NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Technical Rationale

New and Modified Terms, and Exemption Language Used in NERC Reliability Standards | Project 2016-02 Modifications to CIP Standards

Introduction

The standard drafting team (SDT) has in several terms made changes based on the intent that the glossary is a dictionary and defines what something is, not its security requirements or necessarily the scope of systems those requirements apply to. The rationale for such changes is:

- If scoping of which specific systems is included in the definition, the definition can no longer be used in other standards or other requirements with a differing scope. If what the term defines is needed in a differing requirement of a slightly different scope, either the definition must change affecting all uses of it in all standards, or we proliferate more glossary terms to include differing scopes in the definition. Removing specific scoping in definitions alleviates this concern. Several terms below now use a far more generic 'Cyber System' in the definition with the specific scoping of requirements left to those requirements in the standards.
- If implicit requirements are included in the definition (e.g., such as where in relation to an Electronic Security Perimeter (ESP) an Intermediate System must be implemented), then if an entity implements that one aspect incorrectly, that is non-conformant with a glossary term, the unintended consequence is that it may lead to non-compliance with all requirements that rely on that term. Putting any requirement-type language in requirements rather than definitions alleviates this concern.

Proposed Modified Terms:

BES Cyber Asset (BCA)

A Cyber Asset or Virtual 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 (BES). 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.

Rationale

The BCA definition was modified to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). See the VCA and Shared Cyber Infrastructure (SCI) definition below. Note that SCI is not included because if the hardware is supporting VCAs of differing impact levels, it is not a BCA with a single impact category, but it is SCI and subject to the additional "SCI only" requirements. If all the hosted VCAs are treated as "associated PCAs" of the highest impact BCS, then the underlying hardware is no longer SCI and is a BCA of the same impact rating as the highest impact BCS it hosts. The SDT also capitalized the term “Reliable Operation” to tie this to “instability, uncontrolled separation, and cascading” as that is a defined term in the NERC Glossary providing more clarity. Additionally, the glossary term uses the Bulk Power System scope, but the BCA definition uses the specific scope “Reliable Operation of the Bulk Electric System” just as the Reliability Coordinator definition does.

BES Cyber System Information (BCSI)

Information about the BES Cyber System (BCS) that could be used to gain unauthorized access or pose a security threat to the BCS. BCSI 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 BCS, such as, but not limited to, device names, individual IP addresses without context, Electronic Security Perimeter names, or policy statements. Examples of BCSI may include, but are not limited to, security procedures or security information about BCS, Shared Cyber Infrastructure, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that is not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the BCS.

Rationale

The BCSI definition was modified with conforming changes such that BCSI examples include information about SCI that could be used to gain unauthorized access or pose a security threat to the BCS.

Critical Infrastructure Protection (CIP) Senior Manager

A single senior management official with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Cyber Security Standards.

Rationale

The CIP Senior Manager definition was modified by removing explicit reference to the CIP standards as only “CIP-002 through CIP-011” since the body of CIP Cyber Security Standards has grown beyond CIP-011. For example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Assets

Programmable electronic devices, excluding Shared Cyber Infrastructure, including the hardware, software, and data in those devices. Application containers are considered software of Virtual Cyber Assets (VCA) or Cyber Assets. VCAs are not considered software or data of Cyber Assets.

Rationale

The Cyber Asset definition was modified to explicitly exclude SCI from the definition of Cyber Asset such that SCI is a different hardware class on which the other VCAs of differing impact levels execute. SCI is defined separately such that it can be the object of additional requirements based on its unique risks. The definition is also modified to clarify that ‘Application containers’ (i.e., portable, packaged applications) are considered software of a Cyber Asset (or VCA), though they may have some characteristics of a VCA (a container can be instantiated with its own IP address, etc.). This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device. Additionally, executing instances of VCAs are not to be considered simply software or data of the Cyber Asset.

Cyber Security Incident

A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System (BCS), compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, (3) an Electronic Access Control or Monitoring System, or (4) Shared Cyber Infrastructure; or
- Disrupts or attempts to disrupt the operation of a BCS.

Rationale

The Cyber Security Incident definition was modified to add SCI to the scope of compromised or attempted compromises of, the listed perimeters and systems.

Electronic Access Control or Monitoring Systems (EACMS)

Cyber System(s) that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) (ESP) or BES Cyber Systems (BCS), including those not protected by an ESP used by the Responsible Entity to convert routable protocol communications to non-routable communications to a BCS.

Rationale

The EACMS definition was modified to add Cyber Systems so that VCA and SCI are included as two other forms that an EACMS can take. Removed the explicit inclusion of Intermediate Systems as that was moved to the Intermediate Systems definition. Added the inclusion of certain protocol conversion scenarios where the protocol converter is clarified to be an EACMS. This involves a Cyber Asset that does perform electronic access control or monitoring that is also converting from a routable protocol (e.g., IP over Ethernet) to non-routable protocol (e.g., ASCII text over serial) to BCS that are themselves non-routable (serial) only. The SDT intent is this does not include “bump in the wire” type converters (i.e., IP to serial converters) that have no capability to identify users and perform electronic access control or monitoring. It does include those Cyber Assets that users login and select a serial port to then communicate with a BCS and are clearly performing electronic access control or monitoring. In this latter scenario, though the BCS itself is serial non-routable only and therefore has no ESP, the converter is still performing as an EACMS. It may also be performing as an Intermediate System for IRA to the serial only BCS (see changes to the IRA definition).

Electronic Access Point (EAP)

An electronic policy enforcement point or a Cyber Asset interface on an Electronic Access Control or Monitoring Systems that controls routable communication to and from one or more BES Cyber Systems or their associated Protected Cyber Assets.

Rationale

As network security moves deeper into the infrastructure, it’s no longer necessary to prescribe that network security be performed only at a ‘Cyber Asset interface on an ESP’ at one point on a network edge. Zero Trust, for example, highly distributes the network security model and is not perimeter-based, and this is incorporated through the addition of “electronic policy enforcement point or”. With the added flexibility in CIP-005 to adopt these models in addition to the traditional ESP model, the EAP definition was modified to allow for electronic policy enforcement points and no longer prescribes an architecture. The “one or more” and the “associated PCAs” have been added to clarify that EAPs can control communications to a group and not required per individual system.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System through its Electronic Security Perimeter via a bi-directional routable protocol connection.

Rationale

The ERC definition was modified to allow for zero trust or other network models that are not strictly perimeter or network-border based, thus not having concepts of “inside” or “outside”. These concepts are replaced with the language “through its ESP” so that it does not imply a prescriptive network security model. The ERC term is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with ERC as well as to limit the scope of requirements that would require ERC to function. The SDT is maintaining this use of ERC, but also clarifying the relationship between ERC and Interactive Remote Access (IRA) in that a non-routable, serial only BCS (thus with no ESP) may have IRA through a subsequent IP/serial conversion (see changes to IRA definition).

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol; or a logical boundary defined by one or more Electronic Access Points.

Rationale

The ESP definition was modified to provide flexibility and the use of various architectures and access control models. The traditional network border ESP remains a valid network security model, however it is no longer the only prescribed model as CIP-005 allows other access control models that are not based on network perimeters such as Zero Trust architectures. The proposed ESP definition retains its current definition but appends “or a logical boundary defined by one or more EAPs” to incorporate models that move away from implicit trust within network perimeters and using network location as a primary factor in access control decisions. In these models, the perimeter shrinks to increasingly more granular levels, potentially down to a process or resource level on a BCS. The proposed definition allows for an ESP to be (a) a border surrounding an isolated network that has no external connectivity and thus no EAPs, (b) static point(s) on a network boundary such as a traditional firewall as an EAP that is enforcing access policies or configurations (e.g., firewall rulesets), (c) many dynamic, short-lived, session-level ‘perimeters’ established at time of access that are network independent (e.g., users to resources, for example), or (d) hybrid implementations combining elements of more than one model.

The SDT has kept the ‘logical border’ concept for the “surrounding a network” ESP and used the language “logical boundary” for zero trust models. A ‘border’ does indeed surround an object, in this case a network, but a ‘boundary’ may not surround or enclose, it’s a line that can be crossed, such as a policy enforcement point controlling access to a resource. The SDT has also updated language in the standards to remove concepts such as ‘inside’ an ESP and replaced that with more inclusive phrases such as ‘protected by’ an ESP.

Interactive Remote Access (IRA)

User-initiated electronic access by a person using a bi-directional routable protocol:

- To a Cyber System protected by an Entity’s Electronic Security Perimeter(s) (ESP);
- That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System; or
- To a Management Interface.

Interactive Remote Access does not include:

- Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs;
- System-to-system process communication.

Rationale

The IRA definition was modified in two fundamental ways: (1) to incorporate IRA situations where users outside of any of the Responsible Entity’s ESPs have interactive access, using a routable protocol, to a non-routable (e.g., serial) Cyber System through a subsequent IP to serial conversion, and (2) to include Management Interfaces as targets of IRA. Note that the scope of which Cyber Systems and Management Interfaces is contained within the applicable requirements in the standards and are not in the definition. The philosophy is scoping of requirements should be in the requirements to keep the definitions usable in other requirements with a different scope if needed. The references to ownership of the remote client have been removed as they are immaterial to the definition of IRA.

The definition begins with “User-initiated electronic access by a person using a bi-directional routable protocol” to match the human interactive (bi-directional) nature of the access to the requirements that secure such access in CIP-005 R2. For example, a batch process cannot read a multi-factor token and enter its displayed code; that security control is designed for interactive humans initiating a remote access session. Also note the person is using a routable protocol to initiate the access.

The definition outlines three targets of IRA:

1) “To a Cyber System protected by an Entity’s Electronic Security Perimeter(s) (ESP)” covers the typical Cyber System that is connected to a network via a routable protocol and thus is protected by an ESP. In this instance, the remote user is using a routable protocol and is accessing a Cyber System on a routable protocol network, for example in a typical LAN-WAN-LAN, end to end routable protocol communication.
2) “That is converted by the Responsible Entity to a non-routable protocol that allows access to a Cyber System” clarifies IRA scenarios where the user is using a routable protocol to a site where the Responsible Entity then connects that session (e.g., using a gateway or terminal server) to a device’s non-routable serial port to provide interactive remote access to the user. A common example is connecting a serial port on a digital relay in a substation to a terminal server or gateway device which is then connected to a routable network in the substation for the purpose of granting a remote user interactive access to the relay without traveling to the substation. This 2nd target of the definition now clarifies this is IRA even though the device itself may not have an ESP if it is only connected serially.

   Note the clarification and explanation in the EACMS definition above that applies to this scenario. The phrase “converted *by the Responsible Entity*” clarifies certain situations that may involve more than one entity and is best described by an example. Entity 1 has a BCS in a substation or generating resource that Entity 2, a Control Center, needs to access. Entity 2 provides a circuit to Entity 1’s site and provides Entity 1 with a serial cable to connect to their BCS. This phrase clarifies that Entity 1 does not require detailed architectural knowledge of what Entity 2 does upstream with the data once delivered to the serial interface if Entity 1 does not do any conversion to routable protocols. If Entity 2 does convert to routable protocols and does provide IRA, then Entity 2 implements the IRA security controls on their routable protocol portion.
3) “To a Management Interface” adds the Management Interface as a valid target of IRA. Note the scope of Management Interfaces covered by CIP is in the CIP-005 requirements, not in the definition.

The definition then has two exclusions of scenarios that are not IRA:

1) “Communication that originates from a Cyber System protected by any of the Responsible Entity’s ESPs” carries forward this exclusion from the previous definition and is intended to exclude, for example, the scenario of a Control Center operator within one of the Responsible Entity’s ESPs interacting with field devices within its other ESPs, because for it to meet the IRA definition, IRA must originate from somewhere other than one of the Responsible Entity’s protected ESPs.
2) “System-to-system process communication” carries forward this exclusion from the previous definition to clarify that a process that cannot for instance perform multi-factor authentication using tokens or biometrics is not IRA. It is instead covered by CIP-005 R1.

Note that the definition uses the more generic term Cyber Systems. This is in keeping with using the glossary as a dictionary that merely defines a term, in this case a type of access, but does not create or scope CIP requirements within the definition. The scope is in CIP-005 R2's requirement language. The intent is to create definitions that are scope agnostic so they can be used in multiple standards or requirements with varying scope in each.

Intermediate Systems

One or more Electronic Access Control or Monitoring Systems that are used to restrict Interactive Remote Access to only authorized users.

Rationale

The Intermediate System definition was modified by removing embedded requirement language (i.e., where an Intermediate System must reside). That language moved to CIP-005 Requirement R2 within a mandatory requirement. The definition was also updated from a Cyber Asset focus to an EACMS focus to include other forms (i.e., VCA) the Intermediate System may take. This also moves the clarification of "This includes Intermediate Systems" out of the EACMS definition into this one.

Physical Access Control Systems (PACS)

Cyber Systems that control, alert, or log access to the Physical Security Perimeter(s) (PSP), exclusive of locally mounted hardware or devices at the PSP such as motion sensors, electronic lock control mechanisms, and badge readers.

Rationale

The PACS definition was modified to use the term Cyber Systems to add VCA and SCI as two other forms that a PACS can take.

Physical Security Perimeter (PSP)

The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, Shared Cyber Infrastructure, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

Rationale

The PSP definition was modified to add SCI as type of Cyber System to be included within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets (VCA) that:

- Are protected by an Electronic Security Perimeter (ESP) but are not part of the highest impact BES Cyber System (BCS) protected by the same ESP; or
- Share CPU resources or memory resources with any part of the BCS, excluding VCAs that are being actively remediated in an environment that isolates routable connectivity from BCS;

Excluding Transient Cyber Assets.

Rationale

The PCA definition was modified to ensure additional implementation scenarios in a virtualized environment that present similar risks to the BCS are accounted for through PCA protections. The PCA definition exists to identify other Cyber Assets or VCAs that must be protected by various CIP requirements due to what they share with a BES Cyber System. This sharing could allow the PCA to be a 'pivot point', a location from which to access the BCS. In the past, this sharing was limited to local network connectivity; the PCA being a network peer within the same ESP. With virtualization there is now another aspect of sharing and the PCA definition was modified to include "share CPU resources or memory resources with any part of the BCS" to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, Zenbleed, etc.) on SCI. Since virtualization can allow systems of differing trust levels to simultaneously execute on the same hypervisor servers in the hardware underlay and thus share the same CPU resources or memory resources, this addition to the PCA definition requires that those VCAs that do share CPU resources or memory resources with a BCS become associated PCA's of the BCS. This provides the high water marking of VCAs sharing a single hypervisor's CPU resources or memory resources. Affinity rules can be used within the virtualization configuration to prevent this situation and keep other VCAs of differing impact levels from becoming associated PCAs. Thus, there is no "mixed mode" allowed on the same CPU resources or memory resources.

Finally, the definition was modified to account for "remediation VLAN" automation of security controls where a VCA may instantiate in a logical network reserved for vulnerability assessment and updates (e.g., OS patches, AV updates, etc.) that limits its connectivity to only remediation resources during the remediation process. Even though it may share CPU resources or memory resources during the remediation, the intent is to exclude the VCA from becoming a PCA while temporarily in this state as its being updated prior to being connected to its production network.

Removable Media

Storage media that (i) are not Cyber Assets or Shared Cyber Infrastructure (SCI), (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, SCI, a network protected by an Electronic Security Perimeter, or a Protected Cyber Asset.

Rationale

The Removable Media definition was modified to add SCI as a target of the Removable Media connection and incorporate the new ESP definition ("protected by" rather than "within").

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System (BCS) that performs one or more reliability tasks of a functional entity;
- An Electronic Security Perimeter of a high or medium impact BCS;
- An Electronic Access Control or Monitoring System of a high or medium impact BCS; or

- Shared Cyber Infrastructure supporting a BCS.

Rationale

The Reportable Cyber security Incident definition was modified to add compromised or disrupted SCI supporting a BCS as a target.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset (VCA) that is:

1. Capable of transmitting or transferring executable code,
2. Not included in a BCS,
3. Not a Protected Cyber Asset (PCA) associated with high or medium impact BCS, and
4. Connected for 30 consecutive calendar days or less:
    - On a network within an Electronic Security Perimeter containing high or medium impact BCS; or
    - Directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
        - BES Cyber Asset;
        - Shared Cyber Infrastructure; or
        - PCA associated with high or medium impact BCS.

Virtual machines hosted on a physical Transient Cyber Asset (TCA) are treated as software on that physical TCA. Examples of TCAs include, but are not limited to, Cyber Assets or VCAs used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition was modified to add VCA as a form a TCA can take. The SDT is addressing two different transient connection scenarios.

The first scenario is a physical TCA such as a laptop. These TCAs may require older, 32-bit software and OS to connect to and configure older equipment in the field. These are often executed within VM ‘player’ environments on the physical TCA. The SDT asserts these packaged environments in an image file on a physical TCA should not be considered their own distinct virtual TCA and included the statement “Virtual machines hosted on a physical TCA are treated as software on that physical TCA” within the definition. The SDT asserts that a user that is authorized to use the physical TCA should not be required to be separately authorized to execute the software they need to use on the TCA, simply because it’s in an image file and executed in a VM “player” type environment on the TCA. The SDT also asserts that if the user ‘checks out’ a physical laptop TCA to perform a task, it should not be a standard violation if they do not also ‘check out’ any VM images residing on that physical TCA’s disk. The intent is that physical TCA is considered a ‘unit’ to perform a job and not several distinct TCAs on one laptop.

The second scenario is a more recent phenomenon where a service vendor (e.g., a pen-tester or security firm) may send an entity a VCA image (e.g., a vulnerability scanner instance) to temporarily instantiate within their virtualization environment. This VCA may only exist for a few hours and is functionally no different than the vendor bringing a physical laptop and connecting it to a physical network switch to perform the same task as a TCA. This transient VCA is not a part of the entity’s CIP program and is treated as a TCA. This also handles VCAs the entity creates for typical TCA uses but are normally dormant on the same hardware as the BCS (e.g., a VCA with Wireshark for troubleshooting network issues within a virtualized infrastructure).

Additionally, SCI was added as a target to which TCAs can be directly connected.

Proposed New Terms:

Cyber System

One or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

Rationale

The term Cyber System was defined to simplify applicability when referring in the standards or other definitions to all the forms an object may take (Cyber Asset, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards and definitions where it is used.

Management Interface

An administrative interface that:

- Controls the processes of initializing, deploying, and configuring Shared Cyber Infrastructure;
- Is an autonomous subsystem that provides access to the console independently of the host system's CPU, firmware, and operating system; or
- Configures an EAP.

Rationale

The term Management Interface was defined so that requirements are established for SCI and EACMS Management Interfaces to target the unique risks for virtualized environments presented by unrestricted access to the Management Interfaces for such environments. With ‘infrastructure as a service’ (IaaS) environments, the management consoles can not only be used to create, but also to destroy or reconfigure virtual servers, networks, switches, firewalls, etc. The term also includes interfaces commonly known as ILO (Integrated Lights Out), that can be used to remotely access the console. It also includes interfaces used to configure an EAP (such as on firewalls or a network switch that is enforcing an ESP between different virtual networks (e.g., VLANs). Note that scoping is included in requirements in the standard, not in the definition.

Shared Cyber Infrastructure (SCI)

One or more programmable electronic devices, including the software that shares the devices’ resources, that:

- Hosts one or more Virtual Cyber Assets (VCA) included in a BES Cyber System (BCS) or their associated Electronic Access Control or Monitoring Systems (EACMS) or Physical Access Control

Systems (PACS); and hosts one or more VCAs that are not included in, or associated with, BCS of the same impact categorization; or

- Provides storage resources required for system functionality of one or more Cyber Assets or VCAs included in a BCS or their associated EACMS or PACS; and also, for one or more Cyber Assets or VCAs that are not included in, or associated with, BCS of the same impact categorization.

SCI does not include the supported VCAs or Cyber Assets with which it shares its resources.

Rationale

The term SCI was defined to separate the underlying hardware from VCAs in the situation where the shared hardware resources support VCAs of varying impact levels. This allows security requirements to be targeted to SCI to address the unique risks of shared hardware. There are many requirements that now include the newly defined term SCI in the “Applicable Systems” column to maintain security level parity with traditional Cyber Assets.

Beyond security level parity with protecting a typical hardware based Cyber Asset, the SCI can have a more significant impact in a virtualized environment since it can host, and therefore impact, multiple virtualized systems of varying impact levels. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

The phrase “SCI does not include the supported VCAs or Cyber Assets with which it shares its resources” is included to clarify that, for example, electronic access to a hosted VCA by a user is not electronic access to the SCI on which it executes.

Of note is that shared network devices are not in the scope of this definition. Since network switches and firewalls share their resources by nature, this exclusion avoids pulling all network hardware into scope as SCI. However, network switches and other hardware that does enforce an ESP, such as a network switch configured to host different VLANs to which systems of differing impact levels are connected, comes into scope as an EACMS.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware, currently executing on a virtual machine hosted on a BES Cyber Asset, Electronic Access Control or Monitoring System, Physical Access Control System, Protected Cyber Asset, or Shared Cyber Infrastructure (SCI). Virtual Cyber Assets (VCAs) do not include:

- Logical instances that are being actively remediated in an environment that isolates routable connectivity from BES Cyber Systems;
- Dormant file-based images that contain operating systems or firmware; and
- SCI or Cyber Assets that host VCAs.

Application containers are considered software of VCAs or Cyber Assets.

Rationale

The term VCA was defined to allow the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined as is the case in the Cyber Asset definition. The NERC Glossary definition of Cyber Asset has a direct tie to its hardware and software ("including the hardware, software, and data in the device") and assumes the electronic device is self-contained with a one-to-one relationship between a device and its software (including the operating system). This affected the definitions of the "Applicable Systems" terms such as BCS, EACMS, PACS, and PCAs that were all based on the Cyber Asset definition. Because the Reliability Standard is applicable to the aforementioned systems, the security controls for the Cyber Assets also applies to the hardware. The one-to-one relationship between a Cyber Asset and its underlying hardware and software is what virtualization intentionally breaks to increase reliability and resiliency by allowing VCAs to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The phrase "currently executing on a virtual machine" is used to clarify:

- That a VCA does not include disk image files that are not currently instantiated or executing and are thus providing no functions or services.
- That a "logical instance of an operating system or firmware" only refers to those running on a hypervisor as a virtual machine and does not refer to a locally installed OS or firmware on the hardware.

The definition excludes "logical instances that are being actively remediated…" to allow for automated solutions (such as remediation VLANs) to bring newly instantiated instances into compliance in an isolated environment before they are moved to production networks and begin providing their function or service, at which point they become a VCA.

The phrase "hosted on a BCA, EACMS, PACS, PCA, or SCI" is to clarify that an entity for an "all-in" scenario can still classify the underlying hardware as one or several of these types, yet the VCAs remain their own object subject to requirements and are not simply "software in the device" as in the Cyber Asset definition.

Examples of VCAs may include, but are not limited to, logical instances of the following:

- Operating Systems (Virtual Machines (VM));
- Networking devices such as switches, routers, and load balancers;
- Security appliances such as firewalls and VPN concentrators; and
- Helper appliances with logical connectivity (such as malware detection, plugins, etc.).

The definition also clarifies that 'Application containers' (i.e., portable, packaged applications) are considered software of a VCA or Cyber Asset, though they may have some characteristics of a VCA. This is because of their packaged quality, typically being updated as a whole and not as individual components, and the limited capabilities that containers have. When viewing applications containers as something to apply CIP Requirements to, the concept breaks down quickly due to the nature of container platforms. Additionally, the capabilities that containers do possess, that would offer services on a network for example, would then exist on the VCA or Cyber Asset that the container is running on and can be controlled as part of the required set of controls for that device.

Technical Rationale for Exemptions Section:

Rationale for Exemption 4.2.3.1

The term ‘Cyber Assets’ was replaced with the new proposed term ‘Cyber Systems’. Rather than changing this language to a list of all possible forms (Cyber Assets, VCAs, or SCI) as the object of the exemption, the SDT chose to instead use the existing language in the 4.2.3.4 and 4.2.3.5 exemptions such that all five exemptions use a form of ‘systems’ as their object.

Rationale for Exemption 4.2.3.2 and 4.2.3.3

In 4.2.3.2, the term ‘Cyber Assets’ was replaced with the new proposed term ‘Cyber Systems’ which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, VCAs, or SCI), the SDT chose to define a new term that incorporates all forms and use it within the multiple exemptions and at other points within the standards.

For 4.2.3.3, the ability to move workloads or VMs seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESPs at each discrete site (e.g., a layer 2 adjacency across the sites). A “Super ESP” as it has been historically known is created across the sites and thus an exemption based on having a discrete layer 3 ESP at each site no longer works to exclude, for example, the network transport equipment that may belong to carriers. The SDT included the 4.2.3.3 exemption to further clarify this scenario. Responsible Entities should notice the exemption uses the word “between” – when extending an ESP between geographic locations, CIP-005 requires the confidentiality and integrity protection of the data (typically through encryption) between the relevant PSPs. This exemption then covers the related Cyber Systems “between” those encryption points but does not exclude the endpoints performing the encryption.