



## **CUI Notice 2020-04: Assessing Security Requirements for CUI in Non-Federal Information Systems**

June 16, 2020

### **Purpose**

1. This Notice provides guidance on assessing security requirements for CUI within non-Federal information systems in unclassified environments.

### **Authorities**

2. The Director of the Information Security Oversight Office (ISOO), exercises Executive Agent (EA) responsibilities for the CUI Program. 32 CFR Part 2002, Controlled Unclassified Information, establishes CUI Program requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI.
3. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations, establishes security requirements to ensure CUI's confidentiality on non-Federal systems. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, provides procedures for assessing the CUI requirements in NIST SP 800-171 and is the primary and authoritative source of guidance for organizations conducting such assessments.
4. Agencies must use NIST SP 800-171 when establishing security requirements to protect CUI's confidentiality on non-Federal information systems (unless an authorizing law, regulation, or Government-wide policy listed in the CUI Registry for the relevant CUI category prescribes specific safeguarding requirements for protecting the information's confidentiality, or unless an agreement establishes requirements to protect CUI Basic at higher than moderate confidentiality).
5. This guidance document is binding on agency actions as authorized under applicable statute, executive order, regulation, or similar authority. This guidance document does not have the force and effect of law on, and is not meant to bind, the public, except as authorized by law or regulation or as incorporated into a contract.

### **Assessment Guidance**

6. When any entity assesses compliance with the security requirements of NIST SP 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171.
7. The assessment process is an information-gathering and evidence-producing activity to determine the effectiveness of safeguards used to meet the security requirements specified in

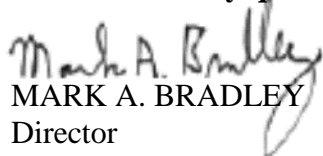
NIST SP 800-171. Organizations can use information and evidence from the assessment process to:

- a. Identify potential problems or shortfalls in the organization's security and risk management programs;
- b. Identify security weaknesses and deficiencies in its systems and in the environments in which those systems operate;
- c. Prioritize risk mitigation decisions and activities;
- d. Confirm that identified security weaknesses and deficiencies in the system and in the operation environment have been addressed; and
- e. Support risk-based decision-making and provide information security situational awareness.

### Scope of Assessment Activities

8. Non-Federal entities use the system security plan to describe how they meet or plan to meet CUI security requirements. They document any security requirements they deem non-applicable (*e.g.*, no wireless capability in the system or the system component processing, storing, or transmitting CUI) as such in the system security plan.
9. Agencies may assess only systems and components that an entity uses to store, process, or transmit CUI, and they assess the systems for performance of requirements in the relevant contract or agreement.
  - a. Prior to engaging in any oversight action of non-Federal systems, the agency must describe:
    - i. the assessment methods and objects it will use/perform;
    - ii. the scope of the assessment (objective); and
    - iii. special emphasis items or other critical discriminators relative to the assessment's scope/objective.
  - b. Assessment activities may be limited to any unimplemented controls and accompanying compensatory controls.
10. Reciprocity. Each agency is responsible for taking appropriate steps to minimize redundant and duplicative security inspections and audit activity. Agencies may execute appropriate inter-agency agreements to avoid or minimize redundant and duplicative oversight actions by agencies or internal component elements.

**Please direct any questions regarding this notice to: [CUI@nara.gov](mailto:CUI@nara.gov)**

  
MARK A. BRADLEY  
Director