# SKILL BRIDGE INTERNSHIP SYLLABUS

FIRST MONTH: Onboarding and Introduction to NIST SP 800-171 and Basic Cybersecurity Concepts

- Objective 1: Intern Onboarding and Familiarization (1 Week)
  - Understand the CyberNINES business - its specialty and its client base.
  - Become familiar with applicable company policies and procedures.
  - Be accessed to the company network (email address, login credentials, requisite training).
- Objective 2: Familiarization with NIST SP 800-171 (1 Week)
  - Understand the purpose and scope of NIST SP 800-171.
  - Explore the different families and controls within the framework.
  - Identify the relevance of NIST SP 800-171 for protecting Controlled Unclassified Information (CUI).
- Objective 3: Cybersecurity Fundamentals (1 Week)
  - Study fundamental cybersecurity concepts, such as confidentiality, integrity, and availability (CIA triad).
  - Learn about common cyber threats and attack vectors.
  - Understand the basics of access controls, encryption, and incident response.
- Objective 4: NIST SP 800171 Control Families (1-7) (1 Week)
  - Dive into the first five control families of NIST SP 800-171.
  - Analyze the specific controls within each family and their implementation requirements.
  - Begin mapping controls to corresponding assessment objectives in NIST SP 800-17 IA.

SECOND MONTH: Advanced NIST SP 800171 Implementation and Assessment

- Objective 1: NIST SP 800-171 Control Families (7-14) (1 Week)
  - Continue exploring the next five control families of NIST SP 800-171.
  - Deepen the understanding of control requirements and implementation best practices.
  - Practice mapping controls to assessment objectives.
- Objective 2: Developing Security Policies and Procedures (1 Week)
  - Learn how to create comprehensive security policies and procedures based on NIST SP 800-171.
  - Understand the importance of policy documentation in compliance and assessments.
- Objective 3: NIST SP 800-17 IA Assessment Objectives (2 weeks)
  - Study the NIST SP 800-17 IA assessment objectives.

THIRD MONTH: NIST SP 800-171 Assessment and Advanced Topics & OJT work with clients

- Objective 1: Conducting NIST SP 800-171 Assessments (4 Weeks)
  - Learn the process of evaluating compliance with NIST SP 800171 security controls. Practice performing control audits. Identify purpose and use of a Plan of Action and Milestone (POA&M)
- Objective 2: Assessing and Addressing Gaps (4 Weeks)

    - Analyze assessment results and identify potential gaps and deficiencies.
    - Practice creating a POA&M entry and gap/deficiency corrective milestone plan.
- Objective 3: Advanced Topics in NIST SP 800-171 (4 Weeks)
    - Explore additional cybersecurity topics relevant to NIST SP 800-171, such as secure configuration management, incident handling, and continuous monitoring.
    - Discuss integration of NIST SP 800-171 with other cybersecurity frameworks like ISO 27001.

Completion of these modules, along with on-the-job training on client projects, will prepare the service member intern with the requisite skills and knowledge to pass the Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner (RP) test and become a Certified RP.

CMMC training and accreditation are delivered by CMMC Advisory Board. Details of the training and certification levels and roles may be accessed at https://www.cyberab.org.