The “Going Dark” Problem

• General concept
  – Law enforcement (LE) is increasingly concerned that widespread use of encryption for protecting data-at-rest and data-in-motion will hamper their ability to gather evidence and conduct investigations.

• Why is this a cybersecurity problem?
  – Encryption is a fundamental technology for ensuring the security of data-at-rest and data-in-transit.

• What
  – When LE seizes a device or wiretaps a real-time communication, LE wants unfettered access to the data stored on the device and the full contents of the communication.
“Going Dark”

• How
  – LE isn’t requiring any specific technical solution, although key escrow schemes are one frequently-sited option.

• Challenge
  – Weakening cryptographic systems in any way for LE makes the encrypted data more vulnerable to attack by lots of parties.

• Related areas
  – Crypto import/export controls, domestic vs. foreign LE, LE vs. national security

• Suggestions for specific people
  – ???