1. **Examples of Reclamation-Specific Controlled Unclassified Information (CUI).** Below are general examples of CUI that pertain to Reclamation's mission areas. This is not intended to serve as an all-inclusive list. The context of the information must always be taken into account when determining if the information is sensitive enough to be CUI.

   A. Documents or drawings that describe information about critical features or areas that could be used to exploit the safety, security, or operational effectiveness of Bureau of Reclamation assets, e.g. as access points, modes of operation, or structural design. The term "critical" is generally refers to any location at a facility where an unauthorized intruder could disrupt the operation, function, or mission of the facility. This includes sensitive documents, such as:

      (1) standing operating procedures (SOP) and Designers' Operating Criteria;

      (2) operating procedures related to equipment at a dam, powerplant, or other facility including equipment operating procedures, locations, and drawings; and

      (3) facility floor plans and drawings showing the layout and access points.

   B. Documents related to information technology systems that control and protect critical facility functions:

      (1) information related to Industrial Control Systems (ICS) such as Supervisory Control and Data Acquisition (SCADA) systems, including documentation, operational drawings, designs, computer source code, communication/control procedures, and protocols for operation of key structures such as dams, powerplants, pumping plants, and waterway systems;

      (2) drawings (including as-built), designs, specifications, and other data related to security systems or measures, including electronic access control and surveillance systems (EACSS).

   C. Sensitive communications and organizational information, may include:

      (1) continuity of operations plans (COOP), emergency action plans (EAP), and related information such as inundation maps;

      (2) HazMat response plans and chemical lists;

      (3) Privacy Act information;

      (4) sensitive personally identifiable information;

      (5) staffing levels related to specific facilities or resources; and

(6) specific information about staff who work in sensitive areas, law enforcement, security, or management positions.

D. Information that describes operational procedures, such as employee schedules, delivery schedules, hours of operation in non-public areas, and locations of sensitive information.

E. Information that could be used to compromise the integrity of the facility, may include:

(1) Risk analyses, or facility review reports, including failure probabilities, failure consequences, estimated life loss and damage estimates, risk calculations, specific structural vulnerabilities, and related estimates from normal loading conditions, seismic events, and floods.

(2) Inundation maps.

(3) Improvement or vulnerability mitigation recommendations (related to facilities, features, or other resources.

(4) Agency decisions regarding actions to address recommendations.

(5) Documentation of activities to address recommendations.

F. Financial, budget, and draft policy information that would not be appropriate for public disclosure until deemed finalized and releasable by the agency.

G. Information associated with bulk electric system (BES) cyber systems and all associated components, as designated by Reclamation in support of the NERC-CIP standards, may include:

(1) the BES cyber system inventory list; and

(2) all non-public information relating to the operation of cyber systems and assets, including:

(a) drawings or documents, including floor plans or equipment layouts, which identify the physical location of specific cyber systems and assets;

(b) BES cyber system network diagrams;

(c) documentation of electronic security perimeters (ESP);

(d) documentation related to physical security protection measures;

(e) security and vulnerability assessments; and

(f) incident response plans and disaster recovery plans.

H. Security information related to facility security and risk management, may include:

(1) descriptions of threats and vulnerabilities;

(a) threat assessments;

(b) security risk assessments or analyses;

(c) security reviews;

(2) protective measures;

(3) security guard information, including:

(a) standing operating procedures (SOP);

(b) defense plans;

(4) site security plans; and,

(5) information from specific security-related research or studies, not raising to the classified level as defined in the DHS Security Classification Guideline dated 2 December 2010.