NAIAC Law Enforcement Subcommittee: Year 1 Report & Roadmap

The National Artificial Intelligence Advisory Committee (NAIAC)
Law Enforcement Subcommittee (NAIAC-LE Subcommittee)

February 2024

TABLE OF CONTENTS

INTRODUCTION

The Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC) has the responsibility to make recommendations and provide advice on matters relating to the development, adoption, or use of AI in the context of law enforcement. The Subcommittee was established in Section 5104 (e) of the National Artificial Intelligence Initiative Act of 2020. It is charged with providing advice to the President, through recommendations that will be considered by the full NAIAC, on a range of legal and ethical issues that will arise as law enforcement increases its use of AI tools. These issues include AI bias, data security, adoption protocols, and legal standards. (Section 5104 (e) (2).)

The Law Enforcement Subcommittee (NAIAC-LE) was established in the summer of 2023 and began its work in August 2023. The very existence of this specially-created Subcommittee is a testament to the complex set of needs and challenges in the law enforcement context. There are longstanding and legitimate concerns about how the communities that most need safety are also the ones that have historically been subject to a disproportionate share of police abuse, including racial profiling, excessive use of force, surveillance, and faulty or manufactured evidence. This background informs and guides NAIAC-LE's work evaluating the uses and potential misuses of AI. When law enforcement uses emerging technologies, the rights, trust, and safety of the community are of paramount importance.

This roadmap, the Subcommittee's first written product, will set out the scope and organization of NAIAC-LE's work, and will identify a few topics on which NAIAC expects to offer recommendations within the first year.

This document is, by design, a work-in-progress that is meant to facilitate input from stakeholders and the public. It is the first version of a living roadmap that will expand and contract as the Subcommittee's knowledge changes. NAIAC invites your feedback about technologies, uses, and ethical issues that you believe are not sufficiently reflected in the current iteration of the roadmap. NAIAC likewise welcomes resources or information on any of the topics listed below. Comments can be submitted at public meetings or at any time via email to naiac@nist.gov.

SCOPE

The Law Enforcement Subcommittee of the National Artificial Intelligence Advisory Committee (NAIAC-LE) will identify and make recommendations to NAIAC about the legal, ethical, and responsible use of AI technologies if or when they are used:

- To influence a law enforcement action with respect to who, what, or where/when to investigate or engage law enforcement, including decisions related to the investigations of all crime (e.g., white collar crime, human trafficking, cybercrime, street crime, and violations of immigration/customs, as well as decisions related to pretrial detention, bail, corrections, and parole)

- To assess whether law enforcement has conducted its work effectively, and within its legal and ethical limits

- With the result of inducing the collection, combination, integration, or disclosure of data (including by private companies that collaborate or cooperate with law enforcement)

Just as NAIAC-LE uses a capacious definition of law enforcement, including pretrial and post-conviction procedures within its ambit, it also uses a capacious definition of AI, adopting the same definition used in the NAIAC Year 1 Report:

> *"An AI system is an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy."*
>
> *(Adapted from: OECD Recommendation on AI:2019; ISO/IEC 22989:2022.)*

Thus, any computer-assisted recommendation, analysis, or decision that makes use of algorithms and automated processes may qualify as AI for the purposes of the NAIAC-LE's work.

OVERARCHING LEGAL & ETHICAL THEMES

The NAIAC-LE has identified 13 legal and ethical issues that arise from law enforcement use of AI. All of these themes should guide the responsible implementation of AI described in the next section. Future guidance developed by the Subcommittee will address one or more of these themes, as it applies to one or more of the AI uses cataloged below.

(A) Does the AI tool function effectively?

1. **Performance and Evaluation**

   A key question with regard to any AI system being used by law enforcement is how that tool impacts police performance of their public safety mission (e.g., the rate at which crimes are solved and deterred, the speed at which regular police tasks can be accomplished, and the success of serving and engaging with communities). Systematic evaluation of such impact is critical, but also difficult. Law enforcement can help illuminate the ultimate impact of AI tools by implementing experimental designs during an initial probationary period or by integrating with research organizations.

   AI tools must also be evaluated for their performance in individual cases. For example, what level of error — both false positive and false negative — should be tolerated in an AI system? The answer is likely to depend on several factors, such as the severity of consequences of the error to individuals and to law enforcement resources; the sensitivity of the personal information analyzed by the AI system; and the comparative accuracy, costs, scalability, or speed of the investigation processes that would be used in the absence of the AI system. Performance can be evaluated both in the lab (before deployment) and in the field, and the thresholds and factors used to determine the minimum accuracy may differ in these two contexts. The amount of time that a tool has been used may also be relevant, as performance in Machine Learning systems often improves with use.

2. **Bias, Disparities, and Discrimination**

   For a wide variety of historical, societal, and institutional reasons, both crime and criminal law enforcement operate with stark disparities. Recognizing this, President Biden's recent executive orders have prioritized advancing equity and examining the potential for bias and discrimination within law enforcement and the federal government.[1] This reality presents difficult questions for how disparate impacts across race, gender, and socio-economic status of any AI system should be measured, and what level of disparity or bias is unacceptable. Some of the factors relevant to determining an acceptable level of performance (see #1, above) are likely to be relevant to determining the threshold for unacceptable bias. In addition to biases that can emerge from decisions made prior to law enforcement procurement (e.g., inadequate or inappropriate training data, an improper objective function, or other methodological problems), where and how a police department deploys an AI system can also result in disparate impact. Thus, under the umbrella of bias, the Subcommittee will also explore how law enforcement agencies can and should ensure the even-handed deployment of AI systems.

3. **Embedded Policy Choices**
   Many AI tools embed policy choices that cannot be evaluated by a simple binary outcome. AI tools can influence how many law enforcement resources should be deployed in a particular context, and can embed what level of risk should trigger an intervention or which factors should or should not be relevant to a determination of law enforcement involvement. These choices in inputs and objective functions are sometimes obscured at the outset. Even when they are transparent, they can blend into the scenery over time and fail to receive evaluation and improvements. The Subcommittee will explore how these policy choices can be surfaced and subject to oversight and evaluation.

4. **Potential Risks and Harms from Underutilization**
   There can be costs and unintended consequences if the limitations or procedural hurdles imposed on law enforcement use of AI are too stringent. In addition to the potential lost opportunities to deter crime, limitations on AI could steer law enforcement to use investigation strategies that exacerbate civil liberties concerns (e.g., reliance on interviews, interrogations, witnesses, or consent-based searches).

   Broad, sweeping requirements could cause problems if they require administrative hurdles that are not relevant for the problem at hand (e.g., algorithms that will only be used for one context being required to be equally

[1] "Executive Order 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices To Enhance Public Trust and Public Safety," Federal Register, May 2022. https://www.federalregister.gov/documents/2022/05/31/2022-11810/advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and; "Executive Order 13985, Advancing Racial Equity and Support for Underserved Communities Through the Federal Government," Federal Register, January 2021, https://www.federalregister.gov/documents/2021/01/25/2021-01753/advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government.

accurate across all contexts anyway). Moreover, the federal government can create incentives and resources to help broadly distribute AI tools that have been successfully and responsibly implemented.

(B) What risks to civil rights and civil liberties may arise from the use of the AI tool?

5. **Misuse**

   When an AI system is incorporated into law enforcement practices, there is always a risk that the agencies or individuals leveraging the tools will misuse them, whether inadvertently or maliciously. A system that is adopted to help solve the most serious crimes could be used to investigate other crimes for which there may be less accuracy or public acceptance (i.e., scope creep). Or a law enforcement agency may over rely on an AI tool when other investigation methods would be more suitable or accurate (i.e., automation bias). And individual police officers may misuse an AI tool, either accidentally or purposefully.

6. **Privacy**

   AI tools require a large amount of data during the training and development process, and they also require some amount of input data when they are used in the field. What constraints should be placed on law enforcement's access to personal information, and on the private companies that develop AI tools for law enforcement use? Should these constraints go beyond the requirements of Fourth Amendment law, to the extent the constitutional limits are known (see #9, below)? If an AI tool was developed using data that was collected or used without consent, should this disqualify its use in law enforcement? The design and use of AI tools will have to achieve a minimum level of privacy and civil liberties while also managing public interests in performance (see #1) and the reduction of bias (see #2), which sometimes require access to personal information in order to make improvements.

7. **Stewardship of Data Held by Law Enforcement**

   When the government collects data for the purpose of training or using an AI system, it has the responsibility of acting as good stewards of that data. This is likely to require minimum standards for data security and reasonable policies with respect to data re-use and third-party access.

8. **Managing Discretionary Application**

   When an AI system is adopted, the units or individual officers with access to the system will have some degree of discretion in its decisions about whether and where to deploy the system. How should law enforcement manage or constrain this discretion? A poorly developed plan can exacerbate some of the issues raised elsewhere, including misuse (see #5), bias (see #2), and under-utilization (see #4). Poorly managed discretion can also lead to public distrust if police use (or are believed to use) AI systems in an arbitrary, haphazard, or uneven manner.

9. **Translating Fourth Amendment Rules to AI Tools**

   Law enforcement use of AI tools may raise novel Fourth Amendment questions that will require thoughtful analysis in the absence of judicial review. For example, Generative AI can be used to create “deep fake” videos, images and voices that mimic real people. These have been used to generate virtual line-ups already. If law enforcement were to spoof the voice of a trusted friend of a suspect, would a recording of the suspect saying something incriminating be constitutional and admissible in a criminal case against them by virtue of the “misplaced trust” doctrine?

10. **Cumulative Impact of Multiple AI Systems on Performance and on Lost Liberty**

    Should the legal and ethical standards that are developed for one AI system be modified when the system is combined with other AI systems? If combinations of AI systems produce a level of accuracy that is greater than the sum of the individual parts, this could justify greater use, or fewer limitations. And if combinations of AI systems create threats to privacy and other civil liberties that are greater than the sum of the individual parts, this could require more restrictions and limitations on their use.

(C) Is there adequate public notice, voice, and oversight with respect to the adoption and use of the AI tool?

11. **Transparency and Public Input**

    The decision to acquire and deploy AI-powered tools for law enforcement is a momentous one. These tools are likely to have profound impact on members of the public, how officers perform their jobs, and the relationship between the police and their constituents. In a democratic society, the public should have information and a voice in these decisions, but what form should transparency and public input take? Should the public have access to source codes or other forms of technical transparency, in addition to descriptive information? Should the form and degree of public input vary from place to place, based on the nature of the tool, based on the purpose of its use, or based on the risks to privacy and civil liberties? Moreover, although most can agree that democracy requires some degree of transparency by the government, there are important questions as to what type and degree of transparency is necessary, especially with regard to new technologies that have not been substantially studied. Transparency may also need to be balanced against the risk of criminal circumvention and other countervailing law enforcement and public safety concerns.

12. **Pre-Adoption Procedures**

What procedures should a law enforcement agency follow before adopting and using a new AI tool? When and how should these procedures be incorporated into procurement decisions and contracts? A well-designed process will provide transparency and accountability. A non-exhaustive list of pre-adoption procedures that have already been proposed include:

- **Licensing or certification of the AI tool.** Before an AI system is adopted and used in the field, it may be appropriate to require the AI system to undergo independent testing and licensing to ensure that the system will work as intended. For example, a licensing or certification process can establish that the system achieves a minimum level of accuracy (see # 1, above), tolerates no more than a maximum amount of bias (see #2), was trained using data that was sourced legally and is stored securely (see #7), and was produced using a reliable supply chain free from national security risks.
- **Use limitation plan.** During the procurement process, it may be appropriate to require law enforcement agencies to draw up a plan that establishes how an AI tool will be used, and when the AI tool will *not* be used. These limits may specify:
    - The purposes for which an AI tool can or cannot be used (for example, restricting an AI tool to suspect identification purposes and prohibiting its use for general surveillance and data-gathering. (See Part 2 for a comprehensive list of purpose-driven uses)
    - A list of crimes for which the AI tool may be used in the course of investigation (e.g., limiting the use to the investigation of violent felonies, or to the investigation of white collar crimes)
    - The conditions, if any, under which the AI tool can be used as a sole basis for issuing a search warrant, making an arrest, or taking another adverse action
- **Consistent use plan.** It may be appropriate to require law enforcement to design protocols that will ensure AI tools are consistently used in contexts where they are likely to make law enforcement more accurate or efficient (see #1), and to reduce the risk that discretionary use of the tool will result in biased over-surveillance or under-protection (see #2)

- **Data stewardship plan.** If use of the AI system is likely to lead to the collection and storage of significant amounts of personal information, it may be appropriate to require law enforcement to draw up a data stewardship plan (see #7)
- **Training and supervising plan.** It may be appropriate to require law enforcement agencies to draw up and follow a plan for training the officers that will use the AI tool, and a plan for monitoring and supervising use to ensure compliance with legal requirements and internal rules
- **Public engagement.** It may be appropriate to require law enforcement to provide a form of notice to the public and to receive input from the community before adopting a new AI tool

13. Post-Adoption Procedures, Audits, and Rights to Appeal

Every system of accountability requires clear rules on the front-end, but also strong mechanisms on the back-end to ensure that those rules are being followed. Law enforcement's uses of technology are no exception. Moreover, many AI tools are dynamic and their performance and use will change over time, particularly as new data is input into the system, requiring ongoing audits and reassessments of compliance with legal and ethical requirements. What auditing and appeals procedures are appropriate after an AI system is deployed? A well-designed post-adoption process will provide accountability and, when appropriate, attestability.

14. Impact on Law Enforcement Employees

The integration of AI into law enforcement will have a profound and not entirely predictable impact on the nature of police work. As is the case in other professions, AI is likely to augment or replace some of the skills that police officers currently use, while making other skills indispensable. AI may also increase the degree to which police officers are monitored and evaluated, echoing some of the surveillance concerns that attend the impact of AI on the civilian population. How will AI affect the quantity and quality of law enforcement jobs? Are there appropriate policies or limitations that can ensure the wisdom and wellbeing of police officers continues to thrive? Effective AI will complement and augment law enforcement as long as officers are trained and assessed effectively. The law enforcement profession is changing and will need to recruit and retain officers who will use AI tools responsibly.

TAXONOMY OF LAW ENFORCEMENT USES OF AI

During the Subcommittee's first year (and perhaps beyond, if it proves to be fruitful), NAIAC-LE will organize its research and deliberations according to the purpose of a law enforcement agency's use of AI, rather than technology-by-technology. This organization is likely to be helpful as NAIAC-LE considers recommendations for difficult ethical and legal issues, because the ethics of a technology will often depend, to some degree, on how it is being used — that is, *to what end*. Moreover, a single technology (e.g., facial recognition) can be used for many different purposes, each of which may call for different protocols and precautions.

What follows is an initial taxonomy of AI uses in the law enforcement context, with several illustrations of techniques that are either in development or currently deployed. This taxonomy is purely descriptive, and should not be read as an indication that the Subcommittee has reached any particular conclusions about the technologies or uses listed here.

1. **Event Detection Methods (Has a crime occurred?)**
   These are technologies that monitor sensor data, internet traffic, or other forms of information (possibly in real time) and alert when the system detects a suspicious pattern (typically, one that the system has been trained to recognize as indicative of criminal activity). This category covers only systems that monitor a general area for signs of victimization, rather than analyzing individual people, cars, or devices for signs of suspicion. Thus, this AI use category is distinct from the suspect identification and risk scoring categories described below. This category of use may alert law enforcement to the fact that an otherwise unreported crime has been committed.

   Examples include:
   - Gunshot detection
   - Anomaly detection
   - Detection of casing activities
   - Analysis of financial trading for insider trading / securities violations
   - Detection of fraud committed using deep fakes and voice clones
   - Threat assessment (e.g., monitoring social media to see if criminal acts have occurred or are about to occur)
   - Human trafficking patterns
   - Cyberattack/DDoS detection
   - Drug trafficking detection (e.g., monitoring social media)
   - Violation of copyright laws
   - Content analysis of social media posts (e.g., Dataminr)

- Weapons/contraband detection
- Speed detection

2. Person Identification Algorithms

These systems take a unique evidentiary sample, set of characteristics, or other information from a specific crime scene and attempt to use that information to identify an individual (often a person suspected of involvement in criminal activity).

Examples include:

- Identifying unique features of people: facial recognition (see #8, below), gait recognition, iris recognition, voice recognition, fingerprint recognition, probabilistic DNA, forensic genetic genealogy, rapid DNA, multi-modal identification (combination of biometrics to identify), pattern of life analysis
- Geofencing
- AI for generating possible images of suspects from witness descriptions (augments composite artists)

3. AI-Assisted Surveillance

This category focuses on surveillance systems that are powered in some way by AI. Some of these surveillance systems operate even absent a specific law enforcement operation, while others are activated in the context of a particular operation. In general, these systems are capable of gathering information on large numbers of individuals across space and time, irrespective of their involvement with crime. AI is sometimes crucial to the technology itself (i.e., enabling the algorithm) and sometimes assists law enforcement with making efficient use of the data (e.g., quickly stringing together video from different times, locations, and vantage points that have captured the same individual).

Examples include:

- Automated License Plate Readers ("ALPR")
- Cell-site simulators/IMSI catchers
- Cross-camera tracking
- Wide-area motion imagery / Wide-Area Persistent Surveillance ("WAPS")
- Cameras combined with facial-recognition capabilities

4. Investigation and Case Development of an Identified Suspect

This category focuses on uses of AI that enhance the investigation of a specific individual (typically a suspect or person-of-interest in a criminal investigation) by gathering and/or analyzing data related to that individual. (Pre-AI analogies include manual searches, interrogations, and eye-witness identification.)

Examples include:

- Real-time and historical location: ALPR, cell-site simulators/IMSI catchers, Cross-camera tracking (in other words, making suspect-driven use of the systems described in #3, above)
- MDFT (analysis of seized devices)
- Lie detection, sentiment analysis, emotion detection
- AI-generated voice cloning and spoofing to interact with suspect under false pretenses (e.g., a twist on undercover operations)
- AI-generated line-ups
- Social network analysis
- Repository for Individuals of Special Concern (RISC)
- Forensic analysis of a computer or software system, or of the provenance of data

5. Risk Assessment / Scoring as a Basis for Adverse Action

This category includes AI and Machine Learning algorithms that are trained to predict the chance that a person has committed a crime (or will commit one in the future, in some cases). The scores or predictions are then used as a basis, either alone or in combination with other evidence, to take an adverse action against a target: a protracted stop, a warrant-based search, or an arrest, for example.

Some risk assessment and scoring tools analyze data that is too voluminous for humans to analyze themselves, or look for differences in information that are too fine-grained or complex for humans to notice. Others analyze a more limited set of data, but do so in a manner that is more consistent, and possibly more accurate, than human decision-makers would.

Examples include:

- Observing relationships: social network analysis, social media analysis, convoy analysis
- Risk assessment algorithms for bail, attacks on infrastructure, etc.
- Content analysis of social media
- Models for differentiating terrorists from non-violent radicals based on online activity

- Real time Border Patrol uses of AI to make reasonable suspicion decisions to determine which vehicles should proceed to an in-depth search
- Weapons detection

6. **Dot-Connecting Methods Not Involving Personal Information**

This set of tools advances a case by linking evidence from a crime to new leads and avenues of inquiry. This category differs from event detection (see #1, above) because event detection marks the beginning of a possible cause: it provides an initial alert that a crime may have occurred. With these tools, the police are already in the process of investigating a suspected crime. This category also differs from suspect identification algorithms because the output of these systems is not expected to be an identified suspect. Rather, both the input and the output of these systems involve non-personal information, but the output may lead, with further investigation, to the discovery of a suspect or witness.

Examples include:

- Image analysis (e.g., identifying hotel rooms based on background in human trafficking images)
- Crime series detection (finding related crimes to detect a series. E.g., NYPD’s Patternizr algorithm)
- Metadata analysis (e.g., Axon building DEMS analytics to identify related videos)
- Chemical analysis to determine drug origin[2]
- Detection of synthetic media (DARPA metaphor and semaphor program)
- Ballistic matching algorithms like National Integrated Ballistic Information Network (NIBIN)

7. **Resource Allocation Decisions/ Investigation and Case-Management Systems**

This set of AI tools help individuals and units spend their time and resources efficiently by ordering or prioritizing tasks. These tools differ from event detection systems (see #1, above) and risk assessment and scoring algorithms (see #6) because these tools still depend on the judgment of the officers using the tools to determine whether a crime has occurred, or whether a person deserves more interest or treatment as a suspect. Instead, these tools typically

[2] “2023 Agency Inventory of AI Use Cases,” Department of Justice, https://www.justice.gov/open/file/1305831/dl?inline=.

provide value by rapidly assessing a large amount of input data and organizing or rank ordering it for additional human scrutiny.

Examples include:

- Predictive policing: predicting locations and times where crimes may occur[3]
- Intervention- predicting a person's risk of victimization or gang involvement
- Prioritizing of TIPS[4]
- Intelligent Records Consolidation Tool[5]
- Privileged Material Identification[6]
- Analyzing which units/teams/individuals to send to a given call
- Triage of data during emergencies

8. **Accountability Algorithms**

Unlike the previous categories, this use of AI is not meant to enhance or enable police investigation, but to ensure that the police themselves are acting in lawful, equitable, and efficient ways. Many of these AI uses operate on police-generated data.

Examples include:

- BWC review algorithms (e.g., Trueleo)
- AI detection of racial disparities in treatment
- Officer training, feedback, and assessment using AI-generated virtual reality
- Officer risk-scoring/psychological evaluations
- Device-generated data (e.g., data generated when a Taser is drawn or fired; smart gun holsters)
- RMS/CAD analytics/visualizations
- Automated creation of reports from audio or BWC data
- Automated review of case files and reports

9. **Private 'Pipelines'**

[3] David Weisburd, Beidi Dong, and Clair White, "Poor Health and Violent Crime Hot Spots: Mitigating the Undesirable Co-Occurrence Through Focused Place-Based Interventions," *American Journal of Preventive Medicine* (June 2020): https://cina.gmu.edu/publications/poor-health-and-violent-crime-hot-spots-mitigating-the-undesirable-co-occurrence-through-focused-place-based-interventions/.

[4] "2023 Agency Inventory of AI Use Cases," DOJ.

[5] "2023 Agency Inventory of AI Use Cases," DOJ.

[6] "2023 Agency Inventory of AI Use Cases," DOJ.

This category focuses on uses of AI by *private* actors that facilitate criminal law enforcement. Law enforcement has always relied on private parties to report crime and assist with investigations, and most every law enforcement investigation relies on private actors in some manner. Here NAIAC-LE focuses on the ways that AI allows private parties to detect and share information potentially relevant to criminal law enforcement.

Examples include:

- Automated detection of child sexual abuse images
- Lateral surveillance platforms (e.g., Axon Citizen, Ring NPSS)
- Facial recognition results performed by private individuals or businesses
- VMS/RTCC (e.g., private cameras in Fusus systems)
- Fraud detection performed by financial institutions and reported to police
- Know Your Customer-related alerts
- Independent "DNA detectives" who develop family trees from genetic databases to locate criminals (e.g., CeCe Moore)
- AI used in response to a law enforcement subpoena/warrant/request (e.g., geofencing, reverse searches)

10. Robotics

This category focuses on law enforcement use of robots, which increasingly are enabled by AI. Because these AI technologies are embodied, they raise unique issues related to the use of force.

Examples include:

- Unmanned aerial vehicles (drones) (e.g., for suspect pursuit)
- Unmanned ground vehicles (robots) (e.g., for bomb defusing or entry into potentially hostile environment)
- Unmanned underwater vehicles (e.g., for locating evidence)
- Satellites (e.g., for capturing and analyzing aerial data at specific points in time)

11. SPECIAL CASE STUDY: Facial recognition

Facial recognition technologies are a subset of biometric-based identification algorithms described in the first set of technologies. However, given the higher stakes involved (that our faces are largely immutable, and are available for observation everywhere we go), these technologies tend to heighten public concern and raise unique ethical issues.

Examples include:

- Event-driven law enforcement (identifying a perpetrator from camera footage or other electronic media)
- Anticipatory surveillance by law enforcement (e.g., at an event where individuals who are known to be dangerous are expected to attend)
- Identification during a stop, arrest, or border crossing
- Locating a suspect (e.g., finding a suspect with an outstanding warrant in a public place or in the course of issuing a new driver's license)
- Detecting victims of human trafficking
- Identification for school security
- Private security by civilian/commercial entities
- Threat detection to witness protection program (monitoring for public images or videos that could put the witness at risk), or other sensitive places such as religious institutions, healthcare facilities (e.g., abortion clinics), and sites of protest

PRIORITY TOPICS FOR YEAR 1

Four of NAIAC-LE's six working groups are actively developing guidance and recommendations at this time. NAIAC-LE expects to transmit recommendations on the following topics:

T-1 Working Group (Identification and Surveillance)

- Person Identification Algorithms (Use Category 2)
- Facial recognition (Use Category 11)
- AI-Assisted Surveillance (Use Category 3)

This working group is preparing guidance on five key technologies: (a) facial recognition; (b) License Plate Readers; (c) video analytics; (d) gunshot detection; and (e) drones.

T-2 Working Group (Predictive Policing Set)

- Event Detection Methods (Use Category 1)
- Investigation and Case Development of an Identified Suspect (Use Category 4)
- Risk Assessment / Scoring as Basis for Adverse Action (Use Category 5)
- Private "Pipelines" (Use Category 9)

This working group is preparing specific guidance related to each of the four use categories listed above.

E-1 Working Group E-1 (Performance and Bias)

- Performance and Evaluation (Law and Ethics Category 1)
- Bias (Law and Ethics Category 2)
- Potential Risks and Harms of Underutilization (Law and Ethics Category 4)

This working group is developing guidance for high-quality evaluation in the field, particularly during an initial probationary period before a police department has fully adopted and integrated the technology. The group expects to provide guidance for departments that want to create the best evaluation of performance, bias, and costs of a tool in the field given the department's particular resources and needs. Some may be able to implement a gold standard randomized controlled trial, but where that is impractical, the group will offer means of conducting pre- and post-tests that can get the most useful and actionable information for the department and the general public.

E-3 Working Group (Process Set)

- Transparency and Public Input (Law and Ethics Category 11)
- Pre-adoption process (Law and Ethics Category 12)
- Post-adoption Procedures and Audits (Law and Ethics Category 13)
- Impact on Law Enforcement Employees (Law and Ethics Category 14)

This working group is creating guidance on three pressing topics: (a) Across-the-board minimum benchmarks and procedures that law enforcement agencies should follow before acquiring an AI tool, including the role of the federal government in facilitating, incentivizing, or mandating such requirements; (b) Additional agency- and context- specific procedures and policies to implement prior to use of an AI-tool; and (c) Post-adoption auditing and accountability procedures.

LAW ENFORCEMENT SUBCOMMITTEE MEMBERS

Armando Aguilar
(April 2023 – March 2026)
Assistant Chief of Police, Miami Police Department

Anthony Bak
(April 2023 – March 2026)
Head of AI, Palantir

Amanda Ballantyne
(April 2023 – March 2026)
Director of the AFL-CIO Technology Institute

Jane Bambauer
(April 2023 – March 2026)
Marion B. Brechner First Amendment Project, Brechner Eminent Scholar at the College of Journalism and Communications and at Levin College of Law, University of Florida

Esha Bhandari
(April 2023 – March 2026)
Deputy Director of the American Civil Liberties Union's Speech, Privacy, and Technology Project

Jennifer Eberhardt
(April 2023 – March 2026)
Professor of Organizational Behavior and Psychology, Stanford University

Farhang Heydari
(April 2023 – March 2026)
Assistant Professor of Law, Vanderbilt Law School

Benji Hutchinson
(April 2023 – March 2026)
Chief Revenue Officer of Rank One Computing

Rashawn Ray
(April 2023 – March 2026)
Vice-President and Executive Director of the AIR Equity Initiative

Cynthia Rudin
(April 2023 – March 2026)
Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, Biostatistics & Bioinformatics at Duke University

ABOUT NAIAC

The National Artificial Intelligence Advisory Committee (NAIAC) advises the President and the White House National AI Initiative Office (NAIIO) on the intersection of AI and innovation, competition, societal issues, the economy, law, international relations, and other areas that can and will be impacted by AI in the near and long term. Their work guides the U.S. government in leveraging AI in a uniquely American way — one that prioritizes democratic values and civil liberties, while also increasing opportunity.

NAIAC was established in April 2022 by the William M. (Mac) Thornberry National Defense Authorization Act. It first convened in May 2022. It consists of leading experts in AI across a wide range of domains, from industry to academia to civil society. https://www.ai.gov/naiac/

###