**Follow Up to March 26, 2019 Question**
**From Chairman Collins**

**Re: Electronic Access Card Encryption**

**Question:**

Chairman Collins asked how the is encryption is handled on these cards? Are they encrypted periodically or after every use?

**Answer:**

The HID iClass Seos Smart cards are encrypted when the cards are created. To prevent the cards from being cloned, HID now encrypts the entire card payload, including the Wiegand code, PIN, password, and other relevant information, in a secure data wrapper in the chip which is tied to that specific card. Additionally, with these cards, HID has incorporated new Master Authentication and encryption keys.

The door transaction consists of three components. The card, the reader and the CBORD Authentication server. These three components provide a high level of security. When the smart card is touched to the reader, the first action is to verify the user on the CBORD server to the card. Once authenticated, the reader will then share a portion of its encryption key for card confirmation. Provided the transaction is confirmed, the door request will then be forwarded back to the CBORD server to fulfill the requested action.

Resource:
Shane Ammons
Chief Information Security Officer
972-881-5769
sammons@collin.edu