MICHIGAN CYBERSECURITY

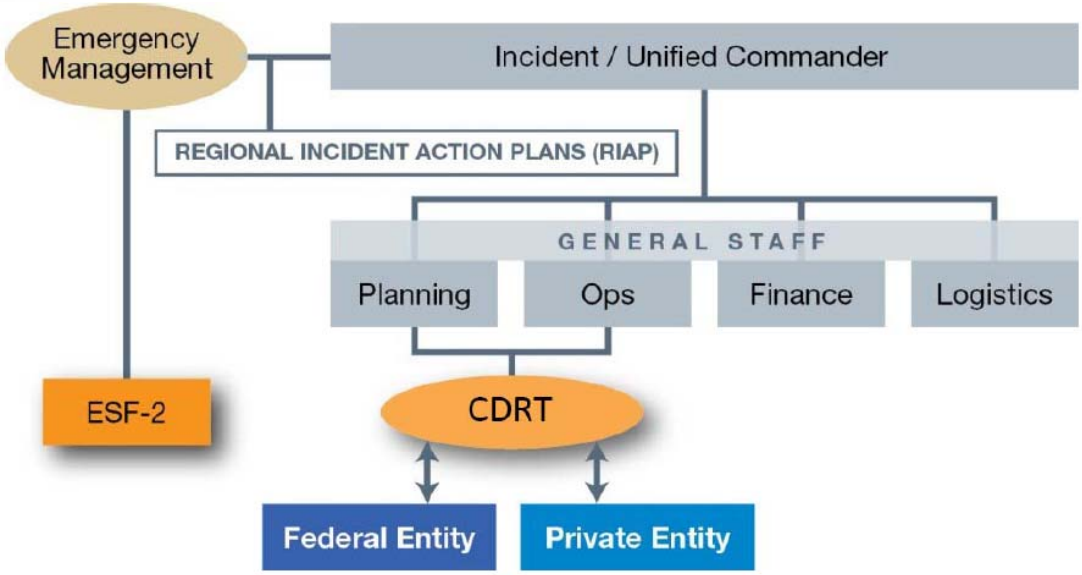
MICHIGAN STATE POLICE
EMERGENCY MANAGEMENT & HOMELAND SECURITY DIVISION

LT. COL. CHRIS A. KELENSKE | July 25, 2018

CYBERSECURITY ECOSYSTEM

CDRP

- Cybersecurity is integrated into our existing EMHS Structure

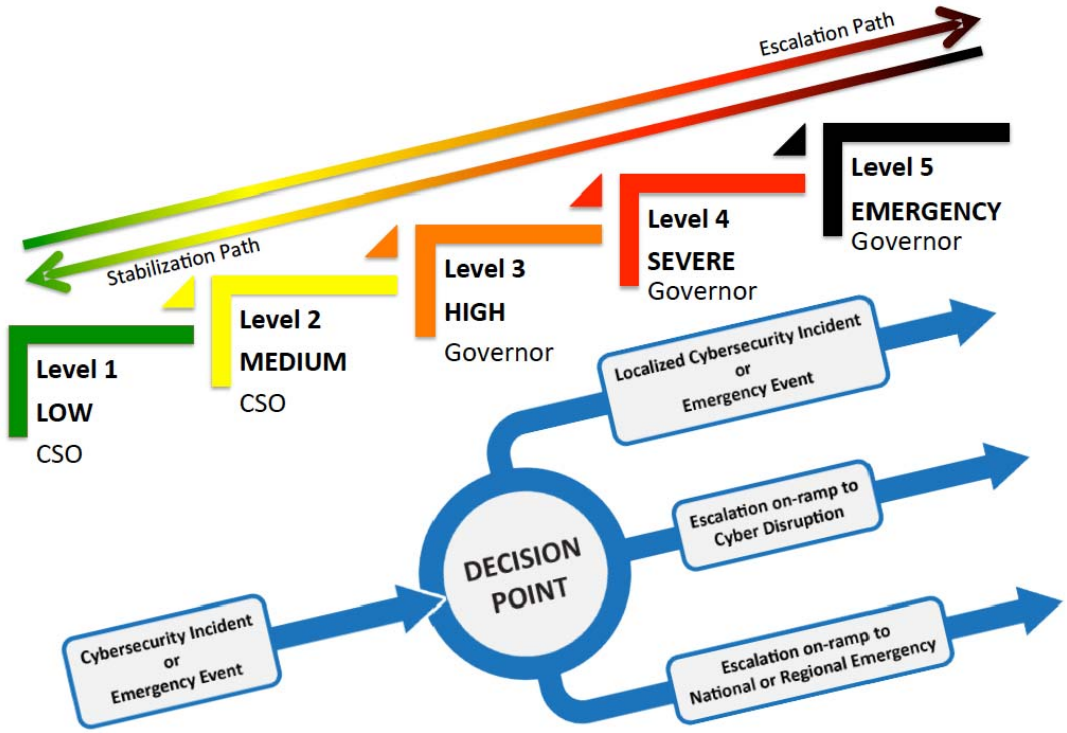


CDRP – THREAT MATRIX

- Five distinct levels (not public).
- Escalation path outlined in CDRP (not public)
  - Definition
  - Escalation Criterion
  - De-escalation Criterion
  - Potential Impact
  - Comms Procedures
  - Responsibilities

Threat Level	Description	Potential Impact
Level 5 Emergency	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services.	Widespread outages and/or significantly destructive compromise to systems with no known remedy or one or more critical infrastructure sectors debilitated.
Level 4 Severe	*Likely to result in a significant* impact to public health or safety.	Core infrastructure targeted or compromised causing multiple service outages, multiple system compromises or critical infrastructure compromises.
Level 3 High	*Likely to result in a demonstrable* impact to public health, safety, or confidence.	Compromised systems or diminished services.
Level 2 Medium	*May impact* public health, safety, or confidence.	Potential for malicious cyber activities, no known exploits identified, or known exploits identified but no significant impact has occurred.
Level 1 Low	*Unlikely to impact* public health, safety, or confidence.	Normal concern for known hacking activities, known viruses or other malicious activity.

CDRP – ESCALATION PATH



A PROUD tradition of SERVICE, through EXCELLENCE, INTEGRITY, AND COURTESY