NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2016-02 Modification to CIP Standards

Definitions and Exemptions Technical Rationale

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. 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 is changing to allow for BCA to be either Cyber Assets (hardware included) or Virtual Cyber Assets (VCA) (software only virtual machines without the underlying hardware). The definition of BCA excludes the underlying hardware for virtualized environments, now defined as Shared Cyber Infrastructure (SCI). The standards drafting team (SDT) recognizes that SCI indeed has the same impact as a virtual BCA and even more so if hosting numerous BCA, and those risks will be addressed in requirements specifically for the SCI. See the VCA and SCI definition below.

BES Cyber System (BCS)

No proposed change to definition, only addition of BCS acronym to the NERC Glossary.

Rationale

In order to shorten several applicability statements within the body of CIP standards, the SDT proposes that "BCS" be added as the defined acronym for "BES Cyber System" to the NERC glossary.

BES Cyber System Information (BCSI)

Information about the BES Cyber System or Shared Cyber Infrastructure 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, or policy statements. Examples of BES Cyber System Information may include, but are not limited to, security procedures or security information about BES Cyber Systems, 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 BES Cyber System

Rationale

Conforming changes such that BCSI includes information about SCI.

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 Critical Infrastructure Protection Standards.

Rationale
Remove explicit reference to the CIP standards as only "CIP-002 through CIP-011" as the body of CIP standards has grown beyond CIP-011. As an example, the CIP Senior Manager also has requirements within CIP-013.

Cyber Asset
Programmable electronic devices, including the hardware, software, and data in those devices; excluding Shared Cyber Infrastructure.

Rationale
Modified to explicitly exclude SCI from the definition of CA such that SCI and CA are two hardware 'forms' on which the other types of cyber systems reside. SCI is another form of 'programmable electronic device' that does NOT include the software and data in the hardware device. SCI is defined separately such that it can be the object of additional requirements based on its unique risks.

Cyber Security Incident
A malicious act or suspicious event that:

- For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) the logical isolation, (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 BES Cyber System

Rationale
Modified to refer to logical isolation instead of ESPs as well as add SCI to the scope of compromised or attempted compromise systems.

Electronic Access Control or Monitoring Systems (EACMS)
Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure that perform electronic access control or electronic access monitoring of the logical isolation of BES Cyber Systems. This includes Intermediate Systems.

Rationale
Modified to add VCA and SCI as two other forms that an EACMS can take. Changed the reference to ESP to 'logical isolation'.

External Routable Connectivity (ERC)

The ability to access a BES Cyber System or Shared Cyber Infrastructure from a Cyber Asset or Virtual Cyber Asset through an Electronic Access Control or Monitoring System controlling communications to and from the BES Cyber System via a bi-directional routable protocol connection.

Rationale

The ERC definition is used throughout the CIP Standards within the Applicable Systems column as a scoping mechanism based on the inherent risk associated with external routable connectivity. In order to maintain the correct ERC scoping the SDT made conforming changes only to the ERC definition. The definition was modified to include Virtual Cyber Assets as potential remote clients, added SCI as potential targets, and replaced the ESP as the only model with the more generic "through an EACMS controlling communications…" that allows non-perimeter-based models.

Interactive Remote Access (IRA)

User-initiated access by a person employing a remote access client from outside of the asset containing the system being accessed or outside of the logical isolation of the system being accessed.

Rationale

The IRA definition is changing to remove its dependency on ESP and remove several requirements and scoping mechanisms that were embedded within it resulting in a simpler definition. The requirements and scoping mechanisms have been moved into CIP-005 R2. The references to ownership of the remote client have been removed as immaterial to the CIP-005 requirements. The reliance on "using a routable protocol" has been removed to incorporate serial non-routable target Cyber Assets that are converted to routable protocols (serial to IP converters) and therefore have the same IRA capability as native routable protocol target Cyber Assets. This clarification was one of the issues from the V5TAG effort the SDT is to address. The "from outside of the asset containing the system being accessed" was added to clarify that local TCA connections even if using a 'remote access client' are not IRA. The "outside of the logical isolation" was used to allow for non-perimeter-based network models, replacing ESP as the only option.

Intermediate Systems (IS)

A type of Electronic Access Control or Monitoring System that is used to restrict Interactive Remote Access.

Rationale

The IS definition is changing to remove requirement language (e.g. where an IS must reside and how it must control IRA) that was embedded within the definition. Such language has been moved to CIP-005 R2 so that it is a mandatory requirement.

Physical Access Control Systems (PACS)

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

Rationale

This definition is changing to allow Virtual Cyber Assets or SCI as a form 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 is changing to add SCI as type of device which must be within a PSP.

Protected Cyber Asset (PCA)

One or more Cyber Assets or Virtual Cyber Assets that:

- Are not logically isolated from a BES Cyber System; or
- Share CPU or memory with a BES Cyber System; excluding Shared Cyber Infrastructure,

excluding logically isolated Cyber Assets or Virtual Cyber Assets that are being actively remediated prior to introduction to the production environment.

Rationale

The PCA definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation. It is also being updated to include "share compute resources (CPU or memory) with a BES Cyber System" to mitigate the risks of hardware-based vulnerabilities (Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure for any virtual machines allowed to run on the same hardware as BES Cyber Systems. 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 and memory, this addition to the PCA definition requires that those VCAs that do share CPU and memory become associated PCA's of any BES Cyber Systems sharing the same hypervisor compute resources. This provides the high water marking of VCAs sharing a single hypervisor's CPU or memory. Affinity rules can be used within the environment to prevent this situation and keep other virtual machines from becoming PCAs. Finally, the definition is being 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 (OS patches, AV updates, etc.). The intent is the VM does not become a PCA while 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, (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, Shared Cyber Infrastructure, or a network that is not logically isolated from high or medium impact BES Cyber Systems.

Rationale

The Removable Media definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation as well as adding SCI as a target of the Removable Media connection.

Reportable Cyber Security Incident

A Cyber Security Incident that compromised or disrupted:

- A BES Cyber System that performs one or more reliability tasks of a functional entity;

- The logical isolation of a high or medium impact BES Cyber System;
- An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System; or
- Shared Cyber Infrastructure of a high or medium impact BES Cyber System.

Rationale

This definition is being modified to remove the dependency on ESP and allow for other methods of logical isolation as well as adding SCI as a target of an incident.

Transient Cyber Asset (TCA)

A Cyber Asset or Virtual Cyber Asset that is:

1. capable of transmitting or transferring executable code,
2. not included in a BES Cyber System,
3. not a Shared Cyber Infrastructure associated with high or medium impact BES Cyber Systems,
4. not a Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
5. directly connected (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) for 30 consecutive calendar days or less to a:
   - BES Cyber Asset,
   - Shared Cyber Infrastructure,
   - Network that is not logically isolated from high or medium impact BES Cyber Systems, or
   - Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Examples of Transient Cyber Assets include, but are not limited to, Cyber Assets or Virtual Cyber Assets used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.

Rationale

The TCA definition is being updated to remove the dependency on ESP and allow for other methods of logical isolation, as well as adding VCA as a form a TCA can take (and excluding the SCI on which the virtual TCA executes). The intent is to handle VCAs that are created for typical TCA uses but are normally dormant (e.g. a Virtual Machine (VM) with Wireshark for troubleshooting network issues within a virtualized infrastructure). Additionally, SCI was added as a target to which TCA's can be directly connected.

Proposed New Terms

Management Interface

A physical or logical interface of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities.

Rationale

This term is being defined so that requirements can be addressed to SCI and EACMS Management Interfaces. For example, if a network switch is enforcing logical isolation between different logical networks (such as VLANs), it is an EACMS and its Management Interface must be protected (e.g. CIP-005 Requirement R1 Part 1.2)

Management Module
An autonomous subsystem of a Cyber Asset or Shared Cyber Infrastructure that provides management and monitoring capabilities independently of the host system's CPU, firmware, and operating system.

Rationale
Management Modules, also known as ILO (Integrated Lights Out), are a type of Management System that can be used to remotely manage hardware (usually including power on/off, remote console access, etc.). This term is being defined such that it can be excluded from the definition of Management System and addressed directly with a requirement (CIP-005 R1.5) to protect access to the Management Interface of the Management Module and to deny access from hosted BES Cyber Systems (tenants) to the Management Module capability of the SCI on which it depends.

Management Systems
Any combination of Cyber Assets or Virtual Cyber Assets that establish and maintain the integrity of Cyber Assets or Virtual Cyber Assets, through control of the processes for initializing, deploying and configuring those assets and systems; excluding Management Modules.

Rationale
This term is being introduced to target the unique risk for virtualized environments presented by the management 'consoles' 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. This intent is to define that capability and then include this within the definition of SCI.

Self-Contained Application (SCA)
Immutable software binaries containing operating system dependencies and application software packaged to execute in an isolated environment.

Rationale
With the advent of application containers and container orchestration platforms, this definition is being created so that containers and their unique attributes can be addressed in CIP-010 for change management.

Shared Cyber Infrastructure (SCI)
One or more programmable electronic devices (excluding Management Modules) and their software that share their CPU, memory, or storage resources with one or more BES Cyber Systems or their associated Electronic Access Control or Monitoring Systems, Physical Access Control Systems, and Protected Cyber Assets; including Management Systems used to initialize, deploy, or configure the Shared Cyber Infrastructure.

Rationale
The SCI definition is being created to separate the underlying hardware from the VCAs that it hosts. This allows security requirements to be targeted to SCI to address the unique risks of virtualization and 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. Because of this capability, some additional controls only apply to SCI, such as the management plane isolation required by the proposed CIP-005 R1.5. Addressing these unique risks requires separation of the hardware underlay into a separate definition.

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 perform logical isolation (such as a network switch configured to logical isolate different VLANs) comes into scope as an EACMS as well and falls under CIP-005 R1.5.

Virtual Cyber Asset (VCA)

A logical instance of an operating system or firmware hosted on Shared Cyber Infrastructure or a Cyber Asset.

Rationale

The NERC Glossary definition of Cyber Asset has a direct tie to the hardware on which it relied. This affected the definitions of the "Applicable Systems" terms such as BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (PCAs). Because the Reliability Standard is applicable to the aforementioned systems, the control for the Cyber Assets also applies to the hardware. This one-to-one relationship between a Cyber Asset and its underlying hardware is what virtualization intentionally breaks to increase reliability and resiliency by allowing Virtual Cyber Assets to be abstracted from the hardware and therefore able move to any available hardware out of a pool of resources.

The proposed NERC Glossary definition of Virtual Cyber Asset (VCA) allows the tie between a specific piece of hardware and the related applicable systems to no longer be singularly defined. The definition of VCA is not inclusive of hardware, and other related definitions (EACMS, PACS, PCA, TCA, etc.) have been updated to allow for VCA versions. With the addition of SCI and revisions to the "Applicable Systems", there can be one or more virtualized instances (each a VCA) of a BCA, EACMS, PACS or PCA that reside on SCI.

Examples of Virtual Cyber Assets 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.).

Proposed Retired Terms

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable Protocol.

Rationale

The Electronic Security Perimeter, while still a valid network security model, is no longer the only prescribed model as CIP-005 now allows other non-perimeter based models in its "logical isolation" paradigm. As such, the glossary term ESP is no longer used within the standard and will move to the inactive section of the NERC glossary. Entities are free to continue use of the term since ESP's remain a valid method to logically isolate BES Cyber System.

Electronic Access Point (EAP)

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.

Rationale

In addition to the rationale for the retirement of ESP, as network security moves deeper into the infrastructure, its no longer necessary to prescribe that network security be performed on 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. With the added flexibility in CIP-005 to adopt these models in place of the traditional ESP model, the term EAP is no longer prescribed or used within the standards. Entities are free to continue to use the term as it will move to the inactive section of the NERC Glossary.

Proposed Retired Terms

Electronic Security Perimeter (ESP)

The logical border surrounding a network to which BES Cyber Systems are connected using a routable Protocol.

Rationale

The Electronic Security Perimeter, while still a valid network security model, is no longer the only prescribed model as CIP-005 now allows other non-perimeter based models in its "logical isolation" paradigm. As such, the glossary term ESP is no longer used within the standard and will move to the inactive section of the NERC glossary. Entities are free to continue use of the term since ESP's remain a valid method to logically isolate BES Cyber System.

Electronic Access Point (EAP)

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.

Rationale

In addition to the rationale for the retirement of ESP, as network security moves deeper into the infrastructure, its no longer necessary to prescribe that network security be performed on 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. With the added flexibility in CIP-005 to adopt these models in place of the traditional ESP model, the term EAP is no longer prescribed or used within the

standards. Entities are free to continue to use the term as it will move to the inactive section of the NERC Glossary.

Technical Rationale for Exemptions Section

Rationale for Exemption 4.2.3.1

The term 'Cyber Assets' was changed to 'Cyber systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) 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 '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 changed to 'Cyber systems'. Rather than changing this language to a list of all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure) 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 'systems' as their object.
In previous versions of the CIP standards, Cyber Assets associated with communication networks and data communication links between discrete ESP's were exempt from the scope of the standards. There are two issues raised by virtualization technologies with this exemption:

1. Perimeter-based network security models are no longer the only model available
2. The ability to move workloads or VM's seamlessly across different sites for increased resiliency can require different sites to be connected without layer 3 ESP's at each discrete site but with layer 2 adjacency across the sites. In other words, a "Super ESP" as its 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 belonging to carriers.

The concept of logical isolation in CIP-005 addresses these issues. First, it allows for models other than the perimeter-based model (such as Zero Trust) and it allows for cyber systems associated with the communication links that are logically isolated from the BES Cyber Systems or the Shared Cyber Infrastructure (SCI) to still meet this exemption. A companion requirement has been added to CIP-005-8 (Requirement 1 Part 1.3) to require protecting the data traversing these links that can't be logically isolated, such as these layer 2 adjacency situations between sites.

Exemption 4.2.3.3 can be viewed as a particular scenario under 4.2.3.2. The SDT is including it to further clarify what is known as the "Super ESP" scenario. Responsible Entities should notice the definition uses the word "between" – when extending logical isolation or a "Super ESP" between geographic locations, CIP-005 requires the protection of the data (typically through encryption) between the relevant PSPs. This exemption will then exempt the related cyber systems "between" those encryption points but does not exclude the endpoints performing the encryption.