We are happy to answer your questions about Anduril's Lattice system. While Lattice is designed to detect and classify object types, not to identify individuals or collect personal information, we take seriously the important issues of transparency and responsibility surrounding use of data. The answers below relate to the current border implementation of Lattice, referenced in your email.

As discussed below, Lattice is designed to alert operators about types of activity--such as pedestrian, vehicle, or drone activity--in remote or difficult to patrol areas. Lattice is not designed to identify specific individuals or collect personal information, including device information. Additionally, Lattice is subject to privacy controls mandated by federal and state laws, and Anduril goes further than that to minimize the impact to privacy and civil liberties.

- **What kind of data is collected by Lattice? (e.g., device IDs such as IMSI and IMEI data, metadata, location data).**
  - Lattice sensors collect image data (day/night images, with no audio) and RADAR data. This data is similar to data collected by existing manned sensor systems deployed at the border for many years. Lattice applies computer vision technology to these images to detect and classify object types (typically a "person," "vehicle," or "drone"), not to identify specific individuals or collect personal information.
- **What are the data sources for the data collected by Lattice?**
  - The sensors referenced above: optical/infrared imaging units and RADAR.
- **Does the platform rely on interception of any kind? (e.g., via IMSI catchers)**
  - No.
- **What kind of access controls does the system have?**
  - Technical and policy access controls are used to ensure data can only be accessed by authorized users and for the authorized Government purposes set by the customer, in this case, the Department of Homeland Security. Data is not used or accessed by Anduril outside of what is necessary to provide technical support to the Government.
- **Are live video feeds made available to CBP or Anduril?**
  - Live video feeds are available to authorized users of Lattice. However, in the more typical workflow a small number of still images are sent to operators as part of a detection alert.
- **Is facial recognition used in Anduril's cameras?**
  - No. Lattice image data is not used to identify individuals, but rather to detect activity (e.g. vehicles, animals, pedestrians) in remote areas along the border.
- **At what point are humans involved in reviewing data collected or analysed by Lattice?**
  - Operators are alerted when a human being, vehicle, or drone is detected by a Lattice sensor in an area of interest. Operators have the option of dismissing the alert or viewing the image feed to determine whether to respond.
- **Who is given access to collected or analysed data?**

    - Data is only accessed by authorized users and for the authorized Government purposes set by the customer, in this case, the Department of Homeland Security. Data is not used or accessed by Anduril outside of what is necessary to provide technical support to DHS.
- **How long will data be stored by Anduril?**
    - Anduril follows applicable legal and agency-specific data retention standards of its customers. In the case of the current border implementation of Lattice, images and other content are held for no longer than 30 days, per existing DHS policy.

In addition to the above, we have taken the following steps to ensure that Lattice is deployed responsibly and consistently with legal and ethical norms:

- The system is designed to detect and classify object types and not to identify individuals or collect personal information. Computer Vision analysis is limited to the identification of object types: detection events are labeled as person, vehicle, UAS, or similar, and sent to operators, minimizing the personal information collected or inferred by the system.
- Populated areas such as roads and cities are typically excluded from sensor scan patterns. By design, sensors are placed in remote, difficult to reach, areas where the smuggling of drugs and persons is a known problem, and where human patrols would be dangerous and expensive.
- The system is designed as “human in the loop”: while initial alerts are generated using computer vision, they are immediately pushed to a human decision-maker for validation and for any action impacting the rights of individuals.