Fundamentals:

Privacy Policy in Government

PRESENTATION BY:
JULIA CHRUSCIEL

Who am I?

- I manage the privacy and surveillance technology work in SF
- Currently work for the City and County of San Francisco
- Experience in advocacy and academic research around privacy, public policy, and emerging technologies

Privacy Policy in Theory and Practice

01. Privacy as Foundational Principle

02. Defining Surveillance Technology

03. Procurement Checks

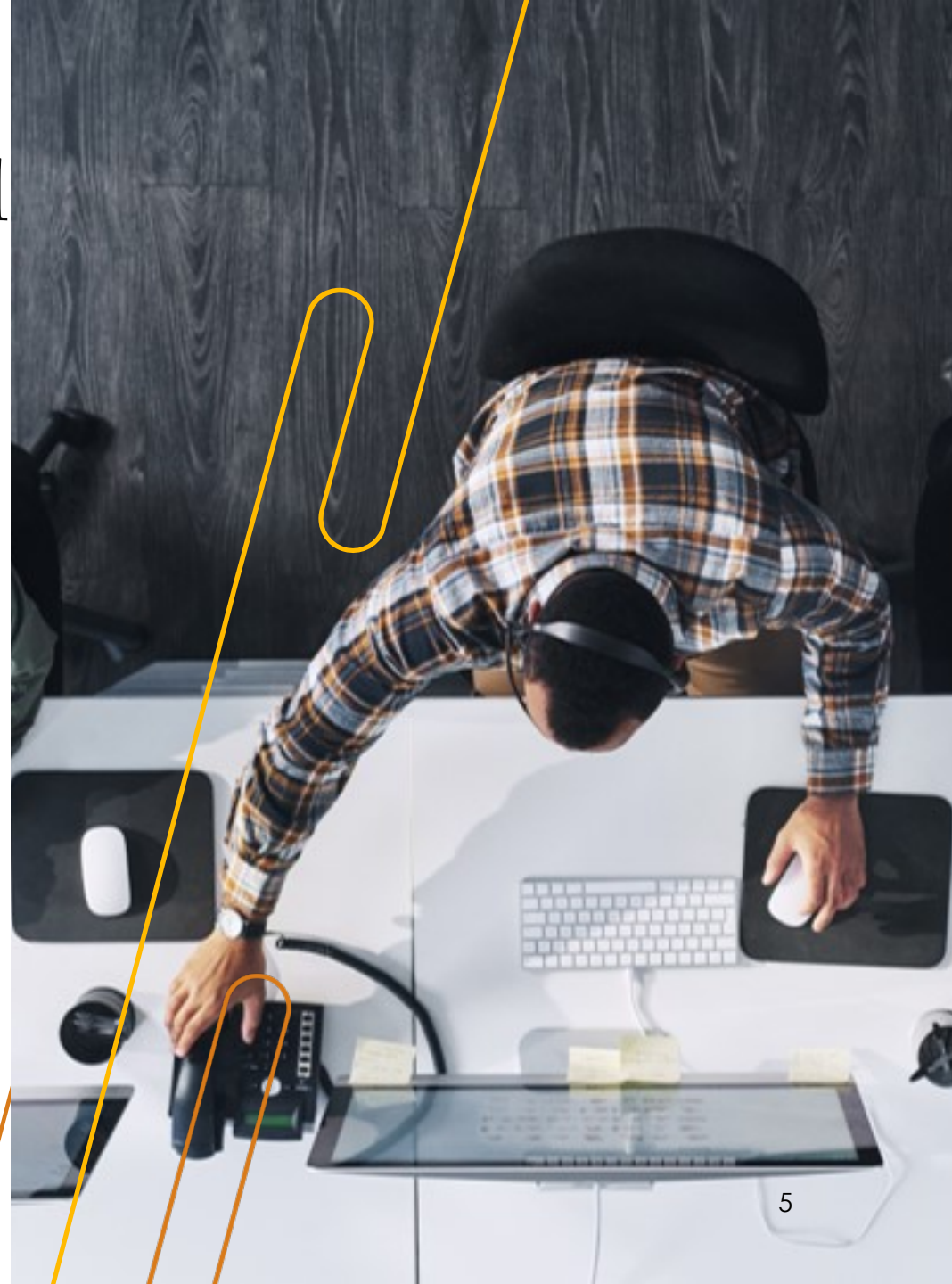
04. Annual Reports

05. Best Practices and Lessons Learned – Recommendations for Privacy Programs

1. Privacy as Foundational Principle

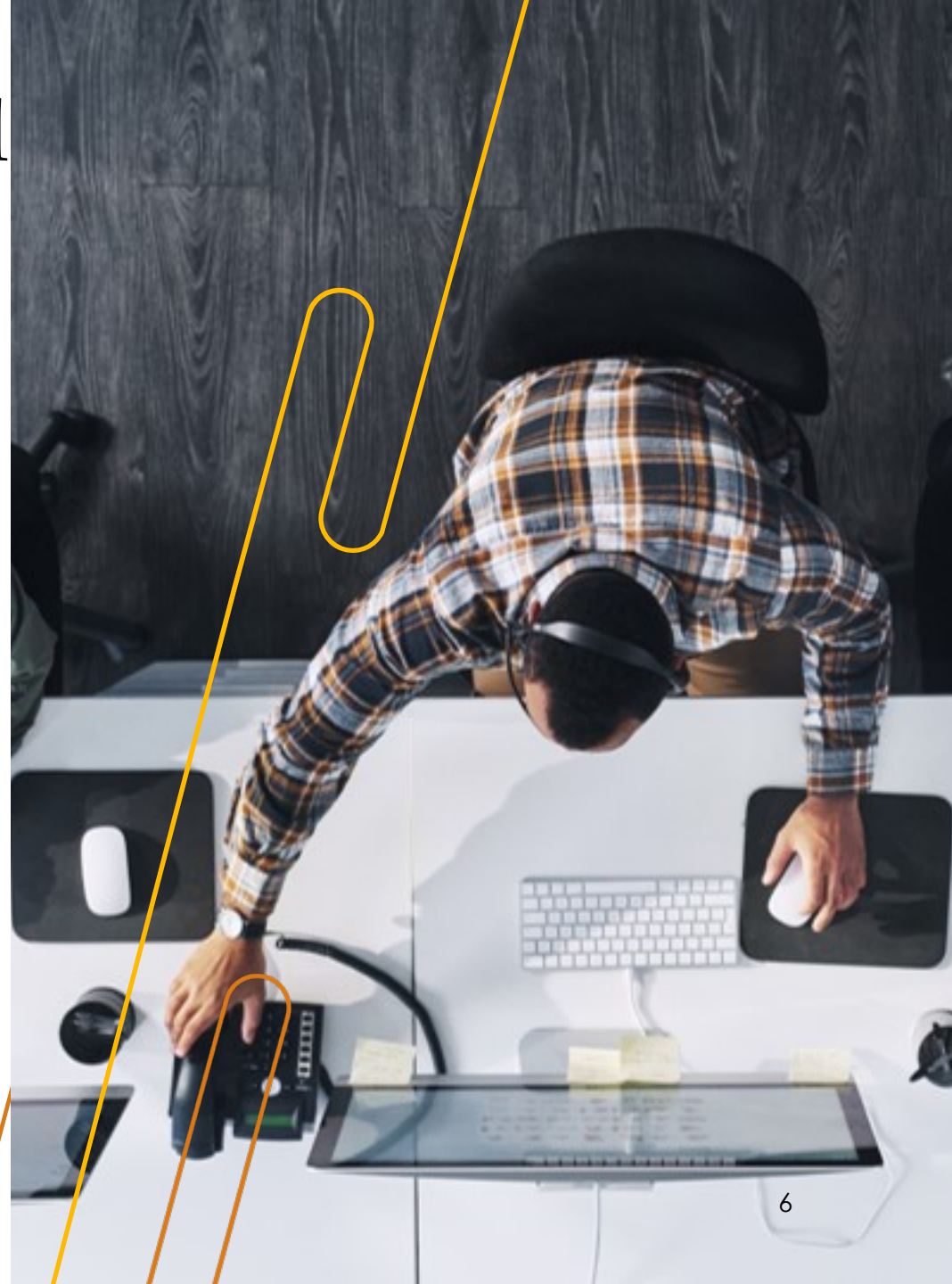
One: Privacy as Foundational Principle

- Establish privacy as foundational to government work
  - Cybersecurity, healthcare and financial examples
  - Government entities have higher expectations of maintaining privacy than corporations
- Meet people where they are, but work to standardize definitions
  - Ideas about what privacy and surveillance technology are can be very personal
  - Need to reference the jurisdictional or another standardized definition
- To have foundation, there should be dedicated privacy staff and a centralized website where materials, such as policies and reports, can be posted for public and departments



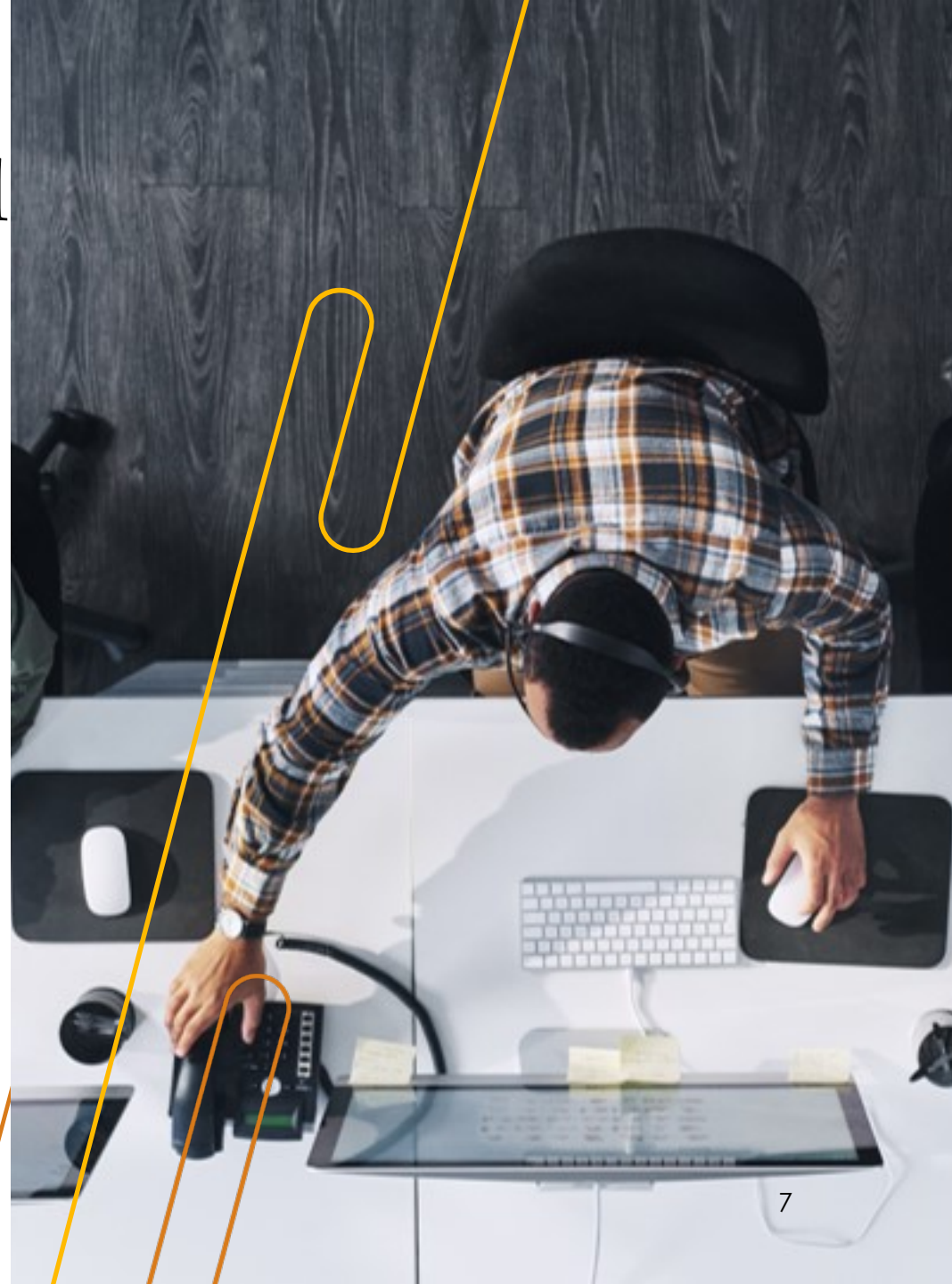
One: Privacy as Foundational Principle (cont.)

- Privacy as a Benefit to Government Work & Departments
  - Some think of privacy solely in terms of compliance
  - Privacy knowledge and frameworks benefit local government departments
    - Proactive problem solving
      - Keeping data safe and anticipating issues
      - Considering every aspect of data lifecycle – collecting, using, storing, sharing and disposing of data
    - Keeping products and services safe for all people
    - Preventing lawsuits
    - Getting ahead of state and federal regulations
- Ultimately – Privacy considered first, not as an afterthought in city technology work
- Privacy experts and professionals can serve as nexus for data, IT, cybersecurity, policy and legal teams to protect user data



One: Privacy as Foundational Principle - Operationalize

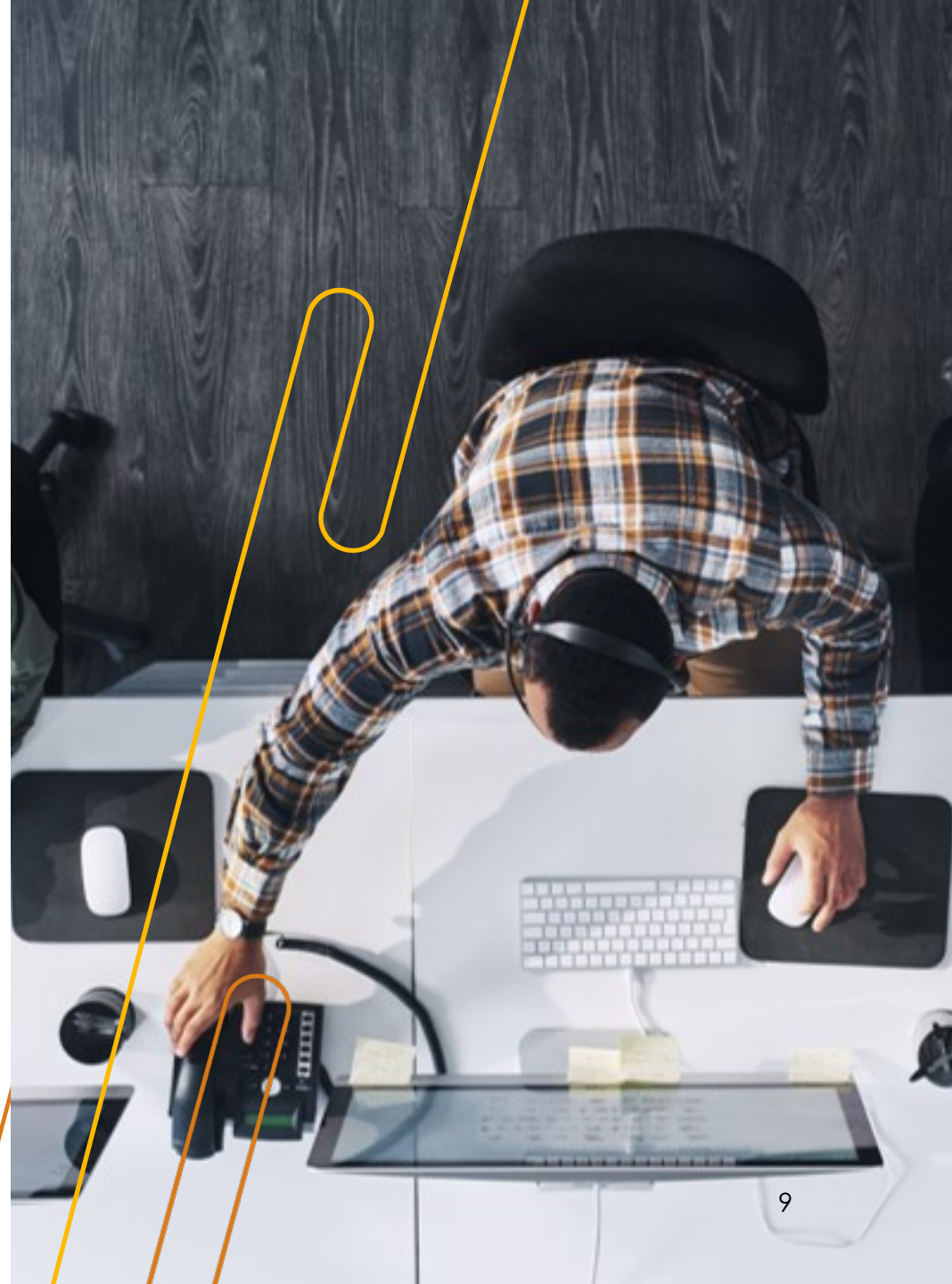
- Every city department should have at least one designated Lead Privacy Policy contact
- This person will be the department's "in-house" contact and will develop familiarity with policy creation, reporting and other privacy processes or requirements
- The contact can communicate with their department, find subject matter experts within dept if necessary
  - Serves as liaison
  - Decreases need to retrain or explain to all department staff oneself
  - Can help privacy staff to flag issues that someone with an insider perspective on the dept would understand
    - For example – extensive internal approvals due to departmental board



2. Defining Surveillance Technology

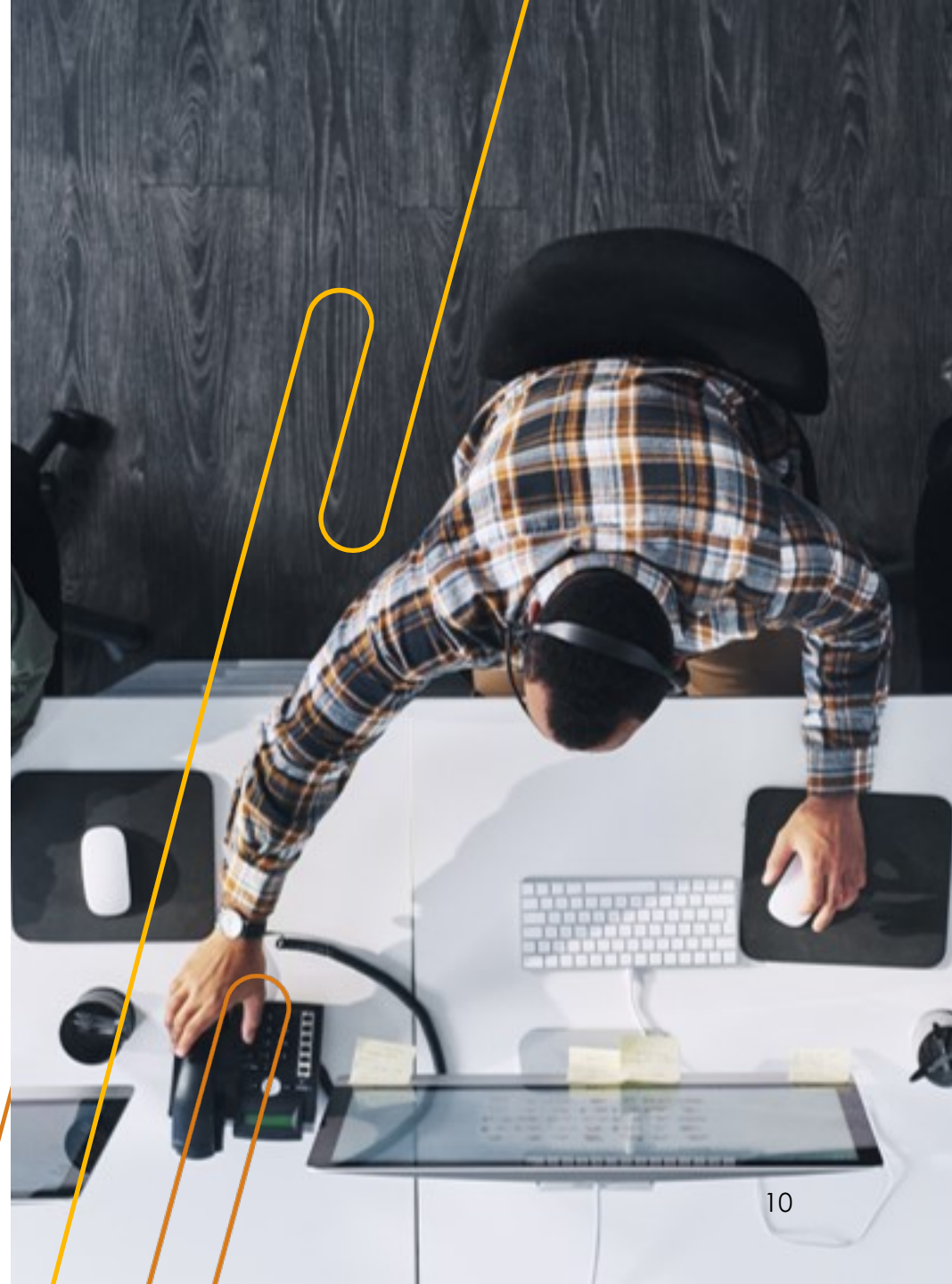
Two: Defining Surveillance Technology

- Surveillance Technology has a legal definition in the context of the TRUST Ordinance (as well as in any other local ordinance)
- However – people have their own personal definitions of surveillance technology
- Communicate that surveillance technology (a) meets the legal definition, (b) does not fall into one of the exemption categories, and (c) has the potential to be used for surveillance
  - Many people think of surveillance as a negative term and may assume that if there is no malicious intent for technology use, there is no surveillance – what is vital is that the possibility is addressed and that the technology and any data collected is managed safely, responsibly, and transparently



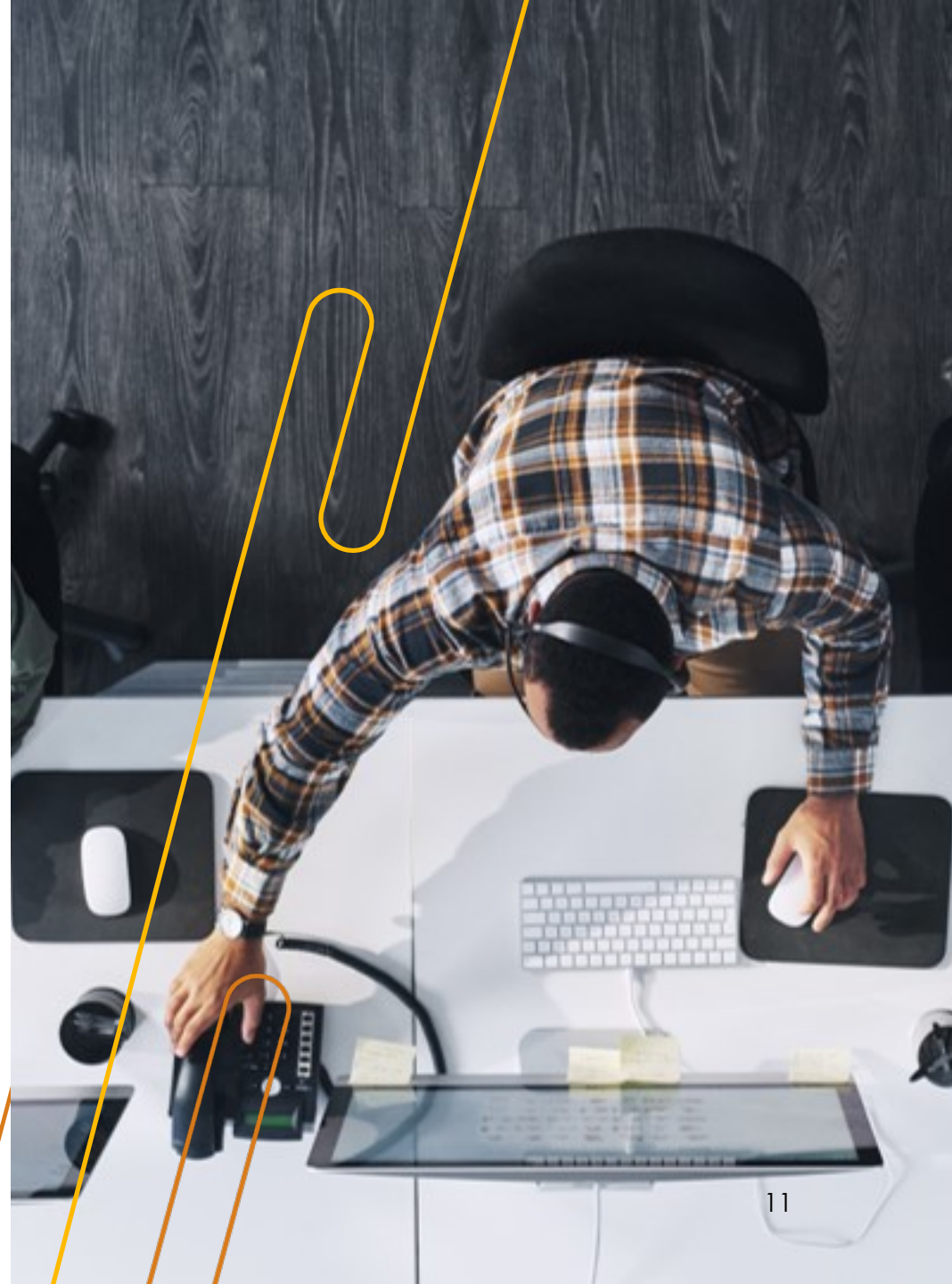
Two: Defining Surveillance Technology (cont.)

- One way to understand definition of privacy and put it into context is to consider it as a matter of scale
- Privacy centers around the data security of the individual, while cybersecurity focuses on the security of networks
  - Privacy and cybersecurity – like cousins
  - Both important, but approaching the same issue – information security – from different perspectives and scales
- Different departments come with differing needs, as well as differing levels of experience, with surveillance technologies
  - However → all need to keep personal data and systems secure to the best of their ability
  - This means anticipating what can go wrong before it does and being proactive about vulnerabilities



Two: Important Surveillance Technology Terms

- **Personally Identifiable Information ("PII"):** Any data that can personally identify an individual (includes, but not limited to, name, address, phone number, license plate number, Social Security number, credit card information, and biometric information.
  - Some PII is more sensitive than others but all data must be mindfully managed
- **Protected Health Information ("PHI"):** Health data that can be linked to an individual (includes, but is not limited to, name, birth date, insurance card numbers, medical records and imaging, medical device IDs and serial numbers)



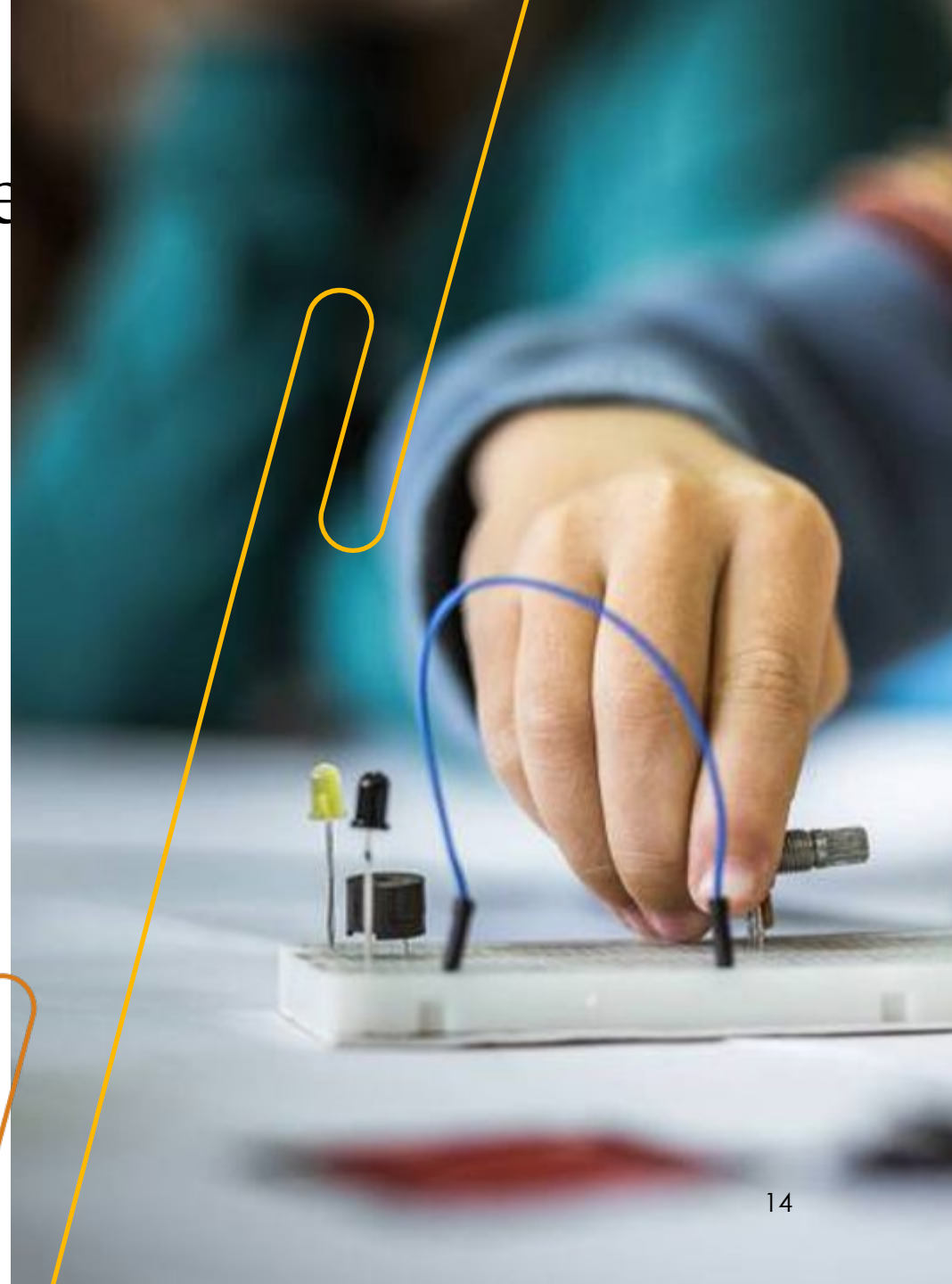
3. Procurement Checks

Three: Procurement Checks

- Even if aware of a surveillance technology definition, department staff are not always able to make their own determinations
- For the most complete inventory, it is helpful to have a procurement check for technology purchase
- This should be conducted by either a privacy professional or a procurement staff member who is familiar with the jurisdiction's legal definition of surveillance technology

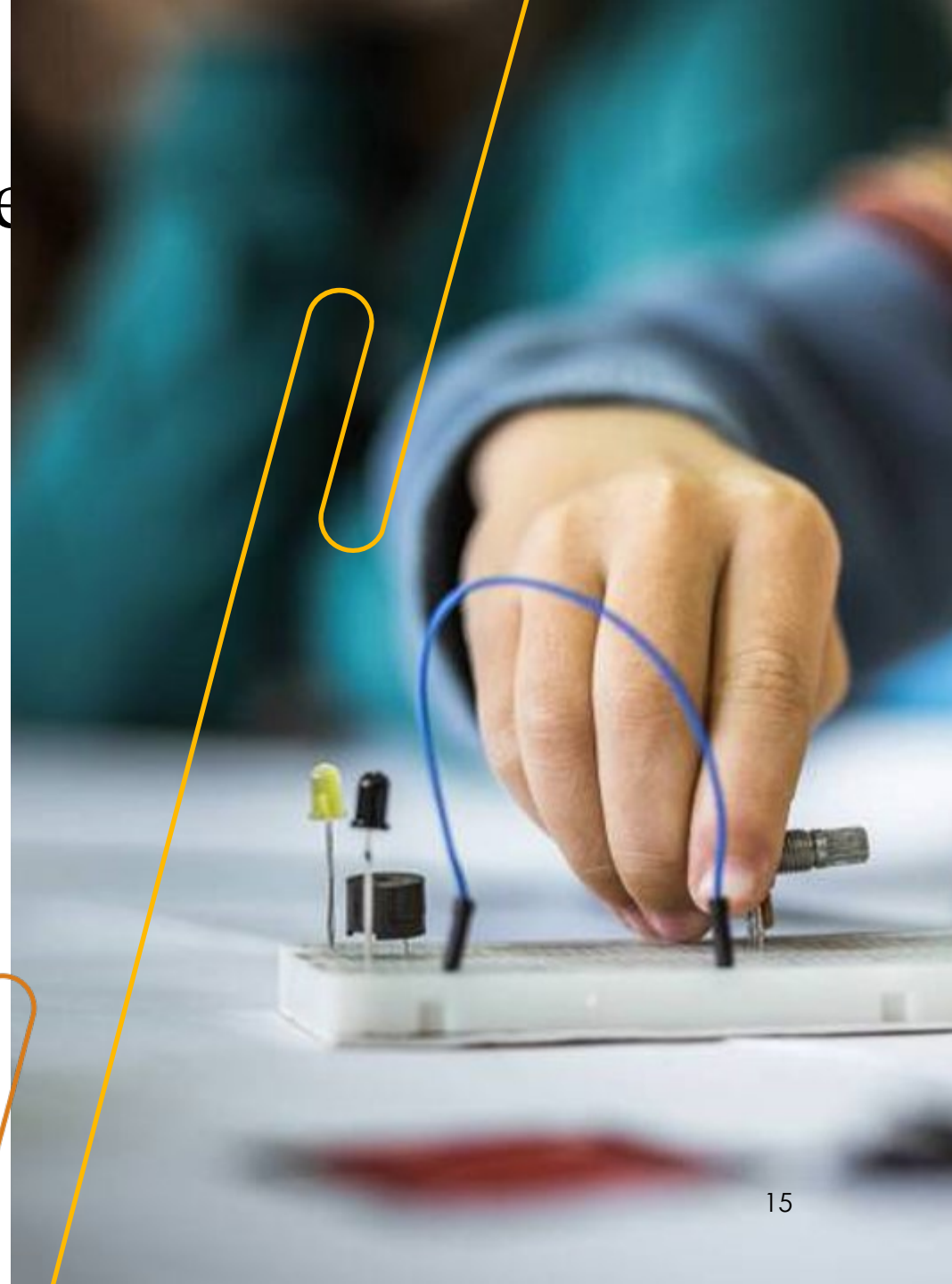
Three: Procurement Recomme

- Surveillance Technology Check should be made a part of the workflow of any other procurement checks (like a cybersecurity check, for example)
- Staff submitting a procurement can fill out a form to give staff evaluating a procurement (either procurement department staff or privacy professional staff) the information they need to make a determination
- Department staff should be given guidance as to what does or does not make something a surveillance technology, so that they can best make these determinations proactively and/or help staff making the determination to provide them with relevant information



Three: Procurement Check – Ne

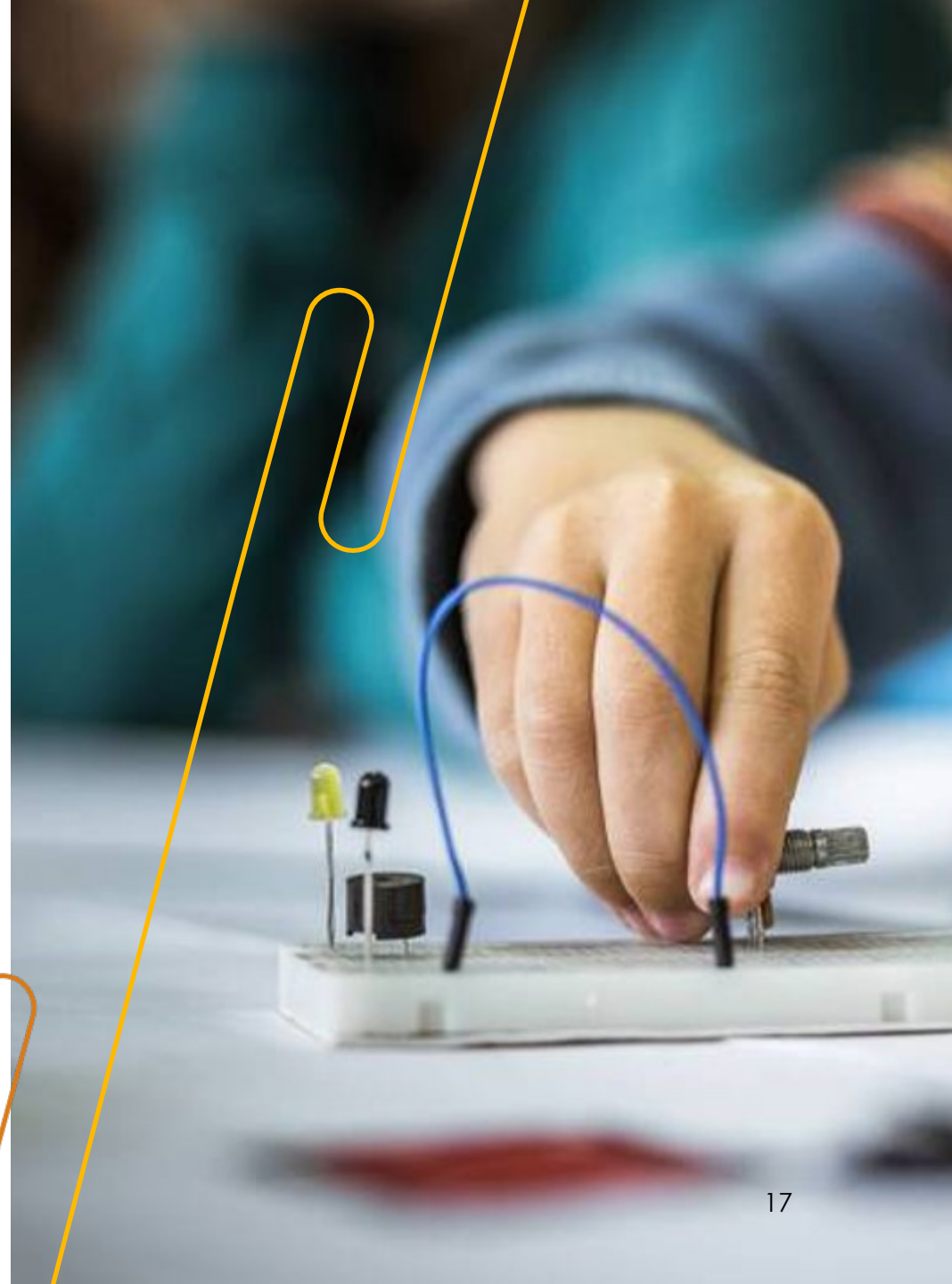
- **Least Effort**
  - Guidance Document for Department Staff
  - Guidance Document and/or Rubric for Staff making Determination and training on surveillance technology definition and all exemptions
- **Middling Effort**
  - Integrating a surveillance technology check into existing processes
  - Comprehensive training for all relevant procurement staff and departmental staff (online or in-person training)
- **Most Effort (more time or staff intensive)**
  - Build form and /or platform to make communication between department staff and procurement check staff easier
  - Create backend database to have inventory of decisions



4. Annual Reports

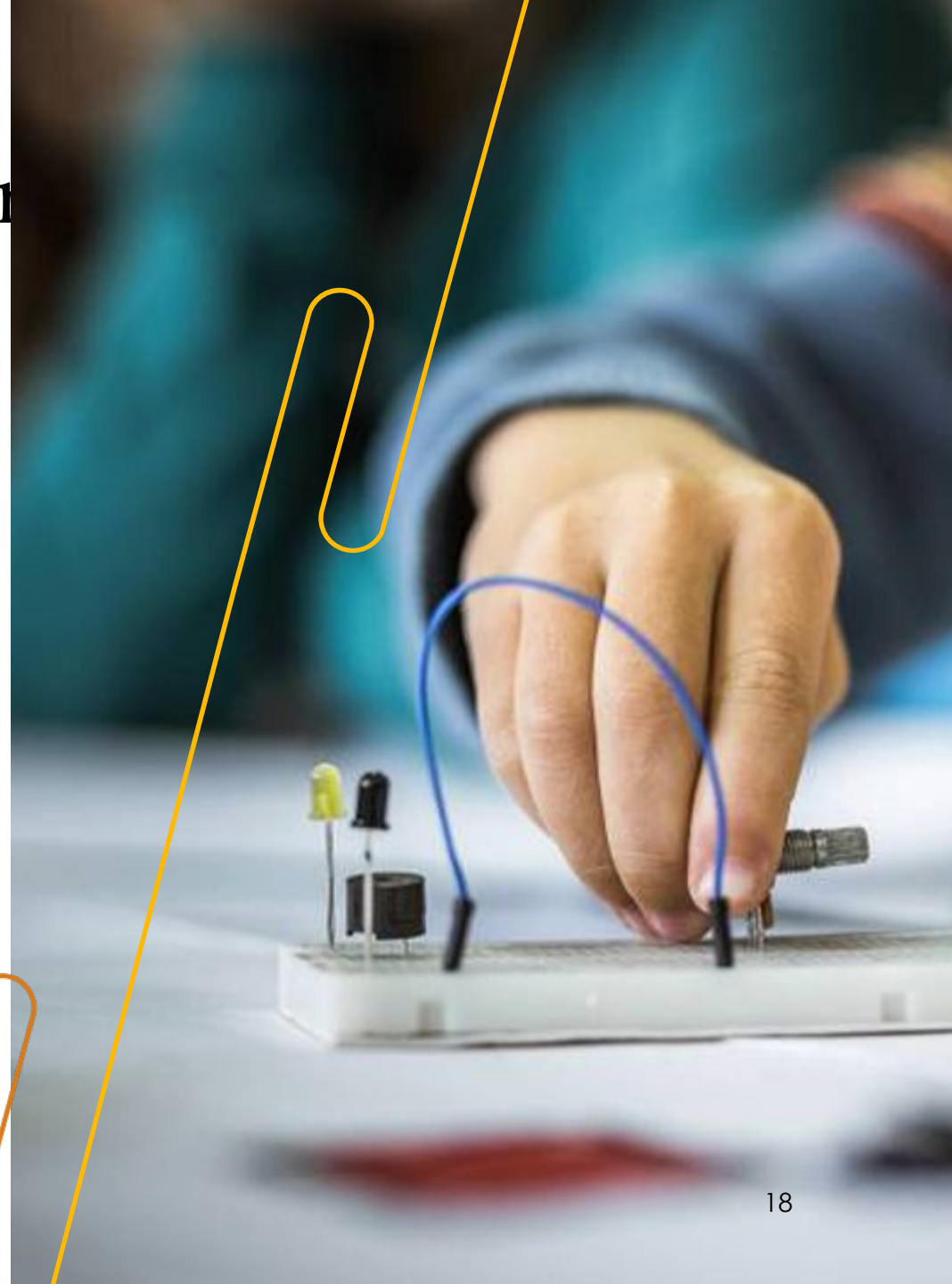
Four: Annual Reports

- Process should be standardized and consistent
- Departments should be provided with a template and/ or form to complete the report
- Departments should be given enough advanced notice to complete the reports
- Privacy staff should then review reports for completeness, thoroughness, and consistency
- Reports should be publicly posted in a centralized place



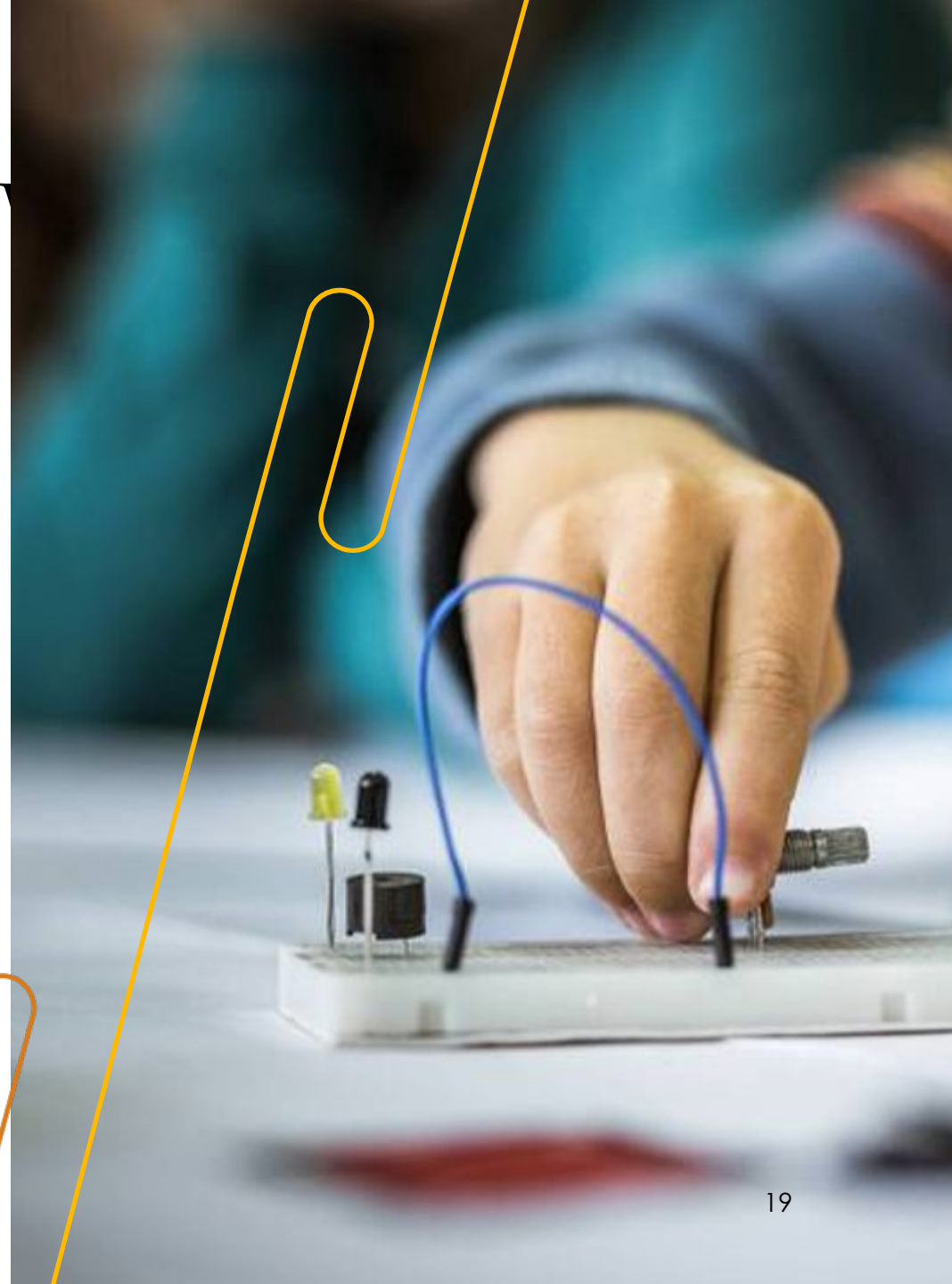
Four: Annual Reports – Repor

- Report intended to be a transparency measure for the public and the jurisdiction's elected officials
- Also: an opportunity for the reporting department to give an accurate account of technology performance over the reporting period
  - Report can be opportunity to demonstrate success of a program and how a certain technology meets goals and serves the community
- Department should assign a lead to complete the report – ideally the department's lead privacy contact or the subject matter expert for the technology
- The Report Lead will gather information from those who need to contribute to the report from the department
- After a review of the report by department leadership, the report should be submitted to the reviewer for input



Four: Annual Reports - Revie

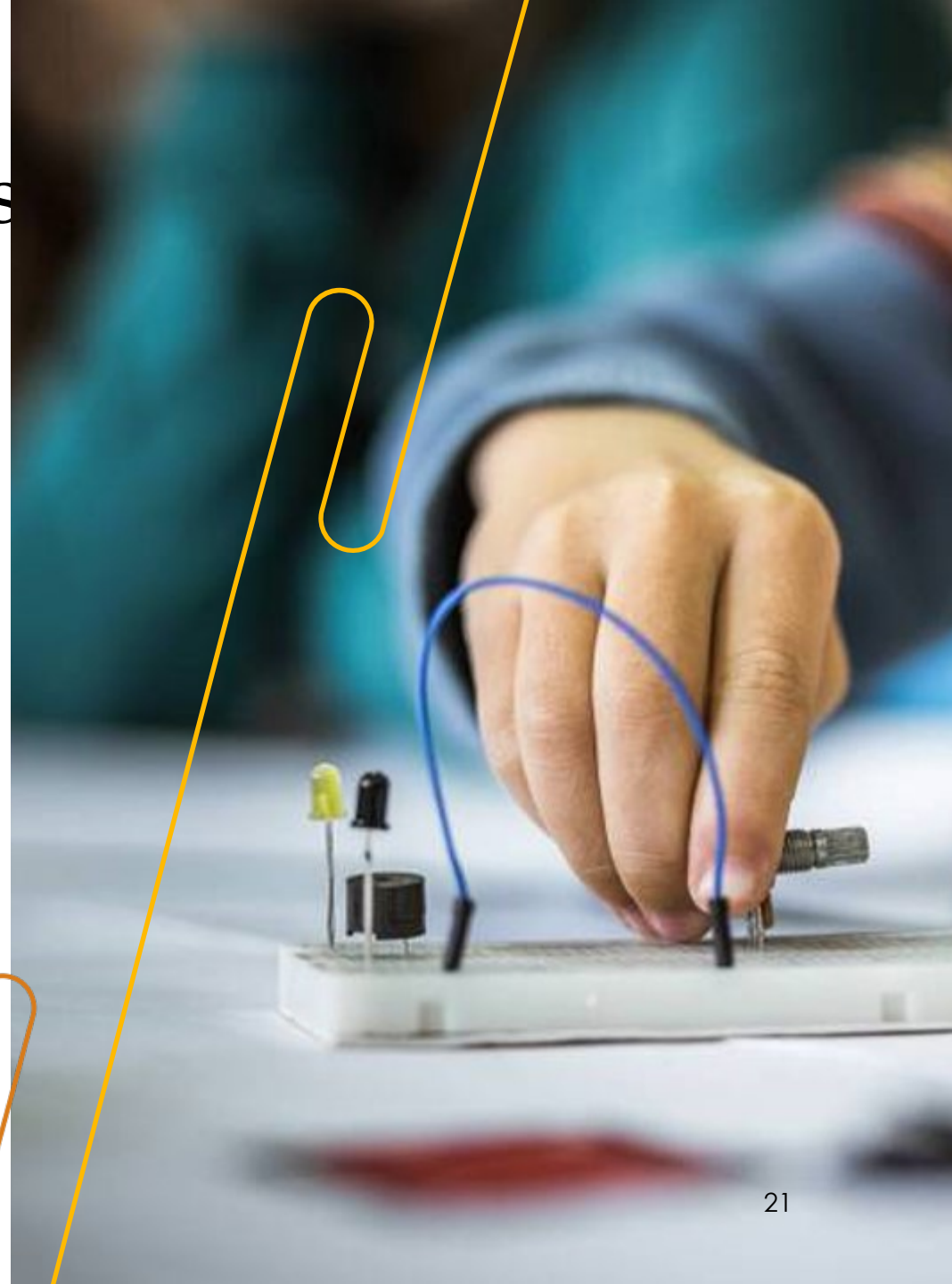
- The people who review the report should provide a guidance document to departments needing to complete the report
- The report should be reviewed by privacy experts for completeness, thoroughness, and consistency
  - Notes on the report should be given back to the reporting department and they can create more complete answers
  - Descriptions of desired answer length and general parameters about content to be included is helpful
- Ideally: someone in a centralized privacy role should keep a tracking document to ensure reports are submitted on time and communicate with departments about deadlines



5. Best Practices and Lessons Learned: Recommendations for Privacy Programs

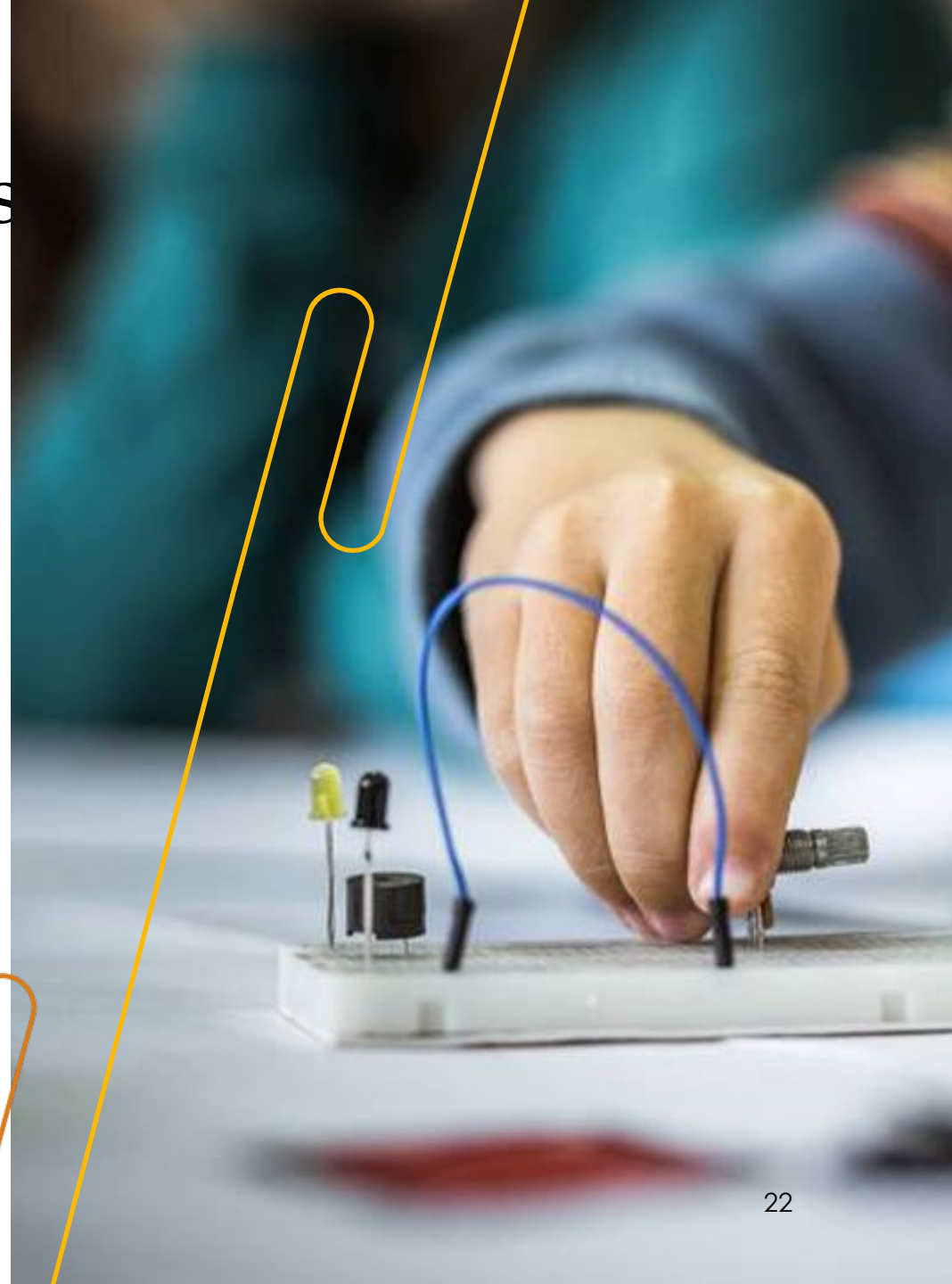
Five: Best Practices & Lessons

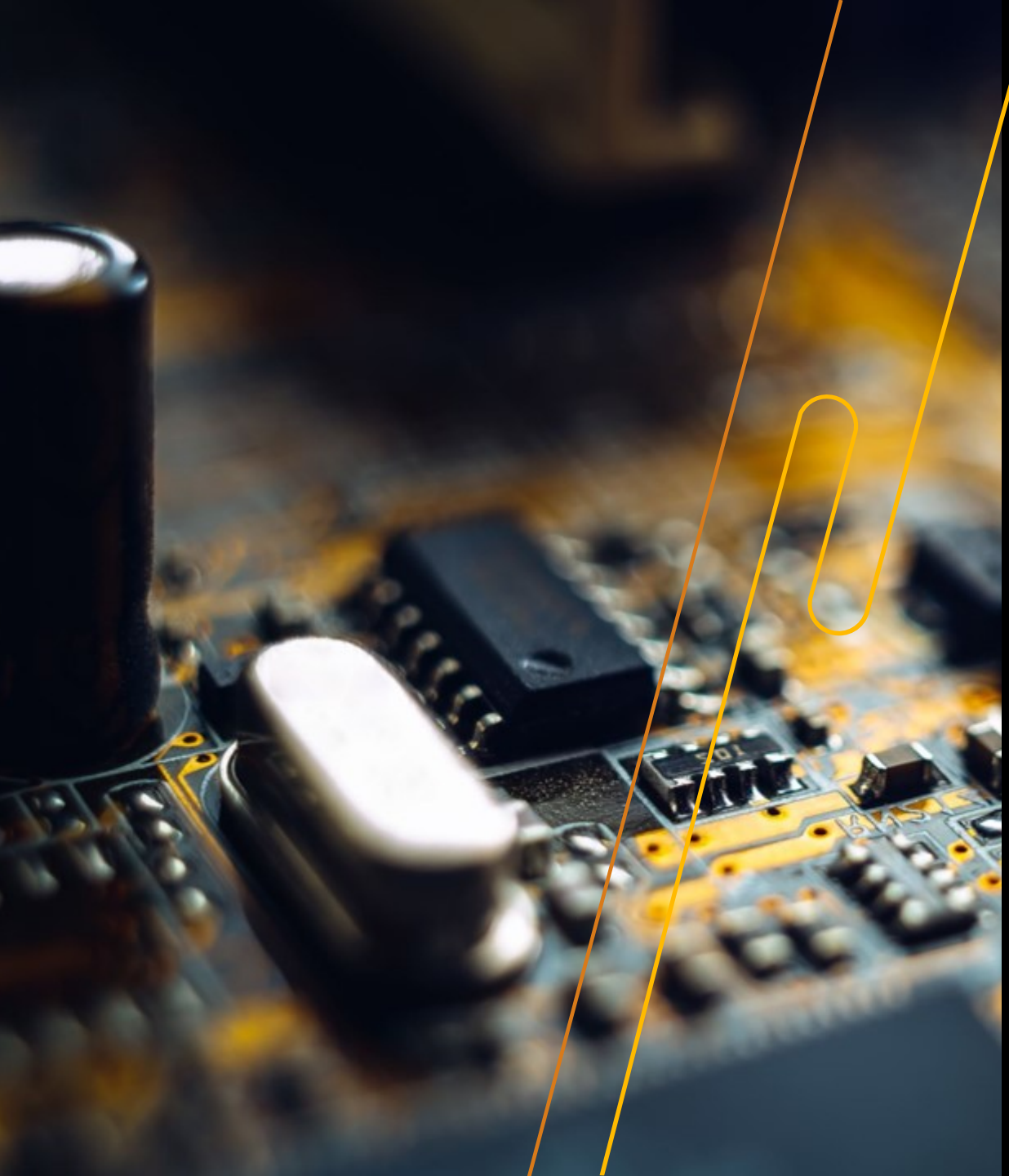
- Privacy programs should go beyond legal compliance
  - Legal compliance is an important part of privacy work in government
  - However: proactively and optionally building privacy practices into processes, programs and technologies benefits departments
    - Builds public trust with local government
    - Departments can be proactive and not need to do as much work when state and federal privacy laws are passed
    - Privacy by design and privacy-enhancing technologies protect personal data and creates more secure systems at every scale
- Privacy programs operate best with dedicated staff
- Consistency and communication with departments is key to program success



Five: Best Practices & Lessons

- Data privacy law may be new to many jurisdictions, but its applications and importance increase every year because of the prominence of new technologies and the nuanced issues they bring to the public sphere
  - Emerging technologies can have public benefits, but risks must be managed to ensure a net benefit to the public
- The bar for data security and privacy in government is high and privacy programs help many government departments
  - Privacy programs help with:
    - Legal Compliance
    - Cybersecuity and Information Technology
    - Data
    - Other Policy Teams





Summary

One

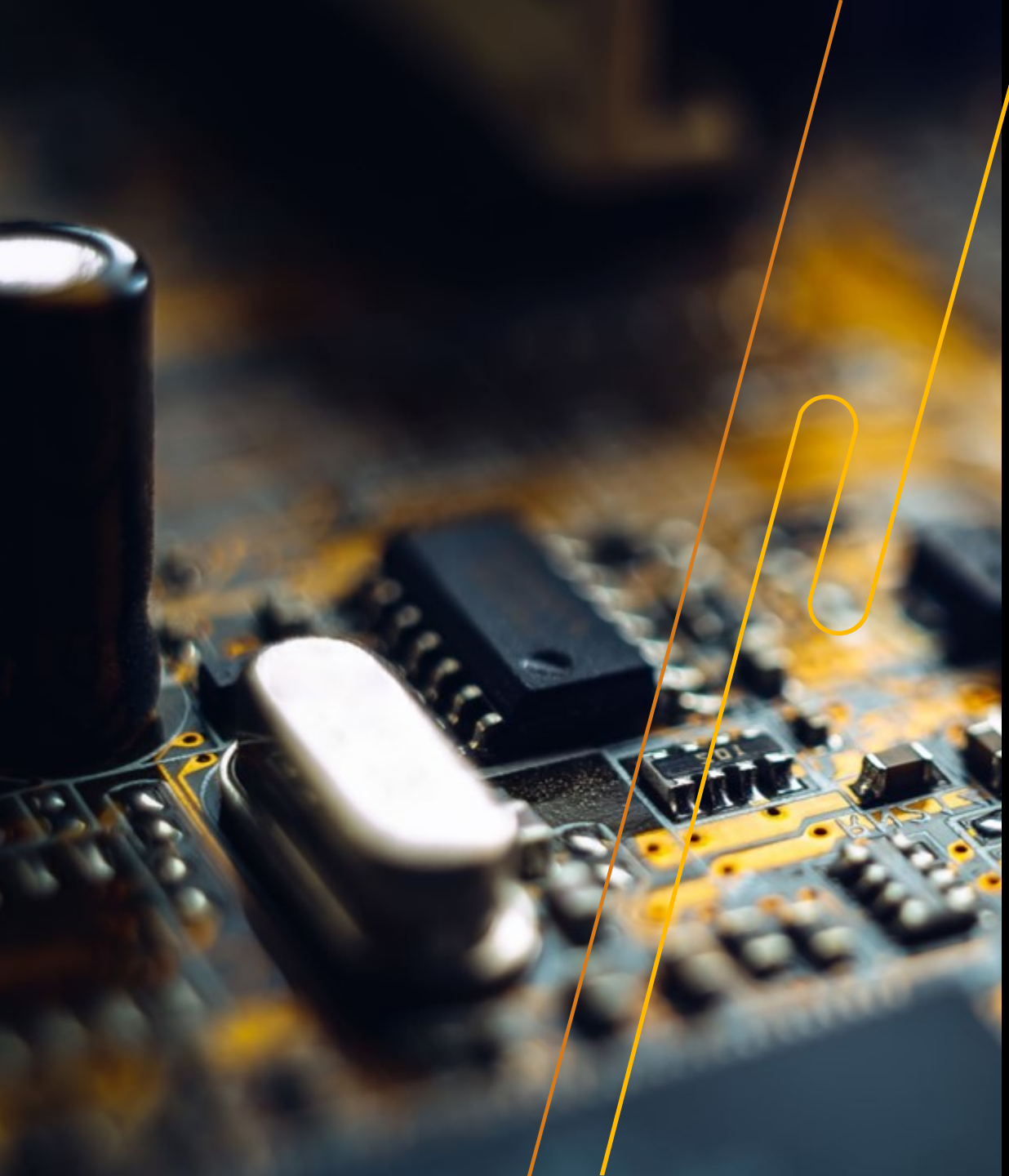
Privacy as a foundation for government work creates many positive outcomes, but standardized understanding needs to be reached

Two

Communicating the jurisdiction's legal definition is important to understanding and buy in from departments

Three

Procurement checks for surveillance technology should ideally be integrated into the procurement process – at the least, depts and procurement staff should have guidance documents to make determination.



Summary, cont.

Four

Annual reports should have clear guidance and there should be dialogue about responses between reporter and reviewer.

Five

Privacy programs serve a larger purpose within the structure of local government – to protect, to look ahead, and to collaborate and support other technology and compliance groups

Thank you!
Questions?