

# SMART PROCUREMENT

Guidance for Governments on Protecting  
Civil Liberties when Procuring Technology

**ACLU** Illinois

# Table of Contents

## **SMART PROCUREMENT: GUIDANCE FOR GOVERNMENTS ON PROTECTING CIVIL LIBERTIES WHEN PROCURING TECHNOLOGY**

Introduction to “smart procurement,” which requires government entities to weigh the benefits of any contemplated technology against vital public interests

## **SMART PROCUREMENT CHECKLIST**

Quick reference to help recognize and understand the types of risks that new technology may pose to privacy, civil rights, and civil liberties interests

## **INHERENT RISK ASSESSMENT**

Questions, divided by topic, that government entities should consider to help reveal and address inherent risks associated with a contemplated technology

## **VENDOR RISK ASSESSMENT**

Summary of an adaptable questionnaire for identifying and addressing risks associated with vendors and their product or service offerings

## **RISK LEVEL CLASSIFICATION**

Framework for classifying the overall risk associated with any contemplated technology

The Appendices and Glossary, which can be found online, provide additional resources for procurement professionals and others seeking further detail.

### **APPENDIX A: SAMPLE VENDOR ASSESSMENT QUESTIONNAIRE**

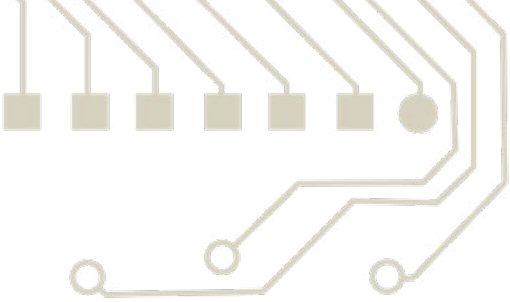
### **APPENDIX B: GOVERNMENT ALLIES FOR SMART PROCUREMENT**

### **GLOSSARY OF TERMS**



[www.aclu-il.org/procurement](http://www.aclu-il.org/procurement)

October 2024



# SMART PROCUREMENT:

## Guidance for Governments on Protecting Civil Liberties when Procuring Technology

This Guidance identifies essential guardrails for ensuring that risks to privacy, civil liberties, and civil rights are adequately considered and addressed whenever the government seeks to procure or utilize technology that affects people.<sup>1</sup> Heightened connectivity, more sophisticated cameras and sensors, and the emergence of powerful artificial intelligence (“AI”) applications are a few of the factors driving governments across the country to seek out new technologies, often times without considering potentially grave implications for the public interest.

Governments seeking to procure technology for public use must adopt a framework for smart procurement. Smart procurement occurs only when governments carefully weigh the impact of contemplated technology against privacy, civil liberties and civil rights interests. Failing to adequately consider and act on those vital interests when purchasing and implementing technological solutions may damage public trust and cause real, and in some cases, irreparable harm to individuals and communities, including any of the following:

- **DISCRIMINATION:** Having a discriminatory impact on protected groups and classes of people, including by increased racial and religious profiling of community members and over-policing where there is a historical distrust of government authority;

---

<sup>1</sup>As used in this Guidance, “technology” is a catchall term intended to apply to any technology (including algorithms, software, and hardware) that may impact the rights, civil liberties, and/or privacy of individuals or communities. This Guidance is not intended to apply to routine hardware (e.g., office supplies, printers, monitors) that are in widespread public use unless they have been equipped with surveillance, artificial intelligence, or other advanced capabilities.

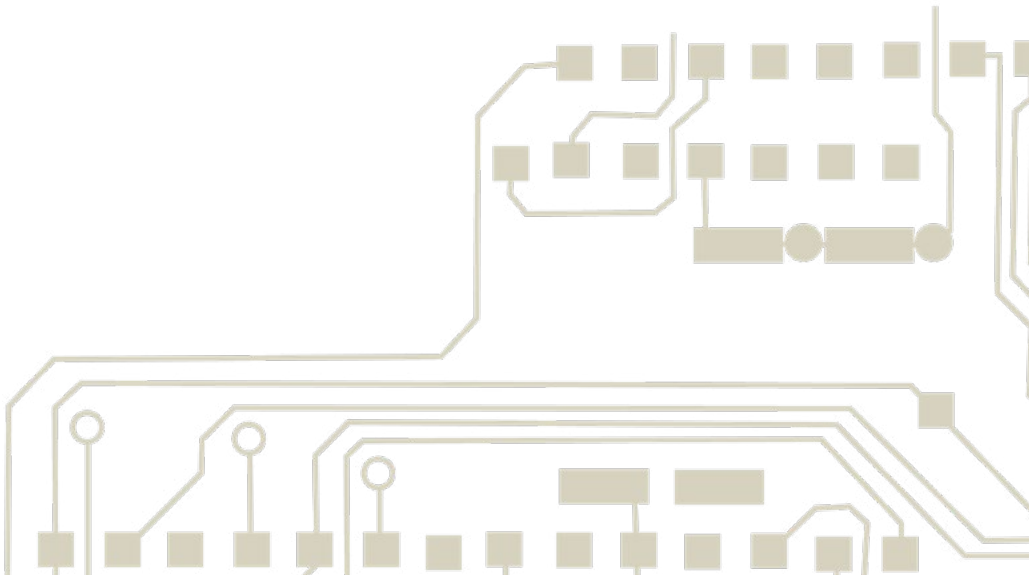
- **UNDERMINING FUNDAMENTAL RIGHTS:** Erosion of civil rights and civil liberties, expanding unwarranted surveillance, violating First and Fourth Amendment rights, and other fundamental rights guaranteed under the Constitution and the law;
- **INCREASING RISK AND LIABILITY:** Making government more vulnerable to cyber-attacks and amplifying liability due to potential civil rights litigation (for example, a Section 1983 lawsuit brought by someone wrongly arrested as a result of a faulty facial recognition technology) that challenges the use of privacy invasive technology by government entities;
- **INEFFICIENCY:** Needlessly purchasing expensive technology that is riskier than existing “analog” options, or adopting inaccurate or ineffective technology that does not meet the identified needs or goals, undermining inter-agency cooperation and coordination, including duplicated efforts and improper use of collected data by other agencies; and
- **SOWING DISTRUST:** Creating distrust between the government and communities served, including due to blurring the boundary between private and public action.

This Guidance is intended to provide government actors, decision-makers, legal and policy staff and non-governmental advocates with resources to facilitate a smart procurement approach. Among the tools included in this guidance are: a best practices checklist, questions to help recognize and understand inherent and vendor risk, and a framework for classifying the level of risk associated with the procurement of new technology.

# Smart Procurement Checklist:

The government's role in evaluating technology is of paramount importance – it is up to the government to understand the costs and risks associated with any procured technology, and to ensure that technology is not deployed or used in a manner that undermines privacy or civil liberties. Use this Quick Checklist on the following page to help recognize and understand the types of risks that new technology may pose to privacy, civil rights, and civil liberties interests.

The Quick Checklist can help provide a snapshot of two closely intertwined types of risk whenever government seeks to procure and deploy new technology on the public: inherent risk and vendor risk. Both types of risk may pose considerable danger to vital constitutional and legal interests, making it vital to assess inherent and vendor risk before procuring technology.



## ☐ **Identify and Focus on Purpose**

- Define the problem or need the government seeks to address through technology.
- Clearly identify a discrete goal or outcome of the technology being considered.
- Evaluate alternatives, including preexisting technological tools and analog solutions.
- Determine whether the technology solves the “entire” problem or just a portion.
- Consider any additional technology or resources needed to support the technology.

## ☐ **Understand the Technology**

- Reach out to government allies, organizations and groups with relevant expertise, and community leaders to learn about the contemplated technology. Do not rely solely on media reports and marketing materials.
- Do not proceed until you understand how the technology works, including the answers to key questions:
  - What types of data will be collected or used, what are the sources of that data, and what are the different ways the data can be used?
  - Will data be shared with others (e.g., other government agencies or private parties)?
- Consider possible situations or circumstances in which the technology may be used and the intended and possible unintended consequences of such use, are there any individuals or groups who may be disproportionately positively or negatively impacted?

## ☐ **Assess and Quantify Both Apparent and Hidden Risks**

- Evaluate the full spectrum of risk associated with any new technology, which requires assessing the impact of technology from diverse perspectives. Input from communities, vulnerable individuals, experts, and other government stakeholders is critical to revealing hidden risks.
- Adopt a risk-centric approach in procurement by regularly discussing questions like:
  - Can this technology have a discriminatory impact?
  - What are the potential harms?
  - Are there other uses of this technology that may amount to unwarranted surveillance?

## ☐ **Build Data Governance**

- Require transparency from vendors as to each important aspect of the technology, how it works, and its core functionality.
- Work with the public and subject matter experts to develop policies and procedures to ensure there is adequate transparency and accountability.
- Implement controls to mitigate risks associated with the technology.
- Maintain ongoing oversight of the technology, underlying data, and all uses.

# Inherent Risk Assessment:

Inherent risk is associated with a particular technology based upon its design, configuration, functionality, and/or use. Government entities should determine the nature and degree of inherent risk before soliciting vendor proposals. A robust and practical inherent risk assessment comprises key questions that touch on different dimensions of privacy, legal, and constitutional concern, including:

- **PURPOSE AND SCOPE**
- **DISPARATE IMPACT AND BIAS**
- **TRANSPARENCY**
- **FAIRNESS**
- **UNDERSTANDING THE TECHNOLOGY**
- **DATA COLLECTION AND USE**
- **COMMUNITY ENGAGEMENT**
- **OVERSIGHT AND ACCOUNTABILITY**

Consider the following questions to help reveal the nature and severity of inherent risk early in the procurement process. Questions that raise significant concerns or require vendor input can be addressed in Requests for Proposals (“RFPs”), the vendor questionnaire, or even in contract negotiations. However, to the extent these questions raise issues that are intractable, government entities should be willing to rethink the technology and their approach.

---

## **PURPOSE AND SCOPE:**

Identify the problems/challenges the government seeks to address, and determine whether the contemplated technology is necessary, or the best way to address the identified concerns.

- What is the specific problem or challenge the government seeks to address?
- Is the goal clearly defined in a way that will allow the government to measure “success”?
- Have existing or non-technological solutions been considered?
  - How do they compare?
- Why is a proposed technology being considered, and would it directly address the goal?
- Are there other urgent needs that should be funded before purchasing additional technology?

## UNDERSTANDING THE TECHNOLOGY:

Technology cannot adequately be evaluated for potential privacy and civil liberties risks unless its operations, functionality, and capabilities are well understood.

- How does the technology work to achieve the desired goal or solve the problem(s)?
- Does the technology use any form of automated decision-making or artificial intelligence?
- Is the technology reliant on any external systems or applications and, if so, what are they?
- What does the technology do with the data it collects, receives, and/or processes?
- Is the technology the least invasive and only means available to achieve the desired goal?
- Has the government agency considering the technology coordinated with other government agencies and offices who may have or may wish to use the technology?
- Will safeguards and controls (e.g., encryption, access controls) need to be put in place to protect the technology and underlying data from unauthorized access or misuse?

---

## DISPARATE IMPACT AND BIAS:

Any technology that affects individuals or communities differently may result in biased, unjust, or unfair outcomes that must be avoided.

- Is there a way to test the technology for features that may result in biased or unfair outcomes?
  - Will testing for algorithmic and other biases occur regularly?
- Can the technology yield outcomes or results that appear correct, but still contain bias (for example, facial recognition software that yields false positive matches for people of color at a higher rate than other people).
- Has someone been tasked with tracking and addressing potential bias in the technology?
- Does the technology use information in any way that may affect, target, or harm any individual, group, or community to a greater degree or in a different manner than the public at large?
- Can it be used in ways that might contribute to the government making any inferences, decisions, or judgments about any individual, group, or community?



- Will the technology collect or use any information related to race, citizenship status, gender, age, socioeconomic level, reproductive choices, sexual orientation, and/or other location-based, identity-based, or affiliation-based characteristics?
  - If so, what safeguards will be in place to limit collection or use?
- Will the technology operate in the same manner across race, gender, age, disability, ethnicity, socioeconomic status, education, etc.?

## DATA COLLECTION AND USE:

The government and the public must understand how data is collected and/or used by the technology.

- Does the technology require personal information to be collected from individuals, will it use existing data sets, or will it do both?
- If personally identifiable information (“PII”) is to be collected:
  - How will the PII be collected or used, and from what sources?
  - What specific types of PII will be collected or used?
  - Will sensitive types of PII (e.g., race, religion, medical information, etc.) be collected?
  - Can PII that is collected be used for any purposes beyond the contemplated technology?
  - Will de-identification or anonymization processes be used to protect identities?
- If only preexisting data sets are to be used (i.e., no new data collection to occur):
  - Who is represented in the data, and are any groups or communities under or over-represented?
  - Are there any assumptions being made about people identified in the data set?
  - What process or technology facilitated the original collection of the data?
  - Is the intended data use consistent with the purpose for which it was first collected?
  - Is the data set from a system prone to human error?
    - Has it been validated as accurate?
  - Are there any fields that should be eliminated from the data set prior to use?
  - What controls are in place to ensure such data sets are used only in the same manner(s) the government may use such data?
- What data may be inadvertently collected during the authorized uses of the technology?

- What information does the technology collect?
- Does it allow real-time monitoring, capture information for future use, or both?
- What measures will be taken to minimize the inadvertent collection of data, and how will such data be expeditiously identified and deleted?
- What will be the applicable retention period(s) and the bases for selecting those time periods?
- Who will be responsible for deleting data, and what will the deletion process be?
- Will there be rules or processes that describe if and how other government agencies or non-government entities, may use or access the technology or any data that has been collected?
- Will the technology generate or use metadata?
  - If so, how will it be handled?

---

## **TRANSPARENCY:**

The way the technology works, the data it uses, and the outcomes it yields should be transparent to the public.

- What information about the technology, its purpose(s), functionality, operations, uses, and underlying data will the government share with the public and what cannot be shared?
- If assumptions are made in connection with the technology or the data used, will those assumptions also be shared with the public?
- Has the government included a transparency requirement in its RFP documentation?
- Who can access the technology (including underlying systems), source code, and data?
- Are there barriers to public disclosure or independent review of the technology, and if so, how can those barriers be eliminated?
- If the vendor requires an NDA, would the vendor waive such concerns as a precondition to contracting with the government?
- Will there be a privacy policy put in place (by the vendor, or by the government in conjunction with the vendor)?
  - If not, why?
  - If so, what information will it contain?
- If the technology incorporates any degree of automated decision-making procedures, are such procedures fair and explainable?
- Can any part of the technology or underlying systems be described as a black box system?

## COMMUNITY ENGAGEMENT:

The government should acquire and implement technology based on community needs and with input from the community and relevant experts.

- Will members of the community have a meaningful opportunity to learn about the technology, ask questions, provide feedback, and raise concerns before a decision to adopt it is made, and if so how?
  - Will there be a public notice and comment period before, during, and/or after implementation of the technology?
    - How will the government agencies ensure that comments shared by the community will be heard, considered and addressed?
  - Will the government consult with relevant organizations and groups, subject matter experts, and other relevant authorities to help assess the technology and/or vendor(s)?
  - Will there be ongoing community oversight (e.g., community boards, task forces, etc.)?
- 

## FAIRNESS:

Assessing contemplated technology for fairness helps ensure that the government and vendor are considering the technology's impact on civil rights, liberties, and other issues of justice and equity.

- Would the technology be deployed in communities with non-citizens, low-income residents, or any group historically vulnerable to disproportionate civil liberties violations?
- Will any information be shared with other government entities or other third parties, and if so, will the government need to put in place privacy-protective policies in place to ensure that information is not used in a way that can harm certain individuals or communities?
- Could the technology be used on groups, public gatherings, or crowds?
  - Can it have an effect (direct or indirect) on First Amendment activities such as protests?
  - What safeguards are in place to limit this?
- Are errors in the technology evenly distributed, and similar in type, across all demographics?
  - If the system works without any errors, can it still perpetuate injustice?
- Will there be a way for individuals or communities affected by the technology to report that they may have been treated unfairly?

## **OVERSIGHT AND ACCOUNTABILITY:**

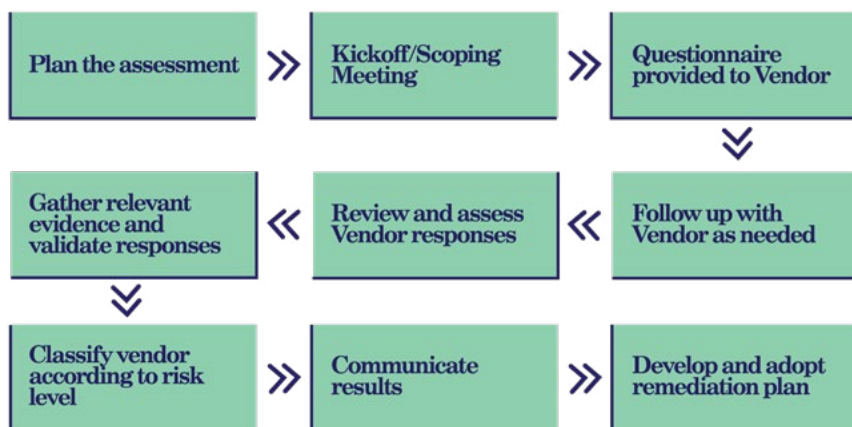
Mechanisms should exist to facilitate ongoing oversight of the technology and ensure accountability to the public.

- How will the impact of the technology be measured over time?
  - What oversight mechanisms will need to be in place to assess the technology and flag any issues?
- Does the vendor have a proven commitment and demonstrable track record of respecting individual privacy and maintaining high standards of information security?
- Has the technology been evaluated for varied use cases?
  - If the technology meets the stated goals, is there a test to assess any negative unintended consequences on privacy, civil liberties and civil rights? If there is a negative impact, how can it be remedied?
- Are there any red flags associated with this technology or the vendor providing it?
- Would the vendor be willing to agree to a review of their system(s) by an independent third party?
  - Can the independent third party continue to check the tech for possible risks once adopted? If not, how will the government audit the vendor's activities?
- What controls are in place to ensure that the vendor will not use the data in ways that the government itself is prohibited from under the Constitution and other applicable laws?
- What specific, affirmative measures will be implemented to safeguard the public from the potential adverse impacts before and after the technology is formally assessed?
- What are the technical, physical, and/or procedural controls and measures in for cybersecurity risks, including breaches and/or malfunctions?
- To what degree will the vendor be able to use or share information that is provided or collected for purposes beyond those contemplated in the draft agreement?
- Has the vendor identified internal privacy, cybersecurity, and other policies, procedures, and/or compliance framework for how they manage information?

# Vendor Risk Assessment:

Vendor risk is the degree and nature of risk associated with a particular vendor, the agreement with the vendor, and the vendor's operations, relationships, activities, and performance under the contract. When governments utilize technology (including algorithms and software) developed and maintained by private vendors, their judgments still represent public policy. In addition to inherent risk, the government must also ascertain risk associated with the vendors themselves. This is typically achieved by requiring vendors to complete a vendor assessment questionnaire ("VAQ"), which is provided to technology vendors at the same time the RFP is posted.<sup>2</sup>

The core components of the vendor risk management ("VRM") process require the vendor to respond to a standard set of questions (i.e., the VAQ), followed by evaluation and scoring of responses to those questions. While questionnaires vary, most VRM frameworks follow a standard process flow, with an emphasis on planning and active engagement, as shown in the figure below.



---

<sup>2</sup> Appendix B contains a draft VAQ, which includes a series of questions divided across several categories, including General, AI, Privacy, Security, Governance, and Miscellaneous. The VAQ is a starting point containing smart procurement questions that vendors should be asked to answer in response to RFPs.

In addition to helping government entities assess the risk(s) associated with a given vendor offering a certain technology, requiring vendors to complete a questionnaire has many additional benefits, including:

- i. vendors may supply answers to questions that government stakeholders may have been unable to answer,
- ii. additional information and details are revealed that can help enhance the government's understanding of risk associated with the technology, and
- iii. balance of power in negotiations shifts in ways that benefit the government and the public. In addition, conducting the VRM process will allow the government to more accurately anticipate vendor risk over time.

# Risk Level Classification:

By assessing inherent risk and vendor risk together, any given procurement purchase can be classified at an appropriate level. The classification should be driven by the outcome of the inherent and vendor risk assessments, considered in view of the government priorities and public's vital interests. While scoring may be informal or precise, the end result should be a risk level classification based on the potential harm to any individual's, group's, or community's:

- privacy, rights and civil liberties;
- health or well-being, including economic, educational, or employment interests;
- access to and availability of goods and services (both private or public); administration of criminal justice;
- and/or freedom of movement or mobility

For example, the following risk scoring classification is predicated on the level of impact to the above rights and privileges.

Score	Impact	Necessary
<b>LOW</b>	The project is likely to have little to no impact on any rights or privileges; to the extent any impact occurs, it likely is reversible and brief in duration. (Example Project: Drone used to perform fully anonymized count of public park visitors over fixed period of time)	Unlikely to warrant major modifications to the agreement or vendor operations.
<b>MEDIUM</b>	The project is likely to have a mild or moderate impact on certain rights or privileges; to the extent an impact occurs, it likely is reversible and short-term, and unlikely to cause harm. More extreme cases may occur, but they will be outliers. (Example Project: Multiple drones used to perform continuous video surveillance of public park)	Some changes to the agreement and/or vendor operations likely will be necessary to mitigate risk; outlier cases should be scrutinized closely to confirm they are true outliers.
<b>HIGH</b>	The project is likely to have a significant impact on rights and privileges; such impacts can be difficult to reverse, and are ongoing or long-term. The impact may be substantial in scope (many individuals impacted) or magnitude (the nature of harm is high, e.g., loss of liberty). (Example Project: Drone video used in facial recognition software to identify/track all park visitors)	Significant and/or extensive changes likely will be necessary to mitigate risk of harm; abandonment of vendor engagement or technology must be considered if risks cannot be sufficiently mitigated.
<b>SEVERE</b>	The project will very likely have a significant impact on rights and privileges in terms of both scope and magnitude; such impacts will be irreversible and perpetual, and may include substantial direct harm to individuals and communities, as well as harmful side effects and other unforeseen consequences. (Example Project: Drone video analyzed by software, and used as basis to search park visitors identified by algorithm as “threatening” based on demeanor, gait, etc.)	Abandonment of vendor engagement or technology highly likely; approach to underlying problem needs to be rethought from different, possibly non-technological approaches.

It is essential to recognize that smart procurement is not just about acquiring new technology but about ensuring that civil liberties and privacy are protected at every step. By adopting a risk-centric approach and fostering transparency, governments can make informed decisions that safeguard public trust. With the right practices, we can embrace technological advancements without compromising the rights and freedoms that are fundamental to our society.



View this guide online, and  
find more resources on smart  
procurement of technology:

[www.aclu-il.org/procurement](http://www.aclu-il.org/procurement)

**ACLU** Illinois