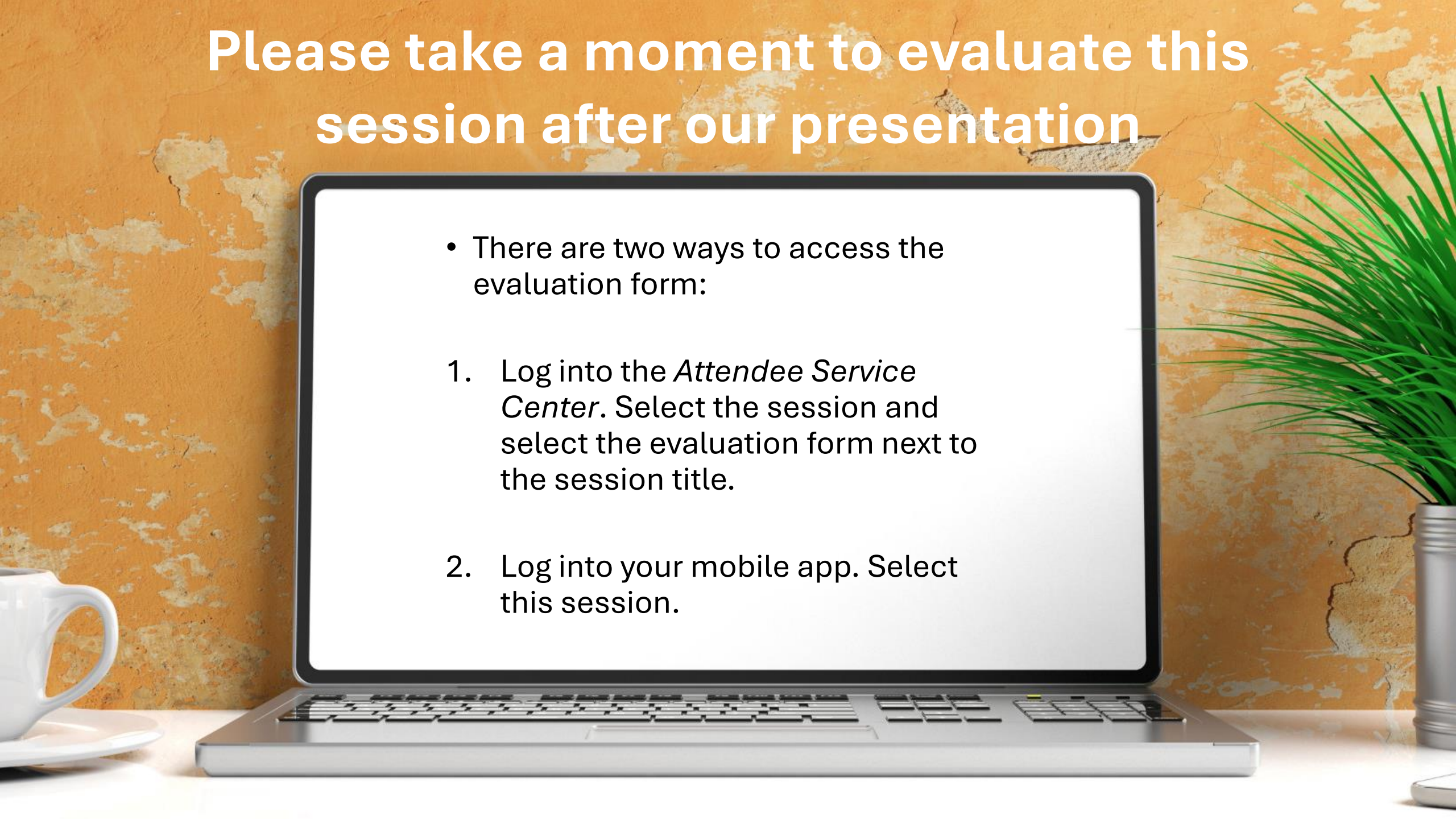
Please take a moment to evaluate this session after our presentation



- There are two ways to access the evaluation form:

1. Log into the *Attendee Service Center*. Select the session and select the evaluation form next to the session title.

2. Log into your mobile app. Select this session.

Cybersecurity Comes to a School Near You - Again

Presented by Ande Smith

DEER BROOK

Deer Brook Consulting

Ande Smith

- President of Deer Brook
- CIO for the Maine Community College System
- CIO for the State of Maine
- CTO for the State of Connecticut

DEER BROOK

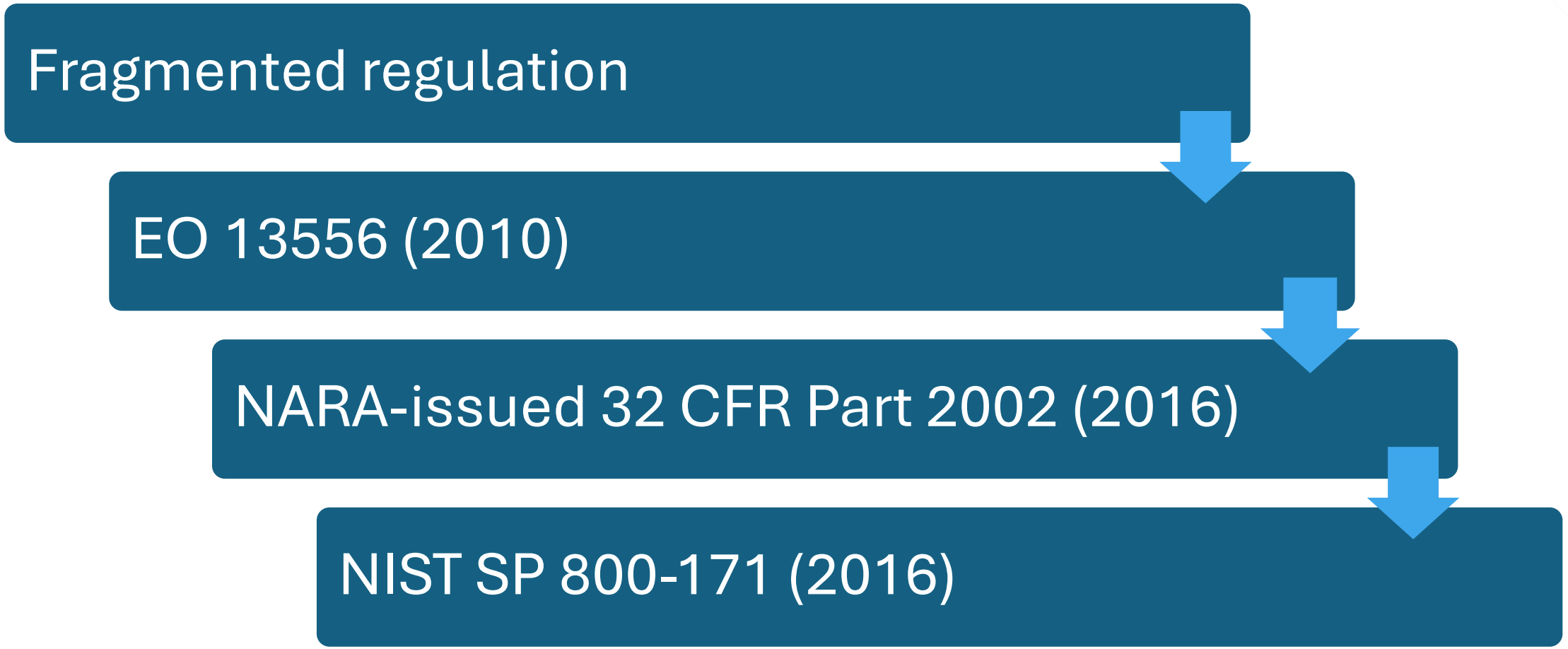
CYBER | TECHNOLOGY | SOLUTIONS

Deer Brook

- Educational technology, IT consulting
- Transformation projects, technology implementation projects

Patchwork of Federal Regulations

- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Gramm-Leach-Biley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Higher Education Act (HEA)
- Payment Card Industry Data Security Standards (PCI-DSS)
- Student Aid Internet Gateway (SAIG) Enrollment Agreement

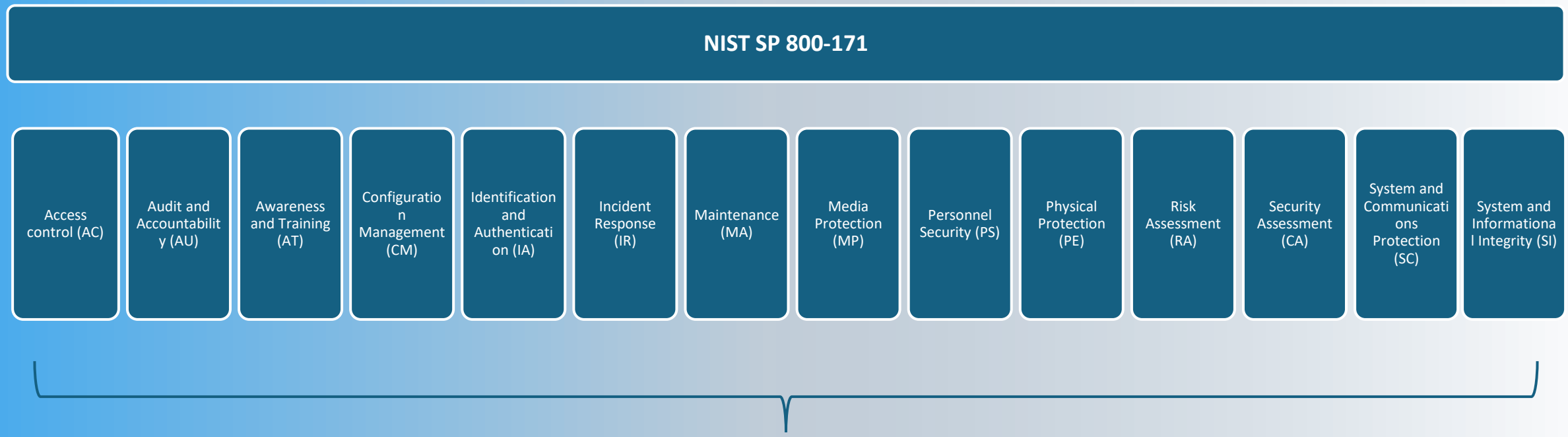


Journey to NIST SP 800-171 as an Applicable Standard

Hey… That Was Nine Years Ago!

- No agency asserted the requirements (except DoD)
- Created the Cybersecurity Maturity Model Certification (CMMC) program
- Phased Implementation in DoD, GSA, and NASA supply chains
- September 2024: DoE issued a notice of intent to engage in rulemaking

What Does NIST 800-171 Provide?



What Has Deer Brook Seen in the CMMC Space From Small Manufacturers?

- Lack of policy documentation
- Policy enforcement
- Limited IT, cybersecurity staff
- Limited budgets
- Reliance on Managed Service Providers
- Timeline
- Emphasis on shared responsibility
- Understanding where data resides
- Technology
  - Configuration baselines, access, controls
  - Endpoint controls for authentication and data access restrictions
  - Vulnerability scanning, remediation processes

Step	Activity
Define Scope	• Identify CUI locations, system boundaries, and shared responsibility models.
Stakeholder Inquiry & Organizational Awareness	• Interview stakeholders, assess training, culture, and awareness. • Identify organizational challenges.
Documentation Review	• Collect and review policies, procedures, and system documentation.
Gap Analysis	• Map current state against 110 controls; classify implementation status. • Confirm how current tools, processes, and responsibilities map to controls.
Control Validation & Effectiveness Review	• Review evidence of technical controls that may evaluate logging and alerting. • Confirm who investigates and responds to alerts. • Assess how well controls are operationalized.
Risk & Impact Assessment	• Prioritize gaps based on risk, impact, and feasibility. • Focus on actionable items and what is most critical to remediate.
Plan of Action & Milestones (POA&M)	• Create a remediation plan with actions, owners, and timelines. • Consider cloud solutions for ERP platforms as a better investment than only protecting on-premise infrastructure. • Identify automation opportunities and resource requirements (but realize that it inevitably requires staff/partners). • There is no set and forget.
Operational Readiness & Maturity Assessment	• Assess sustainability of controls, ownership clarity, monitoring, and resource support.

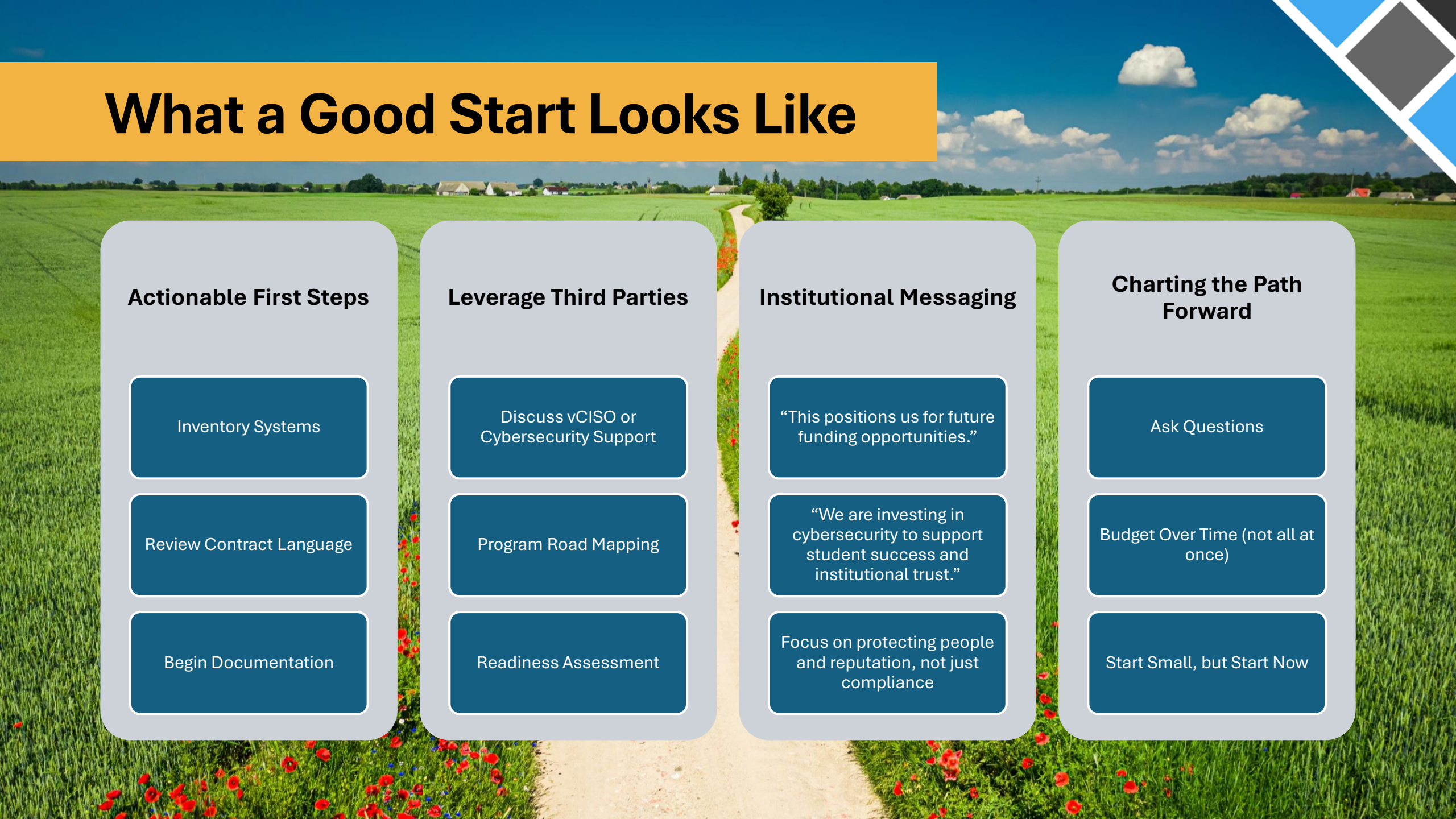
How Should It Be Approached?

What Does It Mean for Community Colleges?

Evolving Regulatory Landscape	• Formal regulations may come. • Will these resemble the CMMC Program?
Policy & Data Drivers	• CUI is personally identifiable information (PII). • Historically minimal prescriptive cybersecurity regulation. • Policy drivers may shift adoption to be expected.
Why Bother?	• NIST SP 800-171 is a reputable cybersecurity framework. • Defensible approach to protecting sensitive data. • Starting early allows colleges to manage budget and disruptions. • Signals institutional maturity for grantors, auditors, regulators.

NIST 800-171 is a strong, forward-thinking investment in securing student and institutional data.

What a Good Start Looks Like



Actionable First Steps

- Inventory Systems
- Review Contract Language
- Begin Documentation

Leverage Third Parties

- Discuss vCISO or Cybersecurity Support
- Program Road Mapping
- Readiness Assessment

Institutional Messaging

- “This positions us for future funding opportunities.”
- “We are investing in cybersecurity to support student success and institutional trust.”
- Focus on protecting people and reputation, not just compliance

Charting the Path Forward

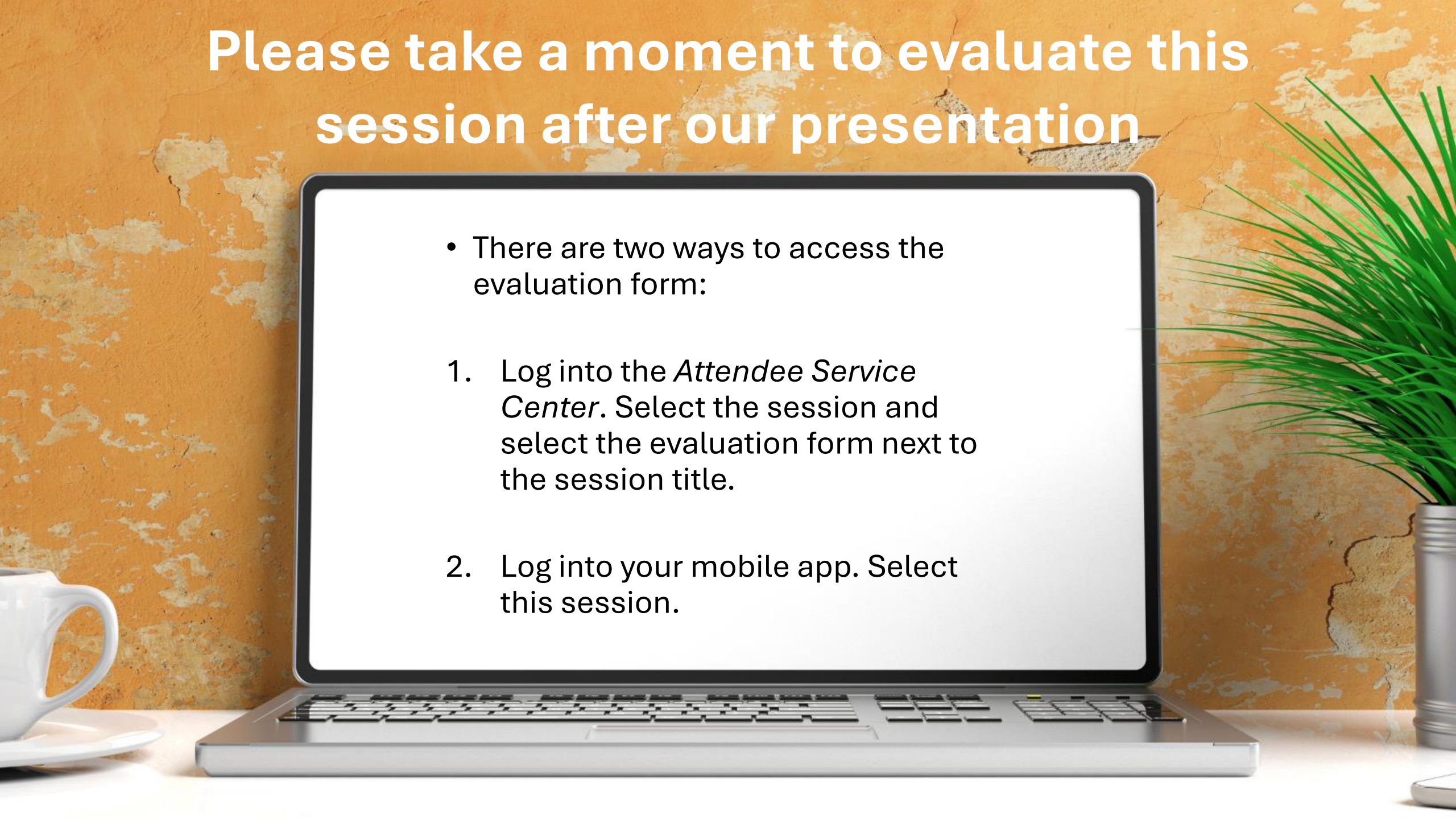
- Ask Questions
- Budget Over Time (not all at once)
- Start Small, but Start Now

Ande Smith asmith@deer-brook.com http://deer-brook.com/aacc

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Please take a moment to evaluate this session after our presentation



- There are two ways to access the evaluation form:

1. Log into the *Attendee Service Center*. Select the session and select the evaluation form next to the session title.

2. Log into your mobile app. Select this session.

Supplemental Resources

CMMC Alignment to NIST SP 800-171 Revisions

- DoD followed federal rulemaking guidelines when aligning CMMC assessment requirements to NIST SP 800-171 **Rev 2**.

- Defense contractors can implement NIST SP 800-171 Rev 3, but must comply with **Rev 2 requirements not covered in Rev 3** to meet CMMC assessment requirements.

- DoD will incorporate Rev 3 with future rulemaking.

CMMC Alignment to NIST SP 800-171 Revisions

Department of Defense – About CMMC
https://dodcio.defense.gov/CMMC/About/

NIST SP 800-171 Rev.2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

NIST SP 800-171 Rev. 3
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

NIST SP 800-171 Requirements

ACCESS CONTROL

AUTHORIZED ACCESS CONTROL

TRANSACTION & FUNCTION CONTROL

CONTROL CUI FLOW

SEPARATION OF DUTIES

LEAST PRIVILEGE

NON-PRIVILEGED ACCOUNT USE

PRIVILEGED FUNCTIONS

UNSUCCESSFUL LOGON ATTEMPTS

PRIVACY & SECURITY NOTICES

SESSION LOCK

SESSION TERMINATION

CONTROL REMOTE ACCESS

REMOTE ACCESS CONFIDENTIALITY

REMOTE ACCESS ROUTING

PRIVILEGED REMOTE ACCESS

WIRELESS ACCESS AUTHORIZATION

WIRELESS ACCESS PROTECTION

MOBILE DEVICE CONNECTION

ENCRYPT CUI ON MOBILE

EXTERNAL CONNECTIONS

PORTABLE STORAGE USE

CONTROL PUBLIC INFORMATION

AWARENESS AND TRAINING

ROLE-BASED RISK AWARENESS

ROLE-BASED TRAINING

INSIDER THREAT AWARENESS

AUDIT AND ACCOUNTABILITY

SYSTEM AUDITING

USER ACCOUNTABILITY

EVENT REVIEW

AUDIT FAILURE ALERTING

AUDIT CORRELATION

REDUCTION & REPORTING

AUTHORITATIVE TIME SOURCE

AUDIT PROTECTION

AUDIT MANAGEMENT

CONFIGURATION MANAGEMENT

SYSTEM BASELINING

SECURITY CONFIGURATION ENFORCEMENT

SYSTEM CHANGE MANAGEMENT

SECURITY IMPACT ANALYSIS

ACCESS RESTRICTIONS FOR CHANGE

LEAST FUNCTIONALITY

NONESSENTIAL FUNCTIONALITY

APPLICATION EXECUTION POLICY

USER-INSTALLED SOFTWARE

IDENTIFICATION AND AUTHENTICATION

IDENTIFICATION

AUTHENTICATION

MULTIFACTOR AUTHENTICATION

REPLAY-RESISTANT AUTHENTICATION

IDENTIFIER REUSE

IDENTIFIER HANDLING

PASSWORD COMPLEXITY

PASSWORD REUSE

TEMPORARY PASSWORDS

CRYPTOGRAPHICALLY-PROTECTED PASSWORDS

OBSCURE FEEDBACK

INCIDENT RESPONSE	MAINTENANCE	MEDIA PROTECTION
INCIDENT HANDLING	PERFORM MAINTENANCE	MEDIA PROTECTION
INCIDENT REPORTING	SYSTEM MAINTENANCE CONTROL	MEDIA ACCESS
INCIDENT RESPONSE TESTING	EQUIPMENT SANITIZATION	MEDIA DISPOSAL
	MEDIA INSPECTION	MEDIA MARKINGS
	NONLOCAL MAINTENANCE	MEDIA ACCOUNTABILITY
	MAINTENANCE PERSONNEL	PORTABLE STORAGE ENCRYPTION
		REMOVEABLE MEDIA
		SHARED MEDIA
		PROTECT BACKUPS

PERSONNEL SECURITY	PHYSICAL PROTECTION	RISK ASSESSMENT
SCREEN INDIVIDUALS	LIMIT PHYSICAL ACCESS	RISK ASSESSMENTS
PERSONNEL ACTIONS	MONITOR FACILITY	VULNERABILITY SCAN
	L1 - MANAGE VISITORS & PHYSICAL ACCESS	VULNERABILITY REMEDIATION
	L2 - ESCORT VISITORS	
	PHYSICAL ACCESS LOGS	
	MANAGE PHYSICAL ACCESS	
	ALTERNATIVE WORK SITES	

SECURITY ASSESSMENT

SECURITY CONTROL ASSESSMENT

PLAN OF ACTION

SECURITY CONTROL MONITORING

SYSTEM SECURITY PLAN

SYSTEM AND COMMUNICATIONS PROTECTION

BOUNDARY PROTECTION

SECURITY ENGINEERING

ROLE SEPARATION

SHARED RESOURCE CONTROL

PUBLIC-ACCESS SYSTEM SEPARATION

NETWORK COMMUNICATION BY EXCEPTION

SPLIT TUNNELING

DATA IN TRANSIT

CONNECTIONS TERMINATION

KEY MANAGEMENT

CUI ENCRYPTION

COLLABORATIVE DEVICE CONTROL

MOBILE CODE

VOICE OVER INTERNET PROTOCOL

COMMUNICATIONS AUTHENTICITY

DATA AT REST

SYSTEM AND INFORMATIONAL INTEGRITY

FLAW REMEDIATION

MALICIOUS CODE PROTECTION

SECURITY ALERTS & ADVISORIES

UPDATE MALICIOUS CODE PROTECTION

SYSTEM & FILE SCANNING

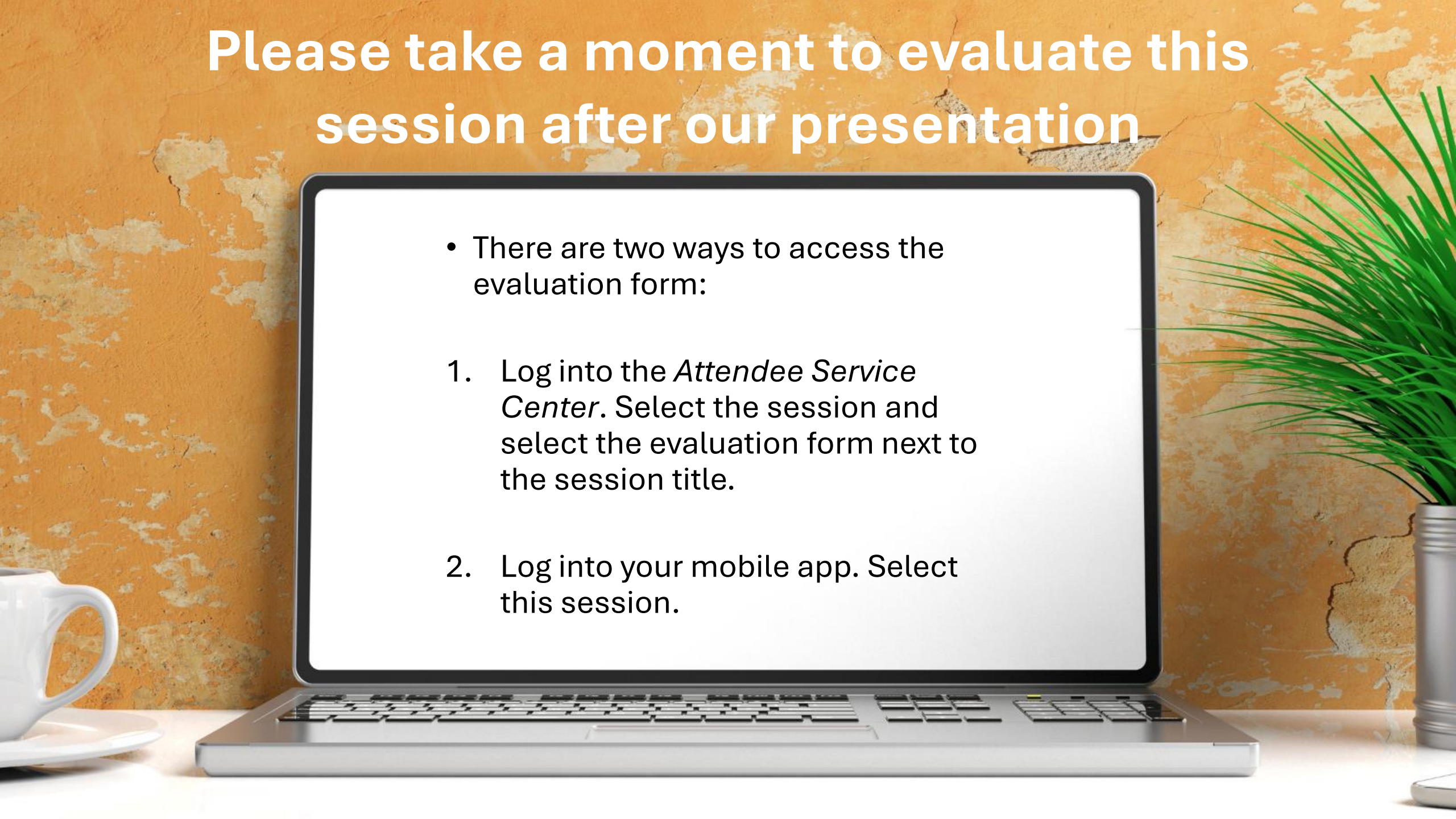
MONITOR COMMUNICATIONS FOR ATTACKS

IDENTIFY UNAUTHORIZED USE

DEER BROOK

CYBER | TECHNOLOGY | SOLUTIONS

Please take a moment to evaluate this session after our presentation



- There are two ways to access the evaluation form:

1. Log into the *Attendee Service Center*. Select the session and select the evaluation form next to the session title.

2. Log into your mobile app. Select this session.