Drafting Team Responses to Comments on Definitions

Commentor: Bob Wallace
Entity: Ontario Power Generation

	Critical Asset	Cyber Security Incident
Comment	OPG feels that there are many incidents that may have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that <<suspicious event>> is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	This definition was approved by NERC's Critical Infrastructure Protection Committee on September 16, 2004. As stated in the minutes of that meeting: The definition of "Critical Asset" proposed by both the Control Systems Security Working Group and the Risk Assessment Working Group was approved (Motion-3). The minutes from that meeting also reflect CIPC's expectation that this definition would be used in security standards and security guidelines. Specificity may be added for a particular standard, which is the case with CIP-002 through CIP-009.	This definition has been revised.

Drafting Team Responses to Comments on Definitions

Commentor: Carol L. Krysevig
Entity: Allegheny Energy Supply Company

	Critical Asset	Cyber Assets	Cyber Security Incident
Comment	Critical Asset -- Recommend changing the definition to read as follows: Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, or would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety. Our recommended change added the word OR at the start of the phrase dealing with detrimental impact. Also, the definition of Critical Asset should refer to the Standard that defines which assets are to be included in the list (CIP-002-1, Requirements).	Cyber Assets -- Since most newer electronic devices in a power station can be programmed (configured), this definition should include verbiage that specifically denotes connection to an externally accessible network. This should eliminate additional unintended devices from being deemed cyber assets. Physical Security. Physical Security Perimeter - Note that in a power station there is network wiring that does not and cannot be reasonably segregated with a physical perimeter. In some cases, this wiring runs through open cable trays throughout the plant. Is the intent of the Standard to require protection for items such as this?	Cyber Security Incident -- Recommend changing the first bullet in the definition to read as follows: Compromises or was an attempt to compromise the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,. As originally written, the definition leads one to believe the word PERIMETER only applies to
Response	The definition used in this standard was approed by NERC's Critical Infrastructure Protection Committee.	This issue has been addressed within the standards themselves.	The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Dave McCoy
Entity: Great Plains Energy Cyber Security Task Force

Critical Asset

Comment The definition for Critical Assets listed in each Definitions of Terms page is fine, but it is much different from the definition in CIP-002 where it says "Those Critical Assets include the following" The former definition allows entities to determine themselves which assets are critical. CIP-002 gives a long list of items that must be considered Critical Assets. Responsbible entities should be left to determine their own Critical Assets.

Response The list in CIP-002 is intended to provide more specificity appropriate for a cyber security application. The definition, if approved, will become part of a greater NERC Glossary and be used in other standards where specificity may not be appropriate.

Drafting Team Responses to Comments on Definitions

Commentor: Earl Cahoe
Entity: Portland General Electric

	Critical Asset	Cyber Security Incident
Comment	Recommendation: Put boundaries around the scope. Terminate the definition after the term "... period of time." The last two phrases "... detrimental impact on the reliability or operability of the electric grid..." and "...significant risk to public health and safety..." can be interpreted to broadly.	Recommendation: At the beginning of the first bullet rephrase the sentence to read "Compromises or was a serious attempt to compromise…".
Response	This definition was approved by NERC's Critical Infrastructure Protection Committee on September 16, 2004. As stated in the minutes of that meeting: The definition of "Critical Asset" proposed by both the Control Systems Security Working Group and the Risk Assessment Working Group was approved (Motion-3). The minutes from that meeting also reflect CIPC's expectation that this definition would be used in security standards and security guidelines.	Definition has been changed.

Drafting Team Responses to Comments on Definitions

Commentor: Edwin C. Goff III
Entity: Progress Energy

Critical Asset

Comment clarification requested - what is meant by "significant impact", "large quantities of customers", and "extended period of time?"

Response The answer is relative, based on Responsible Entities' operating environments.

Drafting Team Responses to Comments on Definitions

Commentor: Francis J. Flynn, Jr.,
Entity: National Grid USA

	Critical Asset	Cyber Security Incident
Comment	National Grid feels that there are many incidents that may have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see reponse to comments by Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Gary Campbell
Entity: MAIN

Responsible entity

Comment Responsible entity must be defined or omitted.

Response Please see NERC Functional Model for the definition of Responsible Entity. .

Drafting Team Responses to Comments on Definitions

Commentor: Guy Zito
Entity: NPCC CP9

	Critical Asset	Cyber Security Incident
Comment	NPCC Participating Members feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	NPCC Participating Members are concerned that "suspicious event" is too broad, and recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see responses to Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Howard Rulf
Entity: We Energies

Cyber Security Incident

Comment Remove "or was an attempt to compromise" from the definition. If this is kept in the definition, you need to quantify what is considered as an "attempt". A virus that is properly quarantined? A port scan on the outside that is properly blocked by the firewall?

Response The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: James W. Sample
Entity: California ISO

Critical Asset

Comment The definition of Critical Asset should be revised. The failure of virtually any facility, system or piece of equipment will cause some definable detrimental impact on the reliability or operability of the electric grid. The phrase, would have a detrimental impact on the reliability or operability of the electric grid should be revised to read, would have a significant impact on the reliability or operability of the electric grid.

Response Please see response to Bob Wallace, OPG.

Drafting Team Responses to Comments on Definitions

Commentor: Jerry Freese
Entity: American Electric Power

Cyber Security Incident

Comment "Electronic" is a proper noun and should be capitalized.

Response Noted.

Drafting Team Responses to Comments on Definitions

Commentor: Jerry Heeren
Entity: MEAG Power

Bulk Electric System

Comment Bulk Electric System needs to be defined clearly. NERC has created confusion by allowing varying definitions to appear in different locations. For example, NERC's Cyber Security Standards FAQ says the Bulk Electric System is above 35kV or as approved in a tariff filed with FERC; NERC's TOP-003-0 Standard shows the Bulk Electric System as greater than 100kV; NERC staff has verbally mentioned that the Bulk Electric System includes those systems above 100kV; and finally, NERC's Version 0 Glossary says the Regional Reliability Organization should define Bulk Electric System, with 100kV as a minimum. MEAG Power believes that the Bulk Electric System should be defined as those systems that operate above 200kV. MEAG's suggested definition of Bulk Electric System follows: "Bulk Electric System -- A term commonly applied to the portion of an electric utility system that encompasses the electrical generation resources and high-voltage transmission system (above 200kV)."

Response Unfortunately the term "Bulk Electric System", although defined in the NERC Glossary of Terms, is subject to some interpretation by its definition. This issue of interpretation has been further clouded by the more generic use of the words. When used in the NERC standards, as capitalized terms, the definition is as provided in the NERC Glossary of Terms.

Drafting Team Responses to Comments on Definitions

Commentor: Jim Hansen

Entity: Seattle City Light

Critical Asset

Comment The definition of Cyber Assets should be clarified to specifically exclude communication links connecting electronic perimeters. You could add the sentence: For the purpose of this standard, communications links connecting discrete electronic permiters are excluded.

Response CIP-005 addresses this point.

Authorized Access

Comment The term 'Authorized Access' is used in CIP-004,005, and 006 but not defined here. Please add a definition for this term, and specifically describe whether it is intended to mean authorized electronic access, physical access, or both. This would help us understand the intent of these sections. It may be appropriate to spell out physical or electronic (or both) where appropriate in the standard. Training requirements for staff granted authorized physical access but not electronic access would be different than staff granted both for example. If this term means physical access, it would be helpful if exemptions (such as escorted visitors) or any special circumstances were identified.

Response This term has been clarified within the standards.

Drafting Team Responses to Comments on Definitions

Commentor: Jim Hiebert
Entity: California ISO

Cyber Assets

Comment The definition of Cyber Assets should be clarified to specifically exclude communication links connecting electronic perimeters. You could add the sentence: For the purpose of this standard, communications links connecting discrete electronic permiters are excluded.

Response CIP-005 addresses this point.

Drafting Team Responses to Comments on Definitions

Commentor: Kathleen M.
Entity: ISO New England Inc.

Critical Asset

Comment

We feel that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>. Further we feel that it needs to be acknowledged that this definition is broad in its scope as a potential standard NERC definition, and that any more specific interpretation is to be addressed within the scope of individual standards, such as CIP002.

Response

Please see responses to Bob Wallace, OPG.

Drafting Team Responses to Comments on Definitions

Commentor: Kurt Muehlbauer
Entity: Exelon Corporation

	Critical Asset	Cyber Assets
Comment	We recommend clarification through a FAQ on what is considered a large quantity of customers and what constitutes an extended period of time. Alternatively, the definition could be modified to reflect that the responsible entity is responsible for defining what it considers to be a significant or detrimental impact.	The association of Cyber Assets to the bulk electric system occurs through the definition of Critical Cyber Assets. Also, the standard now includes other Cyber Assets connected within the Electronic Security Perimeter. The definition of Cyber Assets should not include the association to the bulk electric system assets. We recommend that this definition be changed to: Programmable electronic devices and communication networks including hardware, software, and data.
Response	The drafting team will consider this suggestion.	The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: L.W. Brown
Entity: Edison Electric Institute

Cyber Security Incident

Comment

The definition of Cyber Security Incident is far too vague. In particular the terms “suspicious event,” “attempt to compromise,” and “attempt to disrupt” are all overbroad and subject to numerous interpretations and differing applications. The concern is that an entity may be found out of compliance with the standards simply because a standards-compliance auditor disagrees with a completely reasonable interpretation made by a Responsible Entity. There are no objective, measurable criteria in the Standards or the FAQ by which a Responsible Entity or an auditor can determine what is sufficiently suspicious to trigger action. Moreover, it is simply not knowable whether any specific event is an “attempt,” because that involves knowing the intent of the actor

Instead, it would be more useful if this definition, and perhaps each entire definition section as a whole, were to be clarified by adding language to the effect that interpretations of terms (especially those, like the three here, unable to be further clarified) will be acceptable for compliance purposes, even if they may differ from those of other Responsible Entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making.

Response

The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Laurent Webber
Entity: Western Area Power Administration

Cyber Security Incident

Comment The definition of a Cyber Security Incident is extensive enough to include common events such as port scans or automated programs that attack databases and Web servers. Having to report such events within 60 minutes is an unreasonable requirement. The definition of a Cyber Security Incident must be more clear as to what must be reported or the requirement must allow each company to define Cyber Security Incident in the context of their systems. Suggest adding the phrase (is known or suspected to be of malicious origin) to the definition.

Response The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Lawrence R
Entity: Midwest Reliability Organization

Cyber Security Incident

Comment The definition for Cyber Security Incident Should not include (was an attempt to compromise) or (was an attempt to disrupt). This is too vague and onerous. Depending on the intended meaning, such attempts are made systematically. If an attempted ping is discovered against an IP address, is that an attempt to compromise?

Response The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Lee Matuszczak
Entity: U S Bureau of Reclamation

Cyber Security Incident

Comment The definition of a Cyber Security Incident is difficult to clearly understand. As written, the definition may result in excessive data collection and unnecessary burdening of reporting offices. Consider revising the definition to address incidents as cyber-related events which (1) violate a law or policy, (2) contribute to (1), and/or (3) directly jepordize assets (personnel, infrastructure, and information). Efforts should be made to exclude cyber events such as "Internet noise" (port scans and pings) isolated inconsequential virus outbreaks, scheduled outages, support equipment failures and other events from incident reporting requirements.

Response The definition has been modified.

Electronic Security Perimeter

Comment The definition for Electronic Security Perimeter, while addressing the perimeter boundary, does not address the level of control (or "policy") within the perimeter that would normally establish a security baseline within the controlled area.

Response Please see CIP-005.

Drafting Team Responses to Comments on Definitions

Commentor: Linda Campbell
Entity: FRCC

	Critical Asset	Critical Cyber Assets	Cyber Assets
Comment	1. Critical Asset in Draft 2 was previously identified as "Bulk Electric System Asset" in Draft 1. Areas of concern are: A. The definition should help responsible entities identify critical assets that comprise the "Bulk Electric System" and not make any ambiguous references such as "large quantities", "extended period of time", "detrimental impact", or "significant impact." The NERC Glossary (Version 0 - Draft 4, January 7, 2005) has already defined the Bulk Electric System as being "defined by the Regional Reliability Organization, the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment generally operated at voltages of 100kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included in this definition." None of the definitions in the NERC Glossary use the words, "large quantities", "extended", "detrimental impact", or "significant impact." B. The definition as written in this standard would allow for "scope creep." Scope creep results from a failure to establish clear definitions. It should not be the intent of this standard to impact responsible entities more than necessary. NERC reliability standards should only apply to the facilities of the bulk electric system. The definition now implies facilities all the way down to the distribution level. In fact, including public health and safety is extremely broad. C. This definition will be added to	The definition of Critical Cyber Assets should be changed to incorporate the characteristics as described in CIP-002-1, Section R2.1., R2.2., and R2.3. The proposed definition is as follows: (this definition change has also been added to our comments on CIP-002-1.) Critical Cyber Assets: Those Cyber Assets essential to the reliable operation of Critical Assets having the following characteristics: 1. The Cyber Asset uses a routable protocol, or 2. The Cyber Asset is dial-up accessible. 3. Dial-up accessible Critical Cyber Assets which do not use a routable protocol require only an Electronic Security Perimeter for the remote electronic access without the associated Physical Security Perimeter.	The Cyber Asset definition must be restated, since it refers to the "bulk electric system assets" which have been renamed as only "Critical Asset" in Draft 2. Proposed language would be: Cyber Assets: Those programmable electronic devices and communication networks including hardware, software, and data associated with critical assets.

	the NERC Glossary upon approval, when that happens the definition can be utilized by and have impact on other NERC standards, therefore this standard should be very specific, instead of ambiguous. D. The standards drafting team received 16 comments regarding the ambiguities of words such as "large quantities", "extended period of time", "detrimental impact", and "significant impact" on the previous posting. In response, the drafting team stated on page 226 of 808 of the "Cyber Security Comments and Drafting Team Responses" that "Such phrases as "large quantities of customers" and "extended period of time" have been removed." In fact only the name has been changed, the definition remain exactly same as in Draft 1. E. CIP-002-1 Purpose section states that the standards intent is to ensure measures are in place to protect assets that are needed "for managing and maintaining a reliable bulk electric system." No where in the definition of "Critical Asset" is the bulk electric system mentioned. This definition needs to be changed in order to ensure that the scope of this standard is limited to only the critical assets that support the bulk electric system. Proposed language would be: Critical Asset: Those facilities, systems, and equipment, which if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.		
Response	The drafting team used the definition approved by NERC's Critical Infrastructure Protection Committee (see response to Bob Wallace, OPG). The drafting believes this definition is universal, in keeping with the needs of a standards glossary. It believes specificity can	The drafting team believes specificity is appropriate for the standard and the definition should be universal as it will become part of a larger glossary and perhaps used in other standards.	This association is made in the definition of Critical Cyber Assets.

be introduced within the requirements of standards, as is the case with CIP-002.

Drafting Team Responses to Comments on Definitions

Commentor: Lyman Shaffer
Entity: Pacific Gas and Electric Company

Cyber Assets

Comment Cyber Assets - In this definition you refer to "communication network". For the purpose of this standard, communications links connecting discrete electronic perimeters are not considered. This should be

Response Noted.

Authorized Access

Comment Throughout the standard you refer to the term "authorized access", so shouldn't it be included in the definitions section? Suggested definition would be: is Access that is granted according to an established scheme of

Response This has been clarified in the standards.

Drafting Team Responses to Comments on Definitions

Commentor: Marc Butts

Entity: Southern Company, Transmission, Operations, Planning and EMS Divisions

Cyber Security Incident

Comment Cyber Security Incident definition suspicious event: Isn't this too broad? How will we decide or know an event was an attempt to disrupt if it's only suspicious?

Response The definition has been updated.

Drafting Team Responses to Comments on Definitions

Commentor: Neil Phinney
Entity: GSOC

Critical Asset

Comment

In response to a previous comment the drafting team wrote: "For the purposes of this standard, criticality is defined by the magnitude of vulnerability . . ."

Although this makes clear that vulnerability is a key element of the concept of Critical Cyber Assets, the current definition does not contain even an implied reference to vulnerability. We believe that the term should be Vulnerable Critical Cyber Assets. The definition should be "those cyber assets essential to the reliable operation of Critical Assets that are most vulnerable to malicious attack as determined by a risk based assessment methodology". As currently defined the document is internally inconsistent: the definition itself refers only to the criticality of the assets, while the text of CIP002-1R2 focuses on vulnerability.

Response

The definition must be universal, as it will be included as part of a larger NERC Glossary. Specificity ishould be introduced in individual standards, as is the case with CIP-002.

Drafting Team Responses to Comments on Definitions

Commentor: Patrick Miller
Entity: PacifiCorp

Cyber Security Incident

Comment In section “Cyber Security Incident”, the term “attempt” should be qualified with adjectives such as “obvious”, “clear”, or “definite”.

Response This definition has been updated.

Drafting Team Responses to Comments on Definitions

Commentor: Pete Henderson
Entity: Independent Electricity System Operator

Critical Asset

Comment The definition of Critical Asset should be revised. The failure of virtually any facility, system or piece of equipment will cause some definable detrimental impact on the reliability or operability of the electric grid. The phrase, would have a detrimental impact on the reliability or operability of the electric grid should be revised to read, would have a significant impact on the reliability or operability of the electric grid.

Response See response to Bob Wallace, OPG.

Drafting Team Responses to Comments on Definitions

Commentor: Randy Schimka
Entity: San Diego Gas and Electric Co

	Critical Cyber Assets	Cyber Security Incident
Comment	2. Due to the amount of debate in the community about what sort of assets should be classified as Critical Cyber, we feel that some examples of various types of Cyber Assets and Critical Cyber Assets and additional documentation like a decision tree or flow chart (perhaps in the FAQ document) would help clarify the types of assets that qualify as Critical Cyber Assets and provide ideas that the community could use and compare our own efforts against. in the community about what sort of assets should be classified as Critical Cyber, we feel that some examples of various types of Cyber Assets and Critical Cyber Assets and additional documentation like a decision tree or flow chart (perhaps in the FAQ document) would help clarify the types of assets that qualify as Critical Cyber Assets and provide ideas that the community could use and compare our own efforts against.	This definition refers to a communications network. Our understanding is that a separate standard will cover telecommunications networks at some future time. We suggest a qualifying statement up front in this section that lists certain assumptions, such as 'for the purpose of this standard, communications networks are excluded' or something similar. 2. Due to the amount of debate
Response	Please see the FAQ for CIP-002. term to refer to LANs that include critical cyber assets and communication devices on the electronic perimeter such as modems and routers.	The drafting team intended this

Drafting Team Responses to Comments on Definitions

Commentor: Ray A'Brial
Entity: Central Hudson Gas and Electric

	Critical Asset	Cyber Security Incident
Comment	CHGE feels that there are many incidents that have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see responses to Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Richard Engelbrecht
Entity: Rochester Gas and Electric

	Critical Asset	Cyber Security Incident
Comment	NPCC feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see responses to Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Richard Kafka
Entity: Pepco Holdings, Inc. - Affiliates

	Cyber Assets	Cyber Security Incident
Comment	Cyber Assets definition includes telecommunication networks. As part of the NERC conference call communication systems was deemed out of scope for these Standards. If telecommunications is in scope, a clear defintion is needed to understand what portion is in scope. If out of scope, similar to the comment on Nuclear Facilties being out of scope is needed. one of these terms different from a rartional interpretation used by an entity subject to the standards. It would be useful if this definition, and perhaps each entire definition section as an a whole, were to be clarified by addition of language to the effect that interpretations of terms (especially those unable to be further clarified) will be acceptable for compliance purposes, even if they may differ from those of other entities or of auditors, as long as they are reasonable or justifiable under normal standards of business decision-making. Despite being stated here regarding each Definition section -- and especially if that suggestion is not adopted -- the preceding comment suggesting the inclusion of general language endorsing interpretation made as a result of reasonable business decisions bears repeating at several locations throughout the Standards in regard to terms that are not given a specific definition.	The definition of Cyber Security Incident is far too vague. In particular the terms "suspicious event," "attempt to compromise," and "attempt to disrupt" are all overbroad and subject to numerous interpretations and differing applications. The concern is that an entity may be found out of compliance with the standards simply because an auditor has an interpretation of
Response	The drafting team intended this	The defintion has been modified.

term to refer to LANs that include critical cyber assets and communication devices on the electronic perimeter such as modems and routers.

Drafting Team Responses to Comments on Definitions

Commentor: Robert Strauss
Entity: New York State Electric & Gas Corporation

	Critical Asset	Cyber Security Incident
Comment	NYSEG along with NPCC feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see responses to Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Roger Champagne
Entity: Hydro-Québec TransÉnergie

	Critical Asset	Cyber Security Incident
Comment	HQTÉ feels that there are many incidents have a detrimental impact to the grid. Most of those are outside the scope of this standard. We recommend changing the Critical Asset definition from <<would have a detrimental impact on the reliability or operability of the electric grid>> to <<would have a significant detrimental impact on the reliability or operability of the electric grid>>.	We are concerned that "suspicious event" is too broad. We recommend changing the Cyber Security Incident definition to <<Any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.>>
Response	Please see responses to Bob Wallace, OPG.	

Drafting Team Responses to Comments on Definitions

Commentor: Roman Carter
Entity: Southern Company Generation

Cyber Security Incident

Comment On Page 2, regarding Cyber Security Incident definition suspicious event: Isn't this too broad? How will we decide or know an event was an attempt to disrupt if it's only suspicious?

Response The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Terry Doern

Entity: Bonneville Power Administration, Department of Energy

	Cyber Assets	Cyber Security Incident
Comment	Cyber Assets: change 'communication networks' to 'computer networks'. NERC has stated that telecommunications is excluded and will be addressed in a separate standard.	Cyber Security Incident: '. . . . malicious act include accidental, unintentional.'
Response	Noted. The drafting team intended this term to refer to LANs that include critical cyber assets and communication devices on the electronic perimeter such as modems and routers.	The definition has been modified.

Drafting Team Responses to Comments on Definitions

Commentor: Tim Hattaway
Entity: Alabama Electric Coop

Critical Asset

Comment the terms such as: significant impact, large quantities of customers and extended periods time should be better defined.

Response Please see response to Bob Wallace, OPG.