LSC Technology Baselines Updates

Technologies that Should Be in a Legal Aid Office Today

Introductions

Jane Ribadeneyra,
LSC Program Analyst

Tony Lu,
Senior Consultant,
Just-Tech

Agenda

- About the LSC Technology Baselines
- Overview of Technologies That Should be in Place
- How to Use the Baselines
- Q&A

Audience Poll

About the LSC Technology Baselines

LSC's Strategic Directions 2006-2010 to "develop a strategic vision for technology"

Technologies That Should Be in Place in a Legal Aid Office Today issued in November 2008 and updated in 2015

Written as guidance for legal aid offices that provide a full range of legal services

How the Technology Baselines are Used

The Technology Baselines do not outline specific LSC grantee technology requirements but are instead intended to provide helpful guidance to grantees and other legal aid offices on the use of technology to provide high-quality legal services to clients.

Legal Aid organizations can use the Baselines to help assess their technology and guide technology planning and budgeting.

How to find and comment on the Baselines

Go to LSC's Matters for Comment website:

- https://lsc.gov/matters-comment

COMMENTS ARE DUE April 21, 2023, at 11:59 p.m. Eastern Time

Comments must be submitted as follows:

- Acrobat PDF format.
- Emailed as an attachment to a transmittal message sent to: techgrants@lsc.gov.
- Emailed with the subject line: *Comments on Technology Baselines*.

Questions about the draft revisions to the Baselines should be sent to techgrants@lsc.gov with the subject line: *Questions about Technology Baselines Comments*.

Sections of the Baselines

(Purposes Served)

1. Overall **Program Capacity**
2. Sustainabilitiy (New!)
3. Remote/Hybrid Work (New!)
4. Management **of Client and Case Data**
5. Production **and Supervision of Legal Work**
6. Records **Management**
7. Knowledge **Management**
8. Intake **and Telephonic Advice**
9. Legal **Information for Low Income Persons**
10. Support **for Use of Private Attorneys**
11. Security
12. Training
13. Communication and Collaboration
14. Administration
15. Development **and Fundraising**

Overview of Technologies that Should be in Place

The Baselines

(Technologies that Should be in Place)

- Planning
- Budgeting
- Personnel
- Remote Work Policy (New!)
- Case Management System
- Calendaring
- Document management and production
- Timekeeping
- Supervision
- Online legal research
- Electronic records
- Pleading and brief banks
- Telephone Systems
- Electronic Desk Manual
- Community Legal Education
- Addressing the Digital Divide
- Security policies
- Multi-Factor Authentication
- Cloud Computing and Policies
- Password Management
- Mobile Equipment for Staff Use
- Mobile Device Management
- Security Awareness Training
- Disaster Recovery Plan
- Incident Response Plan
- Endpoint Detection and Response
- Email Security
- Cyber Insurance

The Baselines

Continued

- Training and Technology
- Email, lists, and standard collaboration tools
- Internal communication mechanisms
- Human Resources Information System (HRIS)
- Accounting
- Grants Management
- Fundraising and marketing

Needed Capacities or Functions vs. Important Considerations and Best Practices

March 2023
For Public Comment

1 Overall Program Capacity

1.1 Baseline for Overall Program Capacity – Planning

Needed capacities or functions

- Technology planning should be ongoing and integrated into the overall planning of the program for effective service delivery.
- Technology planning should include an assessment of the program's current needs and capacities to effectively position the program to incorporate new technological advances as they evolve.
- Technology plans should be reviewed and updated as needed every year.
- Technology plans should include measures to increase staff input and engagement in improving technology use, such as forming a technology committee and regularly using staff technology surveys.

Important Considerations and Best Practices

Technology should serve the mission and vision of the legal aid program (ABA Civil Standards, Standards 2.1 and 2.2.). As part of strategic planning, the program should consider how technology can be used to respond to the most significant issues faced by the communities it serves.

As part of technology planning, programs should consider periodically (e.g., every 3-5 years) engaging an independent technology consultant, with expertise with nonprofit and/or legal services organizations, to audit their technology systems and recommend improvements that promote efficiency, effectiveness, and optimize performance. An independent consultant can help an organization understand the value and importance of technology upgrades and the return on investment through greater efficiency and performance.

Overall Program Capacity:

Programs should prioritize staff feedback on technology through the creation of a technology committee and conducting regular staff technology surveys.

Budgeting for technology must reflect the importance of implementing robust security practices and systems in the face of increased cybersecurity threats to legal aid organizations.

Programs should shift from on-premise data storage and servers to more reliable and accessible cloud-based solutions.

Sustainability:

- Budgeting for technology projects should reflect ongoing maintenance costs.

Remote/Hybrid Work – Policies and Procedures:

- Programs must evaluate the lessons learned from the COVID-19 pandemic and develop a policy to account for remote work and hybrid (e.g., remote/on-site) service delivery models.

Intake and Telephone Advice - Telephone Systems:

- Programs should adopt hosted telephone systems as their telephone solutions, to permit advanced functionality, provide more security, reduce administrative overhead, and make remote work possible.

Document Management:

Programs may need to evaluate the need for a document management system ("DMS"):

- Better document organization and improved search
- Reduce duplication of files
- Improved compliance with retention policies
- Automated processes

New Security Baselines

- Security Policies & Procedures
- Multi-Factor Authentication (“MFA”)
- Cloud Computing and Policies
- Password Management
- Mobile Equipment for Staff Use & Mobile Device Management

New Security Baselines (cont'd)

- Security Awareness Training
- Disaster Recovery Plan & Incident Response Plan
- Endpoint Detection and Response ("EDR")
- Email Security
- Cyber Insurance

Ransomware: Think You're not a Target?

- 2021 Study showed an almost ten-fold increase in ransomware attacks in the legal services sector from Q1 to 2020 to Q1 2021
- Attacks have been reported on: Small-Medium Law Firms, Legal Aid Organizations, Court Systems
- **Why?**
  - Easy targets
  - Higher chance of payouts
  - Valuable data

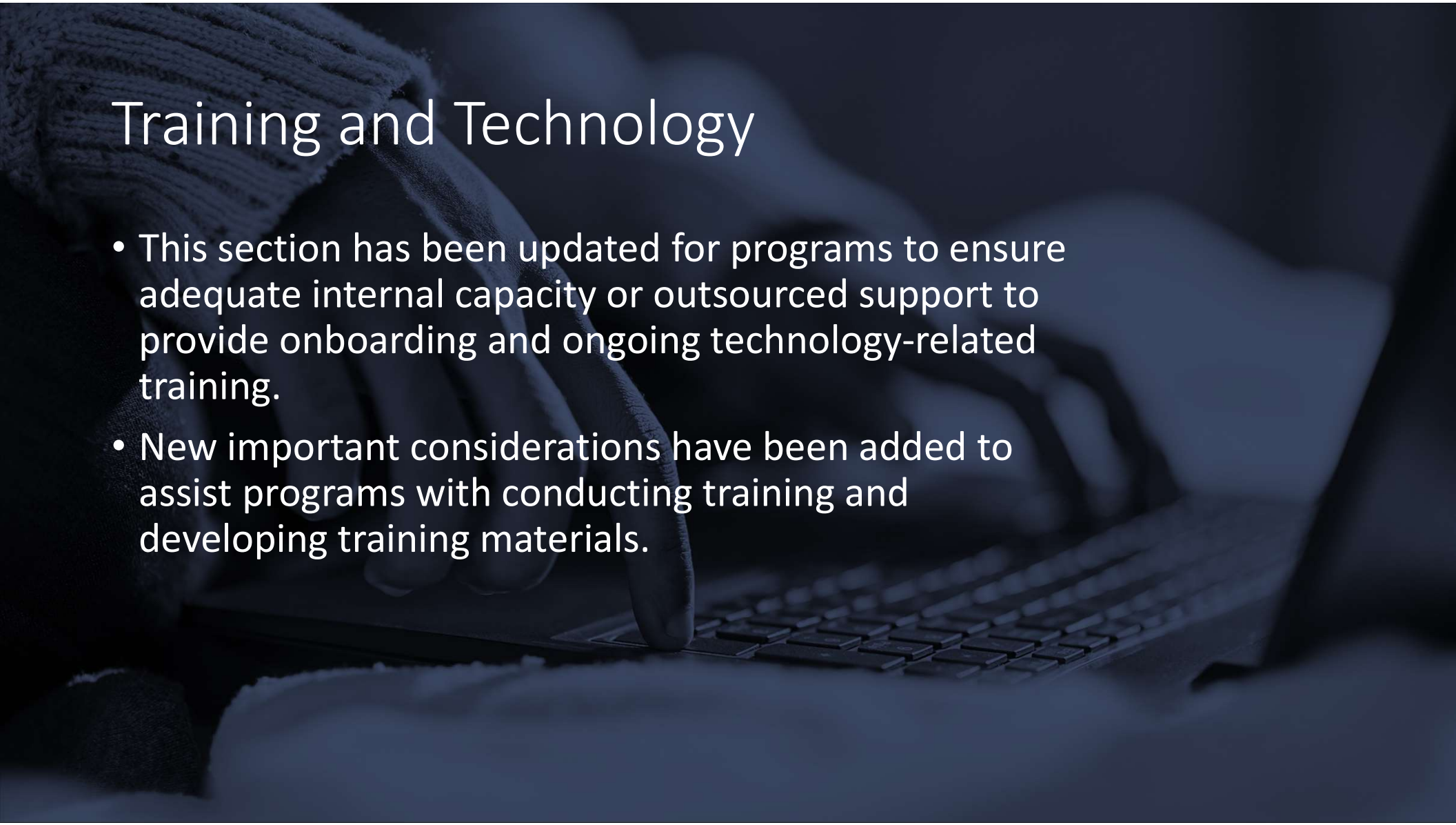
Communication and Collaboration

- Streamline communication tools
- Provide clear guidance

- Programs should develop and use collaborative work environment tools (e.g., Microsoft Teams and Word Online) and should encourage real-time collaboration among staff.

Support for Use of Private Attorneys

- Added considerations for volunteer-facing technology:
  - Combine the case opportunity, training and resource materials, and calendars on one website.
  - Designate who is responsible for which section and how often the pages/resources/materials will be reviewed and updated.
  - Perform user-testing with volunteers who are the target end-users.



Training and Technology

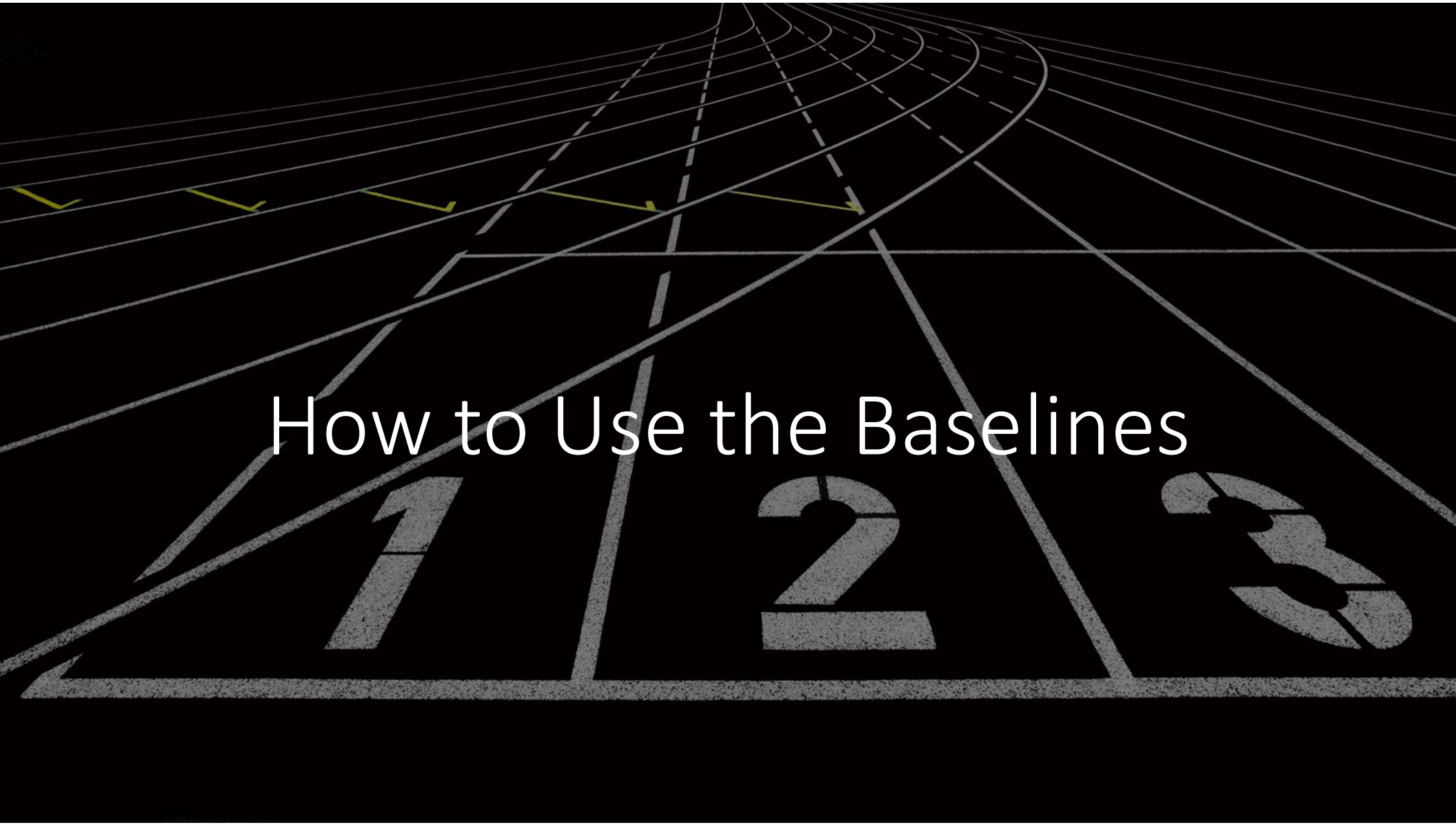
- This section has been updated for programs to ensure adequate internal capacity or outsourced support to provide onboarding and ongoing technology-related training.
- New important considerations have been added to assist programs with conducting training and developing training materials.

Administration:

- This section has been revised to include:
  - Ticketing systems and communication strategies on after-hours support
  - Essential HRIS software and functionalities
- This section was updated to be aligned with the LSC Accounting Guide

Development/Fundraising:

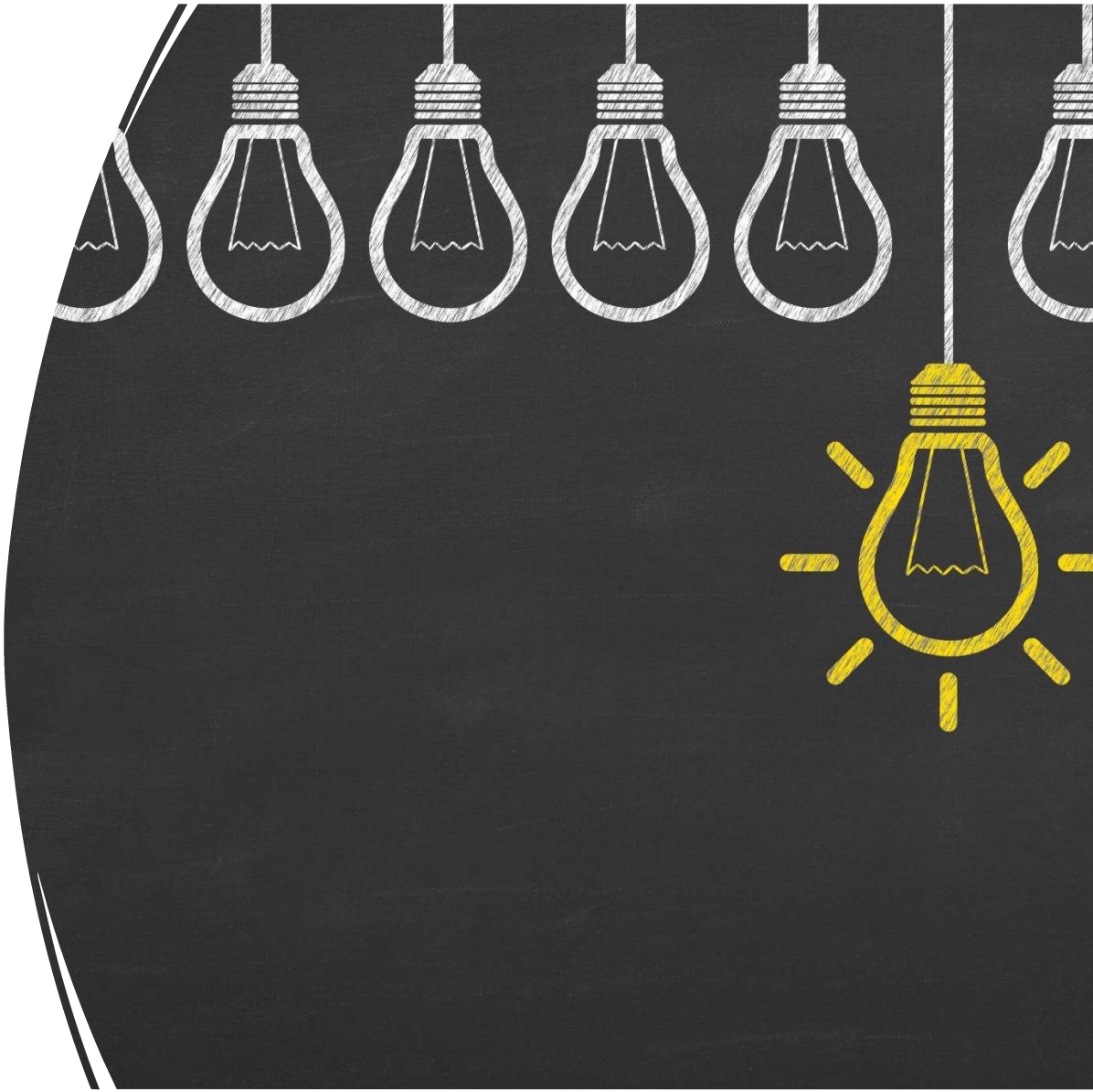
- The Fundraising and Marketing section has new important considerations around Customer Relationship Management (“CRM”) systems and revised needed capacities and functions for fundraising and marketing management.



How to Use the Baselines

Steps for Strategic Technology Planning

- **Assessment** – Inventory assets and capacities, identify pain points
- **Set up Your Tiers** – Allow for progress on multiple fronts
  - **Tier 1: Easy and Cheap** (IT Staff)
  - **Tier 2: Short/Medium Term** (Middle Management)
  - **Tier 3: "Big Goals"** (Executive Team/Board**)**



How to Assess Your Technology

Internal Assessment

- Technology committee
- Staff technology surveys

External Assessment

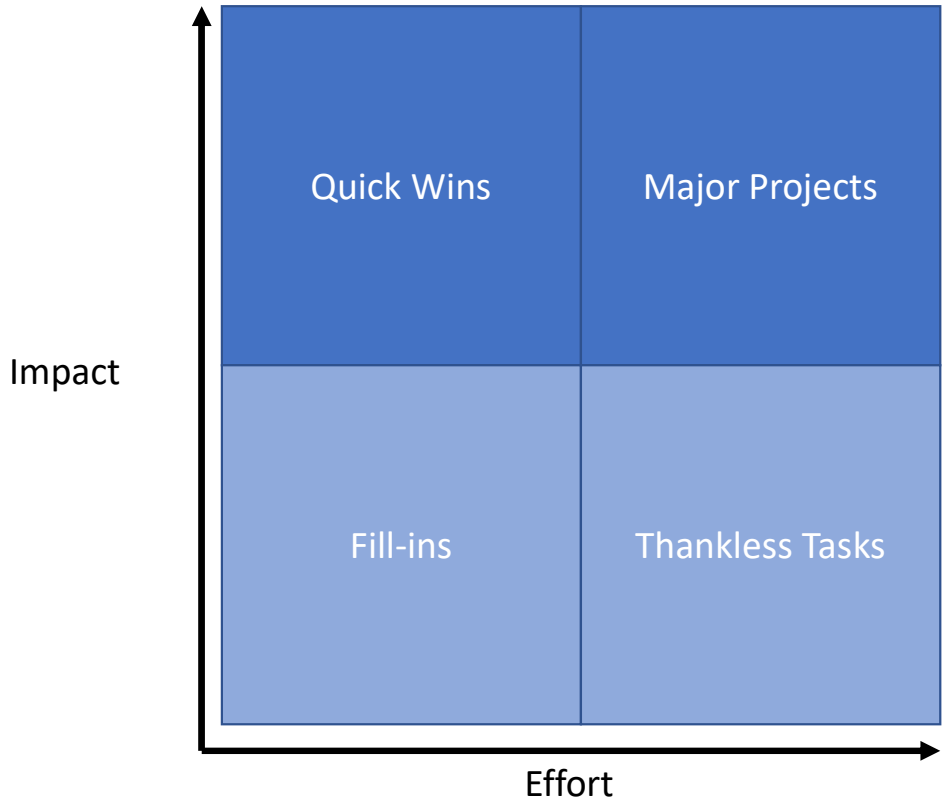
- Third party evaluator

Technology Improvement Plan Considerations

MANAGING CHANGE – DON'T TRY TO DO TOO MUCH TOO FAST.

ADOPT A CULTURE OF CONTINUAL IMPROVEMENTS, WITH ONGOING ASSESSMENTS

Establishing Priorities



Use Baselines to Establish a Framework and Practices

- Can use the baselines to devise your own technology/security assessment framework
- Consider industry standard frameworks (i.e. “NIST”) (but be warned – they can be complex!)
- Consider adapting the Health Industry Cybersecurity Practices (HICP)
  - Scaled for small, medium, and large practices
  - Well-organized, easy-to read, not too “techy”
  - Created specifically for a sector focused on privacy and information security

HICP Small Practice Example: Email

Cybersecurity Practice #1: E-mail Protection Systems

Most small practices leverage outsourced third-party e-mail providers, rather than establishing a dedicated internal e-mail infrastructure. The e-mail protection practices in this section are presented in three parts:

- *E-mail system configuration*: the components and capabilities that should be included within your e-mail system
- *Education:* how to increase staff understanding and awareness of ways to protect your organization against e-mail–based cyberattacks such as phishing and ransomware
- *Phishing simulations:* ways to provide staff with training on and awareness of phishing e-mails

Sub-Practices for Small Organizations

1.S.A	***E-mail System Configuration***	***NIST FRAMEWORK REF:*** PR.DS-2, PR.IP-1, PR.AC-7

Consider the following controls to enhance the security posture of your e-mail system. Check with your e-mail service provider to ensure that these controls are in place and enabled.

- Avoid “free” or “consumer” e-mail systems for your business; such systems are not approved to store, process, or transmit PHI. We recommend contracting with a service provider that caters to the health care or public health sector.

Red Alert! (Way Below Baselines)

- **All baselines aren't created equal.** Apply priority and severity analysis

- Some concepts are considered so fundamental and obvious that they may be left out of baselines

Examples of possible Red Alert baselines:

➔ Stable and reasonably fast internet connections
➔ Functional workstations with some thought to ergonomics
➔ Antimalware tools centrally managed
➔ Personal device policies
➔ Network firewalls
➔ Protected wireless
➔ Passwords – format and management
➔ Backups
➔ Locked doors
➔ Some attempt at standardizing documents/re-using templates

How to find and comment on the Baselines

Go to LSC's Matters for Comment website:

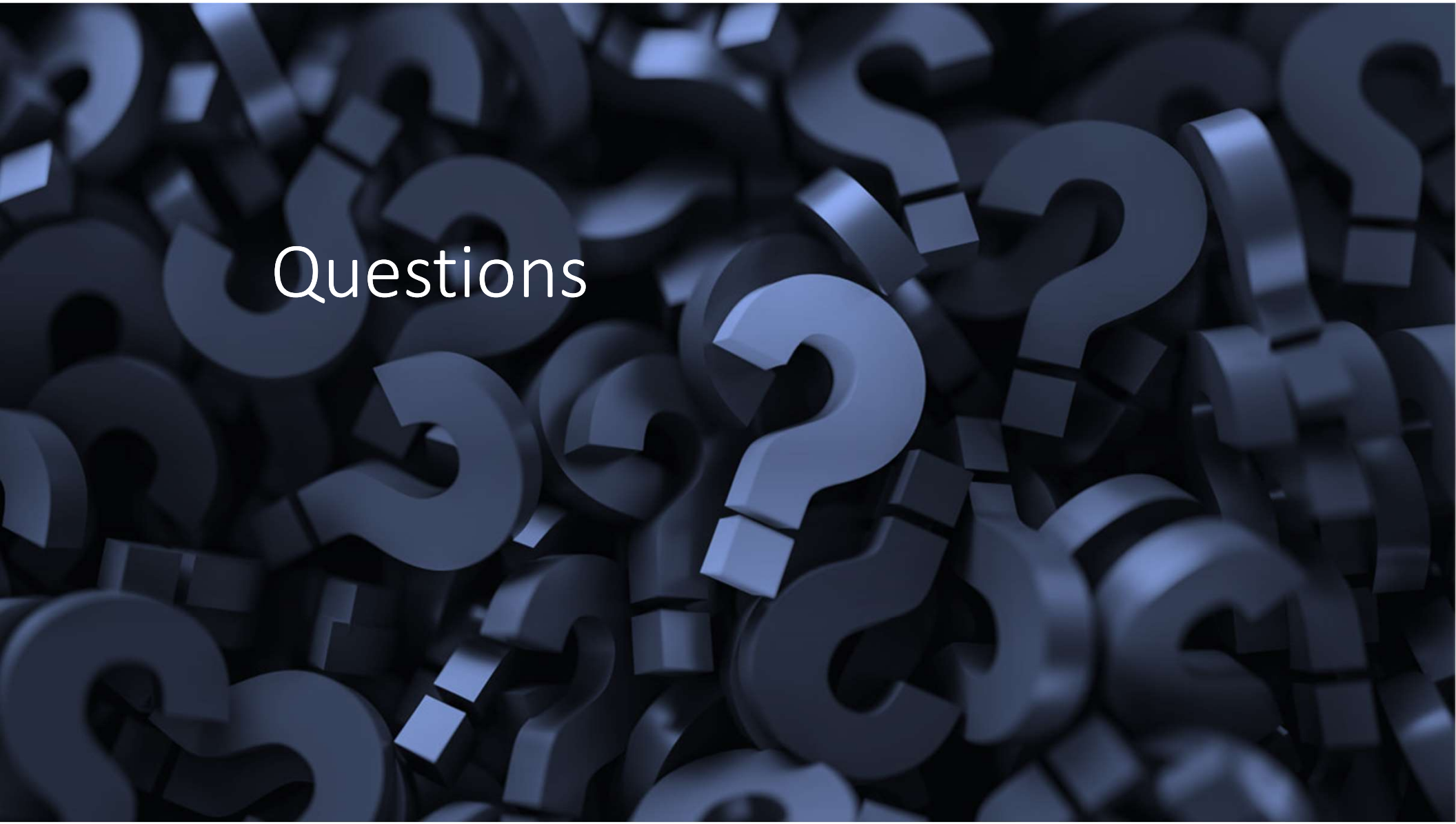
- https://lsc.gov/matters-comment

COMMENTS ARE DUE April 21, 2023, at 11:59 p.m. Eastern Time

Comments must be submitted as follows:

- Acrobat PDF format.
- Emailed as an attachment to a transmittal message sent to: techgrants@lsc.gov.
- Emailed with the subject line: *Comments on Technology Baselines*.

Questions about the draft revisions to the Baselines should be sent to techgrants@lsc.gov with the subject line: *Questions about Technology Baselines Comments*.


Questions