ANSI/TMA-AVS-01

WHAT IS ANSI/TMA AVS-01?

- **A**larm **V**alidation **S**coring – an intrusion alarm scoring or classification standard.

- Three primary components:
  - 1) Accurately and consistently score or classify intrusion alarms
  - 2) Consistent communication method for relaying these events to ECC/PSAP
  - 3) Compliance to help ensure the standard is being followed properly

TMA-AVS-01 STRATEGY

- **Value**
  - An ANSI standard that adds value to security customers, the ECC/PSAP community and the security industry.
- **Credibility**
  - Uses available data to raise the confidence of dispatch requests / Calls for Service to ECCs/PSAPs.
- **Flexibility**
  - Accommodates innovation by allowing new technologies and datasets to be adopted when analyzing alarm activations (automated or manual processes)
- **Adoption**
  - Easily and widely adopted by both the Security Industry and the ECC/PSAP community.

AVS-01 CHAIRS

Mark McCall, Director of Global Operations, Immix

David Holl, Dir Public Safety, Lower Allen Township

Larry Folsom, SVP and Chief Monitoring Officer, ADT

TMA-AVS-01 COMMITTEE MEMBERSHIP

☑ 46 committee members – everyone who applied, was accepted

Committee Balance

Member Categories	Number of members
• Monitoring	18
• Public Safety (IACP, NSA, IAFC, APCO, NENA)	7
• Manufacturing/Service Providers	17
• Consultants/NRTLs	4

STANDARD DEVELOPMENT

Information Gathering

- Public Safety Survey
  - To identify the critical data that will increase or reduce law enforcement response level.
  - To identify what data has value to law enforcement but is not critical information.
  - To identify what data has minimal value to law enforcement.
- Monitoring Center Data Collection
  - Researched available applicable to alarm activations
  - Collected and analyzed actual alarm and false alarm data
  - Determined significance (weighting) of data
  - Modeled processes to create a “score” using available data

STANDARD DEVELOPMENT

Two Working Groups

- Data Working Group
  - Reviewed all the data collected to identify trends and relationships.

- Public Safety Working Group
  - Distributed drafts by IACP Public Safety committee members, PPVAR, and SIAC to PSAP/ECC and Law Enforcement communities.

AVS-01 Committee

- Met several times a month to collaborate on writing the standard.

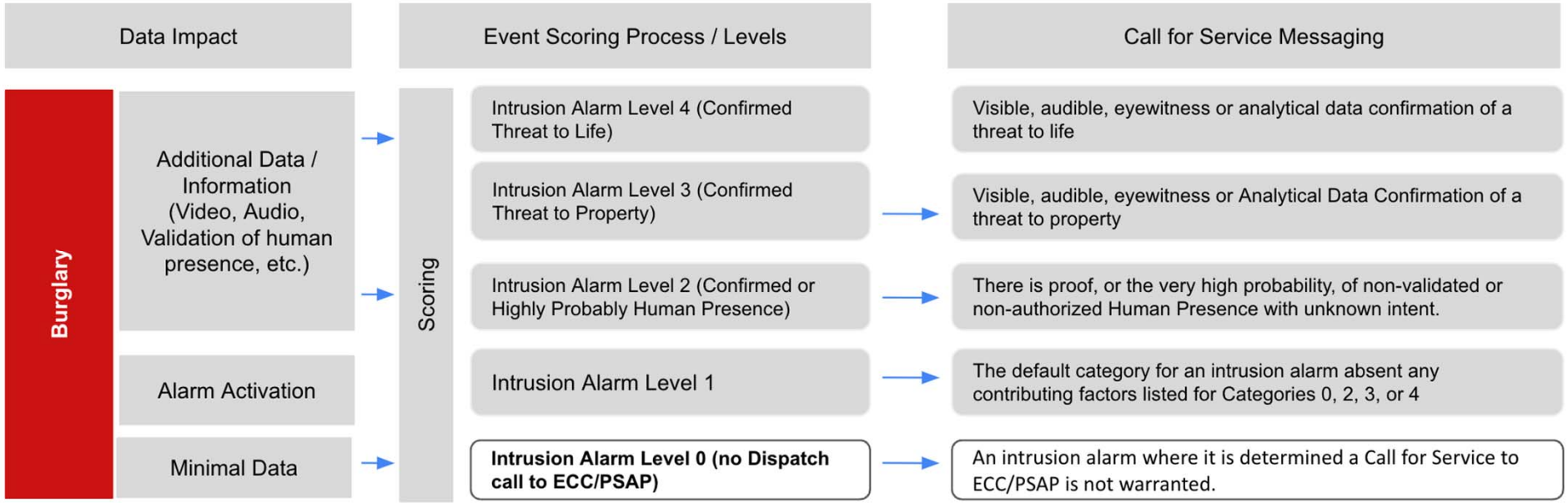
AVS-01 REPORTING CATEGORY DEFINITIONS

Five Levels of Classification

- Intrusion Alarm Level 4 (Confirmed Threat to Life)
- Intrusion Alarm Level 3 (Confirmed Threat to Property)
- Intrusion Alarm Level 2 (Confirmed or Highly Probably Human Presence)
- Intrusion Alarm Level 1 (Call for service with limited or no additional information)
- Intrusion Alarm Level 0 (no Dispatch call to ECC/PSAP)

The Monitoring Association

Public Safety Request
Match Existing Protocols / Policies



AVS01 – REPORTING CATEGORY DEFINITIONS

Intrusion Alarm Level 4 (Confirmed Threat to Life)

- Visible, audible, eyewitness, or analytical data confirmation of a threat to life.
- Examples: Observation by the operator or through analytics, potential life-threatening language or sounds heard, physical altercation seen, the authorized user confirms or perceives a threat to life, analytic confirmation of pre-determined threat, e.g., Weapons presented in a life-threatening manner, firearms heard, Biometrics or similar technologies of a known dangerous person, and the like.

Intrusion Alarm Level 3 (Confirmed Threat to Property)

- Visible, audible, eyewitness, or Analytical Data Confirmation of a threat to property.
- Examples: Observation of broken glass or other Structural Damage, obvious/likely criminal activity, heard, detected, or confirmed.

AVS01 – REPORTING CATEGORY DEFINITIONS

Intrusion Alarm Level 2 (Confirmed or Highly Probably Human Presence)

- There is proof, or a very high probability, of non-validated or non-authorized Human Presence with unknown intent.

- Examples of defined events Manual process:
  - Video of person(s) on premises that cannot be validated or authorized to be onsite, and there is no additional data present that raises to AL3 or AL4.
  - Audio of person(s) on premises that cannot be validated or authorized to be onsite, and there is no additional data present that raises to AL3 or AL4.
  - Open/Close/Cancel/Bypass by unauthorized user code received.
  - Seismic detection with ATM, Vaults and the like.
  - License Plate Recognition activation of 'known foe' within protected area, plus an intrusion alarm.
  - Confirmation of presence of human(s) with unknown intent. (e.g., cell application, any technology that allows observation of premises, and the like)
  - Manual Fire Pull/Emergency phone signal, in addition to intrusion alarm.
  - Eyewitness call that states person is at premise.
  - And the like

AVS01 – REPORTING CATEGORY DEFINITIONS

Intrusion Alarm Level 2 (Confirmed or Highly Probably Human Presence)

- There is proof, or the very high probability, of non-validated or non-authorized Human Presence with unknown intent.

- Automation Examples:
  - Video/Audio analytics or data, where the video/audio is not presented to an operator, but that indicate high probability of Human Presence.
  - Presence detection analytics that determine human device (e.g., cell phone, Bluetooth) is on premises.
  - Lidar/Radar/WIFI or other platforms to indicate that human movement inside is occurring.
  - And the like.

AVS01 – REPORTING CATEGORY DEFINITIONS

- **Intrusion Alarm Level 1**
  - The default category for an intrusion alarm absent any contributing factors listed for Categories 0, 2, 3, or 4

- **Intrusion Alarm Level 0 (no Dispatch call to ECC/PSAP)**
  - An intrusion alarm where it is determined a Call for Service to ECC/PSAP is not warranted.

  - This determination may be modified by:
    - Receipt of a CANCEL/OPEN/CLOSE, a recently armed system
    - Verbal confirmation from the Contact List
    - Visible, audible, eyewitness or Analytical Data confirmation that no threat is present
    - An event, from the site, that could only be the result of an authorized individual. Such as bypass, late to open, and the like.
    - A Data Message, such as from an End User interface, from an authorized individual, indicating there is no emergency at the protected premises.


The Monitoring Association®
THANK YOU
Together. Moving. Ahead.

MH