**Breakout Discussion Goal:**

Our ACT API work group has identified one needed resource for stakeholders across our distribution; a Security Discussion Guide to provide guidance when stakeholders are enacting partnerships involving Application Programming Interfaces (APIs).

A sub-group has begun developing potential discussion areas where partners will need to ensure security aspects are covered before entering into agreements.

***This is where we need your help!***

**Below are some areas we have discussed. Please think about and share in this session:**

* **What aspects of the identified areas need more detail?**
* **What other areas are we missing?**
* **What level of detail should we provide?**

**Background Detail:**

**1)** Create a ‘Partner API Security Discussion Guide’ to help address security needs for APIs.

Develop guide to address what aspects agents and smaller vendors should be concerned about.

Create a checklist’ of Security-related areas to discuss with potential API partners.  Examples:

* Priority: Ensuring my API partner does not increase first party’s risk.
  + Security SLAs
  + Data protection
  + Points at At-Rest
  + Online/Offline point
  + Assignment of rights
  + Is there a right to request data purge (e.g., GDPR ‘be forgotten’)
* Data security vs. systems security
* Who owns the data?
* At what points is ownership impacted or changed?
* How is it secured to fit the Owner?  User?
* Identify market and why this is important to understand –
  + Open (Google Play Store), vs Apple App Store
* Identify vulnerabilities
  + Degradation of performance, systems impacts
* Education on credential protection – ex: shared from agent w/3rd party vendor, also shared w/in management system network
* Infrastructure – physical & digital (server closets, typical equipment concerns)
* Poss: What level of security should be expected, vs. agency size/complexity
  + What do they have in place that should be addressed (vs size/exemptions), who is in charge, testing.
  + Type of PII/PHI
* Does the firm have cyber liability?
* Best practices for Open APIs – Are these being used, modern authentication protocols

Develop variations for potential partnership types;

* 3rd-Party Vendor <-> management system
* Carrier <-> management system
* Carrier <-> Agency/Brokerage
* Agency-initiated/requested connections vs Agency-created (via purchased toolkit)
* Management System <-> Agency Applications
* Other

*\*\* If similar guides/checklists exist, try to leverage those. Must determine if others are willing to share.*

***Other points identified by Breakout participants:***