Reclamation Manual

Directives and Standards

TEMPORARY RELEASE
(Expires 03/30/2013)

Critical Cyber Asset (CCA) Identification Methodology

1. **Introduction.**

A. The Bureau of Reclamation will employ a multi-step methodology to identify CCAs associated with its inventory of critical assets (CAs). The methodology, incorporated into a procedure, is outlined in this appendix. The procedure will initially identify all cyber-based assets associated with a CA. This will be followed by a number of screening steps that will lead to the identification of the cyber asset as "critical," "non-critical," or "out-of-scope." A template, in the form of a *Critical Cyber Asset Inventory Template*, has been prepared to facilitate the recording and identification of CCAs. The utilization of the assessment template is recommended in order to better support the documentation of CCAs and the associated decision making process.

B. The CCA identification procedure consists of: (1) a complete inventory of all cyber assets that are associated with a CA; (2) a determination of which of those cyber assets are "essential;" and (3) an application of the North American Electric Reliability Council (NERC) -identified qualifying criteria. All of the above steps must be completed and their criteria satisfied for the cyber asset to be classified as a "CCA." Although not required to address the identification of CCAs, additional information is provided to identify requirements to which non-CCAs may be subject to a subset of the standards due to location on the electronic security perimeter (ESP) network, in support of physical access control systems, or in support of intrusion detection and electronic monitoring.

C. The strict and orderly approach outlined in this document is necessary to ensure the consistent identification of CCAs across the organization. It is important to acknowledge that the boundary or scope of determining the CCAs begins with a cyber asset's association to a CA. This initial determination and scope establishes the baseline from which all subsequent decisions are made.

2. **Identification Procedure.**

A. **Step 1 – Identify all Cyber Assets.**

(1) Using the inventory of CAs developed and maintained by Reclamation's Power Resources Office, complete a thorough inventory of all cyber assets associated with each CA. Cyber assets are defined by NERC as "programmable electronic devices and communication networks, including hardware, software, and data."

(2) The intent of this first step is to produce an all-inclusive, CA centric cyber asset inventory. After this initial inventory is compiled for each CA, additional criteria will be applied in Steps 2 and 3 to further refine the identified cyber asset inventory to only those that meet the NERC Critical Infrastructure Protection (CIP) criteria for "CCAs."

(3) The inventory effort may take several iterations and involve interviews with plant or facility operations personnel and managers, supervisory control and data acquisition (SCADA) administrators, information technology support staff, and information system security officers. The effort must identify and document all cyber assets such as; plant, unit, transformer, prime mover (turbine), and associated maintenance, control, monitoring, and protection systems or subsystems supporting a critical bulk electric system (BES) asset. The inventory must also include any personal computer (PC) or programmable logic controller (PLC) -based systems (including special protection schemes, such as remedial action schemes (i.e., RAS)); either remote or standalone and all related communication interfaces. No attempt will be made at this stage to determine whether the cyber asset qualifies as "critical" or "essential" as that activity will be determined in the later steps.

(4) The resulting inventory may also identify existing local area network (LAN) segments that host the cyber assets. While the formal designation of an "Electronic Security Perimeter" for these LAN segments is premature at this point in the procedure, the initial observation as to the logical placement of the network layer boundary is appropriate and will assist in defining the boundary of cyber assets that are "associated" with the CA in question.

(5) Reclamation's Denver-based NERC CIP Project Team will maintain inventory templates to document the cyber asset inventory process and results. At a minimum, the inventory template must identify the name of the cyber asset, a description of its function, and the associated CA. The inventory template may also include criteria outlined in Step 2 and Step 3 of this methodology that will further qualify the cyber assets as CCAs.

(6) The section of these procedures titled Approaches for Identifying Cyber Assets, below, provides an approach to identifying all cyber assets located within Reclamation control centers, power plants, and switchyards.

B. **Step 2 – Determine Essential Cyber Assets.**

(1) Employing the cyber asset inventory/inventories prepared in Step 1, evaluate the identified cyber assets to determine if they are *essential* based on whether any one or more of the following criteria is met:

(a) the cyber asset participates in, or is capable of, supervisory or autonomous (automatic) control that is essential to the reliable operation of BES reliability criteria that is provided by the CA (See item (2) below for clarification of "BES reliability criteria that is provided by the CA");

(b) the cyber asset displays, transfers, or contains information relied on to make real-time operational decisions, that are essential to the reliable operation of BES reliability criteria that is provided by the CA; or,

(c) the cyber asset fulfills a function not necessarily identified in conditions (a) and (b), above, but its loss, degradation, and compromise would affect the reliability or operability of the BES based on the following definitions:

(i) the term "loss" means that the unavailability of the cyber asset would have an immediate adverse "impact" on the reliable operation of the BES reliability criteria that is provided by the "associated" CA;

(ii) the term "degradation" means that the cyber asset is not fully functional "and" could adversely impact the reliable operation of the BES reliability criteria that is provided by the "associated" CA; and

(iii) the term "compromise" means that information or control is modified in a way to produce an undesirable outcome that impacts the reliable operation of the BES reliability criteria that is provided by the "associated" CA.

(2) The "BES reliability criteria that is provided by the CA" for Reclamation facilities may include blackstart, generation equal to or greater than 1500MW, or any other criteria that has been considered within the NERC CIP Reliability Standards to require an asset be identified as a CA. Therefore, only cyber assets that support an identified reliability criteria will be declared as essential. For example, if a power plant is declared a CA due to its ability to supply Blackstart

resources to the BES as part of a restoration plan, then only the cyber assets that support the blackstart functions of the plant will be considered essential. These resources will include unit controls, governor controls, voltage controls, and synchronizing/breaking controls. Likewise, if a power plant is considered essential because it is greater than 1500MW, then only the cyber assets that can affect 1,500 MW in aggregate will be declared as essential.

(3) The manner in which the above criteria are applied is significant. It is important that the inventory of cyber assets associated with a CA be developed first, before the criteria discussed in ***Steps 2 and 3*** are applied. This will result in a consistent and repeatable outcome. Applying the ***Step 2*** criteria outside the scope of the established inventory, by including cyber assets not associated with the CA in question, will result in disparity across the organization and an invalid outcome.

(4) It is at this screening level that most administrative networks (e.g., Reclamation Mission Support System - RMSS) and communication systems will be eliminated from the cyber asset inventory. While these assets may have been determined to be "associated" with a CA, they would typically not be "essential" pursuant to the criteria above.

C. **Step 3 – Apply Further Qualifying Criteria.**

(1) Employing the essential cyber asset inventory resulting from the application of ***Steps 1 and 2***, above, use the final qualifying criteria, listed below, to determine if the essential cyber assets qualify as CCAs:

(a) the essential cyber asset must be part of a routed network located within the boundaries of a control center and utilize a routable protocol to communicate within the control center;

(b) the essential cyber asset exists within a control center, power plant, or switchyard and utilizes a routable protocol to communicate outside its local network segment; or

(c) the essential cyber asset is dial-up assessable.

(2) The following examples should help to clarify criteria C.(1)(a) and C.(1)(b), above. If a cyber asset (that has been associated with a CA, per ***Step 1*** and determined to be "essential," per ***Step 2***) utilizes a routable protocol to communicate within a control center, it is classified as a CCA. This requirement,

however, is not similarly applied to essential cyber assets located within power plants and/or switch yards where no control center is located. For example, in the case where an isolated network in a switchyard hosts essential cyber assets that communicate over the LAN using a routable protocol, the essential cyber assets, in this instance, do not rise to the critical level if there is no supported (routable) communication outside their local network segment (e.g., ESP).

(3) Finally, with respect to criteria C.(1)(c) above, an essential cyber asset that is dial-up accessible (and that meets the criteria associated with ***Steps 1 and 2***, above) is further qualified as a CCA due to its dial-up accessibility. This qualification applies regardless of the communications protocol (routable or non-routable) employed, the location (in or out of a control center), or the type of inter-connectivity. For example, an essential remote terminal unit (RTU) with serial connectivity to a SCADA network, where the RTU is dial-up accessible, would be qualified as a CCA on the basis of its being essential and being dial-up accessible, irrespective of the fact that it employs no routable communications. In a similar manner, a dial-up accessible electronic protective relay, if it has been identified as essential, would be qualified as a CCA, even though it is hardwired to the unit protection circuits and has no other connectivity (other than the dial-up).

3. **Electronic Security Perimeter Concerns.**

A. While the formal determination of ESPs is not the intent of this document, it is important to acknowledge that many cyber assets, excluded through the application of the criteria discussed in ***Steps 2 and 3*** above, may be subject to compliance with many of the NERC CIP Standards, depending on their location within or function related to an ESP network.

B. Requirements calling for the protection of cyber assets, even if they have previously been deemed non-critical, are identified in several NERC CIP Standards, specifically:

(1) CIP-005, R1.4 requires that any non-critical cyber asset located within an ESP, must be identified as a part of the ESP and afforded all of the protection measures identified in CIP-005, including network boundary protection, electronic access control, electronic monitoring, and vulnerability assessment;

(2) CIP-005, R1.5 requires that any cyber asset utilized in the access control or electronic monitoring of an ESP must be protected in accordance with a defined subset of the same requirements that apply to CCA;

(3) CIP-006, R2 requires that any cyber asset utilized to monitor or log physical access to a physical security perimeters (PSP) must be protected pursuant to a subset of the same requirements that apply to critical cyber assets; and

(4) CIP-007 targets all cyber assets within an ESP (not just those identified as critical cyber assets) as subject to each of its nine requirements.

C. A careful review these requirements will assist compliance teams in documenting additional cyber assets that may subject to requirements of the NERC CIP Standards, even where those cyber assets have not been formally identified as CCAs.

D. Note: Cyber assets "within an ESP" includes all those cyber assets that are employing a routable protocol to communicate and that are enabled and hosted on the ESP network. Cyber assets interconnected via serial-based (non-routable) protocols are not included within the target of compliance according to the current version of the NERC CIP Standards.

4. **Management Information Assets.**

A. Cyber assets that are components of subsystems designed to provide real-time information monitoring to plant and/or facility personnel for the sole purpose of operational awareness are herein categorized as "Management Information Assets." These assets must not directly support/allow any supervisory or automated control capabilities and are typically:

(1) located outside a formally defined ESP;

(2) interconnected to other cyber assets via a routable protocol; and

(3) restricted through their configuration to only allow the presentation of information regarding the operational status of BES assets or systems supporting BES assets.

B. While Management Information Assets may not meet the formal qualifications for CCAs or be identified as cyber assets within an ESP boundary, they do warrant "risk" based considerations and effective security protective measures in order to minimize any potential misuse. In Reclamation, these Management Information Assets typically include personal computers configured as "view only" display terminals. These "view only" terminals are often located in management or administrative offices, and not in

areas traditionally provided all the physical protection measures of facility control rooms. Accordingly, the following protective measures shall be implemented for these assets:

(1) Management information assets located external to ESPs and their surrounding PSPs must be granted controlled and explicit access permissions into any ESPs to which they require access. This access must be specifically documented in the ESP's access point configuration.

(2) The management information asset's logical access into any ESP must be restricted to a specific interface and port on an access point to the ESP. Electronic access controls and the monitoring of electronic access pursuant to the Standards (e.g., CIP-005-2, Requirements 2 and 3) must also be implemented.

(3) Cyber assets that support management information functions, regardless of their location, must be afforded the logical security management, incident reporting and response, and recovery protective measures identified in the Standards (e.g., CIP-007-2, CIP-008-2, and CIP-009-2.)

(4) Cyber assets that support management information functions may be located in management and administrative offices, provided that the physical access is subject to observation by on-site personnel during business hours and locked within the subject offices during non-working hours.

5. **Approaches for Identifying Cyber Assets.**

A. This section of the methodology provides several approaches to building an inventory of all cyber assets associated with a CA.

B. Several iterations of review may be necessary to ensure that all cyber assets are identified when addressing ***Step 1*** of the CCA identification procedure. The cyber asset identification approach may include reviews by cyber ***asset function*** (monitoring, primary or secondary control of a BES asset, special protection equipment, or electronic physical security), or by cyber ***asset type*** (SCADA, communications). Regardless of the approach chosen, typical cyber assets that can appear on the initial inventory include:

(1) **By Asset Function.**

(a) **Cyber Assets Supporting Monitoring Only.** Identify cyber assets that are used for monitoring activities related to the BES assets. Typical monitoring systems include:

(i) **BES Asset Monitoring – Metering/Monitoring Systems.**

(aa) revenue;

(bb) temperature;

(cc) flow;

(dd) level (forebay, tailbay, etc.); and

(ee) unit/transformer/line quantities and status.

(ii) **Sequence of Events – Recording Systems.**

(iii) **Communications – Line Status/Failure Monitoring Systems.**

(iv) **Real-Time and Historical Data Collection and Archival Systems.**

(b) **Cyber Assets Supporting Control.** Identify cyber assets that are used for the direct and secondary control of critical BES assets. Typical direct and secondary control systems include:

(i) **Direct BES Asset Control.**

(aa) unit start, stop, and emergency shutdown;

(bb) unit breaker – open, close;

(cc) unit synchronizer;

(dd) unit speed (online) – megawatts – raise, lower;

(ee) unit voltage – megavars – raise, lower;

(ff) unit mode – generate, condense;

(gg) unit control mode – local (manual), local (automatic), supervisory;

(hh) set point control (megawatts or voltage) – on, off;

(ii) power system stabilizer – on, off;

(jj) digital exciters;

(kk) digital governors;

(ll) transformer tap changer – raise, lower;

(mm) line breaker – open, close;

(nn) motor operated disconnect – open, close;

(oo) automatic generation control (AGC); and

(pp) automatic voltage control (AVC).

(ii) **Secondary (Indirect) BES Asset Control.**

(aa) air compressors;

(bb) sump pumps;

(cc) cooling systems/chillers;

(dd) high-level applications (plant-level AGC/AVC and power/water modeling and scheduling systems; and

(ee) plant-level control modes – setpoint, AGC, AVC.

(c) **Cyber Assets Providing Critical BES Asset Protection.** Identify cyber assets that are used for system or equipment protection activities related to the BES.

(i) **Digital Unit/Transformer Protection Packages.**

(ii) **Special Protection Systems or Remedial Action Schemes.**

(d) **Cyber Assets Providing Physical and Electronic Access Control.** Identify all cyber assets that are used to support physical access control, video surveillance, alarm intrusion detection, and/or ground-base radar[1].

(e) **Other Cyber-based Assets.** Cyber-based facility, plant, and/or unit monitoring and/or control systems not otherwise identified above, such as an engineering/maintenance network for relays, etc., but that must be identified to ensure a thorough evaluation that demonstrates a "due diligent" approach toward the identification of critical and non-critical cyber assets.

(2) **By Asset Type.**

(a) **Voice and Data Networks.**

(i) Internet Protocol (IP), and similar routed communications protocols (e.g., Transmission Control Protocol over IP – TCP/IP);

(ii) Voice over IP (i.e., VoIP) and/or similar voice communication sub-systems;

(iii) Modbus® over IP and other vendor proprietary protocols over IP;

[1]Systems that provide physical access control capabilities to critical BES assets (or to critical cyber assets, e.g., key card access control, intrusion alarm, and video surveillance systems) are only subject to the CIP protective measures identified below:

- NERC CIP 003-1: Security Management Controls
- NERC CIP 004-1 R3 Personnel Risk Assessment
- NERC CIP 005-1:R2 Electronic Access Controls
- NERC CIP 005-1:R3 Monitoring Electronic Access Controls
- NERC CIP 006-1:R4 Physical Access Controls
- NERC CIP 006-1:R5 Monitoring Physical Access Controls
- NERC CIP 007-1: System Security Management
- NERC CIP 008-1: Incident Reporting and Response Planning
- NERC CIP 009-1: Recovery Plans

(iv) dial-up circuits; and

(v) leased lines/circuits.

(b) **Administrative and Operational Support Systems.** Including LANs (i.e., RMSS) specifically where collocated in control rooms to support high-level applications or email.

(c) **SCADA System Components.**

(i) historical and real-time database servers;

(ii) communication servers and front-end processors;

(iii) operator consoles – control and monitoring;

(iv) administrative consoles – management view nodes;

(v) PC-workstations (programming consoles);

(vi) PC-laptops (plant device programming devices);

(vii) PLCs[2];

(viii) RTUs; and

(ix) distributed input/output devices (specifically intelligent plant/device interface hardware systems).

(d) **Communications Networks/Channels.**

(i) microwave, category 5 (CAT5), synchronous optical networking (SONET) and other radio, fiber-based or direct wired channels;

(ii) serial communications channels (RS232, RS485, RS485-Modbus);

[2]While historical system boundaries for certification and accreditation (C&A) have sometimes excluded plant, unit, transformer, or facility control systems (e.g., PLCs and RTUs) other than SCADA, the NERC CIP Cyber Security Standards are all-inclusive of such systems.

(iii) dial-up access points; and

(iv) telephone exchange systems/servers.

(e) **Network Infrastructure.**

(i) domain controllers;

(ii) routers;

(iii) network switches/hubs;

(iv) virus protection and vulnerability scanning subsystems;

(v) backup subsystems;

(vi) configuration and patch management subsystems;

(vii) network and inventory management subsystems;

(viii) firewall and/or intrusion detection/prevention subsystems;

(ix) communication converters – serial-to-Ethernet; and

(x) log servers (e.g., "Syslog" servers).

(f) **Stand-alone Plant Sub-System(s) and/or Control Sub-Systems.** Status and alarm indication sub-systems (e.g., for plant or unit fire).

6. **Summary.** The application of the methodology discussed in this document is intended to ensure both a consistent approach and results when identifying Reclamation's CCAs. This methodology must be followed in order to help ensure that: (1) all qualifying cyber assets are identified and evaluated to determine if they may be critical cyber assets, and (2) the criteria used to establish cyber asset criticality are applied in a consistent and repeatable manner.

7. **Glossary of Terms.**

A. **AGC.** Equipment that automatically adjusts generation in a Balancing Authority Area from a central location to maintain the Balancing Authority's interchange Schedule Plus Frequency Bias. AGC may also accommodate automatic inadvertent payback and time error correction.

B. **AVC**. Automatic voltage control heightens system efficiency and power quality by automatically monitoring and controlling busbar, line, and transformer voltage. On a power distribution system experiencing varying loading conditions, this application can effectively maintain a steady transformer secondary voltage within preset limits.

C. **BES.** As defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition.

D. **CA**. Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.

E. **CCA**. Cyber assets essential to the reliable operation of CAs.

F. **CIP**. The NERC CIP Reliability Standards consists of 9 reliability standards and a total of 45 requirements. A total of 8 of these 9 standards and a total of 41 of the 45 requirements deal specifically with physical and logical cyber security controls associated with the BES CAs and their supporting CCAs.

G. **Cyber Assets**. Programmable electronic devices and communication networks including hardware, software, and data.

H. **ESP**. The logical border surrounding a network to which CCAs are connected and for which access is controlled.

I. **IP.** IP is one of a set of communications protocols used for the Internet and other similar networks. It is typically teamed with another important protocol: the Transmission Control Protocol (TCP). TCP and IP were two of the first networking protocols defined in the set of Internet protocols. They are important in the CIP Standards due to their widespread use, IP's support of routing, and their well-understood and publicized vulnerabilities.

J. **NERC.** Corporation made up of 10 regional councils and monitors all participating utilities located in the geographic areas of Canada, the U.S., and a small portion of the Baja California Norte, Mexico. Its mission is to ensure that the bulk electric system in North America is reliable, adequate and secure.

K. **Network.** A network is a collection of terminals, computers, servers, and components which allows for the easy flow of data and the use and sharing of resources between those components.

L. **PLC**. A device used to automate monitoring and control of industrial plants and factory automation. Can be used stand-alone or in conjunction with a SCADA or other system.

M. **Protection System**. Protective relays, associated communications systems, voltage and current sensing devices, station batteries and direct current control circuitry.

N. **PSP**. The physical, completely enclosed (”six wall”) border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which CCAs are housed and for which access is controlled.

O. **RMSS**. Reclamation’s wide-area administrative network supporting email, office applications, and other business and mission support software.

P. **RTU**. In SCADA systems, an RTU is a device installed at the remote location that collects data, codes the data into a format that is transmittable, and transmits the data to a center station or master. An RTU also collects information from the master device and implements processes that are directed by the master. RTUs are equipped with input channel for sensing or metering, output channels for control, indication or alarms and a communication port.

Q. **SCADA**. A cyber-based system of remote control and telemetry used to monitor and control the transmission system or a generation facility and related resources.

R. **SONET**. A standard for connecting fiber-optic transmission systems. SONET defines interface standards at the physical layer of the Open Systems Interconnection seven-layer-model. The standard defines a hierarchy of interface rates that all data streams at different rates to be multiplexed. SONET establishes Optical Carrier (i.e., OC) levels from 51.8 Mbps (OC-1) to 9.95 Gbps (OC-192).

S. **WECC**. Council formed on April 18, 2002, from the merger of the Western Systems Coordinating Council (i.e., WSCC), the Southwest Regional Transmission Association (i.e., SWRTA), and Western Regional Transmission Association (i.e., WRTA). WECC is one of eight regional electric reliability councils under NERC authority.