CA DOJ ENCRYPTION BULLETIN ROUND TABLE DISCUSSION

KARL GROVER, CITY OF ROSEVILLE

NORTHERN CALIFORNIA APCO CHAPTER MEETING

11/12/2020

AGENDA

- What's the Bulletin and Why is it Important?
- What is Encryption?
- How Can My Agency Comply?
- When Does My Agency Need to Respond?
- Resources
- Round Table Discussion

WHAT'S THE BULLETIN AND WHY IS IT IMPORTANT?

- CalDOJ Bulletin #20-09-CJIS released 10/12/2020
- FBI and CalDOJ require radio transmission of CJI and PII to be encrypted
  - **Criminal Justice Information-** criminal history i.e. arrest records, wanted persons, etc.
    - Restricted vs. Unrestricted categories in CJIS Security Policy
  - **Personally Identifiable Information-** name, SSN, passport #, military ID, ID #, DL, etc.
- Ensures protection of sensitive data as defined in FBI and CLETS policies, practices and procedures

WHAT IS ENCRYPTION?

- Encryption is a method of scrambling data so that ONLY authorized parties can RX
- Encrypted and "clear" communications typically have the same coverage and clarity
- Encrypted transmissions can only be decrypted by radios that are capable of, provisioned, AND programmed to do so
  - WARNING: encrypting ALL transmissions decreases transparency and increases interoperability challenges with other agencies plus may face additional challenges (i.e. failed AB-1555)
- Different algorithms (i.e. ADP, DES, AES) and key bit sizes (i.e. 40, 128, 256)
  - Federal standard = AES 256-bit
- Encryption best practices – plan, standards, program, train, test, key mgmt., outreach

HOW CAN MY AGENCY COMPLY?

- To comply with FBI and DOJ requirements, there are 2 options:
  - 1- Encrypt radio traffic with acceptable standards
    - Provides the ability to securely broadcast all CJI and all combinations of PII
    - 128-bit or higher per CJIS Security Policy
  - 2- Change agency policy to restrict radio transmission of certain CJI & PII
    - Use the radio except when sending restricted CJI and some combinations of PII
      - Alternative acceptable methods include MDC's and cell phones

WHEN DOES MY AGENCY NEED TO RESPOND?

- If your agency is not currently in compliance, then an Implementation Plan must be sent to Cal DOJ by 12/31/2020
  - Note: DOJ understands this can have significant operational, technical and/or financial impacts so it should be restated DOJ expects a plan not a solution by 12/31/2020
- The implementation plan should include:
  - Agency letter head signed by the Agency Head (i.e. Chief, Sheriff)
  - Detailed description of how:
    - communications will be brought into compliance; or;
    - how the risks will be mitigated via policy change
  - Estimated timeline to implement encryption or policy change in order to achieve compliance

RESOURCES

- CalDOJ bulletin link:

https://oag.ca.gov/sites/all/files/agweb/pdfs/info_bulletins/20-09-cjis.pdf

- CalDOJ contact info:
  - Different agencies have different DOJ reps depending on geographic area
    - Contact your agency's representative via DOJ's CLEW (CA Law Enforcement Web, http://clew.doj.ca.gov/)
  - Or, email the CLETS Administration Section @ CAS@doj.ca.gov or call (916) 210-4240
- FBI CJIS Security Policy (i.e. 5.10.1.2 Encryption, page #64)

https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

- AB-1555: failed, but would require encrypted audio to be provided & released to requestors

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1555

- DHS Cyber & Infrastructure Security Agency – Encryption best practices

https://www.cisa.gov/publication/encryption

ROUND TABLE DISCUSSION

- Q & A
- Discussion