

# Technical Rationale

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

### 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). See the VCA and Shared Cyber Infrastructure (SCI) definition below.

#### **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, ESP names, 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 Assets**

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

### ***Rationale***

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. 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, 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 BES Cyber System.

### ***Rationale***

Modified to 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 Electronic Security Perimeter(s) or BES Cyber Systems or Shared Cyber Infrastructure. This includes Intermediate Systems.

### ***Rationale***

Modified to add VCA and SCI as two other forms that an EACMS can take and add SCI as an object of the access control or monitoring.

### **Electronic Access Point (EAP)**

An electronic policy enforcement point or a Cyber Asset interface on an EACMS that controls routable communication to and from one or more BES Cyber Systems and their associated PCAs.

### ***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 Electronic Security Perimeter (ESP) model, the term EAP is being 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 ESP via a bi-directional routable protocol connection.

### ***Rationale***

The ERC definition is changing 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 External Routable Connectivity 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)**

A 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 EAPs.

### ***Rationale***

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 both.

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 routable protocol:

- To a Cyber System protected by an Electronic Security Perimeter (ESP);
- That is converted by the Responsible Entity to a non-routable protocol to a Cyber System; or
- To a Management Interface of Shared Cyber Infrastructure.

Interactive Remote Access does not include:

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

### ***Rationale***

The proposed IRA definition changes 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 the Management Interfaces of SCI as targets of IRA. 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 routable protocol” to match the human interactive 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 Electronic Security Perimeter (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 to a Cyber System” clarifies as 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 2<sup>nd</sup> 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.

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 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 of Shared Cyber Infrastructure” adds the Management Interface of an SCI as a valid target of IRA.

The definition then has three 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 previous definitions 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 originates from somewhere other than one of the Responsible Entity’s protected ESPs.
- 2) “Communication that originates from an Intermediate System” prevents the ‘hall of mirrors’ situation where an Intermediate System would need its own Intermediate System, ad infinitum.
- 3) “System-to-system process communication” carries forward this exclusion from previous definitions to clarify that a process that cannot for instance perform multi-factor authentication using tokens or biometrics is not IRA.

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 of access that requires an Intermediate System is in CIP-005 R2’s requirement language.

### **Intermediate Systems**

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

### ***Rationale***

This definition is changing to remove requirement language (i.e., where an Intermediate System must reside) embedded within the definition. That language has been moved to CIP-005 Requirement R2 Part 2.6.2 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.

### **Physical Access Control Systems (PACS)**

Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure (SCI) 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***

Modified 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 is changing to add SCI as type of device to be included within a PSP.

### **Protected Cyber Asset (PCA)**

One or more Cyber Assets or Virtual Cyber Assets that:

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

Excluding TCAs.

### ***Rationale***

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 is being updated to include "share CPU or memory resources with any part of the BES Cyber System" to mitigate the risks of hardware-based vulnerabilities (e.g., Spectre, Meltdown, Rowhammer, etc.) on Shared Cyber Infrastructure. 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 resources, this addition to the PCA definition requires that those

VCAs that do share CPU and 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 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. 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.) that isolates its connectivity during the remediation process. Even though it may share CPU/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, (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, a network protected by an ESP, or a Protected Cyber Asset.

#### *Rationale*

The Removable Media definition is being updated to add SCI as a target of the Removable Media connection and incorporate the new ESP definition.

### **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;
- An Electronic Security Perimeter 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 supporting a BES Cyber System.

#### *Rationale*

This definition is being modified to add compromised or disrupted SCI supporting a BCS as a target.

### **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 Protected Cyber Asset (PCA) associated with high or medium impact BES Cyber Systems, and
4. connected for 30 consecutive calendar days or less:
  - a. to a network within an Electronic Security Perimeter containing high or medium impact BES Cyber Systems, or

- b. directly (e.g., using Ethernet, serial, Universal Serial Bus, or wireless including near field or Bluetooth communication) to a:
  - i. BES Cyber Asset,
  - ii. Shared Cyber Infrastructure, or
  - iii. Protected Cyber Asset associated with high or medium impact BES Cyber Systems.

Virtual machines hosted on a physical TCA are treated as software on that physical TCA. 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 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 TCA's 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." 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 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. Corresponding clarifications have been made to the methods in CIP-003 and CIP-010 used to mitigate the risks of TCA software.

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 TCA's can be directly connected.



## Proposed New Terms:

### **Cyber System**

A group of one or more Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure.

#### *Rationale*

This proposed new term is used to simplify applicability when referring in the standards or other definitions to all the forms an object may take (CA, VCA, or SCI). If other forms are needed in the future, their addition to this one definition can reduce needed edits throughout the standards.

### **Management Interface**

An administrative interface that:

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

#### *Rationale*

This term is being defined so that requirements can be addressed to 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 ESP (such as on firewalls or a network switch that is enforcing an ESP between different logical networks (e.g., VLANs).

### **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 VCA or Cyber Assets with which it shares its resources.

### ***Rationale***

The SCI definition is being created 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 VCA 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. 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 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 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 BES Cyber Systems (BCS), EACMS, PACS, and Protected Cyber Assets (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 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 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. Likewise, 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 “on a virtual machine” is used to clarify that a dedicated, non-virtualized Cyber Asset may have a ‘logical instance of an Operating System (OS) or firmware’, but that is not a VCA, only a logical instance of an OS or firewall on a virtual machine is 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 VCA’s remain their own object subject to requirements and are not simply “software in the device” as in the Cyber Asset definition.

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:  
None**

**Technical Rationale for Exemptions Section:**

**Rationale for Exemption 4.2.3.1**

The term ‘Cyber Assets’ was changed to the new proposed term ‘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 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 changed to ‘Cyber Systems’ which is a new proposed glossary addition. Rather than changing these two exemptions to list all possible forms (Cyber Assets, Virtual Cyber Assets, or Shared Cyber Infrastructure), 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 VM's seamlessly across different sites for increased resiliency can require different sites to be connected as a flat network without layer 3 ESP's at each discrete site (e.g., a layer 2 adjacency across the sites). A "Super ESP" as it's 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 is including 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.