Outline

• Introductions/Co-Authors
• Overview of the project
  – History of the publications
  – Why update now?
• Key Objectives
• Work to Date
• Take-aways from pre-draft comments
• Next steps
• Q&A
Introductions/Co-Authors

Co-Author Team

• Marian Merritt, NIST
• Don Walden, IRS
• Brenda Ellis, NASA
• Susan Hansche, CISA/DHS
• Kevin Sanchez-Cherry, DOT
• Julie Snyder, MITRE
• Jessica Dickson, NIST (on leave)
Overview: History of the publications:

- **800-50: “Building an Information Technology Security Awareness and Training Program”**
  - October 2003
  - Foundational document to guide creation of an organization’s cybersecurity A/T program
Overview: History of the publications (cont):

- 800-16 “Information Technology Security Training Requirements: A Role and Performance-Based Model”
- April 1998
- Revised:
  - V1 3rd draft 2014
  - Prelim draft R2 2020 (not published)
Overview: Why Update Now?

• Opportunity to sync NIST guidance with latest updates and recommendations from outside guidance informing this work
  – OMB A-130
  – National Defense Authorization Act (NDAA) for FY2021
  – Cybersecurity Enhancement Act of 2014

• Opportunity to address gaps and open questions within existing guidance
Pre-Draft Call for Comments - Learning continuum

Figure 2-1: The IT Security Learning Continuum

Figure 4-1: Cybersecurity Learning Continuum
Other Comments in the Pre-Draft Call for Comments

• Leveraging other NIST reference material
• Consistent language
• Risk reduction drives training programs
• Challenge of measuring impact of programs
• Role of the training program in setting a cybersecurity culture
Key Objectives

• Update to security awareness and training program lifecycle
• Incorporating privacy awareness and training programs in parallel with security
• Consolidation of 800-50 and 800-16
• Incorporate NICE Workforce Framework KSTs
Themes

• Developing a security and privacy culture in the organization
• Allowing for an iterative approach (to accommodate cybersecurity, privacy, organizational specific events)
• Flexibility, scalability
  – From large agency to smaller organizations
• Standardized terms as found in other NIST documents
• Reflect current work environment and requirements (i.e. remote workforce)
Additional themes

• Incorporate privacy with cybersecurity awareness and training efforts, reflecting organizational reality
• Metrics – what is useful, what can be measured
• Recommended feedback mechanisms
• Post-implementation assessment steps
Discussion Points from Co-Authors

Concepts from the Team

• Awareness and Training Program > Learning Program
  – NICE Framework, “Learner”; organizations have Chief Learning Officer
• Defining Role Based Training simply
• Moving examples of assets to online appendix (i.e. policy examples, posters)
Work to Date

• Co-authoring team formed (some new people):
  – NIST (NICE and Privacy Engineering), DHS, IRS, DOT, NASA

• Pre-draft Call for Comments
  – Issued Sept. 21, 2021
  – Closed Nov. 5, 2021
  – Adjudication completed Jan. 2022

• Anticipated Draft Fall 2022

• Public review through January 2023

• Final February 2023
Thank you!