List of Interesting items

- Biometrics
    - "DNA Capability Expansion: The FBI requests $10,108,000 (all non-personnel) to effectively address the emerging requirements associated with the biometric identification capabilities to maintain public safety" Page 365
    - DOJ FY 2023 Budget "exposure draft" on page 1025
        - Requests $10 million for "DNA Capability." Page 1025
        - "The FBI requests additional resources to effectively address the emerging requirements associated with biometric identification capabilities. Recent legislative changes have increased the requirements for these capabilities to maintain public safety." Page 1028
        - "For example, the number of DNA samples that the FBI received for processing per month increased from a monthly average of 7,000 to 8,000 samples before January 2021 to 53,000 as of September 2021." Page 1028
- Confirmation of earlier contradictions about geolocation
    - The Sally Yates memo, contradicting numerous other slides, states "Law enforcement agents can use cell-site simulators to help locate cellular devices whose unique identifiers are known . . ." Page 17
        - However, they repeat the (technically correct) claim that it does not download location data or function as a GPS locator, page 18.
- Information on airborne surveillance
    - "The ASB provides aerial support for missions throughout the USMS using specially-equipped fixed wing aircraft outfitted with advanced avionics, surveillance, and communications capabilities. The aircraft and pilots, co-located with the RTOCs, provide investigative, surveillance, and reconnaissance capabilities including still and motion aerial imagery and enhancement, aerial RF beacon tracking, mobile communication command and control, and electronic surveillance package deployment in support of fugitive investigative missions. " Page 837
    - "Any use of a cell-site simulator on an aircraft must be approved either by the executive-level point of contact for the jurisdiction . . . or by a branch or unit chief of the agency's headquarters." Page 19
    - "The USMS air surveillance program consists of seven aircraft strategically located across the United States, which are responsible for providing intelligence, surveillance and reconnaissance support to district offices, Regional Fugitive Task Forces (RFTF) and all headquarters operational divisions." Page 881
        - "The USMS aircraft deploy in support of a myriad of USMS operational scenarios that include: photographic reconnaissance, overt and covert

video surveillance, airborne communications relay, mission coordination, route mapping and over-watch. The primary deployment mission is in support of USMS investigations (both CONUS & OCONUS), and involves the deployment of specialized optics and electronic surveillance (ELSUR) equipment . . ." Page 881
        - "The USMS aircraft and specially trained pilots provide a unique investigative surveillance capability not fielded by other Federal, state or local law enforcement aviation programs." Page 881
        - "The unique combination of the USMS ELSUR suite, high resolution video surveillance camera technical expertise of the USMS investigators (both in the air and on the ground) have consistently proven to be the most successful law enforcement package" Page 884

- Cybersecurity and Digital Privacy
    - Dark HunTor mentioned on page 95 might be of interest to digital privacy advocates
    - They are concerned with cryptocurrency, page 105
    - It's interesting the DEA lists malware/ransomware as one of its main priorities, pages 126, 146, 181, whereas the FBI does not
    - "The USMS has created the Open-Source Intelligence Unit (OSINT) to proactively review and research social media content. OSINT identifies threats and situations of concern that may be currently undetected through traditional investigative methods. Analyzing public discourse on social media, its spread (“likes”, comments, and shares), and the target audience, the USMS can effectively manage its resources appropriate to the identified threat." Page 931
    - "Reviewing public discussion, social media and media exposure associated with judges and judicial events will improve the USMS’ ability to assign the right level of resources to trials and other proceedings, potentially saving resource costs and better aligning resources to true needs." Page 983
    - The "Analytics Driven Targeting" team "will analyze potentially illicit transactions and follow the money through bank accounts, wire transactions, shell companies, and virtual currency transactions." Page 705.
        - This seems to mean they'll analyze many innocent transactions
    - Cyber investigative support will "develop web scrapers (tools utilized to extract data from websites) and Artificial Intelligence powered 'bots' (autonomous programs that can interact with computer systems) to glean more information on potential targets." Page 706
    - They seem to be working with local governments to add surveillance tools including license plate readers, page 739

- "The ESB provides state-of-the-art electronic surveillance assistance in fugitive investigations. It deploys sophisticated commercial and sensitive technical surveillance technologies for the interception of hard line and cellular telecommunications, Wi-Fi collection and emitter location, and Global Positioning System (GPS) and radio frequency tagging/tracking. The ESB also conducts computer and cellular exploitation and on-scene forensic extraction, photo/video surveillance, and Technical Surveillance and Countermeasure (TSCM) sweeps to detect surreptitious monitoring devices." Page 837

- Stingrays
  - Interesting new find about devices used in multi-story buildings: "USMS also operates portable CSS and passive wireless collection sensors to specifically locate a fugitive's devices operating on 4G LTE, 5G NR and Wi-Fi networks in cases where vehicular or aerial platforms are ineffective or where the fugitive is believed to be located in multi-dwelling buildings." Page 977
  - Of particular interest: "other cellular devices in the area might experience a temporary disruption of service." Page 21
    - (with stringrays in general, not that new device specifically)
  - DEA 2023: A request for $3.8 million of "Over the Air (OTA) Cell Site Simulators" on page 189. It's unclear what this means, and worth future FOIA requests.
    - There's a partial explanation on page 190: "As the government sells off spectrum bands to the private sector, cellular companies expand their technology, and this creates the need to update equipment. This updated CSS technology allows the DEA to continue to keep pace with the cellular providers to support investigations."
    - 20% of the cost will recur each year for software and licenses, page 192
      - This is more than 1/5th of their annual software/licensing budget, page 196
  - FBI 2021 $16.1 million on cell-site simulators. Page 209.
  - They set a goal of ensuring their stingrays "are capable of operating against evolving wireless communication technology." Page 223
  - They request $13 million for "communication intercept resources," also to be used in international enforcement. Page 695
- Miscellaneous points of interest
  - The DEA shares information with ONSI, page 101.
  - For "Investigative Technology and Cyber Support" they requested close to $8 million in extra budget, for Stingrays and related products and capabilities. Page 107

- More left-leaning partners might be interested in the Sensitive Investigation Units' work in El Salvador, page 111
- DEA has a huge number of foreign offices shown on page 114, in a nice graphic
- Graphic with DEA domestic offices on page 132
- The description of data validation and possible errors in the PTARRS process is interesting. I wonder how much they can manipulate data through varying "validation" procedures. Page 138.