz when you get a minute and we can talk about the GTO.

James H. Ward
Criminal Analyst
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Baggs, Kevin L <[redacted]>
Sent: Friday, February 21, 2025 2:36 PM
To: Ward, James H <[redacted]>
Subject: RE: Greetings old friend

Don't want to create work. Is there some open source reporting that you may have run across.. is just a side point to the how widespread the threats are and from all fronts even real estate..... My presentation is March 5th

---

From: Ward, James H <[redacted]>
Sent: Friday, February 21, 2025 2:33 PM
To: Baggs, Kevin L <[redacted]>
Cc: Colafati, David <[redacted]>
Subject: [EXTERNAL] RE: Greetings old friend

Hey Kevin!

I definitely miss my detail over at the fusion center. That was allot of fun.

I believe you're referring to my Real Estate Geographic Targeting Order (REGTO aka GTO) analysis.

I might be able to plot the Hawaii addresses on a map which you guys could then cross reference with a critical infostructure map with [redacted].

When would you need this product by?

James H. Ward
Criminal Analyst
Homeland Security Investigations
HSI Honolulu
Phone: [redacted]

From: Baggs, Kevin L <[redacted]>
Sent: Friday, February 21, 2025 2:23 PM
To: Ward, James H <[redacted]>
Subject: Greetings old friend

James,

Hope all is well. We miss you at the fusion center! Come back and visit and perhaps some junpuu. Anyways I was wondering if I could ask a favor. You did a presentation on countries of concern purchasing land in US and even HI. Trying to remember if some of the concern was related to the land purchased being in proximity to critical infrastructure. I am doing a threat brief on March 5th on the threat landscape to critical infrastructure and thought I would include a bit on suspicious or concerning purchases of land near CI. Do you have anything open source you can share with me on this. If my memory of your presentation is off then I apologize for being old and clearly memory challenged. Ha

Kevin

From: Forthofer, Molly
To: Forthofer, Molly
Cc: [redacted]; Cites, Clarence D; [redacted]; Kickland, Patricia; [redacted]; Sellers, David G; [redacted]; Baggs, Kevin L; [redacted]; O"Connell, Maureen E; [redacted]; Rita Lee
Subject: HI AOR Analyst Meeting - May 2025
Attachments: image001.png

Aloha, fellow analysts!

I am sending this as a reminder for Thursday's HI AOR Analyst Meeting. Please don't hesitate to reach out with any questions or concerns.

Thank you all who came to the January HI Analyst AOR meeting! Lots of great information exchange and a wonderful briefing by Maria Merry with C&C DTS . Here is the calendar invite for the next quarterly meeting. I have blocked off 0900-1100 on 15 May 2025 in the [redacted]. Please let me know if you have any specific topics you're interested in learning about or questions you would like me to pose to the group, otherwise the main goal of the meeting is to get together to talk/share information. If you would like to invite additional analysts not included in this list, please let me know and I can share the invite with them. I hope to see you all there!

If anyone would like to brief or know someone who can brief a topic of interest to the group, we are happy to host them. It appears everyone enjoyed the last briefing! As always, let me know if you need anything and don't hesitate to reach out with questions.

Date: 15 May 2025

Time: 0900-1100

Location: [redacted]

Parking: [redacted]

Parking is $5 for the day with [redacted] validation, so make sure to get your parking validated before you leave!

Here are the upcoming meeting dates for 2025 in case you want to block off your calendar now:

14 August 2025

13 November 2025

Time: 0930-1130

For our neighbor island/Guam analysts, below is the MS Teams link for the session:

Microsoft Teams Need help? <https://aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now <[redacted]>

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-4853,[redacted] <tel:+18088294853,[redacted]> United States, Honolulu

Find a local number <[redacted]>

Phone conference ID: [redacted]

For organizers: Meeting options [redacted]

[redacted] | Reset dial-in PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

Respectfully,

Molly Forthofer

Lead Intelligence Analyst

(personal) [redacted] <[redacted]>

(main) [redacted] <mailto[redacted]>

Hawai‘i State Fusion Center

(Cell) [redacted]

Submit Tips / Leads at https://hsfc.hawaii.gov/tips <https://hsfc.hawaii.gov/tips>

From: Ko, Christopher E
To: Forthofer, Molly
Subject: [EXTERNAL] RE: Protest on 2/5
Date: Monday, February 3, 2025 9:32:16 AM
Attachments: image002.jpg
image003.png

Thanks Molly.

Thanks,
Christopher Ko
Criminal Analyst
HSI Honolulu
Phone: [redacted]
Email: (unclass) [redacted]
Email: (classified) [redacted]

From: Forthofer, Molly <[redacted]>
Sent: Monday, February 3, 2025 9:28 AM
To: Ko, Christopher E <[redacted]>
Cc: HSFC <[redacted]>
Subject: RE: Protest on 2/5

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

HSFC Reference Number: [redacted]

Good morning!

The HSFC is tracking, but we have [redacted]. We will [redacted].

Please let me know if we can do anything else to be of assistance.

Respectfully,
Molly Forthofer
Lead Intelligence Analyst

(personal) [redacted]
(main) [redacted]
Hawai‘i State Fusion Center
(Cell) [redacted]

Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

From: Ko, Christopher E <[redacted]>
Sent: Monday, February 3, 2025 7:26 AM
To: Forthofer, Molly <[redacted]>
Subject: [EXTERNAL] Protest on 2/5

Morning,
Are you tracking anything on this protest? My Supervisor saw this post on Reddit.
Thanks.

Thanks,
Christopher Ko
Criminal Analyst
HSI Honolulu

Phone: [redacted]

From: Forthofer, Molly
To: Ko, Christopher E
Cc: HSFC
Subject: RE: Protest on 2/5
Date: Monday, February 3, 2025 9:27:00 AM
Attachments: image001.png

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

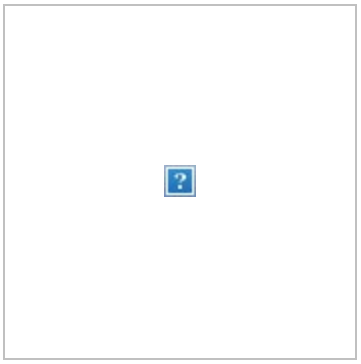
HSFC Reference Number: [redacted]

Good morning!

The HSFC is tracking, but we have [redacted]. We will [redacted].

Please let me know if we can do anything else to be of assistance.

Respectfully,
Molly Forthofer
Lead Intelligence Analyst
(personal) [redacted]
(main) [redacted]
Hawai‘i State Fusion Center
(Cell) [redacted]



Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

approval of an authorized OHS official.

From: Ko, Christopher E <[redacted]>
Sent: Monday, February 3, 2025 7:26 AM
To: Forthofer, Molly <[redacted]>
Subject: [EXTERNAL] Protest on 2/5

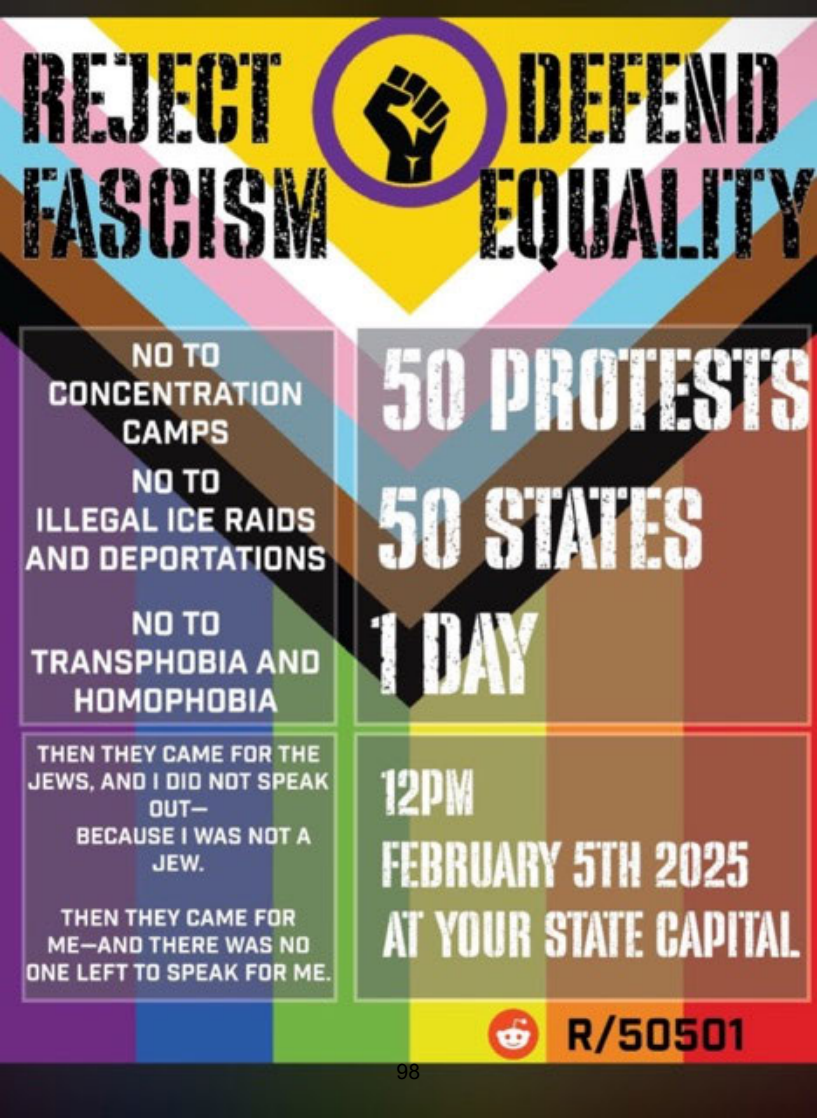
Morning,
Are you tracking anything on this protest? My Supervisor saw this post on Reddit.
Thanks.

Thanks,
Christopher Ko
Criminal Analyst
HSI Honolulu
Phone: [redacted]

From: Ko, Christopher E
To: Forthofer, Molly
Subject: [EXTERNAL] Protest on 2/5
Date: Monday, February 3, 2025 7:26:42 AM
Attachments: IMG_0034.PNG

Morning,
Are you tracking anything on this protest? My Supervisor saw this post on Reddit. Thanks.

Thanks,
Christopher Ko
Criminal Analyst
HSI Honolulu
Phone: [redacted]


REJECT FASCISM
DEFEND EQUALITY
NO TO CONCENTRATION CAMPS
NO TO ILLEGAL ICE RAIDS AND DEPORTATIONS
NO TO TRANSPHOBIA AND HOMOPHOBIA
50 PROTESTS
50 STATES
1 DAY
THEN THEY CAME FOR THE JEWS, AND I DID NOT SPEAK OUT—
BECAUSE I WAS NOT A JEW.
THEN THEY CAME FOR ME—AND THERE WAS NO ONE LEFT TO SPEAK FOR ME.
12PM
FEBRUARY 5TH 2025
AT YOUR STATE CAPITAL.
R/50501

From: Forthofer, Molly
Cc: [redacted]; Clites, Clarence D; [redacted]; Forthofer, Molly; [redacted]; Kickland, Patricia; [redacted]; Sellers, David G; [redacted]; Baggs, Kevin L; [redacted]; Robinson, Jane E. (HN) (FBI); O'Connell, Maureen E; [redacted]; Hiraoka, Victoria A; Higbee, Scott M CIV USCG SEC HONOLULU (USA); Burke, Kelly S CIV (USA)
Subject: HI AOR Analyst Meeting - February 2025
Attachments: image001.png

Aloha, fellow analysts!

Happy New Year! Thank you all who came to the September HI Analyst AOR meeting! Lots of great information exchange and a wonderful briefing by the Missouri NGCD. Here is the calendar invite for the next quarterly meeting. I have blocked off 0930-1130 on 13 February 2025 in the [redacted]. Please let me know if you have any specific topics you're interested in learning about or questions you would like me to pose to the group, otherwise the main goal of the meeting is to get together to talk/share information. If you would like to invite additional analysts not included in this list, please let me know and I can share the invite with them. I hope to see you all there!

If anyone would like to brief or know someone who can brief a topic of interest to the group, we are happy to host them. It appears everyone enjoyed the last briefing! As always, let me know if you need anything and don't hesitate to reach out with questions.

Date: 13 February 2025

Time: 0930-1130

Location: [redacted]

Parking: [redacted]

Parking is $5 for the day with [redacted] validation, so make sure to get your parking validated before you leave!

Here are the upcoming meeting dates for 2025 in case you want to block off your calendar now:

15 May 2025

14 August 2025

13 November 2025

Time: 0930-1130

For our neighbor island/Guam analysts, below is the MS Teams link for the session:

Microsoft Teams Need help? <https://aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now [redacted]

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-4853, [redacted]# <tel:+18088294853,[redacted]> United States, Honolulu

Find a local number <[redacted]>

Phone conference ID: [redacted]

For organizers: Meeting options <[redacted]

[redacted] | Reset dial-in PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

Respectfully,

Molly Forthofer

Lead Intelligence Analyst

(personal) [redacted] <mailto[redacted]>

(main) [redacted] <mailto[redacted]>

Hawai'i State Fusion Center

(Cell) [redacted]

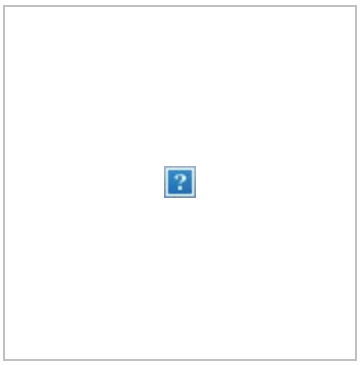
Submit Tips / Leads at https://hsfc.hawaii.gov <https://hsfc.hawaii.gov/> or https://hawaiifusioncenter.org/ <https://hawaiifusioncenter.org/>

From: Forthofer, Molly
To: Ward, James H
Cc: [redacted]
Subject: RE: HI AOR Analyst Meeting - February 2025
Date: Thursday, January 23, 2025 9:33:00 AM
Attachments: image001.png

I totally understand! I hope that you have a lovely time with them.

I wanted to introduce you to our new [redacted]. He is the new [redacted]. He just arrived last week, but I wanted to introduce you two because you work national security. Happy New Year!

Respectfully,
Molly Forthofer
Lead Intelligence Analyst
(personal) [redacted]
(main) [redacted]
Hawai‘i State Fusion Center
(Cell) [redacted]



Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

-----Original Appointment-----
From: Ward, James H <[redacted]>
Sent: Thursday, January 23, 2025 9:29 AM
To: Forthofer, Molly
Subject: [EXTERNAL] Declined: HI AOR Analyst Meeting - February 2025
When: Thursday, February 13, 2025 9:30 AM-11:30 AM (UTC-10:00) Hawaii.
Where: [redacted]

Bummer. I have a school event with my kids on that day. Sorry.

From: Ward, James H
To: Forthofer, Molly
Cc: [redacted]
Subject: [EXTERNAL] RE: HI AOR Analyst Meeting - February 2025
Date: Thursday, January 23, 2025 9:56:07 AM
Attachments: image001.png

Very nice. Welcome aboard [redacted]!

All the best,

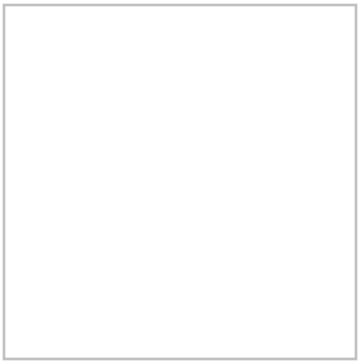
- James

From: Forthofer, Molly <[redacted]>
Sent: Thursday, January 23, 2025 9:33 AM
To: Ward, James H <[redacted]>
Cc: [redacted]
Subject: RE: HI AOR Analyst Meeting - February 2025

I totally understand! I hope that you have a lovely time with them.

I wanted to introduce you to our new [redacted]. He is the new [redacted]. He just arrived last week, but I wanted to introduce you two because you work national security. Happy New Year!

Respectfully,
Molly Forthofer
Lead Intelligence Analyst
(personal) [redacted]
(main) HSFC@hawaii.gov
Hawai'i State Fusion Center
(Cell) [redacted]



Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

WARNING: This communication may contain FOR OFFICIAL USE ONLY (FOUO) and/or LAW ENFORCEMENT SENSITIVE (LES) information. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with OHS policy relating to FOUO and LES information and is not to be released to the public, the media, foreign nationals, or other personnel who do not have a valid "need-to-know" without prior approval of an authorized OHS official.

-----Original Appointment-----
From: Ward, James H <[redacted]>
Sent: Thursday, January 23, 2025 9:29 AM
To: Forthofer, Molly
Subject: [EXTERNAL] Declined: HI AOR Analyst Meeting - February 2025
When: Thursday, February 13, 2025 9:30 AM-11:30 AM (UTC-10:00) Hawaii.
Where: [redacted]

Bummer. I have a school event with my kids on that day. Sorry.

From: Walker, William T
To: Forthofer, Molly
Subject: [EXTERNAL] Automatic reply: HI AOR Analyst Meeting - February 2025
Date: Monday, February 10, 2025 12:02:08 PM

I will be out of the office starting February 10, 2025 and will return on February 18, 2025 . For immediate assistance please contact Supervisory Criminal Analyst Caitlin Soper at [redacted].

From: Lorenzo, Gracelyn M
To: Forthofer, Molly
Subject: [EXTERNAL] Automatic reply: HI AOR Analyst Meeting - February 2025
Date: Monday, February 10, 2025 12:02:09 PM

Thank you for your email. I will be out of the office from 2/7/2025-2/13/2025. If you need further assistance please contact Intel AGS Chris Ko or AGS Chuck Waddell. Thank you.

From: Forthofer, Molly
Cc: [redacted]; Clites, Clarence D; [redacted]; Kickland, Patricia; [redacted]; Sellers, David G; [redacted]; Baggs, Kevin L; [redacted]; Robinson, Jane E. (HN) (FBI); O'Connell, Maureen E; [redacted]; Hiraoka, Victoria A; Higbee, Scott M CIV USCG SEC HONOLULU (USA); Burke, Kelly S CIV (USA); Ward, James H; Achuela, Sam (Consultant)
Subject: HI AOR Analyst Meeting - February 2025
Attachments: image001.png

Aloha, fellow analysts!

I am sending this as a reminder for Thursday's HI AOR Analyst Meeting. Please don't hesitate to reach out with any questions or concerns.

Thank you all who came to the September HI Analyst AOR meeting! Lots of great information exchange and a wonderful briefing by the Missouri NGCD. Here is the calendar invite for the next quarterly meeting. I have blocked off 0930-1130 on 13 February 2025 in the [redacted]. Please let me know if you have any specific topics you're interested in learning about or questions you would like me to pose to the group, otherwise the main goal of the meeting is to get together to talk/share information. If you would like to invite additional analysts not included in this list, please let me know and I can share the invite with them. I hope to see you all there!

If anyone would like to brief or know someone who can brief a topic of interest to the group, we are happy to host them. It appears everyone enjoyed the last briefing! As always, let me know if you need anything and don't hesitate to reach out with questions.

Date: 13 February 2025

Time: 0930-1130

Location: [redacted]

Parking: [redacted]

Parking is $5 for the day with [redacted] validation, so make sure to get your parking validated before you leave!

Here are the upcoming meeting dates for 2025 in case you want to block off your calendar now:

15 May 2025

14 August 2025

13 November 2025

Time: 0930-1130

For our neighbor island/Guam analysts, below is the MS Teams link for the session:

Microsoft Teams Need help? <https://aka.ms/JoinTeamsMeeting?omkt=en-US>

Join the meeting now [redacted]

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 808-829-4853,[redacted] <tel:+18088294853,[redacted]> United States, Honolulu

Find a local number <[redacted]>

Phone conference ID: [redacted]

For organizers: Meeting options <[redacted]

[redacted] | Reset dial-in PIN <https://dialin.teams.microsoft.com/usp/pstnconferencing>

Respectfully,

Molly Forthofer

Lead Intelligence Analyst

(personal) [redacted] <mailto:[redacted]>

(main) HSFC@hawaii.gov <mailto:HSFC@hawaii.gov>

Hawai'i State Fusion Center

(Cell) [redacted]

Submit Tips / Leads at https://hsfc.hawaii.gov <https://hsfc.hawaii.gov/> or https://hawaiifusioncenter.org/ <https://hawaiifusioncenter.org/>

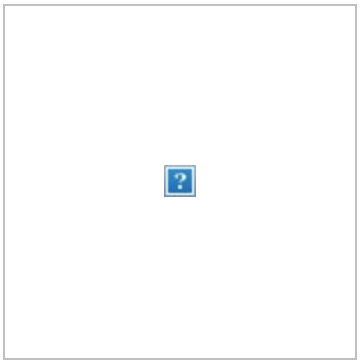
From: Forthofer, Molly
To: Napoleon Arline (HSI); Ward, James H; John Woodruff (FPS) ; Custer, Chantel K
Subject: (U//LES) CBP Product for Officer Awareness
Date: Friday, January 31, 2025 2:51:00 PM
Attachments: image001.png
[redacted].pdf

Hey, Po, James, John, and Chantel.

I wanted to pass along the attached bulletin from our DHS Intel Officer at the HSFC.

Please let me know if there is anything I can do!

Respectfully,
Molly Forthofer
Lead Intelligence Analyst
(personal) [redacted]
(main) HSFC@hawaii.gov
Hawai‘i State Fusion Center
(Cell) [redacted]



Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

DEPARTMENT OF HOMELAND SECURITY
CUSTOMS AND BORDER PROTECTION

U.S. BORDER PATROL
DEL RIO SECTOR OPERATIONS CENTER

Situational Awareness:

[redacted]

[redacted]
Office: [redacted]
Cell: [redacted]

From: Arline III, Napoleon
To: Custer, Chantel K; Forthofer, Molly
Cc: Ward, James H; Woodruff, John
Subject: [EXTERNAL] RE: (U//LES) CBP Product for Officer Awareness
Date: Friday, January 31, 2025 3:10:09 PM
Attachments: image002.png
image003.png

Thanks for sharing.
PO

From: Custer, Chantel K <[redacted]>
Sent: Friday, January 31, 2025 2:53 PM
To: Forthofer, Molly <[redacted]>
Cc: Arline III, Napoleon <[redacted]>; Ward, James H <[redacted]>; Woodruff, John <[redacted]>
Subject: RE: (U//LES) CBP Product for Officer Awareness

Thank you for sharing!

Chantel Custer

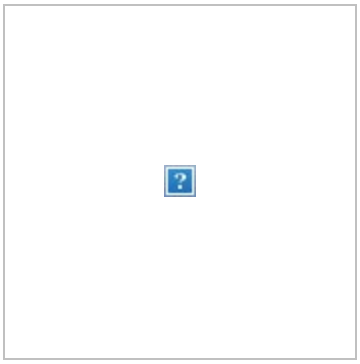
From: Forthofer, Molly <[redacted]>
Sent: Friday, January 31, 2025 2:52 PM
To: Arline III, Napoleon <[redacted]>; Ward, James H <[redacted]>; Woodruff, John <[redacted]>; Custer, Chantel K <[redacted]>
Subject: (U//LES) CBP Product for Officer Awareness

Hey, Po, James, John, and Chantel.

I wanted to pass along the attached bulletin from our DHS Intel Officer at the HSFC.

Please let me know if there is anything I can do!

Respectfully,
Molly Forthofer
Lead Intelligence Analyst
(personal) [redacted]
(main) [redacted]
Hawai‘i State Fusion Center
(Cell) [redacted]



Submit Tips / Leads at https://hsfc.hawaii.gov or https://hawaiifusioncenter.org/

From: Christie, Shannon
To: Hawaii State Fusion Center
Subject: [EXTERNAL] Automatic reply: U-HSFC 2025-0102 Cutting Through the Cyber Noise
Date: Thursday, January 2, 2025 1:54:41 PM

Hello,

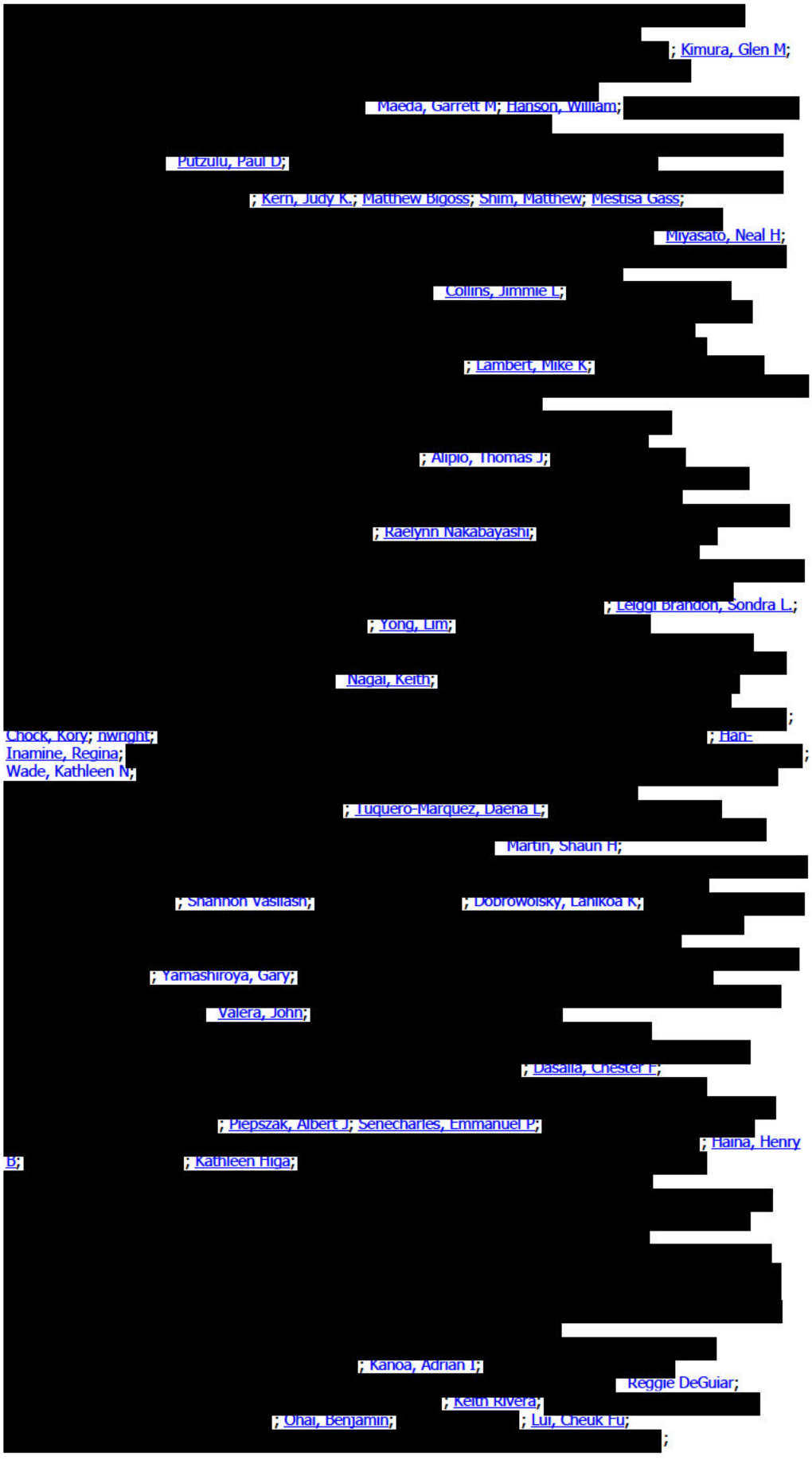
Thank you for your email! I am out of office until Monday, January 13 with limited access to email and will respond upon my return. If this is an urgent matter, please contact me via cell phone at [redacted].

From: Barry Chavez, Paige V
To: Hawaii State Fusion Center
Subject: [EXTERNAL] Automatic reply: U//LES FBI National Partner Call Re: Director Wray"s Farewell
Date: Wednesday, January 15, 2025 10:37:14 AM

I am on leave. I will have limited access to my phone and email. If you need immediate attention, please reach out to GS Dave (David) Colafati, who is acting in my absence.

Thank you,
Paige Barry Chavez

From: Kickland, Patricia
To: HSFC
Bcc: [redacted]; Hartsock, Michael R; HSFC; [redacted]; Frank Castagnetti; [redacted] Tomas Alday-Morales; Phillip Buchanan; Theresa Deamicis; Clites, Clarence D; [redacted]; Baggs, Kevin L; Brad Heatherly; John Kaluna; [redacted] Leonard, Amanda J; [redacted]; Ramson, Clifford; [redacted] Sellers, David G; Daniel Barretto; Nichole Sakai; Toiya, Hirokazu; Hirsbrunner, Tom; [redacted]; Chee, Jonathan; [redacted]; KRISTY DOMINGUES (PID); O"Connell, Maureen E; [redacted]; Melody Bell; Vincent, Michael S; Forthofer, Molly; [redacted]; Barretto, Randi U; Hiraoka, Victoria A; Timothy Kozak; David Uranaka-Yamashiro; Badua, Glen M; [redacted]; Champion, Michael; Ferguson-Brey, Pamela J; [redacted] Thompson, John C; Nadine Castillo; Lan Rap; [redacted]; Sarah Armstrong; [redacted]; Akau, Nova C.; [redacted]; Desanctis, Danielle (HN) (FBI); Taum-Deenik, Malia; Lavina-Lopez, Maria Delia T; Horikawa, Keith K.; Elton Ushio; Sara Fechtelkotter; Mokuahi, Bernard K CIV INDOPACOM (USA); [redacted]; Jamie Newalu; Pace, Frank J; Henderson Nuuhiwa; [redacted]; Perlmutter, Rebecca (USAHI); Steven Taketa; Lynette Cantere; [redacted] Tina Yamaki; [redacted]; Edward Howard; [redacted]; Stafford Oyama; [redacted]; CHUNG-YAN LAU (HNL); [redacted]; Reed, Daniel; Ian Santee; [redacted]; Wise, Gregory L CIV USARMY USARPAC (USA); [redacted]; Kickland, Patricia; [redacted]; Mariano, Valerie S; [redacted] Craig Tanaka; [redacted]; Andre Peters; [redacted]; Isaiah Kaauwai; [redacted]; Baligad; [redacted]; Estores, Susan (USAHI); [redacted]; Lowe, Jordan; [redacted]; Richard Murray; [redacted]; Paul Graham; Yamashita, Stacey R; Koyanagi, Chad; [redacted] Okada, Andrew; [redacted] Gail Tice, Psy. D.; [redacted] Rente Jr, Henry L; [redacted]; D Kamanao; [redacted]; Ross Jr., Walter R BG; [redacted]; Elliott Ke; Wall, Matthew W; [redacted]; Furtado, Ezra E; Hoang, Vincent; [redacted] Redulla, Jason K; Kishi, Arnold T; [redacted]; [redacted]; Logan, Stephen F; Redulla, Jared K; Lopez, David A; [redacted]; Dale Ross; [redacted]; Christian Jenkins; Correia, Aaron P; [redacted]; Kaneshige, Everett S;


; Kimura, Glen M;
Maeda, Garrett M; Hanson, William;
Putzulu, Paul D;
; Kern, Judy K.; Matthew Bigoss; Shim, Matthew; Mestisa Gass;
Miyasato, Neal H;
Collins, Jimmie L;
; Lambert, Mike K;
; Alipio, Thomas J;
; Raelynn Nakabayashi;
; Leiggi Brandon, Sondra L.;
; Yong, Lim;
Nagai, Keith;
Chock, Kory; nwright;
; Han-
Inamine, Regina;
Wade, Kathleen N;
; Tuquero-Marquez, Daena L;
Martin, Shaun H;
; Shannon Vasilash;
; Dobrowolsky, Lahikoa K;
; Yamashiroya, Gary;
Valera, John;
; Dasalla, Chester F;
; Piepszak, Albert J; Senecharles, Emmanuel P;
; Haina, Henry
B;
; Kathleen Higa;
; Kanoa, Adrian T;
Reggie DeGuiar;
; Kelii Rivera;
; Ohai, Benjamin;
; Lui, Cheuk Fu;

; Shiraishi, Jonathan;
Marciel, Bryan D;
; Anthony Abalos;
; Woodruff, John;
Robinson, Jane E. (HN) (FBI);
; Richard Witt;
; Ikeehu;
Rodrigues, Howard J;
Kekaulike, Keola M;
; Edwards, Maurice;
; Jason Overmyer;
; Malani, Colin K;
; Sayers, Shelagh J; Hirst, Michael E; Bautista, Ernest D; michael.h.borruso.mil@army.mil; Brandao, Scott A; Aguon, Ralph P; Machado, Ryan K; Ching, Gavin M; ; Peters, Chon K; Lee, Christopher S; English, Deven K;
Graham, Noah; ; Ryan Yamane;
; Marciel, Bryan D; ; Hanohano, Mark M;
; Mario Pagni;
Sonobe Hong, Renee R;
; Otaguro, Curt T;
Melanie Dorado Wilson;
Benson Choo;

Subject: Space available: Training on topic related to targeted violence and terrorism prevention
Date: Friday, March 21, 2025 11:15:58 AM
Importance: High

Aloha from the Hawai`i State Fusion Center to our targeted violence and terrorism prevention stakeholders:

HSFC had **some folks drop out** of the scheduled training on 27-28 March by the Federal Law Enforcement Training Center. The **27th is reserved for sworn law enforcement and Fusion Liaison Officers**. The **28th is open to diverse stakeholders** whose job duties include violence prevention in the broad sense: social workers, mental wellness professionals, educators and EDU security, disability service providers, victim services/comp, etc. Topics include case studies of targeted attacks, tactics in terrorism (including sextortion and 764) and other topics — **agenda below**.

If you are interested, in order to avoid over-booking, **please fill out an interest survey ASAP** at [redacted]

HSFC will respond by close of business whether we have space left, and then we will forward the link to register with FLETC.

Thursday, March 27th (Fusion Liaison Officers (FLO) and sworn law enforcement (LE) only)
7:30 - 8:00: Opening
8:00 - 9:00: Threat Picture Overview and The Threat of Violent Extremism
9:00 - 10:00: Targeted Violence, Threat Assessment, and The Pathway to Violence Overview
10:00 - 11:30: Targeted Violence Case Study: 2022 Attack on Tops Friendly Markets - Buffalo, New York
11:30 - 12:30: Lunch on your own
12:30 - 1:30: The Incel Movement and Mass Violence
1:30 - 2:30: Targeted Violence Case Study: 2009 Attack on LA Fitness Club – Pittsburgh, Pennsylvania
2:30 - 4:00: Threat Management: Multidisciplinary Teams
4:00 - 4:30: Review, Questions, Discussion and Feedback

Friday, March 28th (FLOs, LE, and civilian stakeholders)
7:30 - 8:00: Research, Resources and Partnerships
8:00-9:30: Targeted Violence Case Study: 2021 Atlanta Spa Attack
9:30-11:30: Emerging Threats and Tactics in Terrorism (Sextortion/764, Social Media, Gaming Platforms, and Funding)
11:30 - 12:30: Lunch on your own

12:30-2:00: Targeted Violence Case Study: 2021 Attack on Oxford (MI) High School
2:00-3:00: Targeted Violence Outliers: Female Mass Attackers
3:00-4:00: Targeted Violence Prevention: Recognizing Warning Behaviors/Leakage
4:00 - 4:30: Review, Questions, Discussion, Feedback and Survey

LOCATION ([redacted]):
[redacted]

Mahalo and stay well,
Pati Kickland

Patricia Kickland
Threats Program Manager
Hawai‘i State Fusion Center
c/o Hawai‘i Office of Homeland Security
3949 Diamond Head Rd.
Honolulu, HI 96816
[redacted]

From: Tobon, John F
To: Smith, Selwyn; Hiraoka, Victoria A; Pace, Frank J
Subject: [EXTERNAL] RE: MDM
Date: Monday, January 27, 2025 1:03:42 PM
Attachments: ohs-mdm-hsi.pdf
SM-MDM-11012024.pdf

Aloha everyone,

Apologies for the delay in sending out this introductory email.

Deputy Assistant Director @Smith, Selwyn,

@Pace, Frank J is the Administrator of Hawaii's Office of DHS. @Hiraoka, Victoria A works at Hawaii DHS and was instrumental in helping the state combat Mis/Dis/Mal information during and after the Maui fires. I think their work can help us with the wave of MDM that we have been and are currently facing.

Frank/Tori,

DAD Smith oversees our Public Safety and Border Security Division, which includes narcotics, gangs, and human smuggling investigations, among others. During our conversation we spoke specifically about the challenges in the human smuggling space, where we are fighting a wide variety of MDM.

It is my hope that we can connect the HSI SMEs with Tori to help chart a course of action going forward.

I will let you talk amongst yourselves as I enter retirement at the end of this week.

Respectfully,

John F. Tobon
Assistant Director
Countering Transnational Organized Crime Division
Homeland Security Investigations
Mobile: [redacted]
Email: [redacted]

Follow us on X @HSI_HQ
Visit our website: www.hsi.gov

Sign Up To Receive HSI Cornerstone Newsletter HSI Cornerstone
HSI Cornerstone Homepage

From: Hiraoka, Victoria A <[redacted]>
Sent: Tuesday, January 14, 2025 10:19 AM
To: Pace, Frank J <[redacted]>; Tobon, John F <[redacted]>
Subject: Re: MDM

John,

It was very nice to chat with you this morning. If you are able to give me examples of the MDM that you are combatting regarding smuggling, I can rework parts of the presentation for you to be more specific.

Mahalo!

Victoria Hiraoka
Communications Lead, State of Hawai'i Office of Homeland Security
VISIT US ON TWITTER | LET'S GET LINKED IN

From: Pace, Frank J <[redacted]>
Date: Tuesday, January 14, 2025 at 9:18 AM
To: Tobon, John F <[redacted]>
Cc: Hiraoka, Victoria A <[redacted]>
Subject: MDM

Aloha,

Here are some of Tori's products.

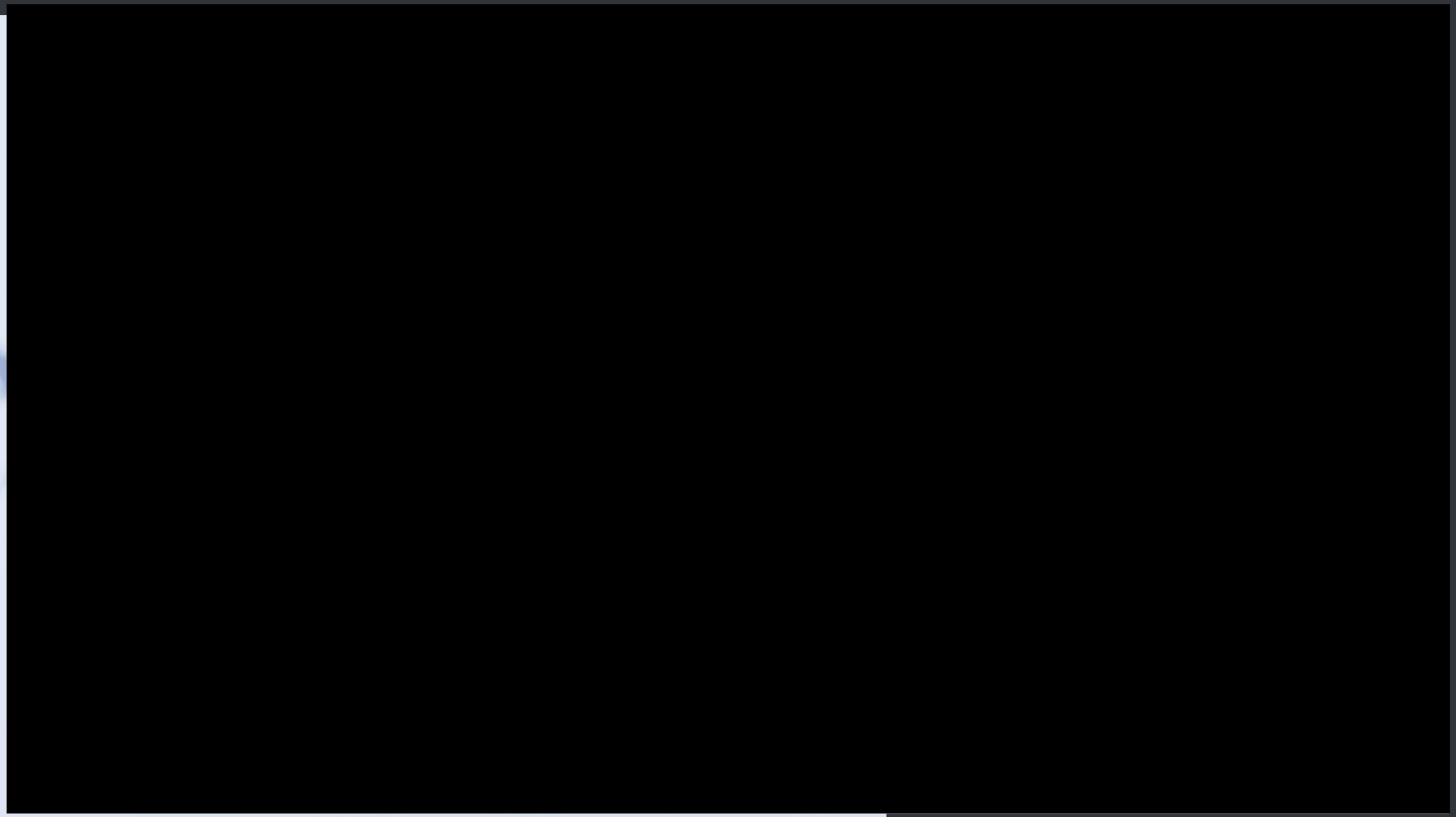
v/r

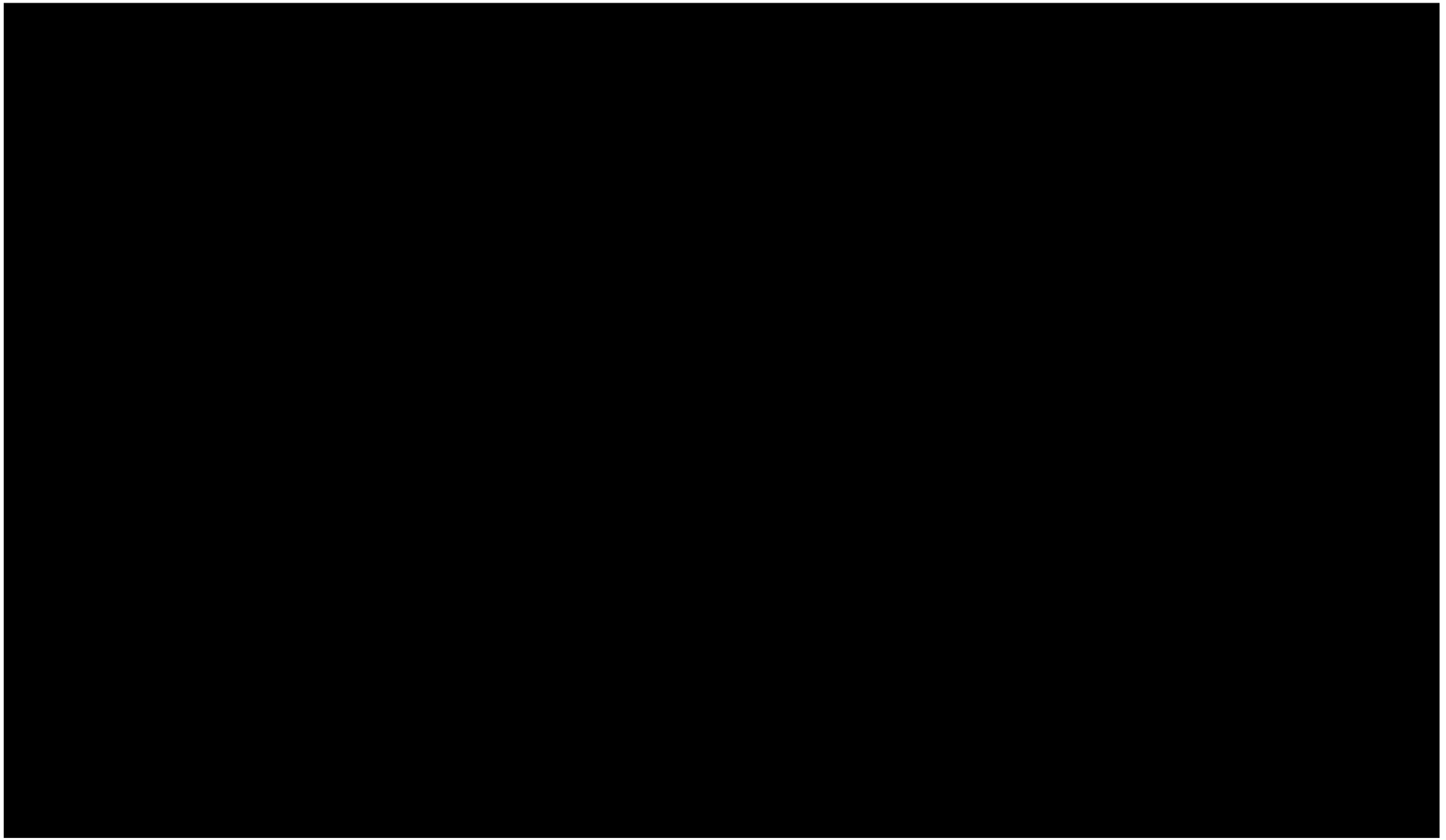
Frank

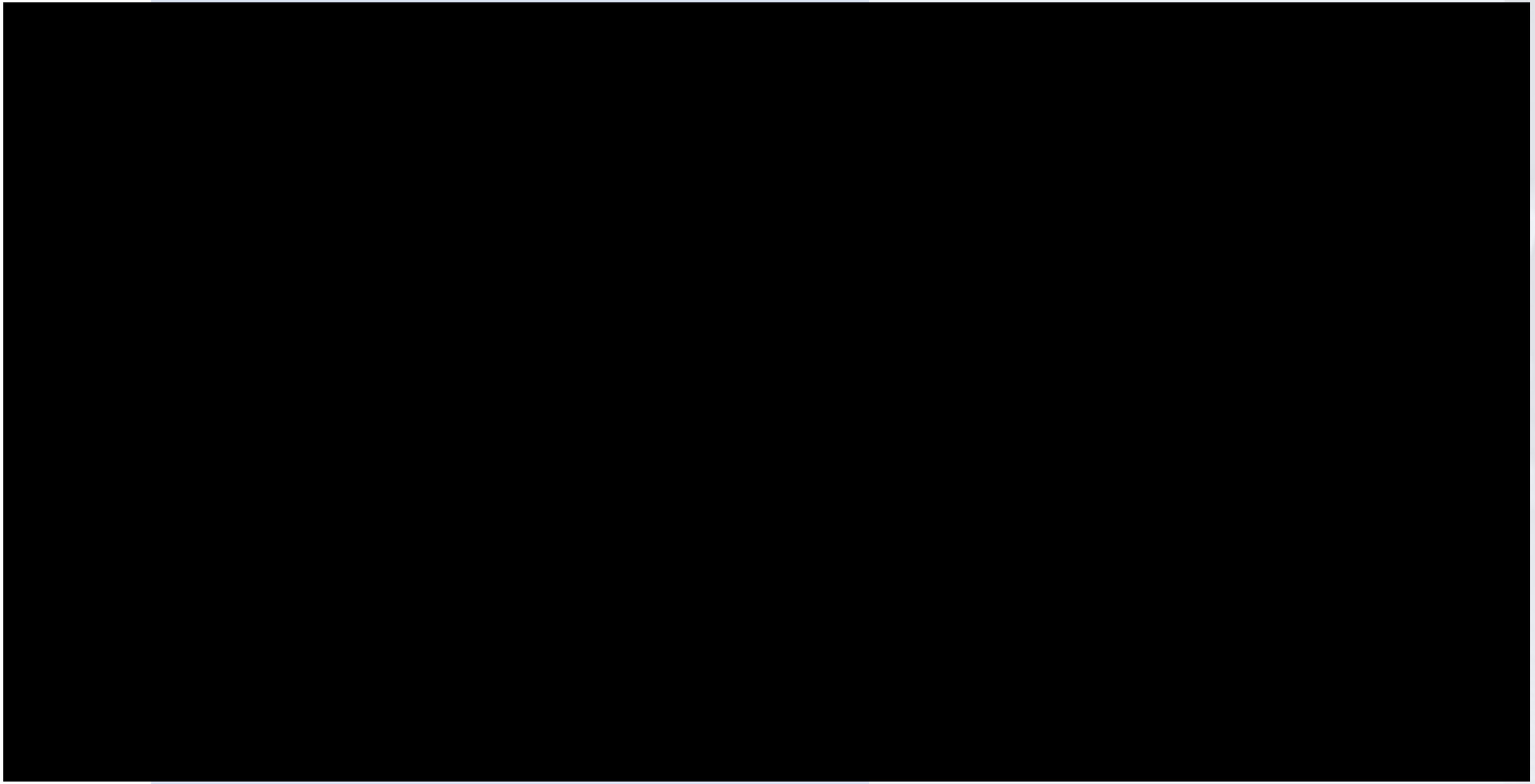
Frank J. Pace, Administrator
Office of Homeland Security
Hawaii Department of Law Enforcement
(O) [redacted]
(M) [redacted]
[redacted]

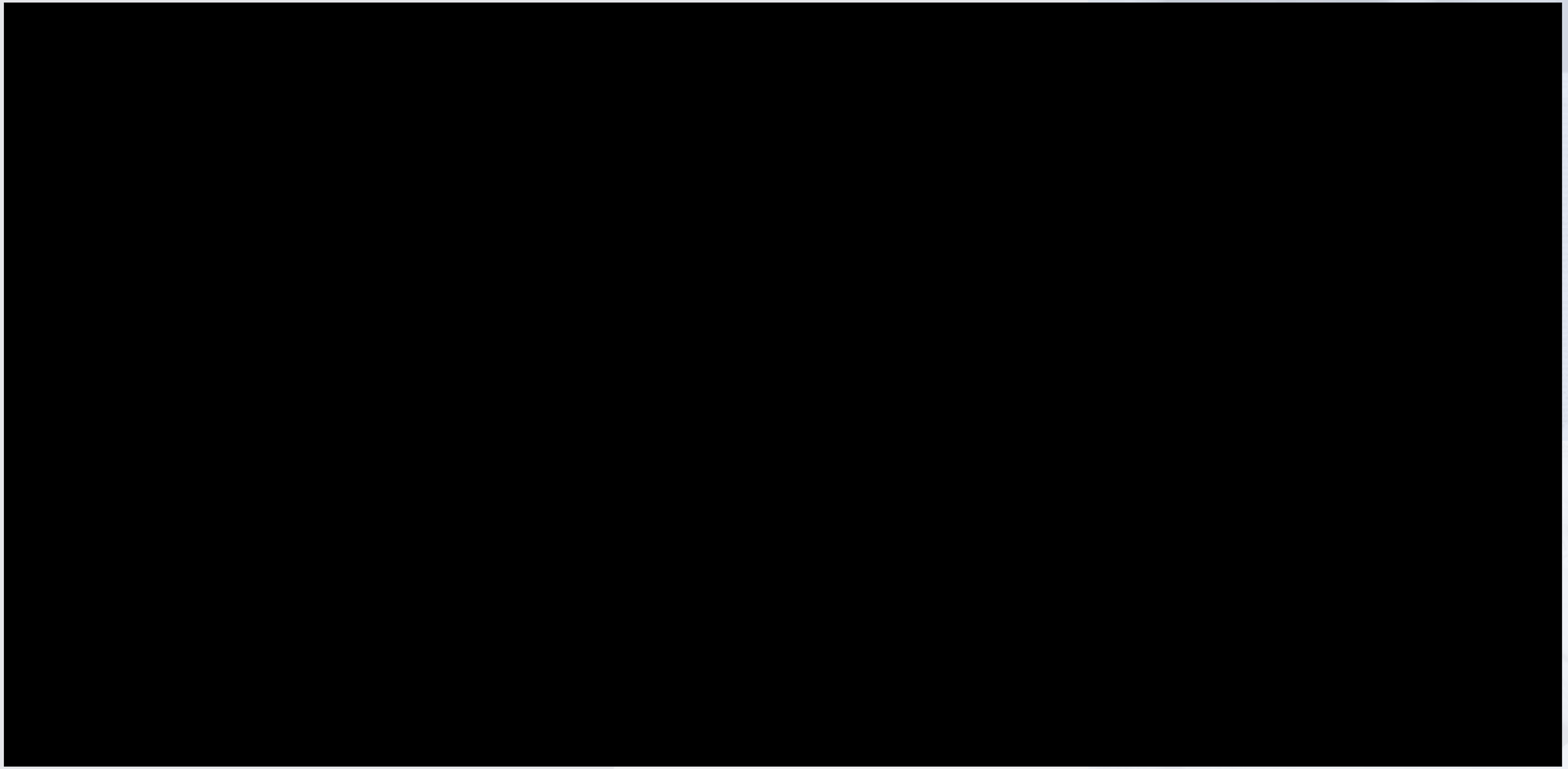
NOT FOR DISTRIBUTION

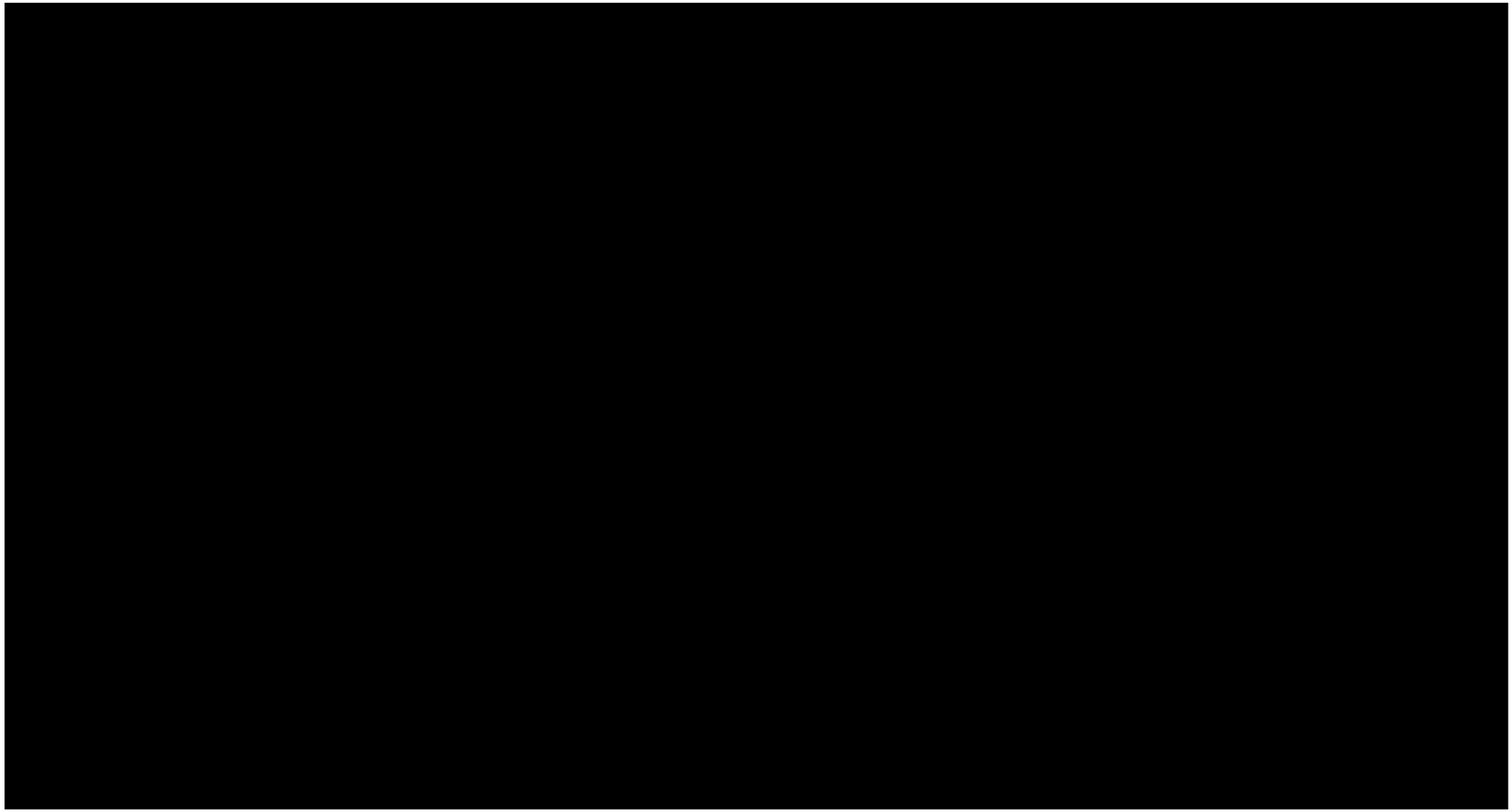
Prepared by the State of Hawai‘i Office of Homeland Security for Homeland Security Investigations

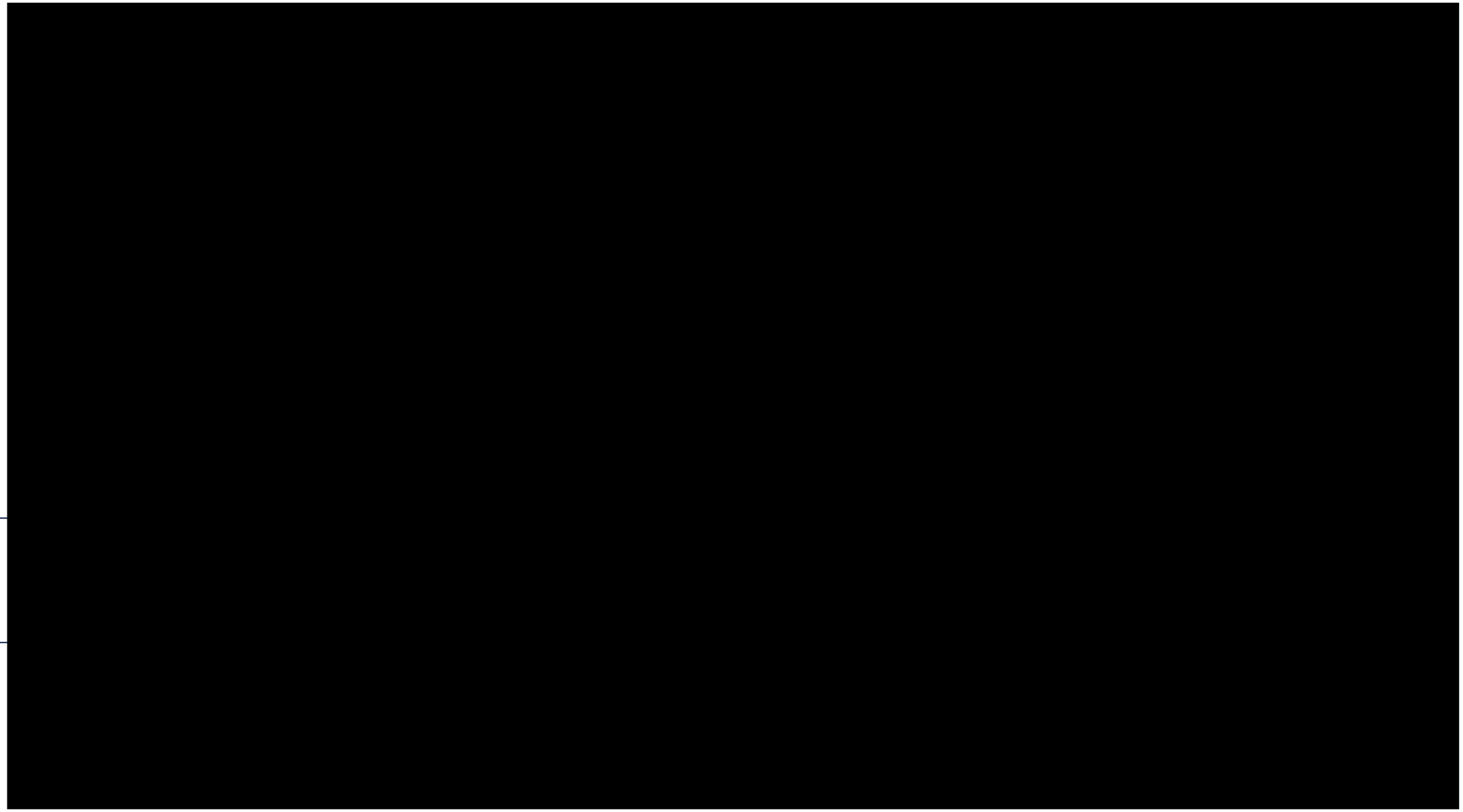


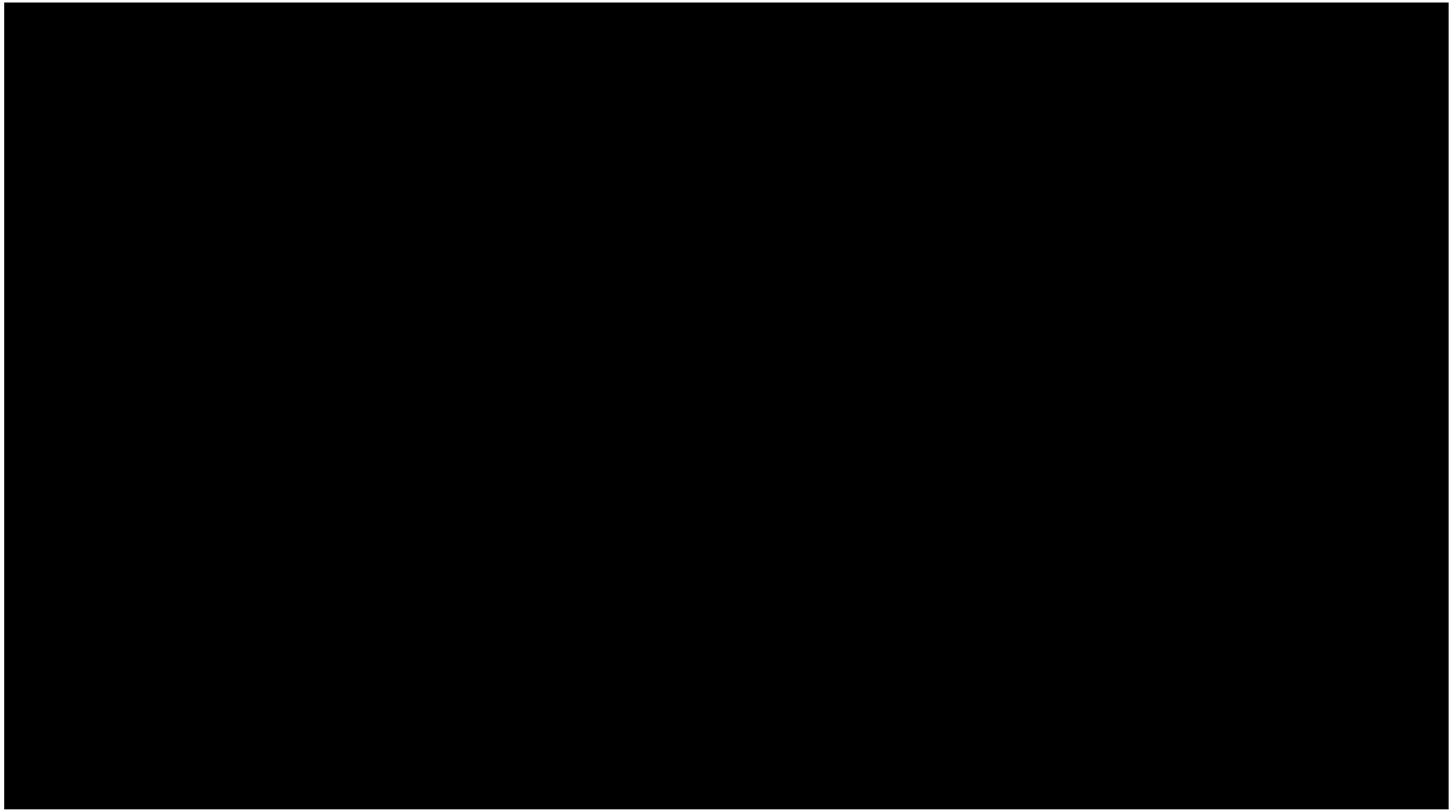




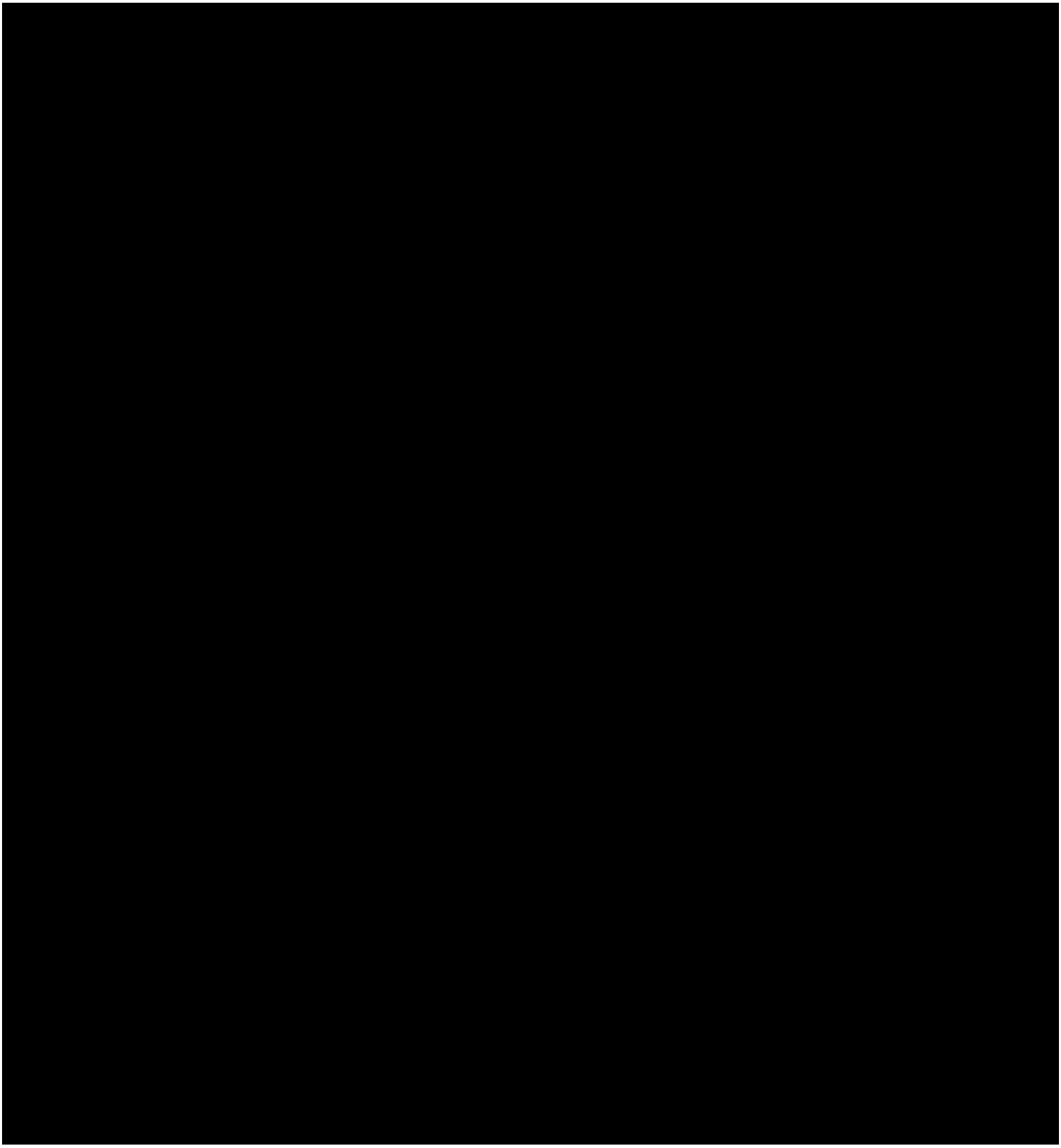


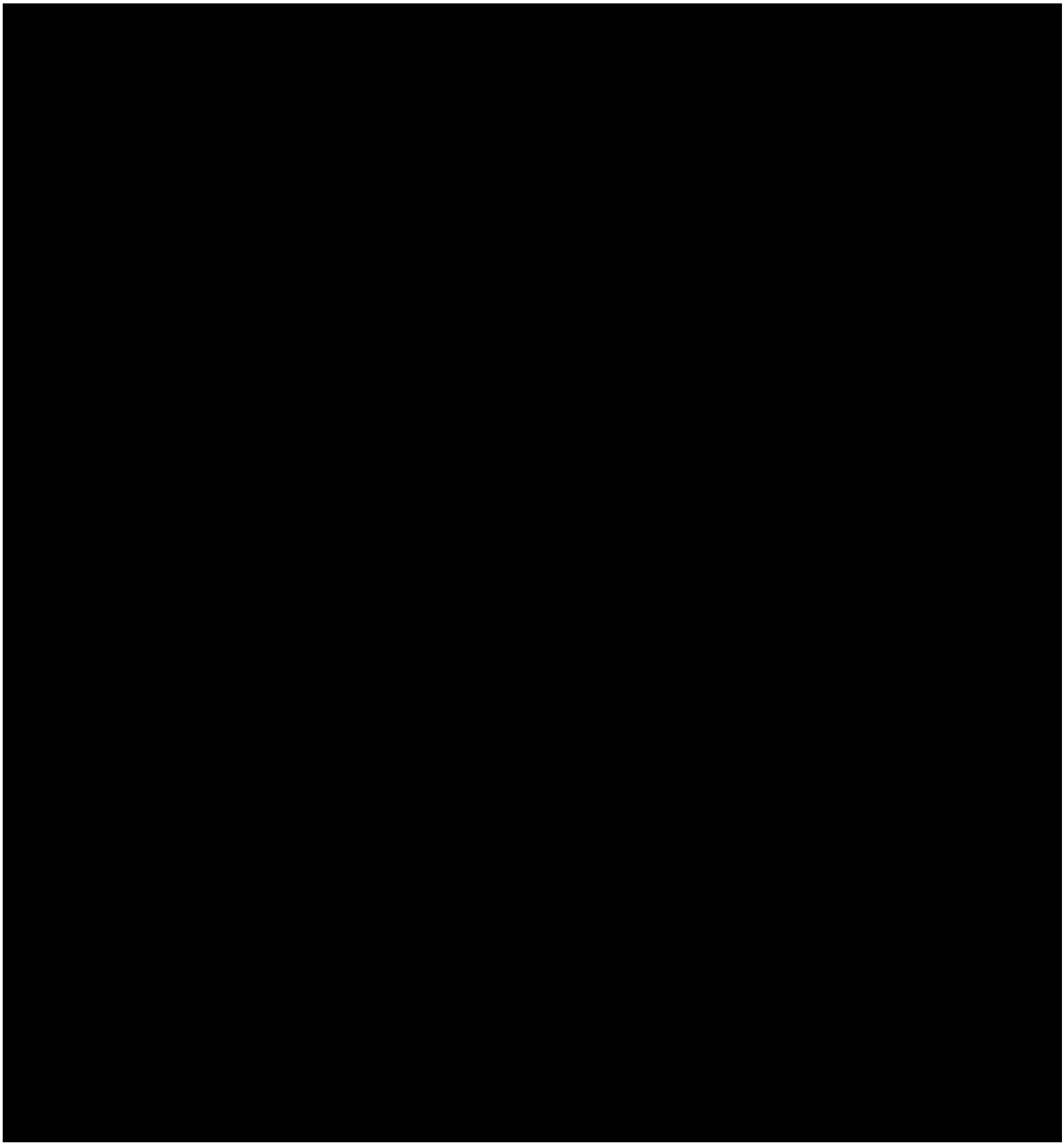


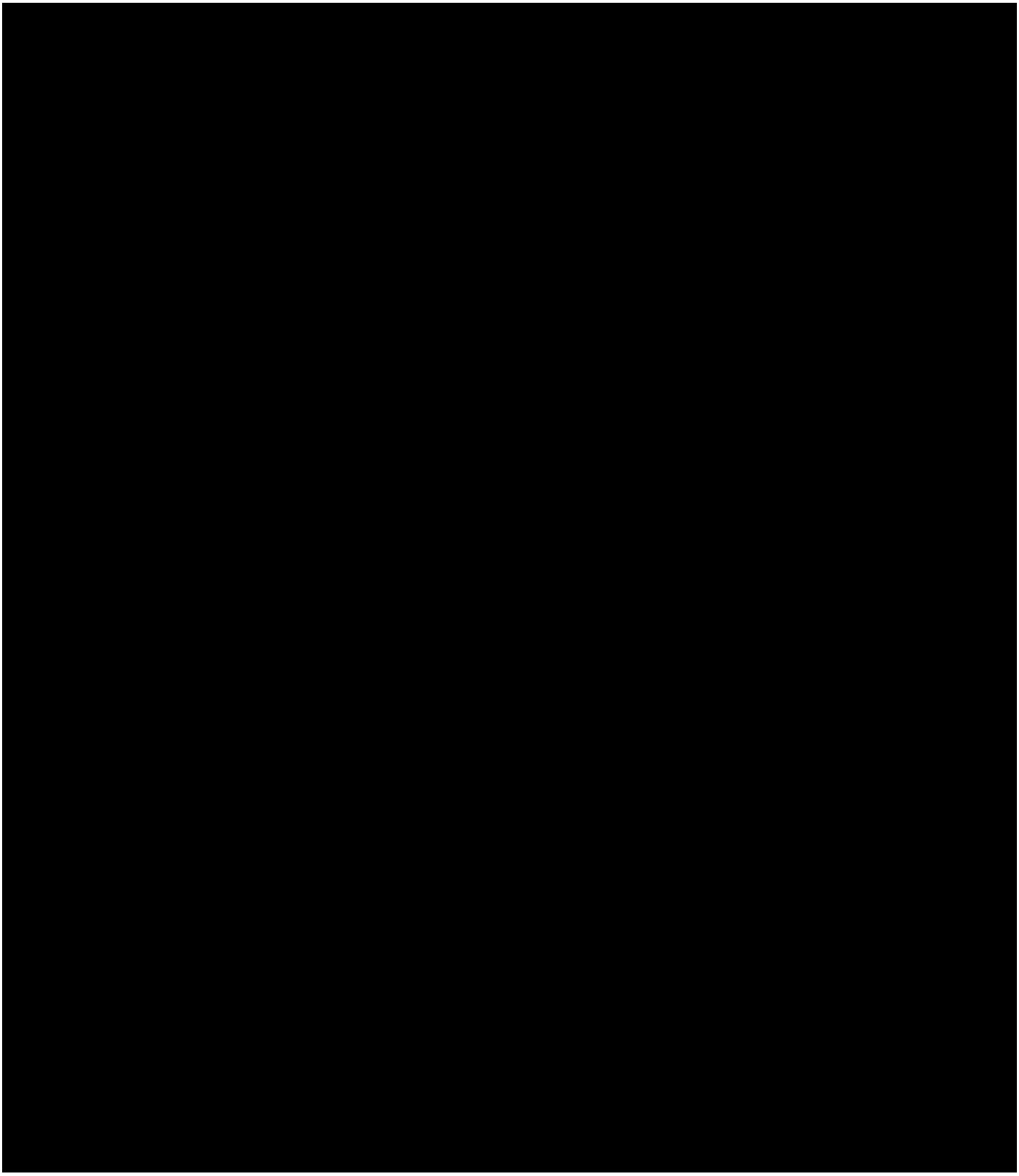


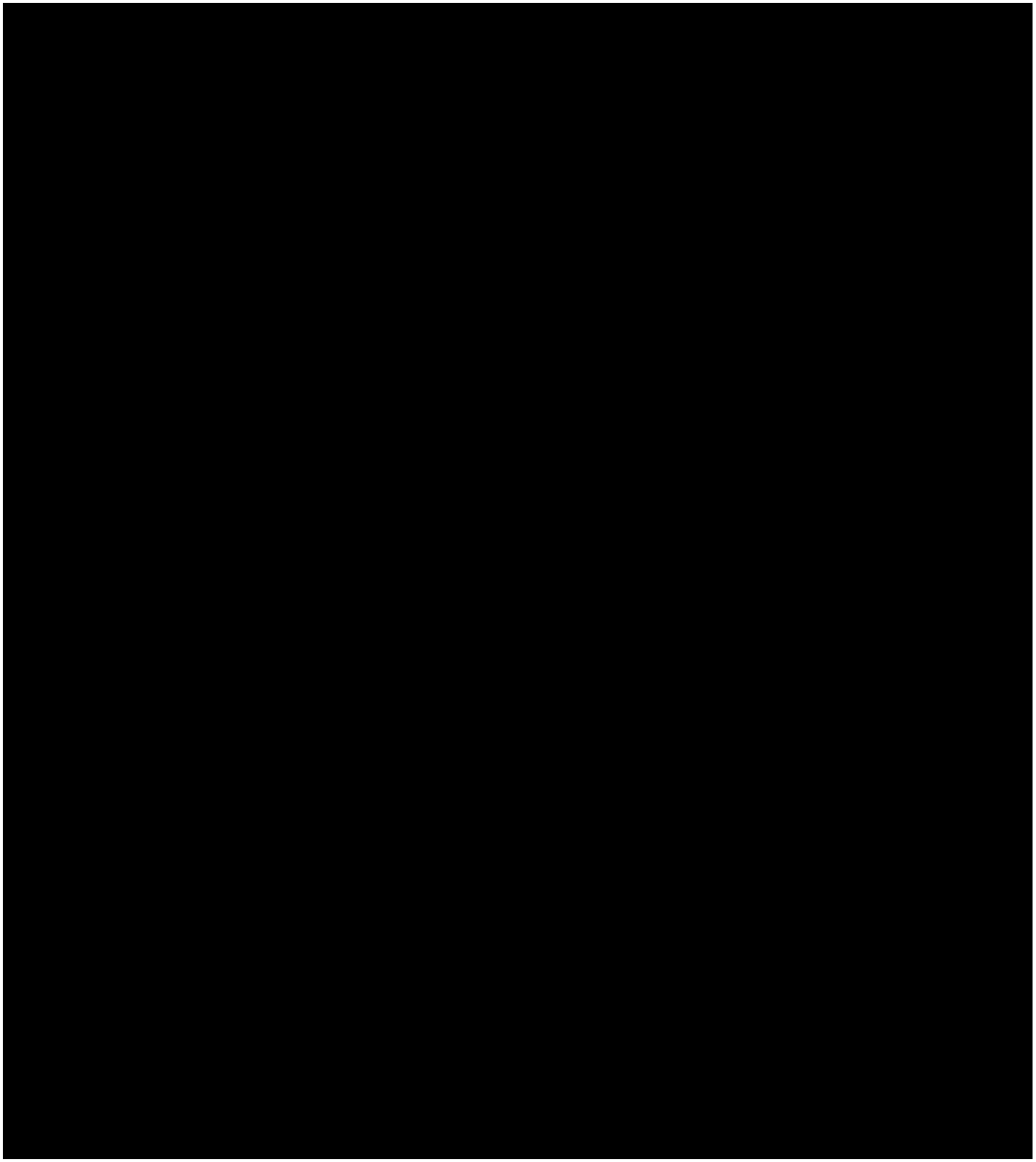


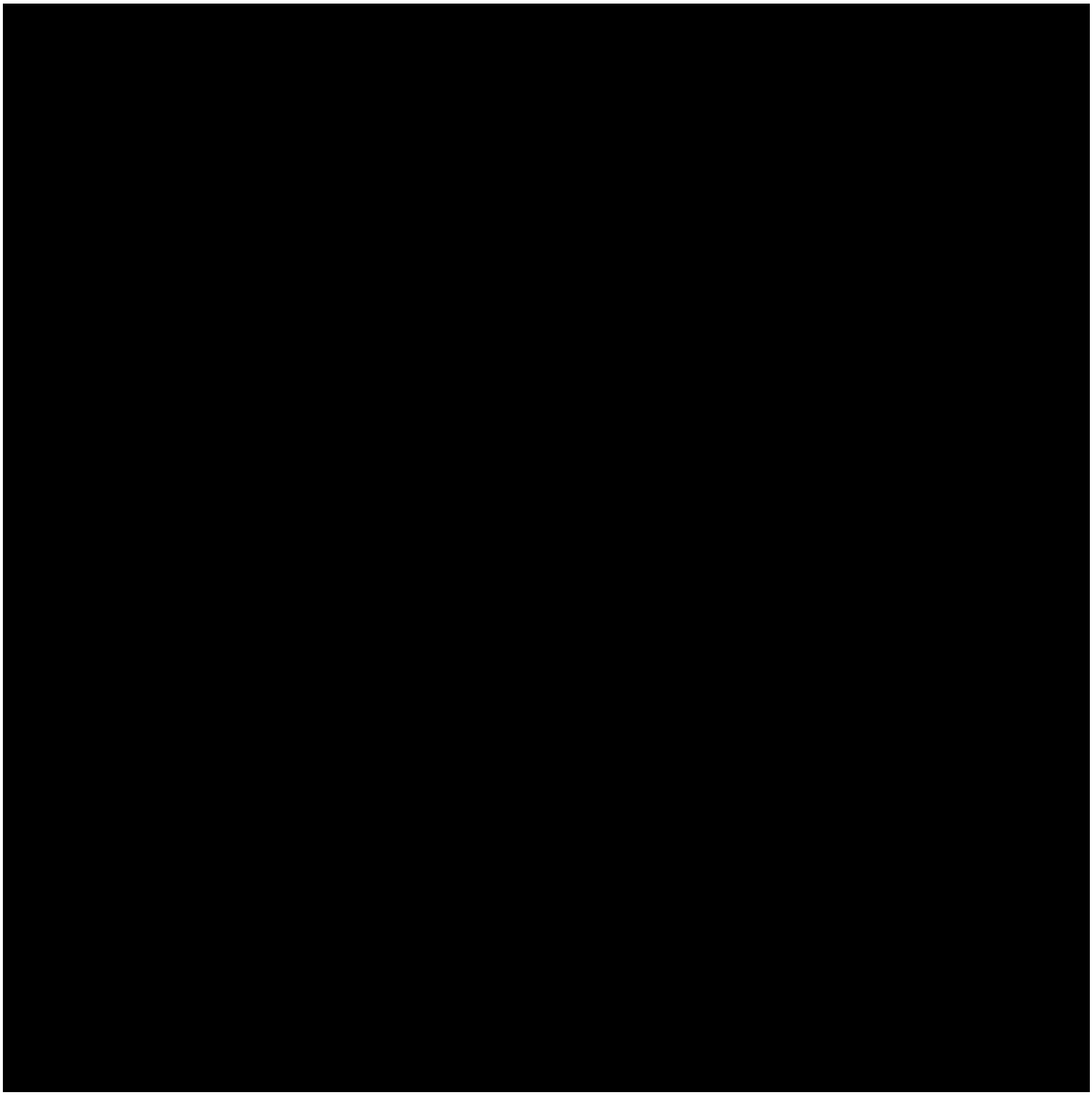
[redacted]

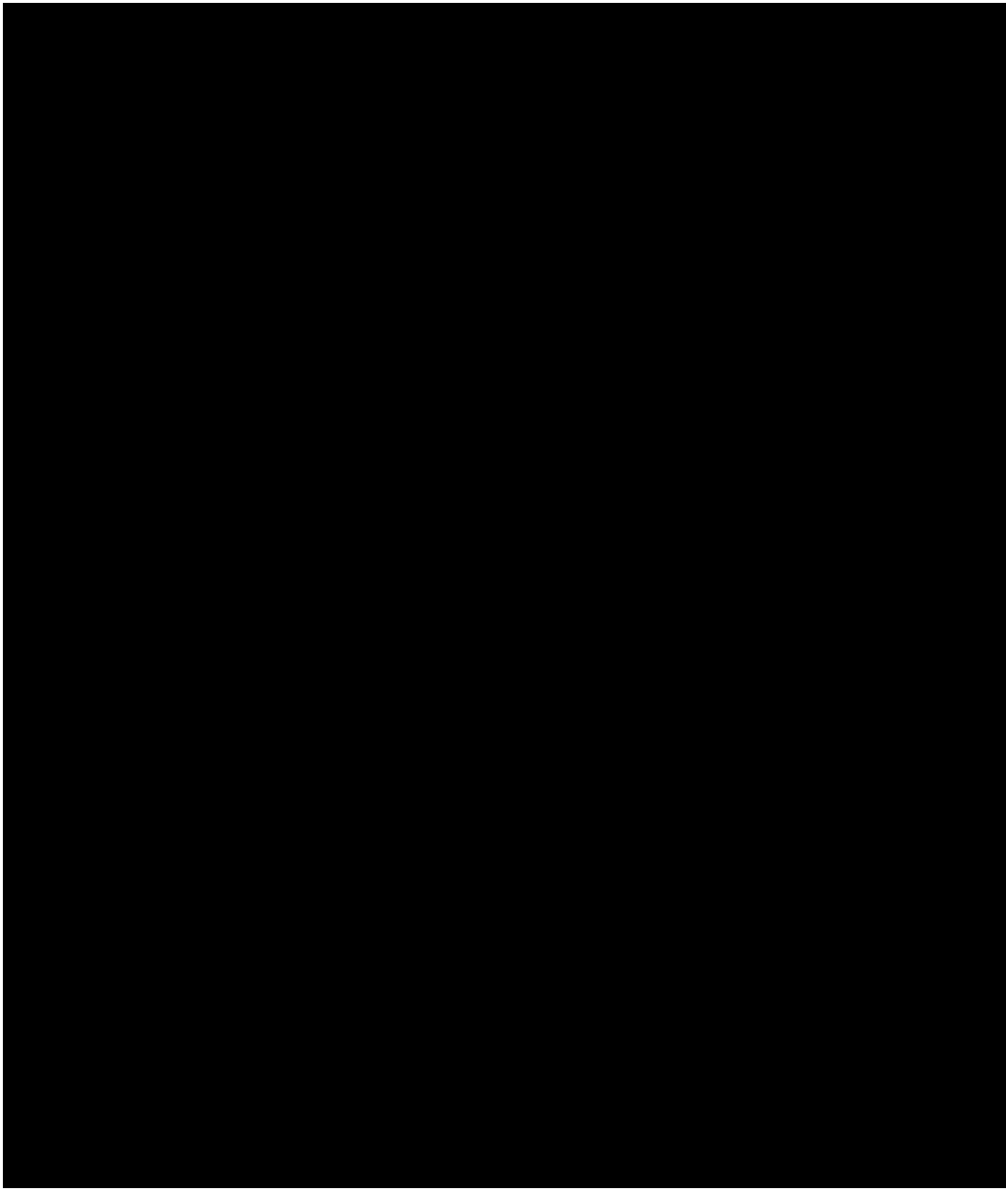


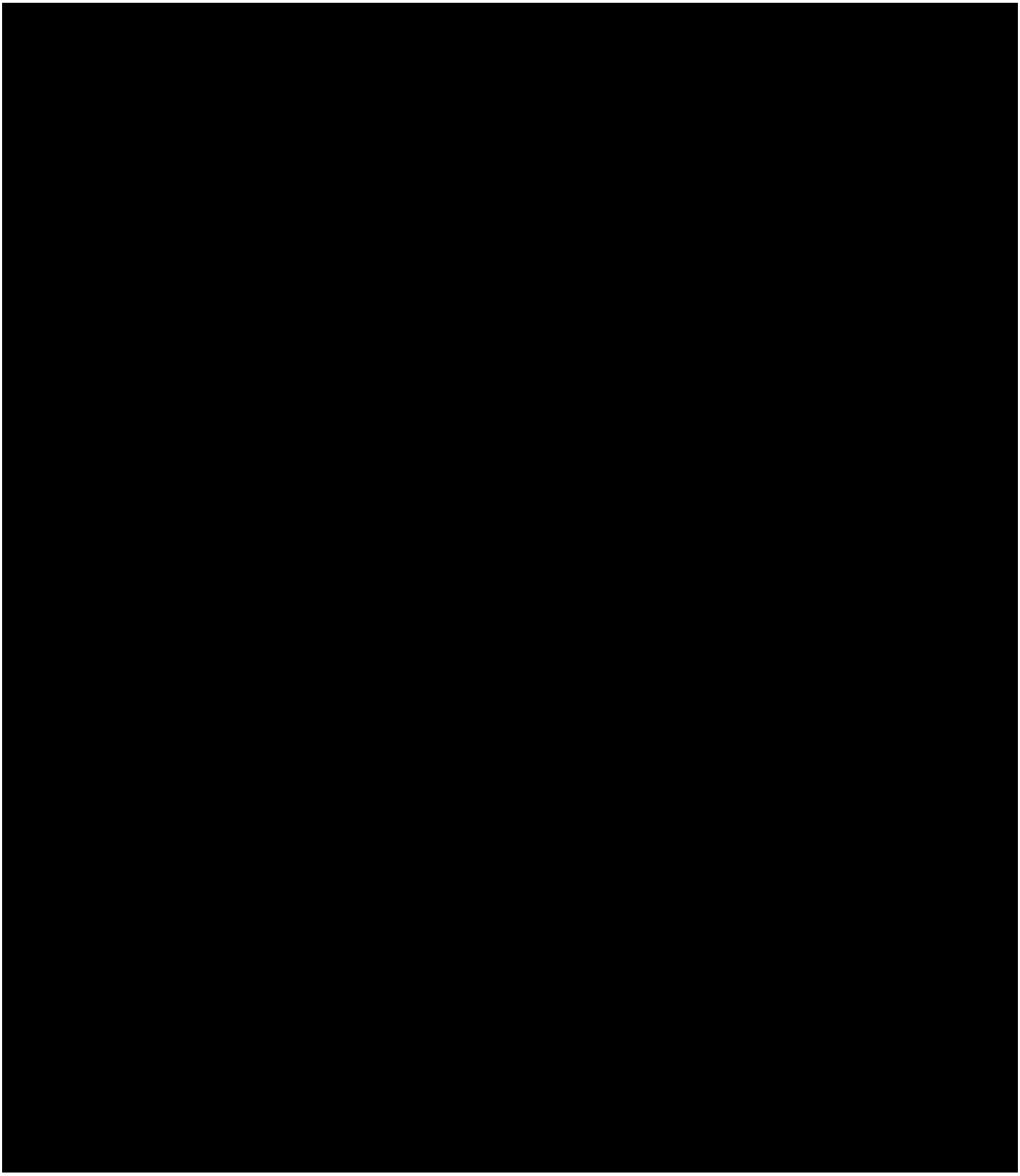


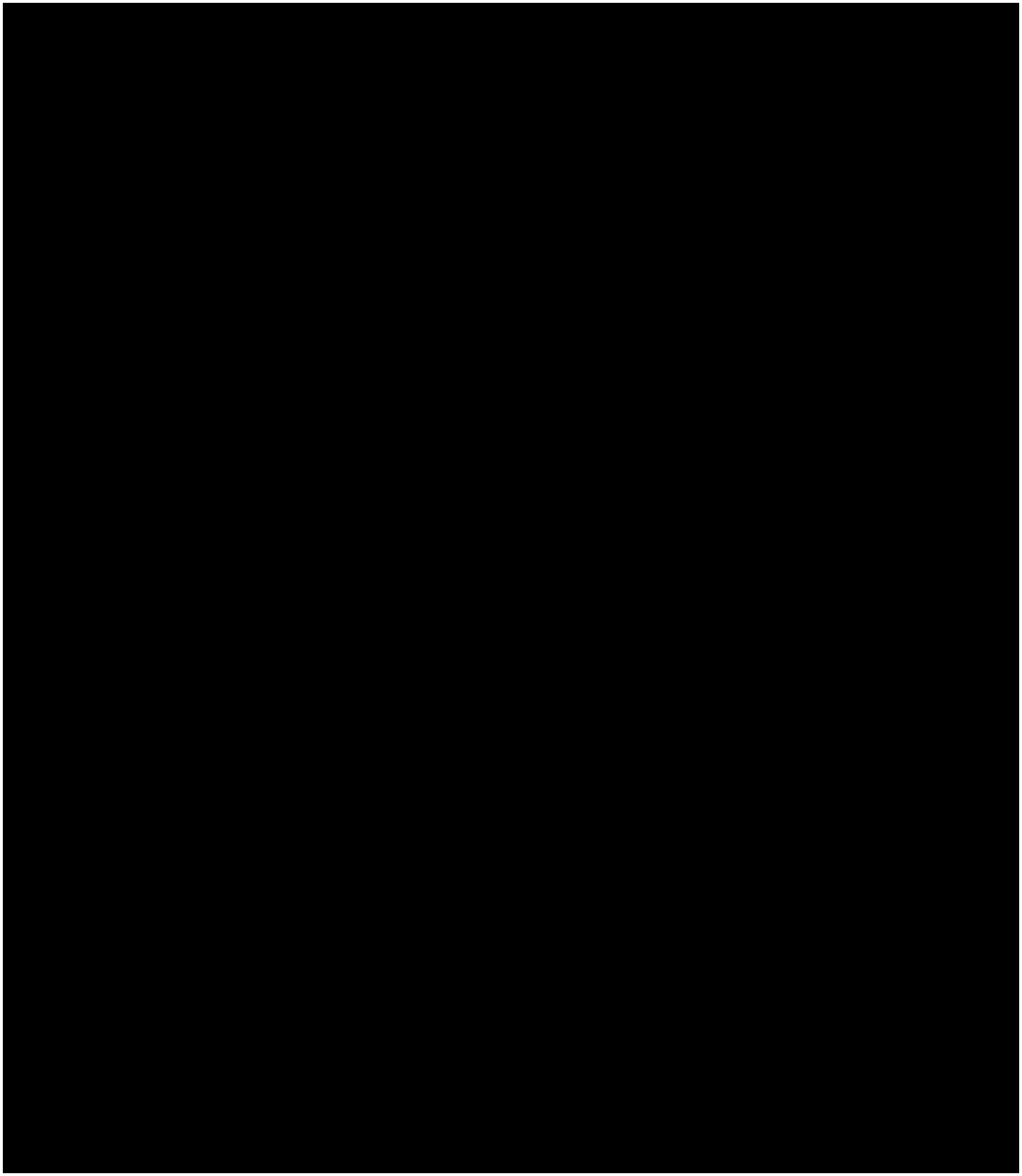


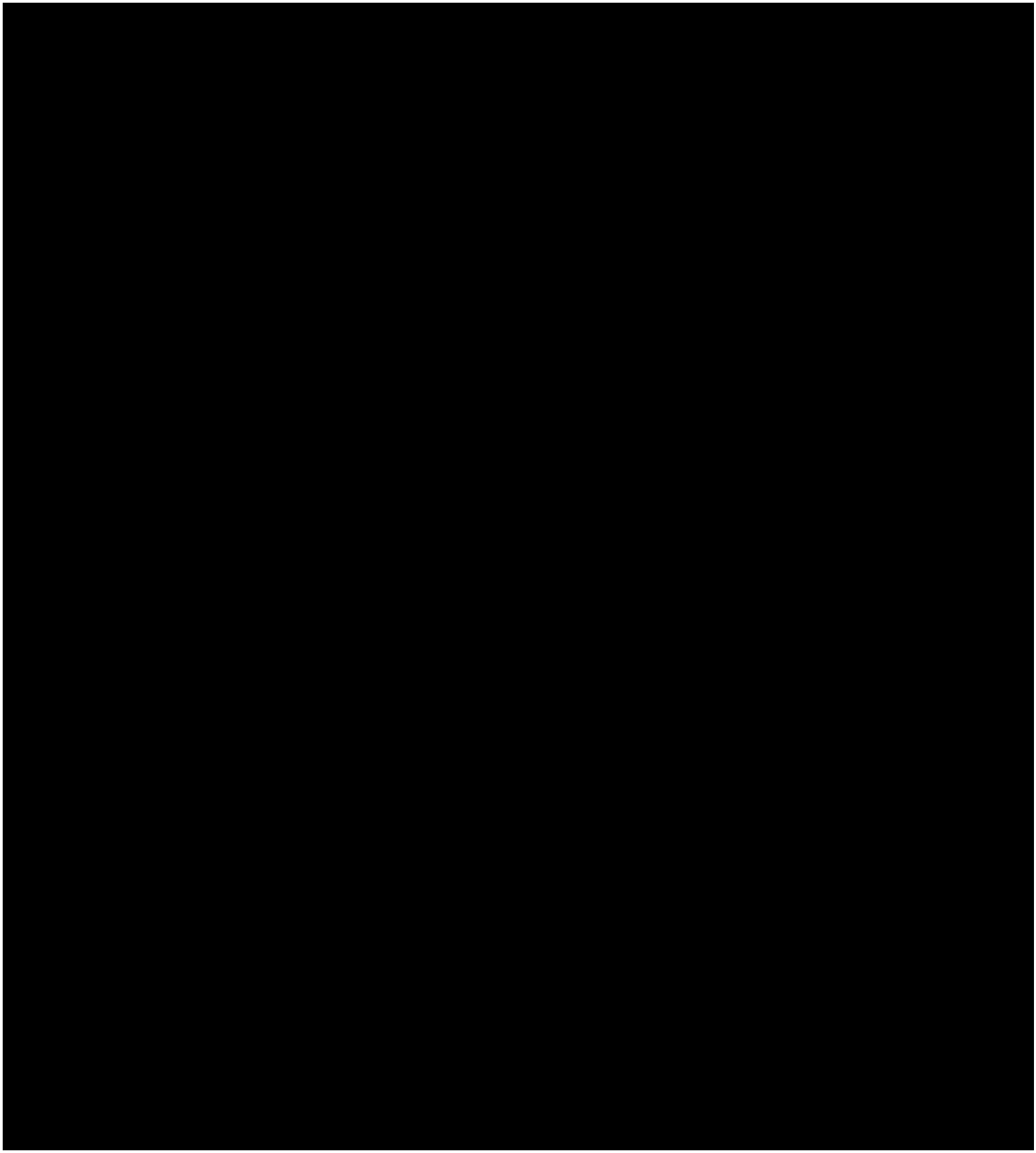










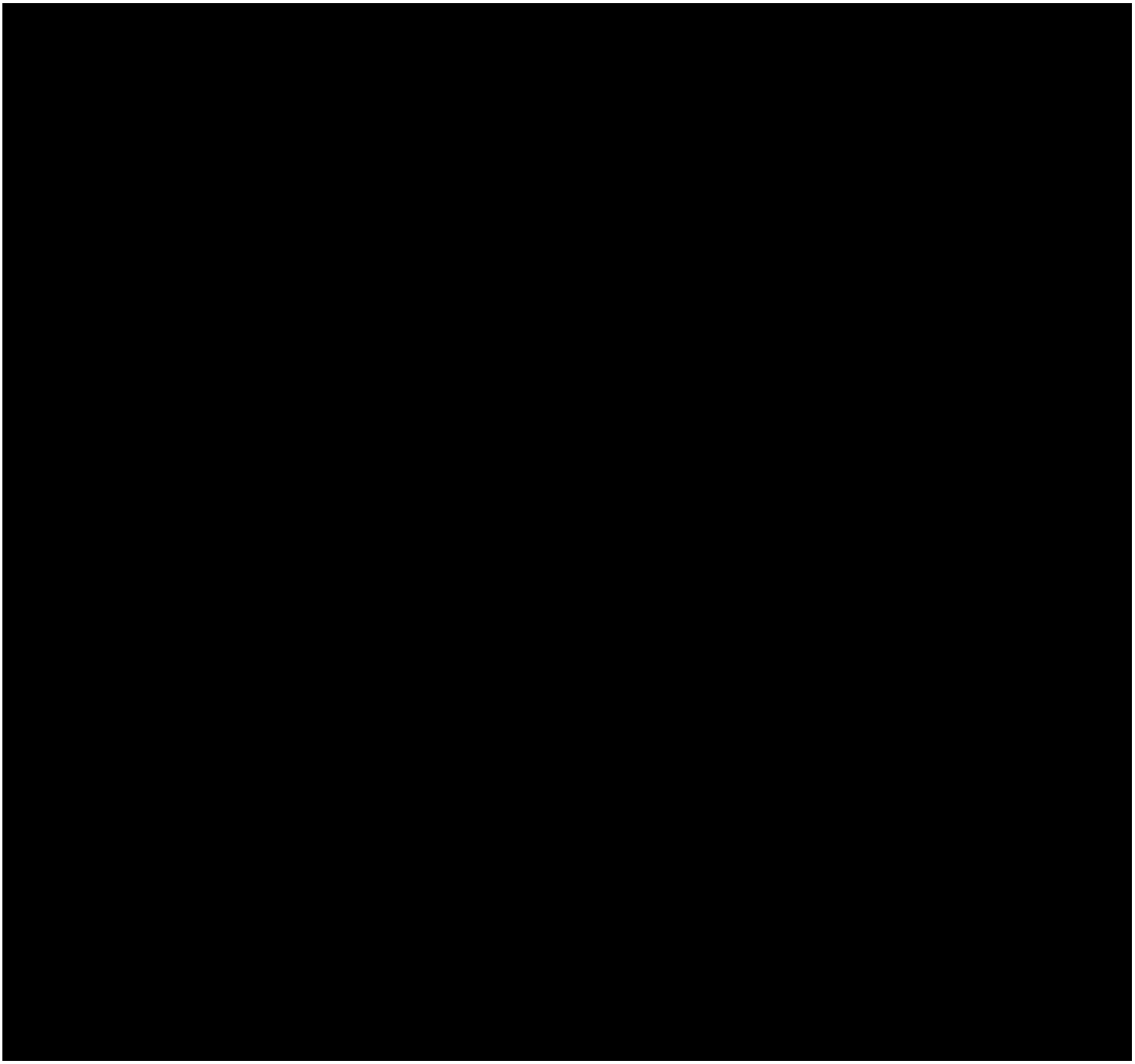


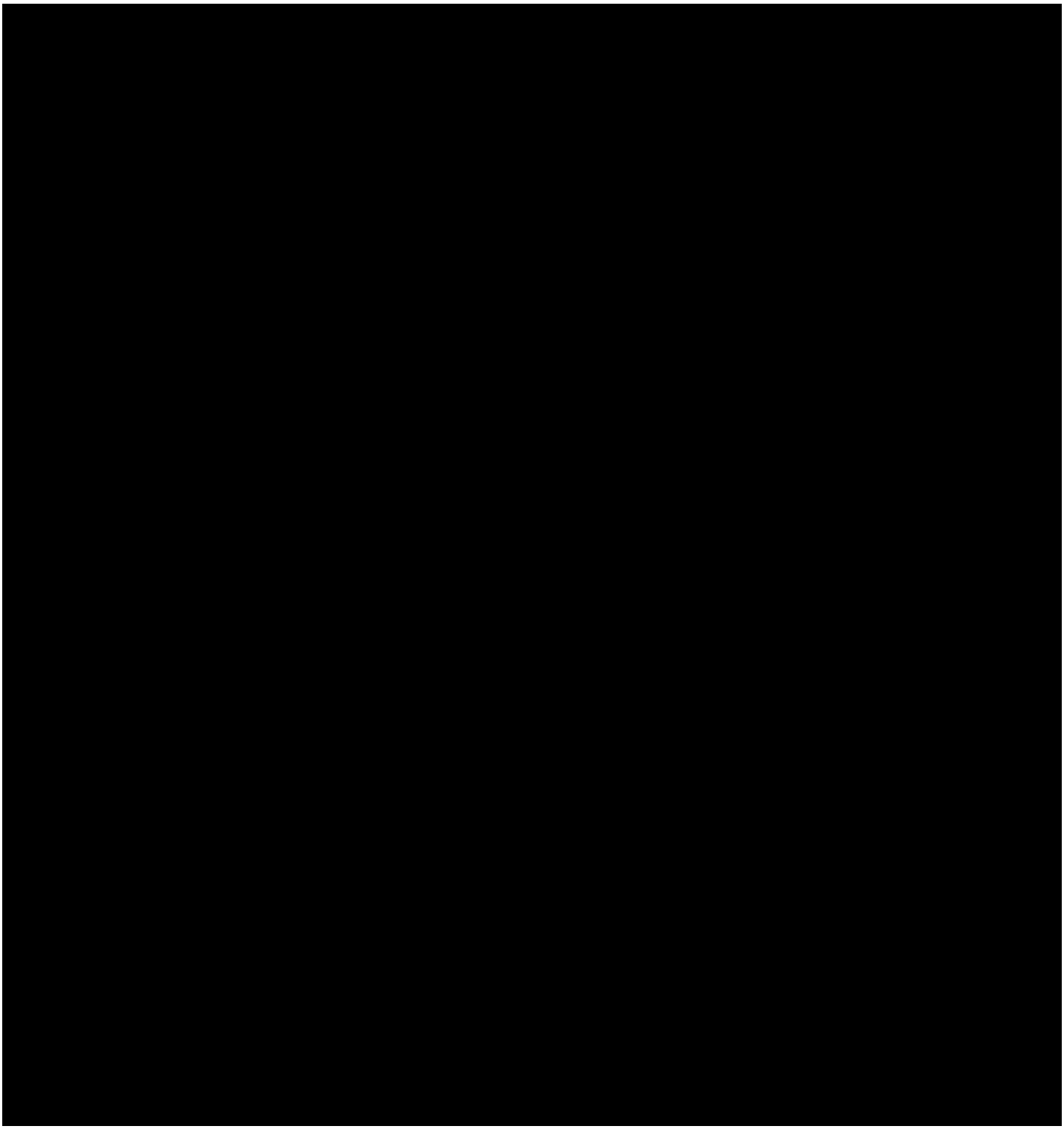
UNCLASSIFIED//FOR OFFICIAL USE ONLY

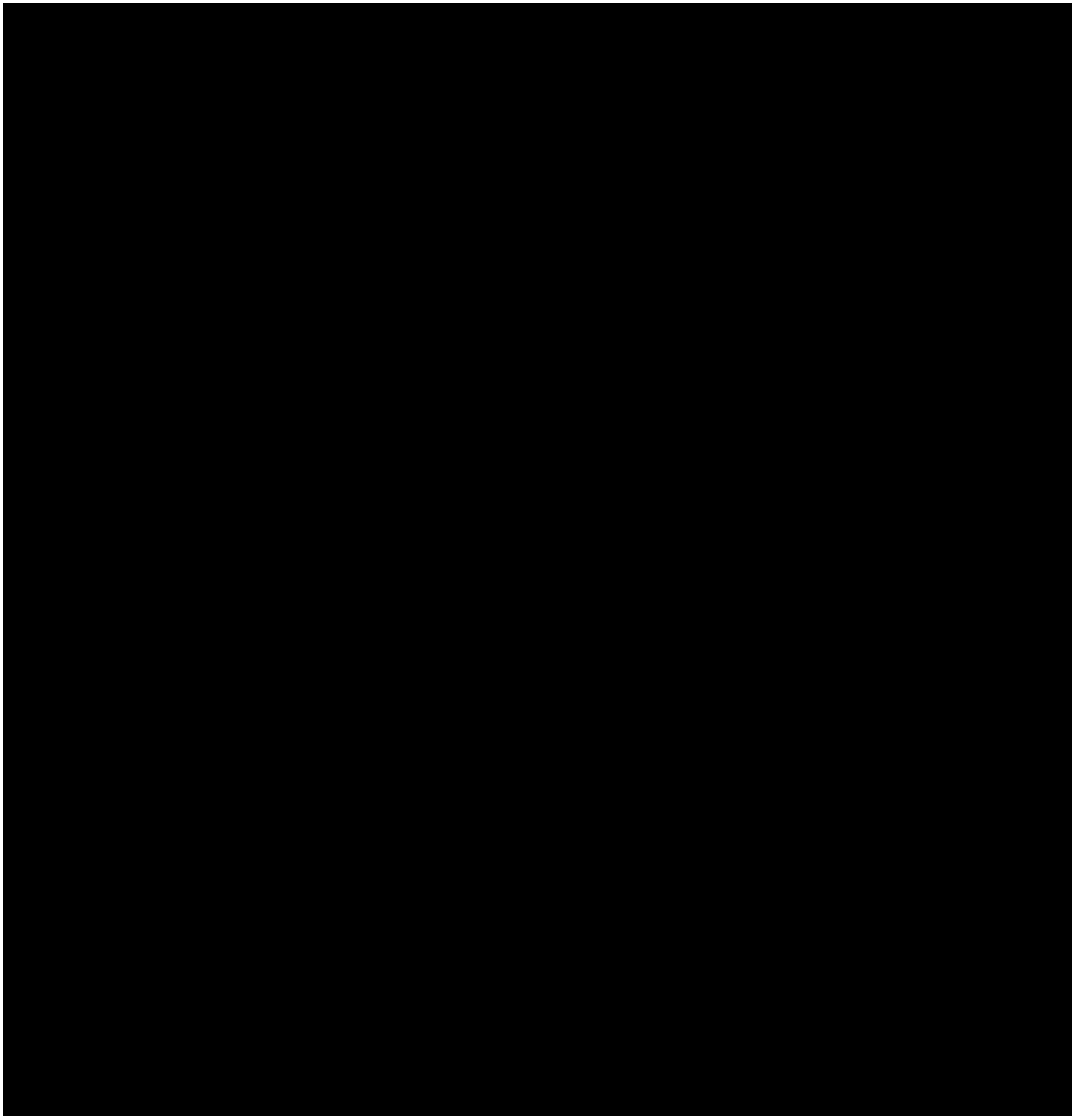
[redacted]

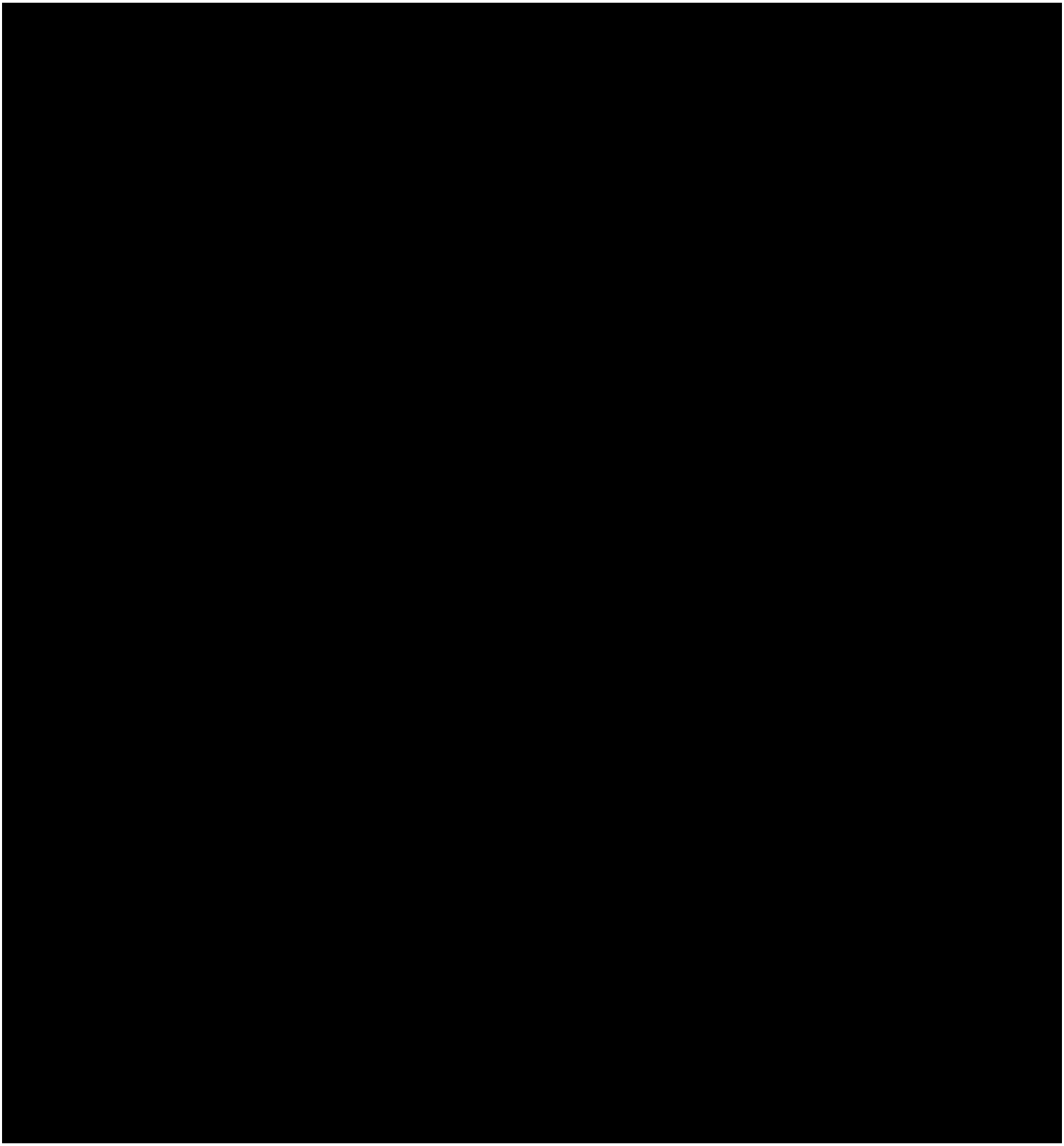
UNCLASSIFIED//FOR OFFICIAL USE ONLY

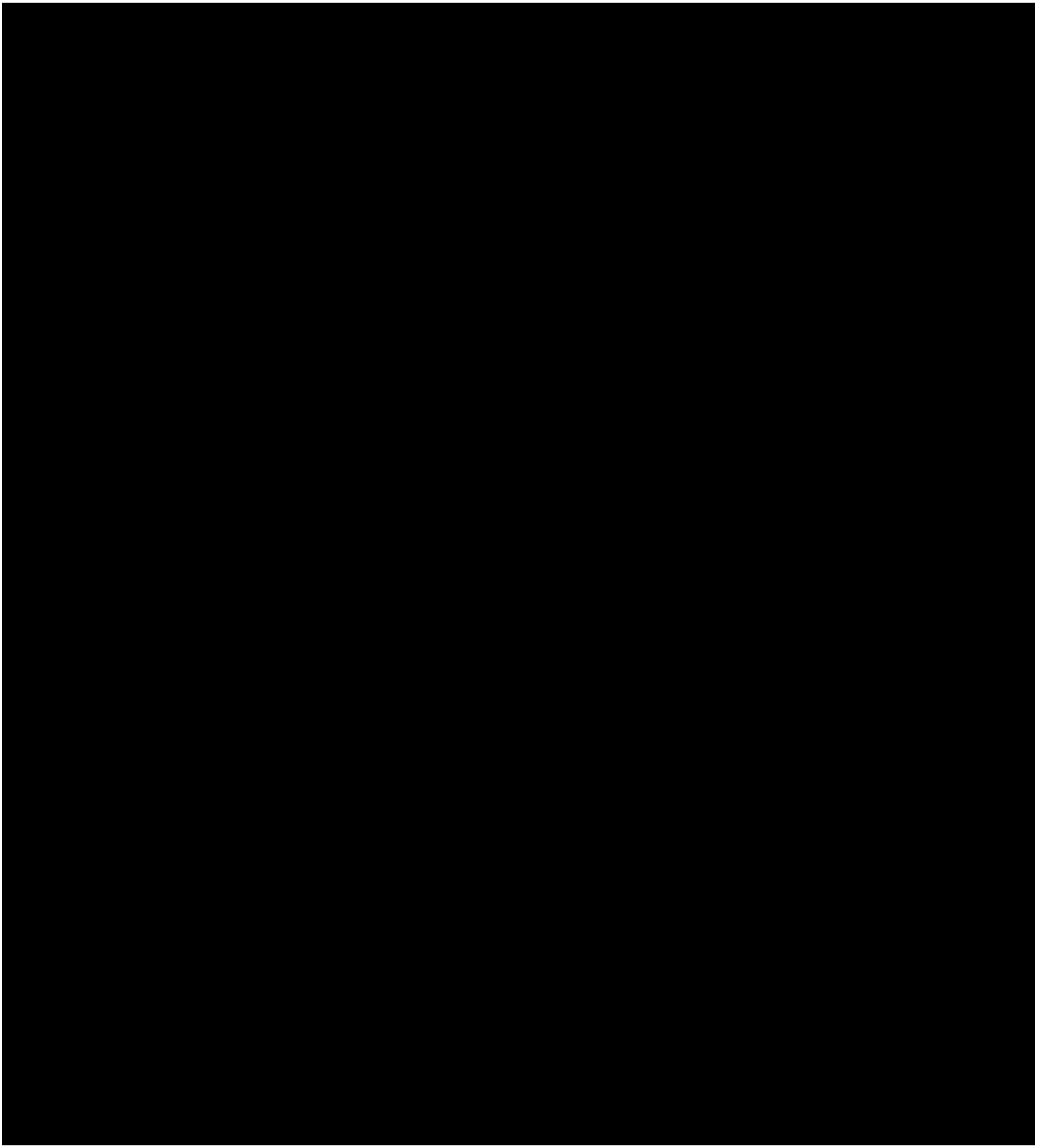
(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It is subject to release restrictions as detailed in the Homeland Security Act of 2002 (6 U.S.C. 482) and the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized need-to-know without appropriate prior authorization. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

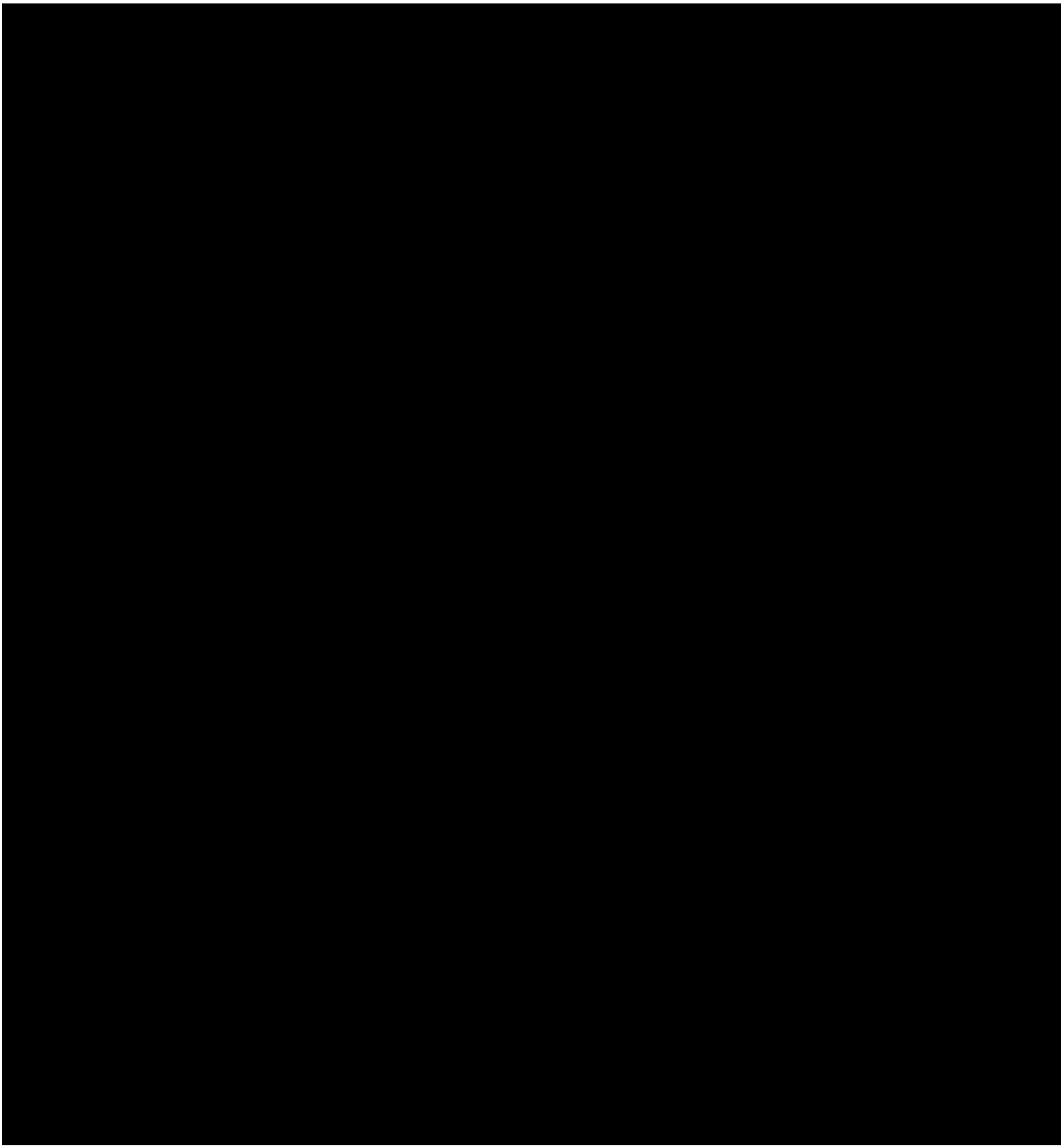


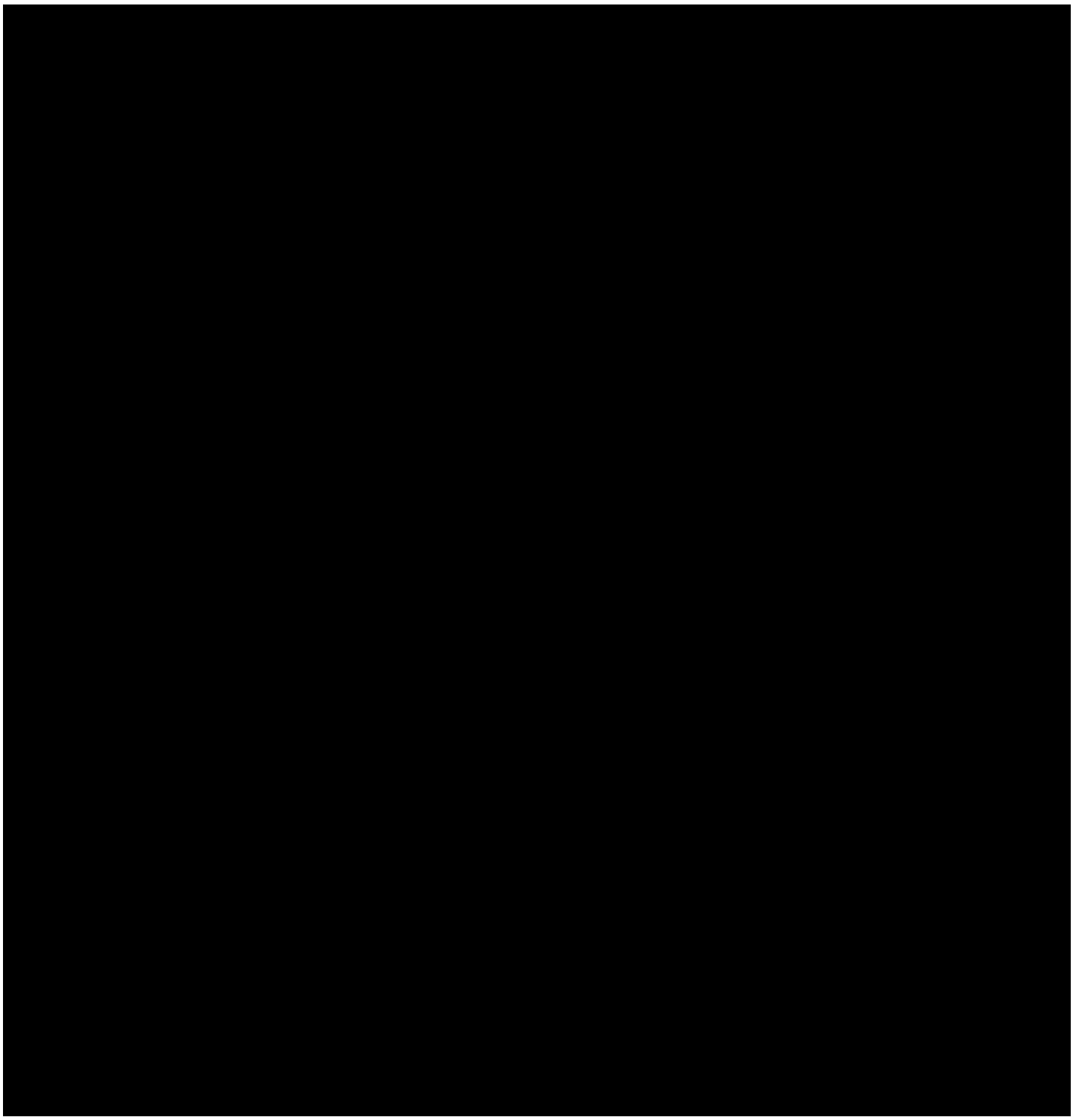












From: Hiraoka, Victoria A
To: Pace, Frank J; Tobon, John F
Subject: Re: MDM
Date: Tuesday, January 14, 2025 10:19:05 AM

John,

It was very nice to chat with you this morning. If you are able to give me examples of the MDM that you are combatting regarding smuggling, I can rework parts of the presentation for you to be more specific.

Mahalo!

Victoria Hiraoka
Communications Lead, State of Hawai'i Office of Homeland Security
VISIT US ON TWITTER | LET'S GET LINKED IN

From: Pace, Frank J <[redacted]>
Date: Tuesday, January 14, 2025 at 9:18 AM
To: Tobon, John F <[redacted]>
Cc: Hiraoka, Victoria A <[redacted]>
Subject: MDM

Aloha,

Here are some of Tori's products.

v/r

Frank

Frank J. Pace, Administrator
Office of Homeland Security
Hawaii Department of Law Enforcement
(O) [redacted]
(M) [redacted]
[redacted]

From: Tobon, John F
To: Pace, Frank J
Cc: Baggs, Kevin L; Hiraoka, Victoria A
Subject: [EXTERNAL] Re: Aloha
Date: Monday, January 13, 2025 9:57:36 AM

Frank,

Tomorrow at 0900 works for me, I will send an invite and get my DC folks on as well since it will be virtual.

Appreciate it!

Respectfully,

John F. Tobon
Assistant Director
Countering Transnational Organized Crime Division
Homeland Security Investigations
Mobile: [redacted]
Email: [redacted]

Follow us on X @HSI_HQ
Visit our website: www.hsi.gov

Sign Up To Receive HSI Cornerstone Newsletter HSI Cornerstone
HSI Cornerstone Homepage

From: Pace, Frank J <[redacted]>
Sent: Monday, January 13, 2025 9:54:54 AM
To: Tobon, John F <[redacted]>
Cc: Baggs, Kevin L <[redacted]>; Hiraoka, Victoria A <[redacted]>
Subject: RE: Aloha

Aloha,

Let's go with 0900 on Teams, I'll loop in our Comms Lead (Tori) who helps lead the MDM effort for OHS.

Happy to meet with Lt. Horos. Although I'm only available until 1030, Kevin Baggs may have more flexibility and can cover anything FC-related. I'll also find a POC for the JIATF-W.

Best,

Frank

Frank J. Pace, Administrator
Office of Homeland Security
Hawaii Department of Law Enforcement
(O) [redacted]
(M) [redacted]
[redacted]

From: Tobon, John F <[redacted]>
Sent: Monday, January 13, 2025 9:48 AM
To: Pace, Frank J <[redacted]>
Subject: [EXTERNAL] RE: Aloha

Aloha sir,

Let me know what date/time work for you and I will accommodate. We can do in person or virtual, whatever is easier.

On an unrelated note, a friend of mine referred a Professor at APCSS to me with the below request:

"I'm trying to help a friend and colleague who would like to speak with someone associated with the Hawaii State Fusion Center. Also possibly JIATF-W if there's any appropriate POC there.

Lt Andrew Horos is the DC Harbor Master and was DC SWAT before that. He's in Hawaii doing research on OSINT info sharing between law enforcement and with DoD/IC. His past work focused on OSINT intel prior to the Jan 6th events. He's currently on Kauai speaking with PD there and will be here for the day on Tues. "

I was thinking of sending them your way, any objection? I will be speaking with him sometime on Tuesday.

Respectfully,

John F. Tobon
Assistant Director
Countering Transnational Organized Crime Division
Homeland Security Investigations
Mobile: [redacted]

Email: [redacted]

Follow us on X @HSI_HQ
Visit our website: www.hsi.gov

Sign Up To Receive HSI Cornerstone Newsletter HSI Cornerstone
HSI Cornerstone Homepage

From: Pace, Frank J <[redacted]>
Sent: Friday, January 10, 2025 10:43 AM
To: Tobon, John F <[redacted]>
Subject: RE: Aloha

Aloha John,

Happy New Year! Following up on the request for MDM support. How does next week look for you?

Best,

Frank

Frank J. Pace, Administrator
Office of Homeland Security
Hawaii Department of Law Enforcement
(O) [redacted]
(M) [redacted]
[redacted]

From: Tobon, John F <[redacted]>
Sent: Saturday, December 21, 2024 5:13 AM
To: Pace, Frank J <[redacted]>
Subject: [EXTERNAL] Re: Aloha

Frank,

Excellent! Much appreciated! Enjoy your vacation.

Respectfully,

John F. Tobon
Assistant Director
Countering Transnational Organized Crime Division
Homeland Security Investigations
Mobile: [redacted]
Email: [redacted]

Follow us on X @HSI_HQ
Visit our website: www.hsi.gov

Sign Up To Receive HSI Cornerstone Newsletter HSI Cornerstone
HSI Cornerstone Homepage

From: Pace, Frank J <[redacted]>
Sent: Friday, December 20, 2024 12:16:17 PM
To: Tobon, John F <[redacted]>
Subject: Re: Aloha

Aloha John,

Great to hear from you! we'd be happy to collaborate on the issues with MDM. In fact, my Comms Lead just created new materials on the subject. I'm OOO until 2 January. I'll be available to meet anytime after 1/8/25.

Look forward to seeing you soon.

Best,

Frank

Frank J. Pace
Administrator
Office of Homeland Security
[redacted]

From: Tobon, John F <[redacted]>
Sent: Friday, December 20, 2024 11:36:46 AM

To: Pace, Frank J <[redacted]>
Subject: [EXTERNAL] Aloha

Aloha sir,

Hope you are well. I'm reaching out to tap into the expertise your office has developed on countering misinformation as a result of your work on the fires on Maui. We are having issues with misinformation on social media platforms that is being promoted by human smuggling organizations.

As part of my new role, I would like to develop a campaign to counter the misinformation, hoping you would be interested in collaborating.

I'll be around in Honolulu until at least the end of January, let me know when you are available and I will accommodate your schedule.

Respectfully,

John F. Tobon
Assistant Director
Countering Transnational Organized Crime Division
Homeland Security Investigations
Mobile: [redacted]
Email: [redacted]

Follow us on X @HSI_HQ
Visit our website: www.hsi.gov

Sign Up To Receive HSI Cornerstone Newsletter HSI Cornerstone
HSI Cornerstone Homepage

From: CDP
To: [redacted]
Subject: [EXTERNAL] FEMASID Registration Confirmation
Date: Tuesday, January 7, 2025 1:48:26 PM

Victoria Hiraoka,

You have successfully registered for your FEMASID. Please save this information in a safe place or commit it to memory.

Your FEMASID: [redacted]

This is an automated email. Replies to this email address may not be read. Instead, send questions or comments to [redacted]

From: Pace, Frank J on behalf of Tobon, John F
To: Hiraoka, Victoria A; Baggs, Kevin L
Subject: FW: Mis-Dis-and Malinformation (MDM) Discussion

-----Original Appointment-----
From: Tobon, John F <[redacted] <mailto:[redacted]> >
Sent: Monday, January 13, 2025 10:05 AM
To: Tobon, John F; Smith, Selwyn; Semidey, Jose L; Pace, Frank J
Subject: Mis-Dis-and Malinformation (MDM) Discussion
When: Tuesday, January 14, 2025 9:00 AM-9:45 AM (UTC-10:00) Hawaii.
Where: Microsoft Teams Meeting

Microsoft Teams Need help? <[redacted]>

Join the meeting now [redacted]

Meeting ID: [redacted]

Passcode: [redacted]

Dial in by phone

+1 332-249-0712,[redacted]# <tel:+13322490712,[redacted]> United States, New York City

Find a local number [redacted]

Phone conference ID: [redacted]

For organizers: Meeting options <[redacted]> |
Reset dial-in PIN
[redacted]
