# Shared Ownership of Bulk Electric System Facilities

## Critical Infrastructure Protection Committee

## Implementation Guidance October 10, 2017

## 1 Introduction

The Critical Infrastructure Protection Committee (CIPC) developed this document to provide implementation guidance for CIP Reliability Standard CIP-002-5.1a. This document is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing reliability standards nor provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other ways to fulfill the obligations of the requirements that are not expressed within this document.

### 1.1 Background

The CIP Reliability Standards provide the criteria that applicable Responsible Entities can use to identify BES Cyber Systems that would impact the reliable operation of the Bulk Electric System (BES) Cyber Systems (BCS). For many Responsible Entities, BCS are located in a facility that is shared with one or more other Responsible Entities. The CIP Reliability Standards do not address security measures and control mechanisms that specifically address circumstances where multiple entities share common facilities.

### 1.2 Scope

A Responsible Entity that owns BES Cyber Systems is required to implement protective measures; this implementation guidance provides examples for addressing compliance responsibilities in situations when a BCS is located in a facility/location that the system owner does not own or manage. All parties must agree on the responsibility and accountability for protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. This implementation guidance is not intended to explain how to physically secure an asset boundary nor to describe electronic security measures that can be used to protect BES Cyber System(s).

The specific objectives are:

- Provide a common understanding of the challenges surrounding shared facilities relating to CIP Reliability Standards and compliance.
- Provide suggested solutions to some of the issues related to these challenges, specifically focused on ways to meet compliance obligations through joint agreements between entities.

## 1.3 Definitions

The following definitions are provided to convey a common understanding of terms that are used in this document:

| | |
|---|---|
| **Joint ownership** | Joint ownership implies more than one owner of a specific thing (e.g. asset, Facility, Element, land, fence, control building, RTU). It can be expressed as a percentage (i.e. Entity A 55% owner and Entity B 45% owner). |
| **Shared facility** | A shared facility is a location containing BES equipment where two or more entities/utilities claim ownership of either a physical building, parcel of land, or devices inside the property line of the location. |
| **Shared ownership** | Shared ownership implies more than one owner of things within a given container (e.g. Facility, asset, fence, control building, rack). |
| **Tenant** | An entity with ownership of a piece of equipment in an asset or Facility they do not own. |

# 2 Ownership Issues

The following topics should be considered by any Registered Entity that owns equipment in a shared physical space with another entity/utility. Note that the other entity may not be a Registered Entity – this is covered under Section 3.1.5.

## 2.1 Shared physical security

For shared facilities where more than one entity is responsible for security or where the shared facility has areas where each entity may be responsible for security, the coordination of security might best be handled by a committee or other named individuals designated by a formal agreement. Joint ownership agreements typically contain provisions for the structure of a committee to coordinate activities. Each member who has equipment in the facility should participate in the committee.

The committee needs to ensure that highest level of security of one entity is not compromised by the security of others. The committee should appoint one entity as the head of security for the facility. The head of security will be responsible to make sure that all entities are following the security procedures for the facility in total.

If possible, assign responsibility for compliance with physical security standards to a single entity. A Compliance Enforcement Authority (CEA) evaluates each Physical Security Perimeter (PSP) according to the requirements of the standard; thus, a PSP with multiple owners would mean each owner is required to demonstrate compliance with the standards.

There are a number of different ways shared facility ownership can exist. Depending on the relationships with the other entities involved, an agreement will likely need to take into account each situation and address them on a case-by-case basis. Some examples of the various ways the ownership can vary are:

- Shared relationship: When shared facility ownership is equally split, a contract typically is used to describe the determination of an action on the asset and the land that it utilizes. That contract should determine the appropriate action to resolve a conflict between two entities. Each entity will have to follow the policy and procedures as adopted by their joint use contract to determine how to apply the CIP standards.

- Majority and Minority Owners: For entities that have a shared facility that has one entity as a majority owner and the other as a minority owner, the majority owner's policy and procedure usually dictates unless the contract between the owners states differently. The minority owner will have to follow the procedures as outlined as set by the contract or the majority owner.

- More than two owners: For land/asset owners that involve more than two parties, the ownership contract may contain a voting structure to allow certain decisions by majority votes and other decisions by super majority vote. It is possible that the efforts to determine responsibility of policy and procedures to meet a NERC standard is not fully defined in a land/asset agreement, especially if the agreement predates the NERC CIP standards. An ownership contract typically defines a method for discussion on items not clearly stated in the agreement. The entities will have to get together and find common ground on how to handle the coordination of the responsibility.

  Land ownership and asset ownership not equal: With some joint facilities, the ownership percentage of the land may not equal the ownership of the facilities. For example, a power plant substation might contain breaker(s) that are jointly owned and that connect the plant to the electrical grid. The substation may have multiple lines and breakers that belong to one entity as part of its BES assets. What can further complicate this arrangement is if some of the equipment in the transmission substation meet the criteria of one NERC standard but the jointly owned equipment does not qualify under that NERC standard. In this situation, the entity that owns the breaker but has no ownership of land will find that he has equipment located in an area that has equipment governed by NERC standards not applicable to that entity's asset. This situation is further discussed in other sections in this document.

- Easements and Licenses: One Registered Entity may be operating a generating or transmission station on an easement granted by another Registered Entity that has a generating or

transmission station adjacent to the other Entity's station(s). Easements and licenses may need to be revised to consider physical protection changes, such as modified fences.

## 2.2 Shared devices

While the CIP Reliability Standards provide bright-line criteria for categorizing BCS, it can be difficult for entities to recognize that another entity's equipment may impact their compliance obligations. Depending on the methodology used, data provided by one entity's RTU may be used by another entity for reliable operation(s) of the BES. These situations can create a conflict if "Entity A" identifies the information as a component of their own situational awareness. In these types of cases, the entities should reach an agreement about how the device will be afforded protections for any applicable requirements. The details of this agreement should be handled in an MOU (memorandum of understanding) or other such arrangement as outlined in the "Types of Agreements" section.

There may be other examples where multiple entities share the same device, or information from the same device, such as a tie line meter, and the owner of the device has identified it as a BES Cyber Asset (BCA). This situation is common where one entity is the registered Transmission Owner (TO) owning the equipment while a different entity is the registered Transmission Operator (TOP) responsible for its operation. It is very important that all equipment and ports used to operate the device (in the case of a digital relay) are only available to the TOP including the ability to program the device. All communication paths should be identified. If the TO is also the owner of the substation/facility, it would likely be the case that they would be the lead for physical security as well. However, if the TOP has medium impact BES Cyber Systems in the substation/facility and the TO does not, the TOP would need to make sure the additional CIP standards that apply to medium impact (or medium impact with External Routable Connectivity (ERC)) BES Cyber Systems have been addressed in the MOU. Documentation of how these shared devices are used and who/where control is allowed from is vitally important to supply as audit evidence. Any non-TOP entity needs to take extra care to ensure they do not have the ability to control from any port(s) they might use for monitoring.

# 3 Implementation Guidance

## 3.1 CIP Impact Levels

### *3.1.1* Medium, Low, Medium/Low and CIP-014

Transmission stations and substations identified and protected under the NERC Reliability Standard CIP-014 - Physical Security present additional considerations. The protection of those transmission assets take precedent in a multi-owner mixed impact environment.

The entity identifying the transmission asset through the risk assessment should take the lead acting as the head of security for the transmission asset. In cases in which multiple entities have identified the

asset, an agreement should be entered in which one entity is designated as the lead. The lead entity should notify the other owners or tenants as allowed by the entity's information protection constraints and on a need to know basis.

An evaluation should be done to determine whether the other owners and tenants can be moved out of the asset. Strategies such as change of ownership, relocating equipment or providing additional physical protections (e.g. fencing or secured dividers) may be considered. It may be determined due to safety, reliability or economic considerations, the other equipment cannot be moved. In those cases, the other owners and tenants have a responsibility to follow the direction set by the lead entity.

The lead entity should conduct the threat and vulnerability assessment required by CIP-014 considering the other owners or tenants of the asset. The joint or Shared Ownership characteristics may be considered a unique characteristic of the asset. In some instances, the presence of another entity may provide additional physical protections by providing additional preventative, detective or corrective controls. The evaluation should recognize the trade-off between additional controls and additional risk.

The lead entity should develop the Physical Security Plan in collaboration with the other entities. Physical security controls implemented may be considered for dual purposes to provide physical security controls for other owner or tenant BES Cyber Systems regardless of impact classification. The collaboration should identify resiliency or security measures which could deter, detect, delay, assess, communicate or respond to potential physical threats.

Electronic security controls by all owners and tenants should be communicated to each other for purposes of risk identification and mitigation. Communication paths may be considered as it increases electronic threat vectors. Electronic security may be considered in the threat and vulnerability assessment as breaches may lead to kinetic affects.

Consideration should be given to operational response to physical security events. The lead entity should collaborate and disseminate expectations for operational responses to physical security events. The lead entity should consider requesting each of the owners or tenants include the lead entity in their incident response specific to the transmission asset. Response and recovery planning should be coordinated by the lead entity. All owners and tenants in a CIP-014 site should consider participating in Cyber Incident Response exercises with each other.

Special consideration should be given to evaluating unescorted physical access to the asset. The lead entity should collaborate with the owners and tenants to arrive at a risk informed decision as to whether to allow other owner and tenant unescorted physical access. Factors such as the maturity of the other owner and tenants security programs, stability of workforce and experience with medium impact BCS or CIP-014 transmission assets may be considered. The extra eyes and ears may be beneficial. Conversely, additional personnel access increases the insider threat or misuse of knowledge risk. If other owner or tenants are allowed unescorted physical access, consideration should be given

to training and exercises to ensure a shared understanding of the physical security plan as allowed by information protection constraints.

It is also important to consider the confidentiality and information protection aspects of a CIP-014 site. In order to effectuate this consideration, entities sharing a CIP-014 site should consider executing non-disclosure agreements between the parties if any sensitive information is shared as a precautionary measure.

### *3.1.2 Medium/Medium*

For entities that both have medium impact BES Cyber Systems in a location, it can be a slightly harder situation compared to low, or if the BES Cyber Systems are medium impact with External Routable Connectivity (ERC), it can be a much bigger task to deal with. For BES Cyber Systems without ERC, there are a few additional standards that should be included in the consideration of the MOU, but will generally be handled by the BES Cyber System owner and not necessarily impactful to all parties in the shared facility. The entity that does not have ERC to their BES Cyber Assets should obtain or produce network diagrams showing how the ERC enters the shared facility, and the boundaries of their equipment in order to assist the ERO[1] during audits.

For shared facilities that contain medium impact BES Cyber Systems with ERC, there can be a few situations that need to be addressed. The most simple would be a single entity that has medium impact with ERC BES Cyber Systems, with the others in the shared facility not owning medium impact with ERC BES Cyber Systems. In this situation, the entity with the medium impact with ERC BES Cyber Systems should be the one in charge of all physical security at the facility, or their equipment should be physically isolated or separated from the rest of the facility so they can control all physical access to their BES Cyber Systems and associated devices. Because the entity with medium impact with ERC BES Cyber Systems has so many more requirements to comply with, they can process other entity's staff/contractors by escorting or providing PRA's as they see fit. The best scenario would be to isolate the equipment, however. This way it keeps the burden of maintenance required by other parties off of the entity with the ERC equipment. For example, if there were a long-term outage (such as a transformer replacement at a substation), this would require the entity with ERC BES Cyber Systems to either escort on a long-term basis anyone needing access into the facility, or they would have to clear the staff of another entity and agree to the terms to ensure compliance obligations are not missed. This is a difficult task to complete without errors.

For entities where multiple parties have medium impact BES Cyber Systems with ERC, physical separation of equipment/devices may be the cleanest way to maintain compliance. If this is not possible, a Compliance Enforcement Authority (CEA) will evaluate each Physical Security Perimeter (PSP) according to the requirements of the standard; thus, a PSP with multiple owners would mean each owner is required to demonstrate compliance with the standards.

### *3.1.3 Medium / Low*

Where a shared facility only contains medium without External Routable Connectivity (ERC) BES Cyber Systems, there is not a lot of change from a shared facility only containing low impact BES Cyber

[1] Electric Reliability Organization (ERO) is NERC and the eight Regional Entities

Systems. The owner of the medium impact BES Cyber Systems will have some additional requirements to comply with, but they should have minimal impact on the other entities in that same shared facility.

However, if one or more of the entities has medium impact with ERC BES Cyber Systems, the issues and concerns outlined in the "Medium/Medium" discussion above should be observed.

### *3.1.4 Low/Low*

Shared facilities with multiple entities owning low impact BES Cyber Systems is probably the most common situation. For these situations, all parties should appoint a lead entity to handle the physical security of the shared facility. This might be the majority owner of the facility itself, or it might be the entity with the majority of BES Cyber Systems in the facility. The lead entity should share their development of the physical security plan with the other entities, and an MOU or other such agreement should be reached well before the current September 1, 2018 deadline for physical security compliance.

Electronic security should be handled individually by each entity. This may not be feasible in instances where one entity may perform maintenance of BCAs as the TOP and the other entity is the owner of the BCA. In these types of instances, the electronic security should be discussed and agreed upon by both parties. All entities in the facility should also share information or diagrams regarding any network connectivity coming into the facility regardless of its direct impact on a BES Cyber Asset. This effort will assist the ERO when auditing to assure the appropriate controls have been applied to meet the electronic security plan requirements under CIP-003.

Inventories may not be required by the standard, but there should be some kind of documented process that enables the auditor to understand who has what equipment. This could be simply in the form of "All of Entity A's equipment is in Bay 1" or use of a color-coding scheme – "All of Entity A's equipment has a purple dot in the right-hand corner of the device". This way a visual inspection of the substation will indicate all devices have at least been identified. Note entities may also desire to use indications of Cyber Assets that are not BES Cyber Assets as well (a different color, for example).

### *3.1.5 Medium/Low/None*

There are some situations where the owner of the shared facility might not have any BES Cyber Assets because they don't qualify under Section 4 of CIP-002. This can be for a number of reasons, but the most common is DP registrations that don't meet the full qualifications under Section 4. In these situations, careful consideration of how an entity is going to meet the CIP requirements is paramount. For entities with medium with ERC BES Cyber Systems, sections 3.1.1 and 3.1.2 of this document outline similar concerns. The entity with the responsibility for CIP requirements should take the lead and secure access, both physical and electronic, to their equipment. If this is not possible, consideration of moving these devices to a separate area/building may be the only way to ensure compliance. If the owner of the shared facility is not required to meet CIP standards for the shared facility, it will be challenging to author an MOU sharing the compliance burden, and therefore should be thoroughly explored before any such agreement is entered into.

### 3.2 Multiple standards affecting outcome

The CIP family of standards identifies both the Functional Entities and Facilities (Section 4) that are specified explicitly for consideration. The DP providers may operate Remedial Action Schemes or Protection Systems, that exclude UFLS and UVLS, that are subject to NERC or Regional Reliability Standards, such as PRC-005.

NERC's Glossary of Terms indicates that the definition of a Protection System includes the batteries and battery chargers, and therefore these devices may need to be considered since they are covered under PRC-005. For example, NERC CIP controls may need to be applied to battery chargers with the capability of remote monitoring and/or remote control of the batteries.

### 3.3 Importance of Notification

When there are multiple entities in the same shared facility, dialog between them becomes much more important. Aside from understanding each other's equipment and processes, letting each other know when an event happens helps. For example, there could be a situation that might be easily dismissed by one entity as unimportant but it may mean more to another entity in the same shared facility. This allows each entity in the shared facility to flow events through their own Cyber Security Incident Response Plans.

Other items that can have an effect on other entities would be equipment modifications/changes, communication changes, or modifications to site physical security. For example, when bringing a routable protocol into a location that previously did not have it, or bringing in an additional one that previously was not documented may be something that all entities need to identify and possibly update their own documentation.

MOU's should outline the agreed upon ways to gain access to the location (e.g., notify Entity A's Operations Center 24 hours in advance), if these provisions are not addressed in a separate agreement such as an Interconnection Agreement.

Planning plays a big part. Adding lines can shift BES Cyber Systems at substations from low impact to medium impact (or even non-CIP to low impact). It would be courteous to think of these issues during the planning phases to notify other entities of these planned activities, even if it may not have an impact. There are already planning processes in place – NERC CIP should be included as part of those processes.

### 3.4 Types of agreements

There are a number of agreements that address the compliance obligations for entities with a shared facility. The following outlines each of the agreement types as well as the issues from a responsible entity point of view:

#### *3.4.1 Coordinated Functional Registration (CFR)*

According to the NERC ERO Registration Procedure, as of April of 2017 a CFR registration "represents an agreement between two or more Registered Entities sharing and/or splitting compliance responsibility for Requirements/sub-Requirements within particular Reliability Standard(s) applicable to a specific function."

The issue with a CFR is that it applies to an entire Requirement/sub-Requirement. In the case of many shared facilities, this would be CIP-003. The way CIP-003-6 R2 is worded, all low impact BES Cyber Systems apply to the sub-requirements of R2. So therefore if one Registered Entity wanted to take on the physical security (R 1.2.2) for CIP-003 for another Registered Entity, they would have to do so for ALL assets containing low impact BES Cyber Systems, not just a single substation. This might be satisfactory for a Registered Entity with only one substation, but that is not likely to be the case for the majority of Registered Entities.

A CFR is a tool for the ERO as it gives them insight into these agreements as they do the Inherent Risk Assessment for the Registered Entity.

### *3.4.2 Joint Registration Organization (JRO)*

A JRO, as stated in the NERC ERO Registration Procedure as of April of 2017 is:

"An entity may register as a JRO on behalf of one or more of its members or related entities for one or more functions for which such members or related entities would otherwise be required to register and, thereby, accept on behalf of such members or related entities all compliance responsibility for that function or those functions including all reporting requirements."

A JRO is not the most effective way to address shared facilities as it requires the other Registered Entity to take on the entire registration (such as TO, for example). In the context of shared facilities the Registered Entities are generally concerned with a small subset of CIP-003, not an entire registration function. The JRO also has the same "all or nothing" problem that the CFR does, in that it does not allow multiple entities that have shared facilities with multiple other entities.

### *3.4.3 Memorandum of Understanding (MOU)*

An MOU is an effective tool for shared facility issues due to the complex nature of the relationships between the parties in a shared facility. It functions as an agreement that can be crafted by two or more entities to state what responsibilities will be shared between them. The important part of the MOU is that it outlines all of the compliance obligations and clearly states which party is responsible for what parts of the CIP requirements.

Sometimes this style of agreement may take another similar form and not be called an "MOU", but the concepts can be the same. Some entities may use Interchange Agreements or other types of agreements to reach the same result.

It is suggested that any agreement for a shared facility that only has low impact BCS contain or reference the following information:

- Identification of all Cyber Assets in the location to avoid gaps in protection
- Identification of all routable connectivity into the shared facility (if any)
- Identification of the entity responsible for physical access to the shared facility or BCS
- Process for gaining access to the shared facility for those that do not control physical access
- Understanding and agreement of cooperation during audits, with the ability to provide evidence upon request
- Agreement on responsibility for fines for any enforcement actions taken by the ERO
- Process/policy that states access will be escorted by authorized individuals when necessary
- Inclusion of, or access to, Cyber Incident Response Plans for the entity controlling physical access, and training on these policy/plans by anyone with unescorted access
- Cyber Awareness that includes notifying other entities in the same facility of anything out of the ordinary ("If you see something, say something" policy).
- Identification of and/or a process for handling confidential information

Multiple agreements between different parties should be structured in the same manner, making them as similar as possible. However, it is expected that each agreement will be at least slightly different depending on the parties involved, locations, access rules, etc.

See Attachment 1 for a sample MOU for a low impact asset. This is only an example; each agreement should include legal review.

It is suggested that if the shared facility contains medium impact BCS, the entity with the medium impact BCS should review the additional requirements (e.g., CIP-004, CIP-006, CIP-009, CIP-010) that apply to their BCS to ensure compliance will not be compromised by the parties in the agreement.

CIP-008 should be included in the agreement to ensure both parties agree to the cyber incident response plan for the entity with medium impact BCS.

If the shared facility contains medium impact with ERC, the agreement should state which of the entities in the shared facility is the "lead". This lead should be the entity with the medium impact with ERC BCS. The agreement should be clear regarding physical access controls and cyber incident response. It is generally understood there may be additional physical security controls involved for the other entities in the agreement, and electronic access control, when applicable, will be handled by each entity independently.

### *3.4.4 Delegation agreements*

Delegation agreements can exist between entities. Similarly to MOUs, they are not filed with the ERO and therefore does not shift the compliance between entities. As such, these agreements should spell

out the handling of compliance violations in the event there are any. Delegation agreements should include the same items as an MOU.

# Attachment 1 – Sample Agreement (MOU)

**MEMORANDUM OF UNDERSTANDING**

This Memorandum of Understanding ("MOU") is made on this _____ day of _____, 2017, by and between ENTITY A and ENTITY B.

The purpose of this MOU is to assist ENTITY A and ENTITY B in their respective compliance with NERC Reliability Standards CIP-003-6, as it applies to low impact BES Cyber System(s) located at the ASSET NAME.

Capitalized terms used in this MOU that are not otherwise defined herein shall have the meaning set forth in the NERC Reliability Standards, NERC Glossary of Terms, and NERC Rules of Procedure.

Pursuant to [*agreement*], ENTITY B [*describe asset ownership*]; however ENTITY A [*describe* ENTITY A *ownership of certain facilities*] [*entity may want to define the term "Shared Facilities" for use in this MOU*].

Certain items within the ASSET NAME are BES Cyber Assets, requiring physical as well as electronic controls (to the extent there is External Routable Connectivity) pursuant to CIP-003-6. ENTITY A and ENTITY B hereby agree to implement and abide by the Physical Access Plan and Cyber Incident Response Plan as set forth in this MOU as they pertain to shared facilities.

**Section 1. Identification of shared facilities and BES Cyber Assets**

1.01. Attached to this Agreement as "Attachment 1" is a complete identification and listing of ENTITY A's shared facilities and BES Cyber Assets at the ASSET NAME, as well as the Party that owns such shared facilities or BES Cyber Assets.
[*Address who is responsible for keeping Attachment 1 up to date. Note while an inventory isn't required for low impact BES Cyber Assets, having a way to track ownership in shared facilities is important. Each entity should evaluate the cost/benefit of various ways of tracking this information. External routable connectivity into the shared facility (regardless of association to a BES Cyber System) should also be identified by each party.*]

**Section 2. Compliance Responsibility for shared facilities**

2.01. Except as otherwise expressly provided for in this MOU, ENTITY A and ENTITY B shall retain compliance responsibility for their respective BES Cyber Assets.

2.02. Both parties will use reasonable efforts to provide data for audits related to the ASSET NAME upon request.

[*Address or agree on responsibility for fines for any enforcement actions taken by the ERO, if appropriate*]

**Section 3. Physical Access Policy**

3.01. ENTITY B shall develop and provide to ENTITY A a policy governing physical access to ASSET NAME that, at a minimum, meets the requirements of CIP-003-6. A copy of ENTITY B's Physical Access Plan is attached to this MOU as "Attachment 2".

3.02. The Physical Access Plan shall, at a minimum [*list minimum elements that must be included in the physical access policy, consider escort requirements*]

3.03. ENTITY A shall use reasonable best efforts to comply with ENTITY B's Physical Access Policy when ENTITY A's employees physically access the ASSET NAME.

**Section 4. Cyber Security Incident Response Plan**

4.01. Attached to this MOU as "Attachment 3" is the Cyber Incident Response Plan for the shared facilities.

4.02. The Cyber Incident Response Plan shall, at a minimum [*list minimum elements that must be included, such as shared/joint training/exercises. Also include notification in the event that something suspicious is found at the location.*]

**Section 5. Changes to Physical Access Plan, Cyber Security Incident Response Plan or External Routable Connectivity**

5.01. ENTITY B may amend the Physical Access Plan at any time; provided, however, that ENTITY B shall provide ENTITY A with [# days] advance notice prior to any such amendment. Upon the effective date of any such amendment, ENTITY B shall amend the appropriate attachment of this MOU to reflect such amendment and shall provide ENTITY A with a written copy. If either entity adds or removes External Routable Connectivity to the ASSET NAME, they shall notify the other entity.

**Section 6. Term & Termination**

6.01. This MOU shall be effective upon the date first written in the introductory paragraph of this MOU. Either Party may terminate this agreement upon [# days] advance written notice to the other Party.

**Section 7. No Other Amendments**

7.01. [*Include language that this agreement does not change any responsibilities of the parties under other agreements (e.g. Interconnection Agreements, Compliance Responsibility, any confidentiality agreements, NDAs, etc.)*]

\By signing below, the Parties agree to the foregoing.

**ENTITY A**

_____

By:
Its:

**ENTITY B**

_____

By:
Its: