1. **Examples of Reclamation For Official Use Only (FOUO) Information.** Below are general examples of types of FOUO information and 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 actually sensitive.

   A. Documents or drawings that describe information about critical features or areas that could be used to exploit any Bureau of Reclamation assets, such as access points, modes of operation, or structural design. The term "critical" is generally intended to refer 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 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) floor plans and drawings showing the facility 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) information about industrial control systems and system components; and

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

   C. Sensitive communications and organizational information, such as:

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

      (2) personal (home or cell) telephone numbers;

      (3) Privacy Act information;

      (4) personally identifiable information;

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

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

D. General security information, such as site security plans (that do not reveal vulnerabilities), tables and general descriptions of Reclamation's threat condition protective measures, security prioritization information, and supporting data.

E. Information that could be used to compromise the integrity of the facility, such as:

(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. This could include:

(a) freeboard information;

(b) cross-sections of the dam;

(c) safe downstream channel capacity; and

(d) gate drawings or details.

(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 (prior to completion of issue evaluation).

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, such as:

(1) the BES cyber system inventory list

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

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

(b) 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.

2. **Examples of HIGHLY SENSITIVE FOUO Information.** In general, information which describes specific structural vulnerabilities, attack scenarios, or other specific data that could be used to detrimentally exploit a specific facility, such as to fail an asset, is considered highly sensitive if it does not rise to a level of classified information. The following types of FOUO information, in context, are considered highly sensitive and require additional protective measures (see Paragraph 7.G. of SLE 02-01):

A. any information related to security risk management such as threat assessments, security risk assessments or analyses, security reviews, security surveys, security evaluations, defense plans, security guard information and standing operating procedures, and site security plans that reveal asset vulnerabilities or attack scenarios for specific facilities; and

B. information from specific security-related research or studies.