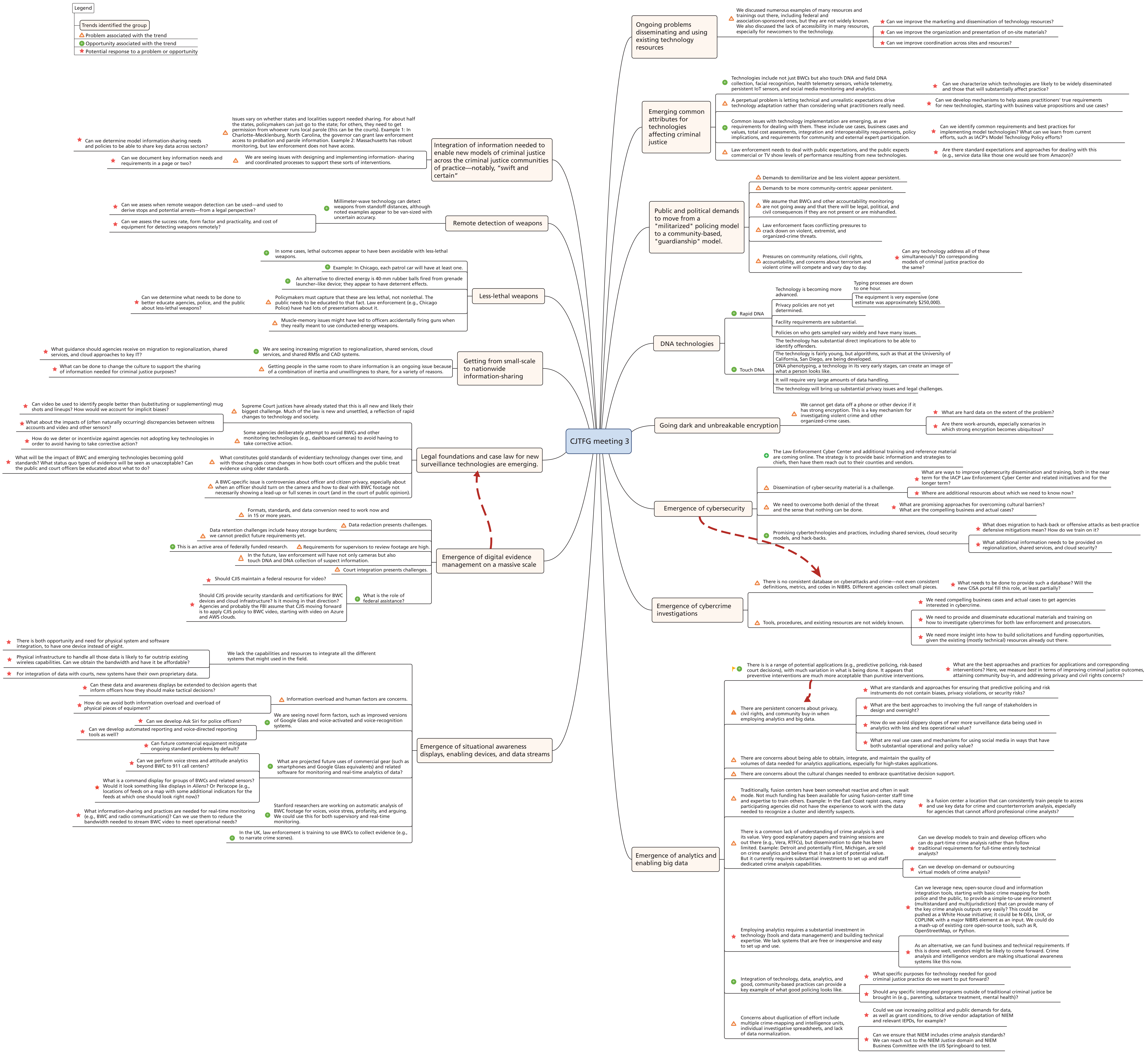

Legend
- Trends identified the group
- ⚠ Problem associated with the trend
- ⊕ Opportunity associated with the trend
- ★ Potential response to a problem or opportunity

CJTFG meeting 3

Integration of information needed to enable new models of criminal justice across the criminal justice communities of practice—notably, "swift and certain"
- ⚠ Issues vary on whether states and localities support needed sharing. For about half the states, policymakers can just go to the state; for others, they need to get permission from whoever runs local parole (this can be the courts). Example 1: In Charlotte–Mecklenburg, North Carolina, the governor can grant law enforcement access to probation and parole information. Example 2: Massachusetts has robust monitoring, but law enforcement does not have access.
  - ★ Can we determine model information-sharing needs and policies to be able to share key data across sectors?
- ⚠ We are seeing issues with designing and implementing information- sharing and coordinated processes to support these sorts of interventions.
  - ★ Can we document key information needs and requirements in a page or two?

Remote detection of weapons
- ⊕ Millimeter-wave technology can detect weapons from standoff distances, although noted examples appear to be van-sized with uncertain accuracy.
  - ★ Can we assess when remote weapon detection can be used—and used to derive stops and potential arrests—from a legal perspective?
  - ★ Can we assess the success rate, form factor and practicality, and cost of equipment for detecting weapons remotely?

Less-lethal weapons
- ⊕ In some cases, lethal outcomes appear to have been avoidable with less-lethal weapons.
- ⊕ Example: In Chicago, each patrol car will have at least one.
- ⊕ An alternative to directed energy is 40-mm rubber balls fired from grenade launcher–like device; they appear to have deterrent effects.
- ⚠ Policymakers must capture that these are less lethal, not nonlethal. The public needs to be educated to that fact. Law enforcement (e.g., Chicago Police) have had lots of presentations about it.
  - ★ Can we determine what needs to be done to better educate agencies, police, and the public about less-lethal weapons?
- ⚠ Muscle-memory issues might have led to officers accidentally firing guns when they really meant to use conducted-energy weapons.

Getting from small-scale to nationwide information-sharing
- ⊕ We are seeing increasing migration to regionalization, shared services, cloud services, and shared RMSs and CAD systems.
  - ★ What guidance should agencies receive on migration to regionalization, shared services, and cloud approaches to key IT?
- ⚠ Getting people in the same room to share information is an ongoing issue because of a combination of inertia and unwillingness to share, for a variety of reasons.
  - ★ What can be done to change the culture to support the sharing of information needed for criminal justice purposes?

Legal foundations and case law for new surveillance technologies are emerging.
- ⚠ Supreme Court justices have already stated that this is all new and likely their biggest challenge. Much of the law is new and unsettled, a reflection of rapid changes to technology and society.
  - ★ Can video be used to identify people better than (substituting or supplementing) mug shots and lineups? How would we account for implicit biases?
  - ★ What about the impacts of (often naturally occurring) discrepancies between witness accounts and video and other sensors?
- ⚠ Some agencies deliberately attempt to avoid BWCs and other monitoring technologies (e.g., dashboard cameras) to avoid having to take corrective action.
  - ★ How do we deter or incentivize against agencies not adopting key technologies in order to avoid having to take corrective action?
- ⚠ What constitutes gold standards of evidentiary technology changes over time, and with those changes come changes in how both court officers and the public treat evidence using older standards.
  - ★ What will be the impact of BWC and emerging technologies becoming gold standards? What status quo types of evidence will be seen as unacceptable? Can the public and court officers be educated about what to do?
- ⚠ A BWC-specific issue is controversies about officer and citizen privacy, especially about when an officer should turn on the camera and how to deal with BWC footage not necessarily showing a lead-up or full scenes in court (and in the court of public opinion).

Emergence of digital evidence management on a massive scale
- ⚠ Formats, standards, and data conversion need to work now and in 15 or more years.
- ⚠ Data redaction presents challenges.
  - ⚠ Data retention challenges include heavy storage burdens; we cannot predict future requirements yet.
- ⚠ Requirements for supervisors to review footage are high.
  - ⊕ This is an active area of federally funded research.
- ⚠ In the future, law enforcement will have not only cameras but also touch DNA and DNA collection of suspect information.
- ⚠ Court integration presents challenges.
- ⊕ What is the role of federal assistance?
  - ★ Should CJIS maintain a federal resource for video?
  - ★ Should CJIS provide security standards and certifications for BWC devices and cloud infrastructure? Is it moving in that direction? Agencies and probably the FBI assume that CJIS moving forward is to apply CJIS policy to BWC video, starting with video on Azure and AWS clouds.

Emergence of situational awareness displays, enabling devices, and data streams
- We lack the capabilities and resources to integrate all the different systems that might used in the field.
  - ★ There is both opportunity and need for physical system and software integration, to have one device instead of eight.
  - ★ Physical infrastructure to handle all those data is likely to far outstrip existing wireless capabilities. Can we obtain the bandwidth and have it be affordable?
  - ★ For integration of data with courts, new systems have their own proprietary data.
- ⚠ Information overload and human factors are concerns.
  - ★ Can these data and awareness displays be extended to decision agents that inform officers how they should make tactical decisions?
  - ★ How do we avoid both information overload and overload of physical pieces of equipment?
- ⊕ We are seeing novel form factors, such as improved versions of Google Glass and voice-activated and voice-recognition systems.
  - ★ Can we develop Ask Siri for police officers?
  - ★ Can we develop automated reporting and voice-directed reporting tools as well?
- ⊕ What are projected future uses of commercial gear (such as smartphones and Google Glass equivalents) and related software for monitoring and real-time analytics of data?
  - ★ Can future commercial equipment mitigate ongoing standard problems by default?
  - ★ Can we perform voice stress and attitude analytics beyond BWC to 911 call centers?
  - ★ What is a command display for groups of BWCs and related sensors? Would it look something like displays in *Aliens*? Or Periscope (e.g., locations of feeds on a map with some additional indicators for the feeds at which one should look right now)?
- ⊕ Stanford researchers are working on automatic analysis of BWC footage for voices, voice stress, profanity, and arguing. We could use this for both supervisory and real-time monitoring.
  - ★ What information-sharing and practices are needed for real-time monitoring (e.g., BWC and radio communications)? Can we use them to reduce the bandwidth needed to stream BWC video to meet operational needs?
- ⊕ In the UK, law enforcement is training to use BWCs to collect evidence (e.g., to narrate crime scenes).

Ongoing problems disseminating and using existing technology resources
- ⚠ We discussed numerous examples of many resources and trainings out there, including federal and association-sponsored ones, but they are not widely known. We also discussed the lack of accessibility in many resources, especially for newcomers to the technology.
  - ★ Can we improve the marketing and dissemination of technology resources?
  - ★ Can we improve the organization and presentation of on-site materials?
  - ★ Can we improve coordination across sites and resources?

Emerging common attributes for technologies affecting criminal justice
- ⊕ Technologies include not just BWCs but also touch DNA and field DNA collection, facial recognition, health telemetry sensors, vehicle telemetry, persistent IoT sensors, and social media monitoring and analytics.
  - ★ Can we characterize which technologies are likely to be widely disseminated and those that will substantially affect practice?
- ⚠ A perpetual problem is letting technical and unrealistic expectations drive technology adaptation rather than considering what practitioners really need.
  - ★ Can we develop mechanisms to help assess practitioners' true requirements for new technologies, starting with business value propositions and use cases?
- ⊕ Common issues with technology implementation are emerging, as are requirements for dealing with them. These include use cases, business cases and values, total cost assessments, integration and interoperability requirements, policy implications, and requirements for community and external expert participation.
  - ★ Can we identify common requirements and best practices for implementing model technologies? What can we learn from current efforts, such as IACP's Model Technology Policy efforts?
- ⚠ Law enforcement needs to deal with public expectations, and the public expects commercial or TV show levels of performance resulting from new technologies.
  - ★ Are there standard expectations and approaches for dealing with this (e.g., service data like those one would see from Amazon)?

Public and political demands to move from a "militarized" policing model to a community-based, "guardianship" model.
- ⚠ Demands to demilitarize and be less violent appear persistent.
- ⚠ Demands to be more community-centric appear persistent.
- ⚠ We assume that BWCs and other accountability monitoring are not going away and that there will be legal, political, and civil consequences if they are not present or are mishandled.
- ⚠ Law enforcement faces conflicting pressures to crack down on violent, extremist, and organized-crime threats.
- ⚠ Pressures on community relations, civil rights, accountability, and concerns about terrorism and violent crime will compete and vary day to day.
  - ★ Can any technology address all of these simultaneously? Do corresponding models of criminal justice practice do the same?

DNA technologies
- ⊕ Rapid DNA
  - Technology is becoming more advanced.
    - Typing processes are down to one hour.
    - The equipment is very expensive (one estimate was approximately $250,000).
  - Privacy policies are not yet determined.
  - Facility requirements are substantial.
  - Policies on who gets sampled vary widely and have many issues.
- ⊕ Touch DNA
  - The technology has substantial direct implications to be able to identify offenders.
  - The technology is fairly young, but algorithms, such as that at the University of California, San Diego, are being developed.
  - DNA phenotyping, a technology in its very early stages, can create an image of what a person looks like.
  - It will require very large amounts of data handling.
  - The technology will bring up substantial privacy issues and legal challenges.

Going dark and unbreakable encryption
- ⚠ We cannot get data off a phone or other device if it has strong encryption. This is a key mechanism for investigating violent crime and other organized-crime cases.
  - ★ What are hard data on the extent of the problem?
  - ★ Are there work-arounds, especially scenarios in which strong encryption becomes ubiquitous?

Emergence of cybersecurity
- ⊕ The Law Enforcement Cyber Center and additional training and reference material are coming online. The strategy is to provide basic information and strategies to chiefs, then have them reach out to their counties and vendors.
- ⚠ Dissemination of cyber-security material is a challenge.
  - ★ What are ways to improve cybersecurity dissemination and training, both in the near term for the IACP Law Enforcement Cyber Center and related initiatives and for the longer term?
  - ★ Where are additional resources about which we need to know now?
- ⚠ We need to overcome both denial of the threat and the sense that nothing can be done.
  - ★ What are promising approaches for overcoming cultural barriers? What are the compelling business and actual cases?
- ⊕ Promising cybertechnologies and practices, including shared services, cloud security models, and hack-backs.
  - ★ What does migration to hack-back or offensive attacks as best-practice defensive mitigations mean? How do we train on it?
  - ★ What additional information needs to be provided on regionalization, shared services, and cloud security?

Emergence of cybercrime investigations
- ⚠ There is no consistent database on cyberattacks and crime—not even consistent definitions, metrics, and codes in NIBRS. Different agencies collect small pieces.
  - ★ What needs to be done to provide such a database? Will the new CISA portal fill this role, at least partially?
- ⚠ Tools, procedures, and existing resources are not widely known.
  - ★ We need compelling business cases and actual cases to get agencies interested in cybercrime.
  - ★ We need to provide and disseminate educational materials and training on how to investigate cybercrimes for both law enforcement and prosecutors.
  - ★ We need more insight into how to build solicitations and funding opportunities, given the existing (mostly technical) resources already out there.

Emergence of analytics and enabling big data
- ⊕ There is is a range of potential applications (e.g., predictive policing, risk-based court decisions), with much variation in what is being done. It appears that preventive interventions are much more acceptable than punitive interventions.
  - ★ What are the best approaches and practices for applications and corresponding interventions? Here, we measure *best* in terms of improving criminal justice outcomes, attaining community buy-in, and addressing privacy and civil rights concerns?
- ⚠ There are persistent concerns about privacy, civil rights, and community buy-in when employing analytics and big data.
  - ★ What are standards and approaches for ensuring that predictive policing and risk instruments do not contain biases, privacy violations, or security risks?
  - ★ What are the best approaches to involving the full range of stakeholders in design and oversight?
  - ★ How do we avoid slippery slopes of ever more surveillance data being used in analytics with less and less operational value?
  - ★ What are real use cases and mechanisms for using social media in ways that have both substantial operational and policy value?
- ⚠ There are concerns about being able to obtain, integrate, and maintain the quality of volumes of data needed for analytics applications, especially for high-stakes applications.
- ⚠ There are concerns about the cultural changes needed to embrace quantitative decision support.
- ⚠ Traditionally, fusion centers have been somewhat reactive and often in wait mode. Not much funding has been available for using fusion-center staff time and expertise to train others. Example: In the East Coast rapist cases, many participating agencies did not have the experience to work with the data needed to recognize a cluster and identify suspects.
  - ★ Is a fusion center a location that can consistently train people to access and use key data for crime and counterterrorism analysis, especially for agencies that cannot afford professional crime analysts?
- ⚠ There is a common lack of understanding of crime analysis is and its value. Very good explanatory papers and training sessions are out there (e.g., Vera, RTFCs), but dissemination to date has been limited. Example: Detroit and potentially Flint, Michigan, are sold on crime analytics and believe that it has a lot of potential value. But it currently requires substantial investments to set up and staff dedicated crime analysis capabilities.
  - ★ Can we develop models to train and develop officers who can do part-time crime analysis rather than follow traditional requirements for full-time entirely technical analysts?
  - ★ Can we develop on-demand or outsourcing virtual models of crime analysis?
- ★ Employing analytics requires a substantial investment in technology (tools and data management) and building technical expertise. We lack systems that are free or inexpensive and easy to set up and use.
  - ★ Can we leverage new, open-source cloud and information integration tools, starting with basic crime mapping for both police and the public, to provide a simple-to-use environment (multistandard and multijurisdiction) that can provide many of the key crime analysis outputs very easily? This could be pushed as a White House initiative; it could be N-DEx, LInX, or COPLINK with a major NIBRS element as an input. We could do a mash-up of existing core open-source tools, such as R, OpenStreetMap, or Python.
  - ★ As an alternative, we can fund business and technical requirements. If this is done well, vendors might be likely to come forward. Crime analysis and intelligence vendors are making situational awareness systems like this now.
- ⊕ Integration of technology, data, analytics, and good, community-based practices can provide a key example of what good policing looks like.
  - ★ What specific purposes for technology needed for good criminal justice practice do we want to put forward?
  - ★ Should any specific integrated programs outside of traditional criminal justice be brought in (e.g., parenting, substance treatment, mental health)?
- ⚠ Concerns about duplication of effort include multiple crime-mapping and intelligence units, individual investigative spreadsheets, and lack of data normalization.
  - ★ Could we use increasing political and public demands for data, as well as grant conditions, to drive vendor adaptation of NIEM and relevant IEPDs, for example?
  - ★ Can we ensure that NIEM includes crime analysis standards? We can reach out to the NIEM Justice domain and NIEM Business Committee with the IJIS Springboard to test.

Excerpted from *Addressing Emerging Trends to Support the Future of Criminal Justice: Findings of the Criminal Justice Technology Forecasting Group*,by John S. Hollywood, Dulani Woods, Andrew Lauland, Brian A. Jackson, Richard Silberglitt, Santa Monica, Calif: RAND Corporation, RR-1987-BJA, 2018 (available at www.rand.org/t/RR1987).