SIA EDUCATION at ISC

Building a Modern SOC: Best Practices From UKPD

Nathan Brown, Deputy Chief, University of Kentucky Police Department

Logan Steele, Major, University of Kentucky Police Department

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses

About Us

Nathan Brown, MPA, CPP, PMP, CPD
Deputy Chief
University of Kentucky Police Dept
(859)218.2305
Nathan.brown@uky.edu
FBINAA Session #243
linkedin.com/in/nathan-brown-510b1278

Logan Steele
Major
University of Kentucky Police Dept
(859)218.2377
Logan.steele@uky.edu
FBINAA Session #288
www.linkedin.com/in/steele-logan

University of Kentucky

- Founded in 1865
- President Eli Capilouto
- 34,000 enrollment
- 26,000 employees
- 325,000 Lexington
- 75,000 campus population
- 900 acres
- 3 major medical centers*

Learning Objectives

- Participants will be able to articulate a compelling case to explore the need for a security operations center (SOC) through University of Kentucky's case study.
- Participants will understand the understand stakeholder engagement and how to survey needs to plan for a SOC.
- Participants will understand the design considerations for constructing a new soc.
- Participants will learn the elements that comprise UK's new soc.

Campus Adjacent Shooting (Nov. 3)

University of Kentucky
@universityofky · Follow

At 1 a.m. Sunday morning, UK Police responded to reports of shots fired in the area of Winslow and S. Upper St. At the same time, UKPD sent a UK Alert notifying the campus community that shots had been fired, but mistakenly omitted the location details. UKPD quickly sent out a... Show more

10:47 AM · Nov 3, 2024

60 Reply Copy link to post

Read 5 replies

Community Expectations

- Expectations from our community:
  - Quicker response times
  - Quickly share information
  - Accurate situational awareness
  - Hollywood artificial intelligence
  - Quicker investigations

Community Stakeholders

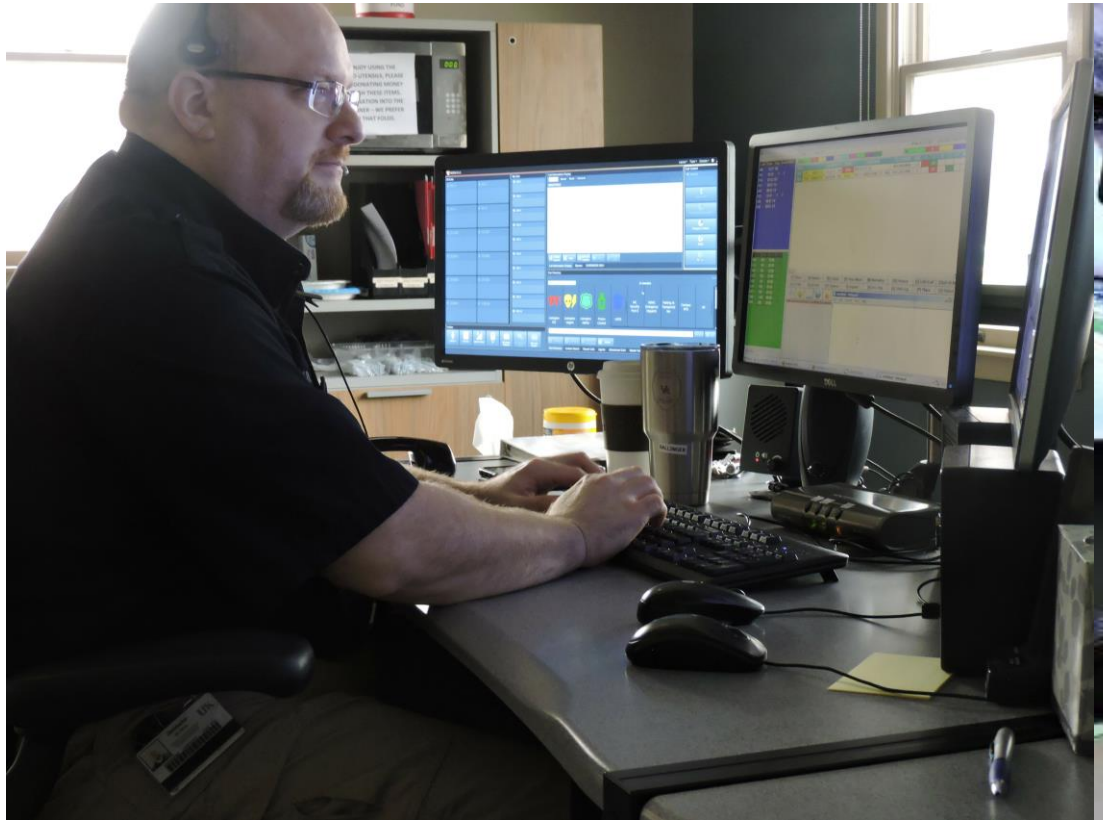
City Within a City:

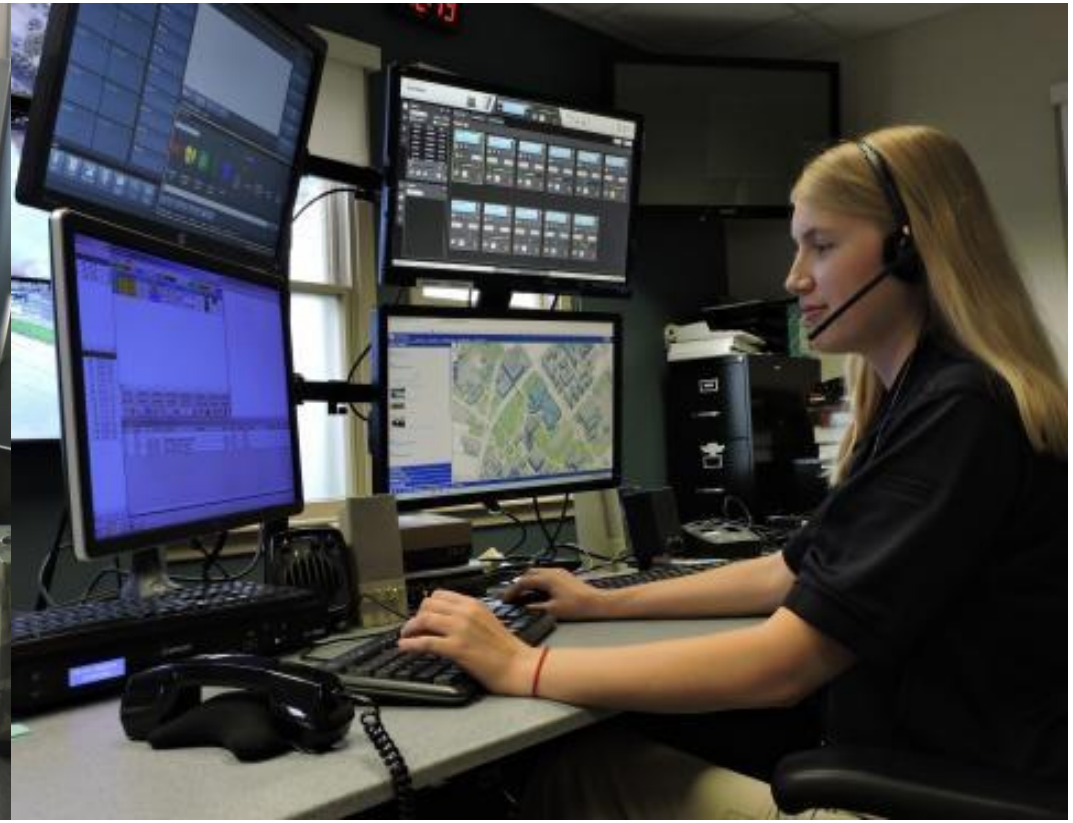
- Internal stakeholders
  - Facilities (Utilities and Works)
  - Information Technology
  - Public Safety (Police, Security)
  - Students, Faculty, Staff, Visitors
  - Media
- External (Lexington)
  - Non-UK First Responder Agencies
  - Emergency Management
  - Lexington Residents
  - City Leaders
  - Media
  - Opportunists

State and Beyond:

- 120 Counties of UK
- UK HealthCare Services
- State Leaders
- Parents
- Fans
- Media

Police Dispatch (Legacy)

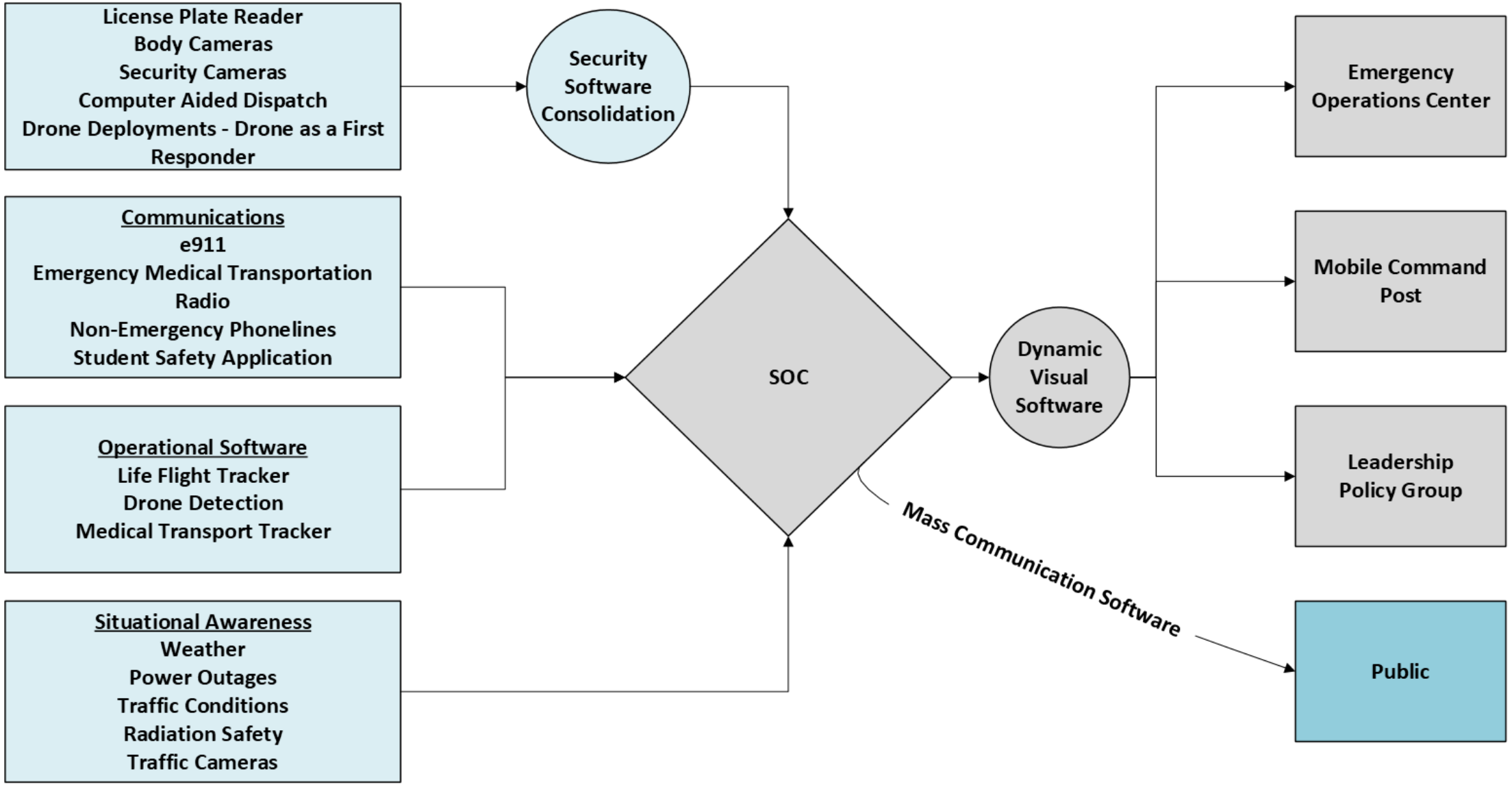




Scope of Security Operations Center

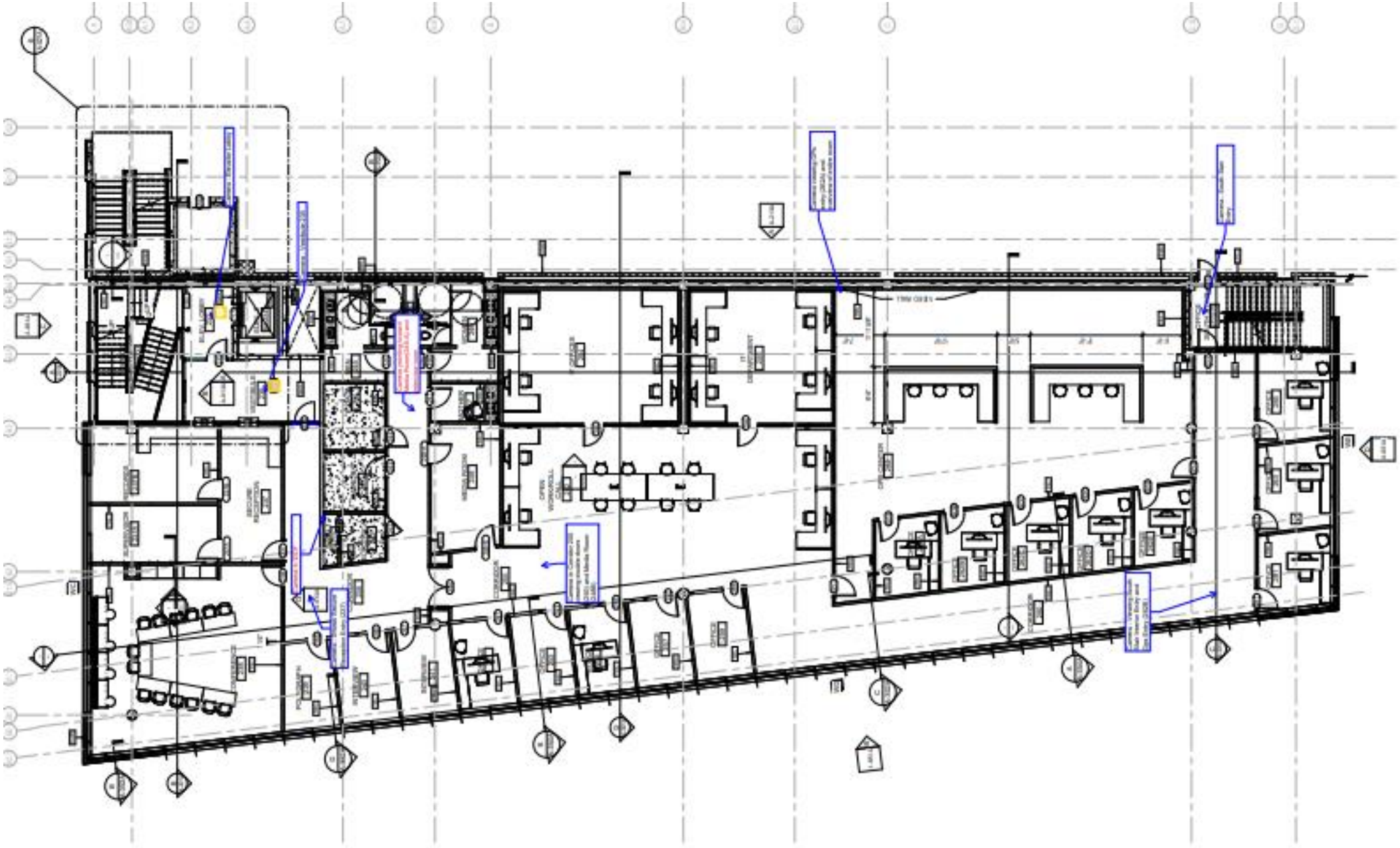
- What is your purpose of the SOC?
  - UK – “To protect public safety: anticipate, respond, inform, restore.”
- Who (disciplines) needs to be in the SOC?
  - UK – Police Communications, Police Operations, Intelligence, Physical Security, Emergency Medical Dispatch
- Who (disciplines) doesn’t need to be in the SOC?
  - UK – Fire Department, Emergency Management/EOC, Physical Plant, Cyber
- What functions is the security operations center responsible for? …

Information Overload - Sources



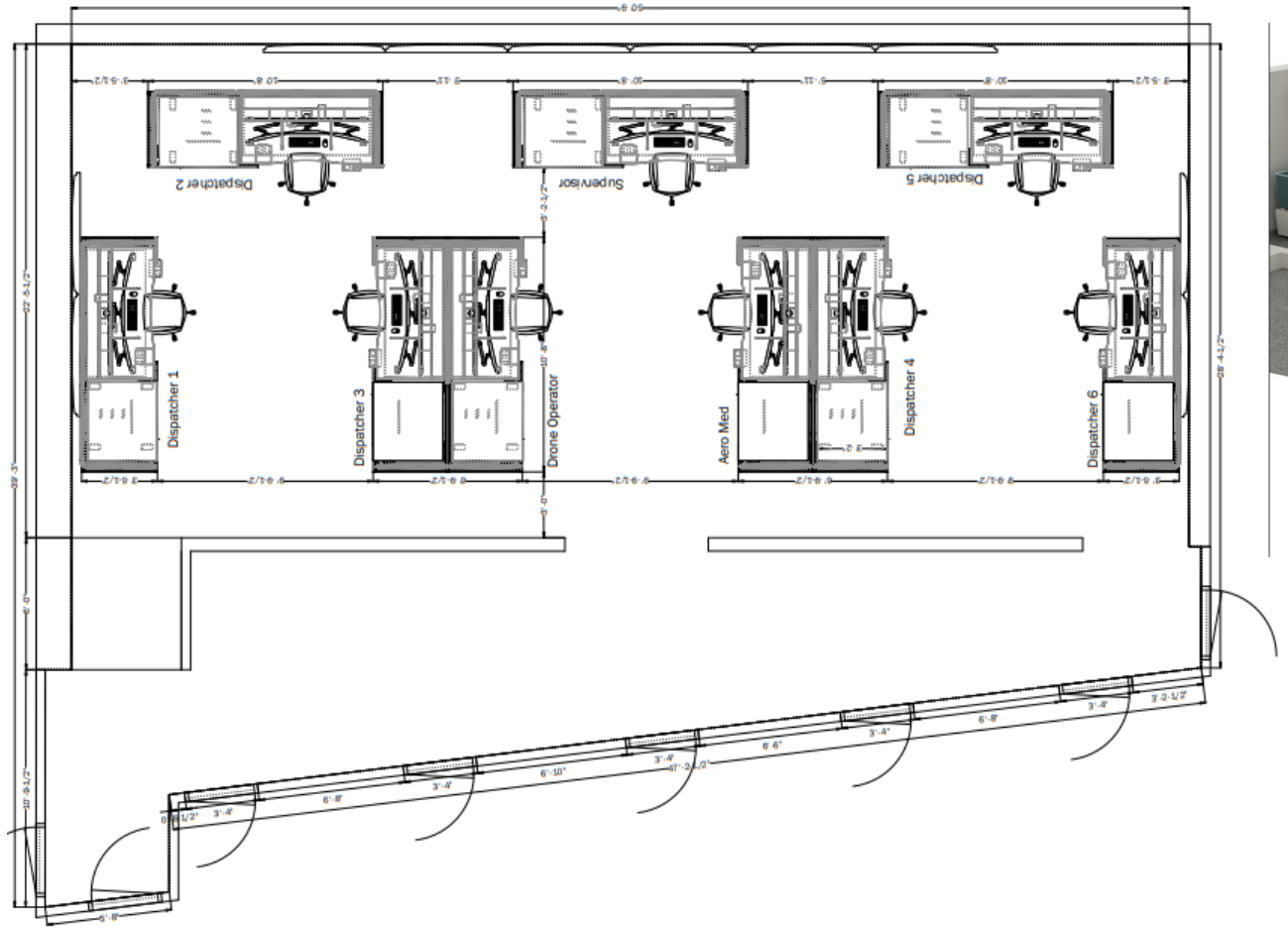
Room Considerations

- Room Layout
  - Outlet Availability and Locations
    - Power
      - Emergency Power
    - Ethernet
  - Screen Use and Locations
    - Which screens will be used for camera monitoring, dashboard monitoring?
    - Will screens be dedicated for Satellite/Cable monitoring?
- Environment
  - Ambient Lighting vs. Natural Lighting
  - Temperature Control
  - Noise levels
- Communication methods
  - Video Conferencing cameras
  - Team station layout
  - Supervisor location
- Server Location
  - What in that room is connected to emergency power?
  - Does it have the correct amount of HVAC to control the temperature?

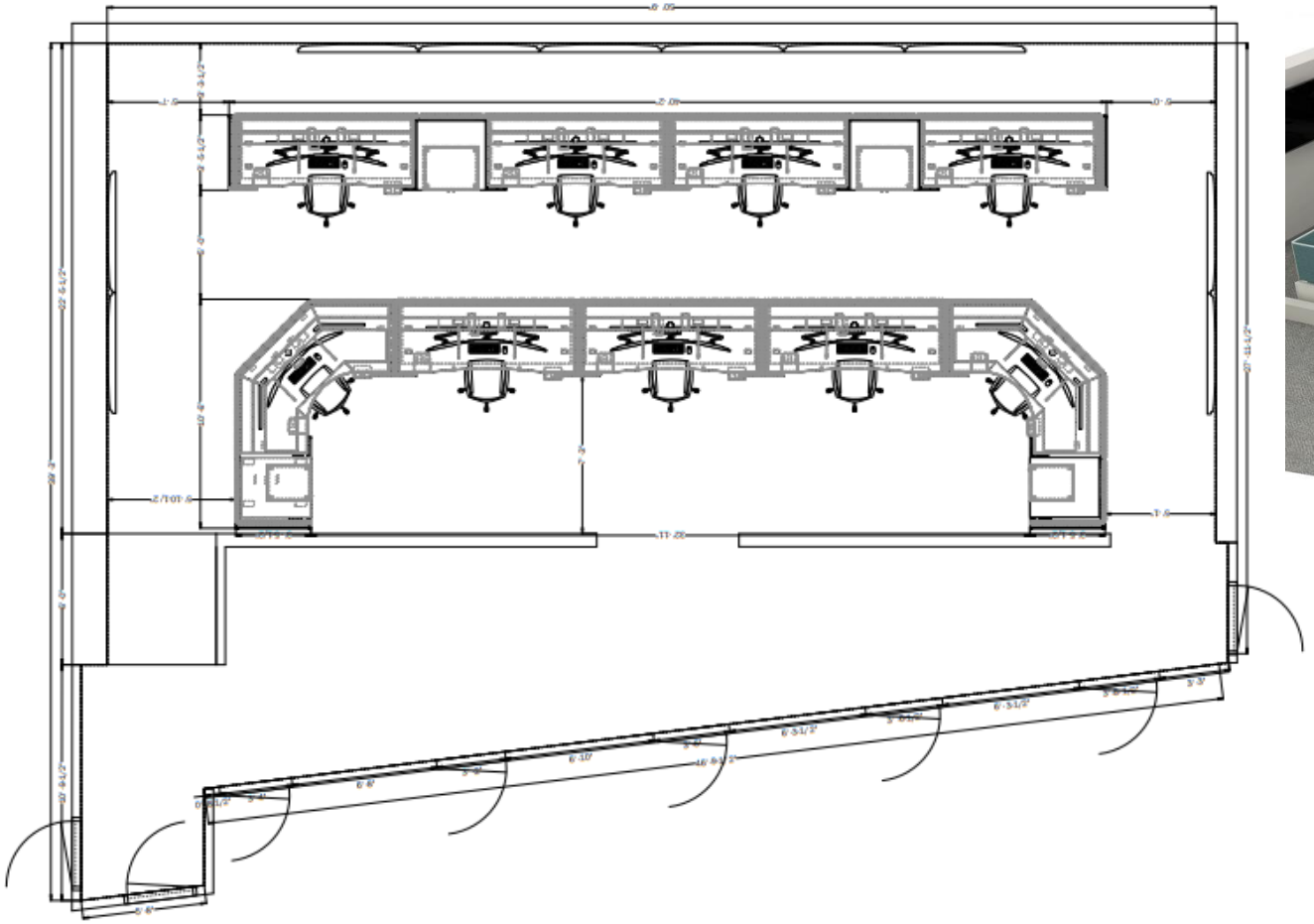


SOC Power

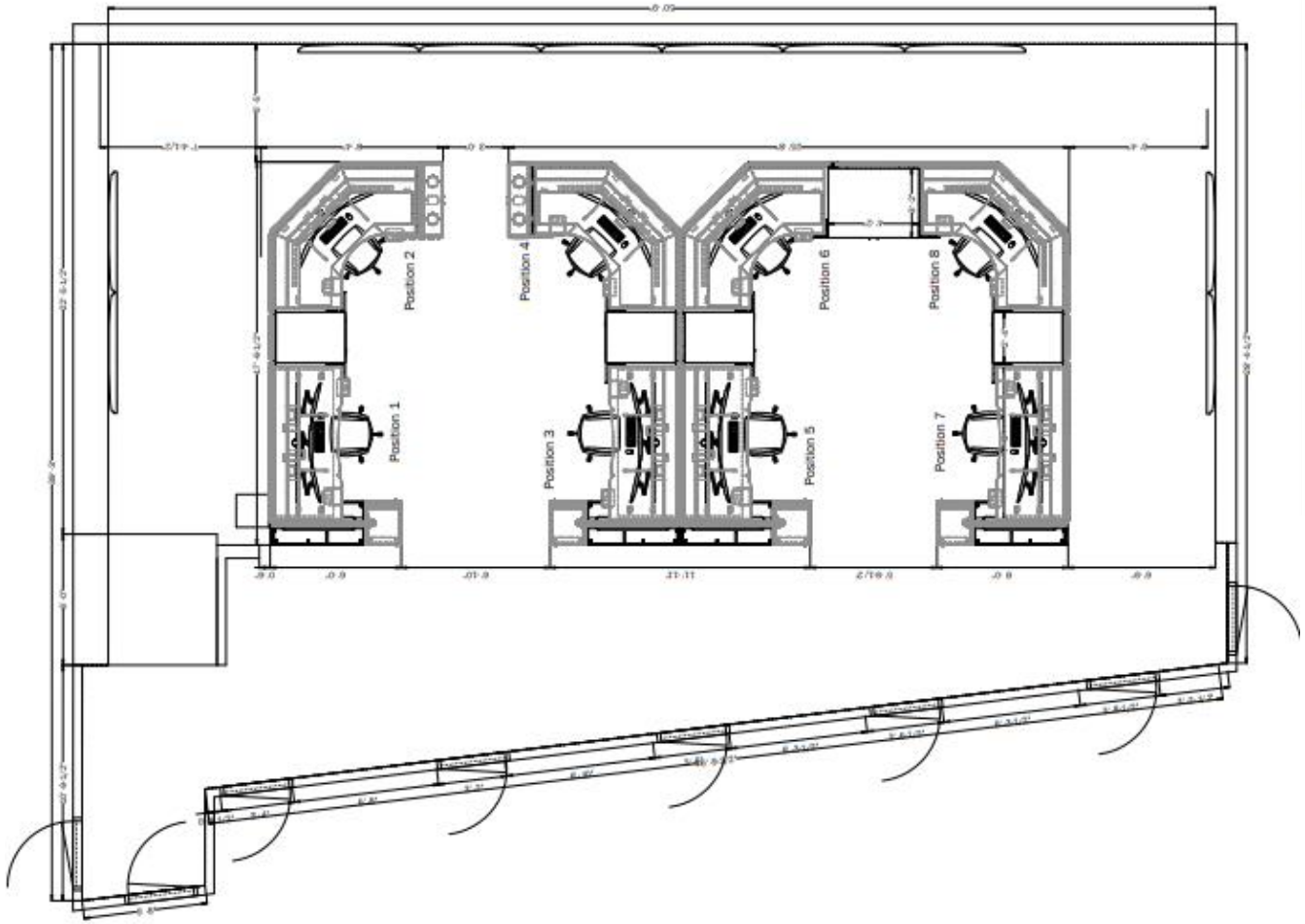
Layout 1



Layout 2



Layout 3



Operational Considerations

- Personnel
  - Generalist vs specialists
  - Chain of command
  - Specialty support
- Security requirements
  - Screening/background
  - CJIS awareness
  - Access control (dual)
  - Terminal dual authentication
  - Security cameras
  - Data security
- Radio/Phone Operations
  - Headsets
  - Backup operations
  - Channel support
  - Redundancy
  - Encryption
  - Instant playback
  - Station assistance lights

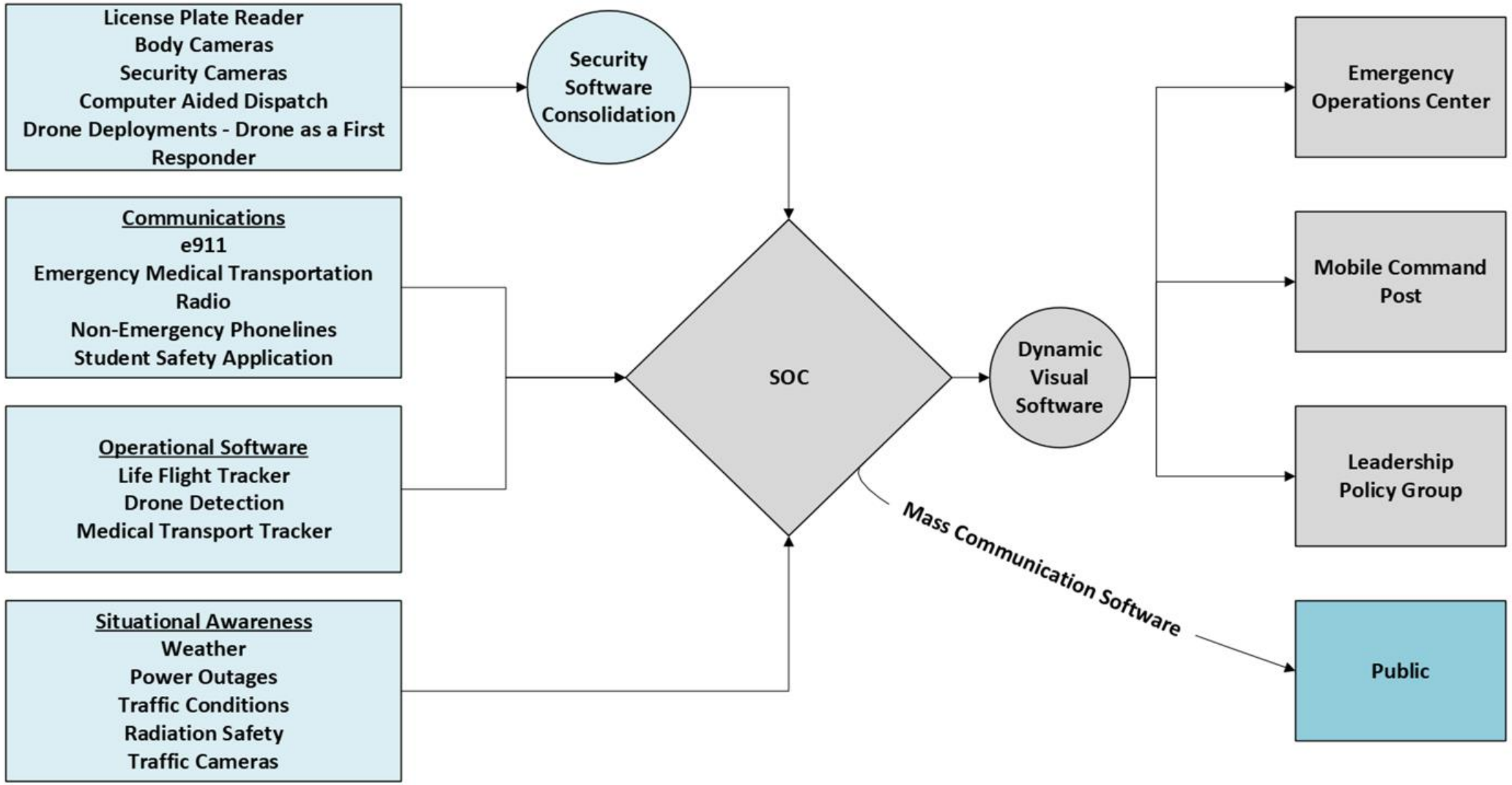
Advanced Operations

- Drone as a First Responder
- Situational awareness monitoring
- Real-time video aggregation
- License Plate Recognition alerts
- Inter-agency cooperation
- Lockdown
- Utility outages
- Traffic and engineering

Considerations

- Budget
  - Seek partnerships
  - Expect recurring costs
  - Storage is expensive but coming down
  - Software is expensive and not coming down
  - Capital refresh planning
- Training
  - Cross-train
  - Table-top and full-scale exercise
  - Spot tests
  - Awareness training for community
  - Patrol commander training
- Information Technology
  - CIO support crucial
  - Ports
  - Wifi
  - Communications redundancies
- Full systems failure
- Call center rollover

Information Overload - Sources



Questions?
Thank you!

Have thoughts about SIA Education@ISC?

Scan the QR Code on the left to provide your feedback on SIA Education@ISC Sessions at ISC West

In partnership with SIA EDUCATION at ISC

Built by RX In the business of building businesses