

requires safeguarding or dissemination controls, unless doing so conflicts with the underlying law, regulation, or Government-wide policy. In addition, central authorities, like the Archivist of the United States, may direct decontrol of CUI across agencies. The NASA CUI Handbook covers the processes by which CUI is decontrolled.

2.12.2 Centers or Mission Directorates, and HQ offices may designate in their CUI policies which personnel it authorizes to decontrol CUI, consistent with law, regulation, and Government-wide policy.

2.12.3 NASA personnel shall not decontrol CUI to conceal, or to otherwise circumvent accountability for, an unauthorized disclosure.

2.12.4 When laws, regulations, or Government-wide policies require specific decontrol procedures, NASA personnel shall follow such requirements.

2.13 Safeguarding and Storage

2.13.1 The objective of safeguarding is to prevent the unauthorized disclosure of or access to CUI. These guidelines set forth the minimum standards for safeguarding; however, organizations may adopt specific organization requirements for safeguarding CUI within their organization per FIPS 140-2.

2.13.2 Unless different protection is specified in the CUI Registry, physical documents containing CUI will be stored in a locked office, locked drawer, or locked file cabinet if unattended. Electronic files will be protected using NASA approved methods such as encryption and access restriction. See CUI Handbook for more detailed information.

2.13.3 NASA personnel working with CUI Specified shall comply with the safeguarding standards outlined in the underlying law, regulation, or Government-wide policy in addition to those described in this policy.

2.13.4 Safeguarding During Working Hours. NASA personnel working with CUI shall be careful not to expose CUI to unauthorized users or others who do not have a lawful Government purpose to have, transport, store, use, or process CUI. Cover sheets may be placed on top of documents to conceal the contents from casual viewing. Personnel may use cover sheets to protect CUI documents while in use, but will secure CUI documents in a locked location, such as a desk drawer, file cabinet, or office, when not in use. Other precautions include the following:

a. NASA personnel should reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations where CUI is discussed.

b. CUI should be kept in a controlled environment which is defined as any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers and managed access controls) for protecting CUI from unauthorized access or disclosure.

c. If it is necessary to remove CUI from a controlled environment of the work location (e.g., telework, official travel), NASA personnel shall keep CUI under their direct control at all times or protect it with at least one physical barrier (i.e., a cover sheet) and reasonably ensure that they or the physical barrier protects the CUI from unauthorized access or observation.