Final New Critical Infrastructure Protection Alberta Reliability Standards Terms and Definitions to be included in the *Consolidated Authoritative Document Glossary*

Effective October 1, 2017

Terms and definitions to be added to the *Consolidated Authoritative Document Glossary* for use in the Critical Infrastructure Protection Alberta Reliability Standards:

"adverse reliability impact" means the impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the **Interconnection**.

"BES cyber asset" means a **cyber asset** that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the **bulk electric system**. Redundancy of affected facilities, systems, and equipment shall not be considered when determining adverse impact. Each **BES cyber asset** is included in one or more **BES cyber systems**. (A **cyber asset** is not a **BES cyber asset** if, for 30 consecutive **days** or less, it is directly connected to a network within an **electronic security perimeter**, a **cyber asset** within an **electronic security perimeter**, or to a **BES cyber asset**, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.)

"BES cyber system" means one or more **BES cyber assets** logically grouped to perform one or more reliability tasks for a functional entity.

"BES cyber system information" means information about the **BES cyber system** that could be used to gain unauthorized access or pose a security threat to the **BES cyber system**. **BES cyber system information** does not include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to **BES cyber systems**, such as, but not limited to, device names, individual IP addresses without context, **electronic security perimeter** names, or policy statements.

"blackstart resource" means a **generating unit(s)** or **aggregated generating facility** and its associated set of equipment which has the ability to be started without support from the system or is designed to remain energized without connection to the remainder of the system, with the ability to energize a dead bus, meeting the **ISO**'s restoration plan needs for **real power** and **reactive power** capability, frequency and voltage control, and that has been included in the **ISO**'s restoration plan.

"CIP exceptional circumstance" means a situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or **bulk electric system** reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a **cyber security incident** requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

"CIP senior manager" means a single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the CIP **reliability standards**, CIP-002 through CIP-011.

"control centre" means one or more facilities hosting operating personnel that monitor and control the **bulk electric system** in real-time to perform the reliability tasks, including their associated data centres, of: 1) the **ISO**, 2) an **operator** of a **transmission facility** for **transmission facilities** at two (2) or more locations, or 3) an **operator** of a **generating unit** or an **operator** of an **aggregated generating facility** for either **generating units** or **aggregated generating facilities** at two (2) or more locations.

"cranking path" means a portion of the electric system that can be isolated and then energized to deliver electric power from a generation source to enable the startup of one or more other **generating units** or **aggregated generating facilities**.

"cyber asset" means programmable electronic devices, including the hardware, software, and data in those devices.

"cyber security incident" means a malicious act or suspicious event that:

- compromises, or was an attempt to compromise, the **electronic security perimeter** or **physical security perimeter**, or
- disrupts, or was an attempt to disrupt, the operation of a **BES cyber system**.

"dial-up connectivity" means a data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.

"electronic access control or monitoring systems" means **cyber assets** that perform electronic access control or electronic access monitoring of the **electronic security perimeter**(s) or **BES cyber systems**. This includes **intermediate systems**.

"electronic access point" means a **cyber asset** interface on an **electronic security perimeter** that allows routable communication between **cyber assets** outside an **electronic security perimeter** and **cyber assets** inside an **electronic security perimeter**.

"electronic security perimeter" means the logical border surrounding a network to which **BES cyber systems** are connected using a routable protocol.

"external routable connectivity" means the ability to access a **BES cyber system** from a **cyber asset** that is outside of its associated **electronic security perimeter** via a bi-directional routable protocol connection.

"interactive remote access" means user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a **cyber asset** that is not an **intermediate system** and not located within any of the Responsible Entity's **electronic security perimeter**(s) or at a defined **electronic access point**. Remote access may be initiated from: 1) **cyber assets** used or owned by the Responsible Entity, 2) **cyber assets** used or owned by employees, and 3) **cyber assets** used or owned by vendors, contractors, or consultants. **Interactive remote access** does not include system-to-system process communications.

Note: the "Responsible Entity" referred to in this definition is identified in the applicability section of each Version 5 CIP Cyber Security **reliability standard**.

"intermediate system" means a **cyber asset** or collection of **cyber assets** performing access control to restrict **interactive remote access** to only authorized users. The **intermediate system** must not be located inside the **electronic security perimeter**.

"physical access control systems" means **cyber assets** that control, alert, or log access to the **physical security perimeter**(s), exclusive of locally mounted hardware or devices at the **physical security perimeter** such as motion sensors, electronic lock control mechanisms, and badge readers.

"physical security perimeter" means the physical border surrounding locations in which **BES cyber assets**, **BES cyber systems**, or **electronic access control or monitoring systems** reside, and for which access is controlled.

"protected cyber assets" means one or more **cyber assets** connected using a routable protocol within or on an **electronic security perimeter** that is not part of the highest impact **BES cyber system** within the same **electronic security perimeter**. The impact rating of **protected cyber assets** is equal to the highest rated **BES cyber system** in the same **electronic security perimeter**. A **cyber asset** is not a **protected cyber asset** if, for 30 consecutive **days** or less, it is connected either to a **cyber asset** within the **electronic security perimeter** or to the network within the **electronic security perimeter**, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

"reportable cyber security incident" means a **cyber security incident** that has compromised or disrupted one or more reliability tasks of a functional entity.