National Association of Attorneys General – Fall Consumer Protection Conference

23 October 2017
What is the FBI’s Message?

Commitment
• The FBI is committed to combating crimes against children and vulnerable populations

Awareness
• The way we think about child safety issues is evolving with technology
• Convenience and entertainment comes with security implications – connecting to the Internet introduces new risks

Support
• The FBI values and supports the work of the security researcher communities and child protection groups
• The FBI strives for continued engagement with other government agencies, law enforcement, researchers, advocacy groups, industry, and the public to support efforts in child safety issues
Why Are There Concerns?

Security
• Market growth is expansive and sufficient security may be overlooked

Knowledge of the Issues
• Consumers may not fully consider the risks associated with Internet-connected devices
• Threat landscape grows and changes so often, difficult to keep up

Interaction
• This generation never knew life without the Internet
  • Children often naturally provide sensitive and personal information without consideration for implications
Why Are There Concerns (continued)?

For consumers: The game has changed – children’s conversations and sensitive information are recorded and transmitted

- Where is it going, who can access it (authorized and unauthorized), how secure is it when it’s transmitting, how secure is it when it’s stored

For Law Enforcement

- How could potential access to the toys and data be used by bad actors to exploit children and consumers
Connecting to the Internet introduces risks for hacking and exploitation - Toys could be at greater risk if these types of security measures are not used:

- **Device**
  - Built-in security measures on the device
  - Secure connections to Wi-Fi or Bluetooth – use of encryption, passwords/PIN when pairing

- **User/Parent Applications**
  - Secure sites to host recorded conversations, access controls to the toy, and personal information of children and families

- **Data in transit**
  - Use of encryption and digital certificates

- **Data in storage**
  - Secure data storage sites – servers, cloud services, third-party services

- Closely monitoring a child’s use of any device that’s connected to the Internet, especially toys and other devices that incorporate personal information and interactions.

- Carefully read privacy disclosures and policies (from the company and for third parties) and consider the following:
  - If the company is a victim of a cyber intrusion and your data may have been accessed, will the company notify you?
  - If vulnerabilities in the toys or devices are discovered, will they notify you and make patches or updates available?
  - Where is the data being stored?
  - Who has access to the data?
  - If changes are made to the privacy policies, will they notify you?
  - Is the company contact information openly available in case you have questions or concerns?
• Conduct thorough research using consumer product reviews, cyber security research, and consumer advocacy and privacy resources.

• Provide only what is minimally required when creating user accounts (some companies offer special features if additional personal information on the child is provided)

• Research how the toy or device connects to the Internet (Bluetooth, Wi-Fi) and what types of security measures it uses to connect (use of PIN or other authentication) and transmit data (encryption)

• Ensure the toy is turned off when not in use, particularly those with cameras and/or microphones.
Who to Contact

• Local Field Offices – [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field)

• Internet Crime Complaint Center (IC3) – [www.ic3.gov](http://www.ic3.gov)

• Cyber Division, Technology Cyber Intelligence Unit - [TCIU@fbi.gov](mailto:TCIU@fbi.gov)