The Evaluation Criteria for Designation of Critical Information Infrastructure

Soontai Park
Korea Internet & Security Agency
78, Garak-dong, Songpa-Gu, Seoul
KOREA
cptpark@kisa.or.kr

Wans Yi
Korea Internet & Security Agency
78, Garak-dong, Songpa-Gu, Seoul
KOREA
wsyi@kisa.or.kr

Abstract: - Increasing to dependency on information infrastructures involves various threats to cyber incidents. Most of nations or organizations work on protect to infrastructure. Korea established Critical Information Infrastructure Protection Act in 2001 that include 5 evaluation criteria for designation of National CII. This research makes a suggestion that detailed evaluation criteria for objectification and measuring for designation of CII. Also shows the result of simulation using proposed criteria.

Key-Words: - CII (Critical Information Infrastructure), CIIP (CII Protection), Cyber incident, Designation Criteria

1 Introduction

CIIP means Activities for protecting critical information infrastructures related to communication, finance, military, energy and so on areas from various cyber attacks

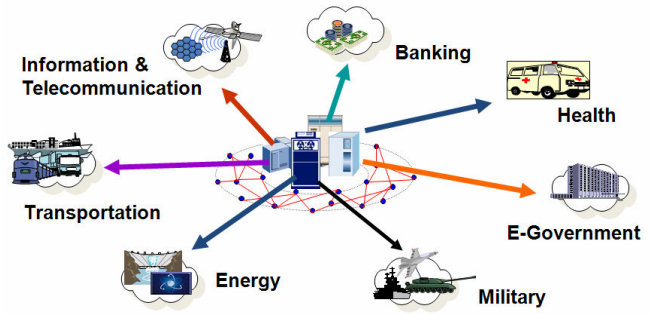

Fig 1 Critical Information Infrastructure in various areas

Each Nations have diversity information infrastructures. The Korean Government enacted a law to protect the major CIIP in January 2001 at the level of national society. This CIIP activities deal with not only Information & Communication Technology sector but also Military, Banking, E-government, Healthcare etc. This research will propose the improved criteria that designation for protect in many information infrastructures.

2 Related research

2.1 CIP Reliability Standards

US FERC (Federal Energy Regulatory Commission) approved new CIP (Critical Infrastructure Protection) Reliability Standards by NERC (North American Electric Reliability Corporation) for prevention of damage on US electric system against cyber threat in Jan 2008. Fig 2 Venn diagram shows the necessary relationships related to the NERC Cyber Security Standards (CIP-002 through CIP-009).

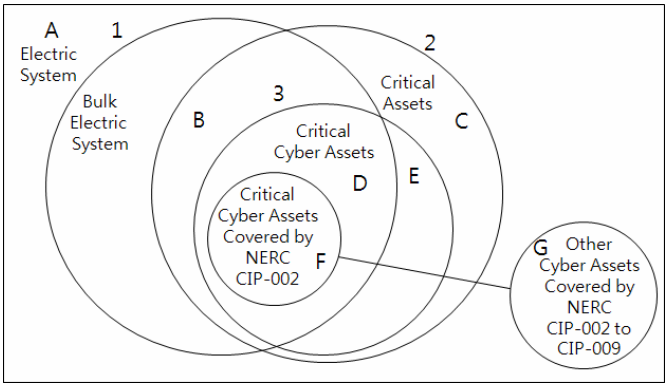

Fig 2 Necessary relationships related to the NERC Cyber Security Standards

2.2 Designation Process and Criteria for CII in Korea

2.2.1 Designation of CII

Below Fig.3 shows the procedure and method of designating the major elements of CIIP

Fig 3 Information Infrastructure versus CII

The electronic control and management system, information system, and communication network can be designated as major components of the CIIP. If any infrastructure can affect the country, economy, or society significantly, the government agency in the corresponding area can make public information on the major CIIP based on the review conducted by the Infrastructure Protection Committee. Fig 4 shows 5 phase of designation of CII.

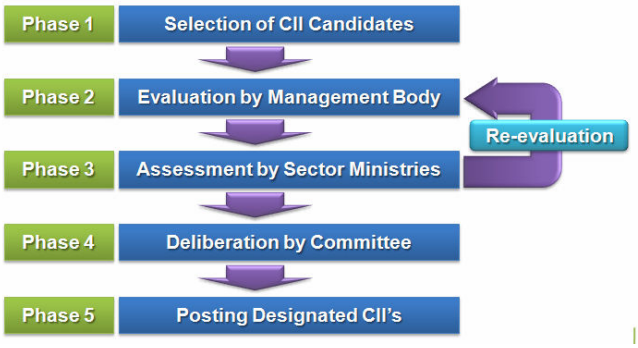

Fig 4 Phase for designation of CII

Self evaluation criteria for designation of CII in the field of communication and broadcasting are composed of 5 domains 10 detailed criteria. Below Table 1 shows detailed criteria and scores.

Table 1 Original designation criteria and score

Designation Criteria category	Score
1. Importance of nation and/or society of Infrastructure	20
2. Dependency for Information Infrastructure's own business	15
3. mutual relation against other information infrastructure	20
4. scale and extent of damage in cyber incident	30
5. possibility of cyber incident or easiness of recovery	15
Total	100

2.2.2 Criteria 1 - Importance of nation and/or society of Infrastructure

Table 2 shows Original evaluation criteria 1-A. Criterion 1 means applicable level of public service that needs to national security and/or maintain of social order for its own service of business.

Table 2 Original criteria 1 and score

Evaluation criteria	Score			
Application level - public service in the field of national security, keeping social order, maintenance of stability and/or national life	H	M	L	N/A
	20	16	12	0

2.2.3 Criteria 2 - Dependency for Information Infrastructure's own business

Table 3 shows original evaluation criteria. A criterion 2 is dependency of the providing operation on the IC infrastructure.

Table 3 Original criteria 2 and score

Evaluation criteria	Score			
Business dependency level – Do critical mission using infrastructure and computing system (include rental)	H	M	L	N/A
	15	13	5	0

2.2.4 Criteria 3 - Mutual relation against other information infrastructure

Table 4 shows original evaluation criteria. Criteria 3 concerned interconnection with other infrastructures.

Table 4 Original criteria 3 and score

Evaluation criteria	Score			
3-A	H	M	L	N/A
Relation level – mutual relation against information communication network, computing system in the field of non-government and government	12	10	5	0
3-B	H	M	L	N/A
ripple effect of obstacle of business function	8	6	3	0

2.2.5 Criteria 4 - Scale and extent of damage in cyber incident

Table 5 shows original evaluation criteria. Criteria 4 related size and scope of potential damage to national security, economy and society.

Table 5 Original criteria 4 and score

Evaluation criteria	Score			
4-A	H	M	L	N/A
Capability level - perform business continuously for example substitution in case of incident to target infrastructure	0	3	6	8
4-B	H	M	L	N/A
Level of bring about national crisis - out of public service in case of incident to target infrastructure	15	13	5	0
4-C	H	M	L	N/A
damage level – cause information leakage and modification about confidential, data, technology, privacy etc. when incident to target infrastructure	7	6	4	0

2.2.6 Criteria 5 - Possibility of cyber incident or easiness of recovery

Table 6 shows original evaluation criteria. Criteria 5 related possibility of incident occurrence and the convenience of recovery after considering these five factors, an internal appraisal is carried out in order to simulate the necessity of designation as a major element of information communication infrastructure.

Table 6 Original criteria 5 and score

Evaluation criteria	Score			
5-A	H	M	L	N/A
Possibility of cyber incident against target infrastructure	5	4	1	0
5-B	being		nothing	
Existing of prevention and/or response plan and operate backup system	1		3	
5-C	Over 2	within	Within	within
required time for recovery	days	24 hour	12 hour	1 hour
from incident	7	6	4	0

3 Criteria Proposal for Designation of CII

Original criteria for designation of CII have some point of issues those are shortage of objectivity and measuring. So this research make proposal of improved and detailed criteria.

3.1 Summary of detailed Evaluation Criteria

Below Table 7 shows proposed criteria for that have integrity, objectivity and correctness.

Table 7 Improved detailed designation criteria

Designation Criteria	Detailed Criteria	Score
1. Importance of nation and/or society of Infrastructure	A. Service importance for nation and/or public	10
	B. Importance of information handling	10
2. Dependency for Information Infrastructure's own business	A. Business dependency for infrastructure	10
	B. Dependency for Service Continuity	5
3. mutual relation against other information infrastructure	A. relation of other infrastructure - quantity	5
	B. relation of other infrastructure - quality	5
	C. ripple effect of obstacle of business function	10
4. scale and extent of damage in cyber incident	A. business continuing capability	10
	B. measuring national crisis – regional scope of damage	5
	C. measuring national crisis - sensory scope of damage	5
	D. damage scope of information leakage	10
5. possibility of cyber incident or easiness	A. possibility of cyber incident	5

of recovery	B. required time for recovery	10
Total		100

The criteria that show above Table 7 separated and tailored 13 detailed criteria from 10 detailed criteria for fully evaluation in the scope of 5 designation criteria. Proposed criteria exclude evaluator's subjectivity and get an objectivity of evaluation by embodiment or make a measuring. Also there is improved correctness of evaluation by subdivision of evaluation measure of detailed evaluation criteria.

3.2 Improved Criteria 1

The Criteria means qualitative measure against how much importance reflected nation stability and/or social publicity for information that infrastructures deal and process. Sub evaluation contents include service importance for nation and public and importance level of handled information. Allocated score is totally 20.

3.2.1 Service importance for nation and public

This criterion has total 10 score which zero through 10. The contents shall using independently or combination of criteria.

Table 8 Improved criteria 1-A and Score

criteria	Evaluation contents & measure	
Service importance for nation and public	Business Area	Business Importance Level
		VH(10), H(8), SH(6), M(4), L(2), N/A(0)
	Connection - Broadcasting & Communication	
	Exchange - Broadcasting & Communication	
	Service - Broadcasting & Communication	
	Infrastructure - Broadcasting & Communication	

3.2.2 Importance of Service Handling

This criterion has total 10 score which zero through 10. Require level means N/A (Not Applicable), Low, Medium, Some High, High, and Very High. The contents shall using independently or combination of criteria.

Table 9 Improved criteria 1-B and Score

criteria	Evaluation contents & measure	
Importance of information handling	Security Requirement of Information	Required Level
		VH(10), H(8), SH(6), M(4), L(2), N/A(0)
	Confidentiality	
	Integrity (or Correctness)	
	Availability	
	In time	

3.3 Improved criteria 2

The Criteria – business dependency means qualitative measure against how much dependent for infrastructure which controlled under management body to business. Sub evaluation contents include business dependency for infrastructure and service continuity dependency. Allocated score is totally 15.

3.3.1 Business dependency for infrastructure

This criterion has total 10 score which zero through 10. For example DNS (Domain Name System) failure means impossible because there are no alternative means.

Table 10 Improved criteria 2-A and Score

criteria	Evaluation contents & measure	
Business dependency for infrastructure	Dependency Level	Density concerned Business
	Impossible - Broadcasting & Communication	Very High(10, 9)
	Obstacle - Broadcasting & Communication	High(8, 7)
	Business Delay - Broadcasting & Communication	Some High(6, 5)
	Business Quality Down -	Medium(4), Low(3)

	Broadcasting & Communication	
	Not Concern - Broadcasting & Communication	N/A(0)

3.3.2 Dependency for Service Continuity

This criterion has total 5 score which zero through 5. If there are very complex dependencies, apply above dependency concept.

Table 11 Improved criteria 2-B and Score

criteria	Evaluation contents & measure	
Importance of information handling	Business Continuity Level	Required Level
	Real time	Very High(5,4)
	Non Real time	High(4,3)
	Allowed Short term interruption	Some High(3)
	Allowed middle term interruption	Medium(2)
	Allowed long term interruption	Low(1)
	Allowed interruption	N/A(0)

3.4 Improved criteria 3

The Criteria – mutual relation with other infrastructure adopted using not only its own infrastructure but also other organization's infrastructure. Allocated score is totally 20. It concerned with quantity, quality and ripple effect.

3.4.1 Relation of other infrastructure - quantity

This criterion has total 5 score which zero through 5. For example CAS (Certified Authority System) is medium strength relation and IAN (Internet Access Network) is weakness strength relation.

Table 12 Improved criteria 3-A and Score

criteria	Evaluation contents & measure	
Relation of other infrastructur	Quantity of Relation	Degree of Relation
	Relation strength – Medium	High(5)
e - quantity	Independency Business	N/A(0)

3.4.2 Relation of other infrastructure - quality

This criterion has total 5 score which zero through 5. For example CAS (Certified Authority System) is medium strength relation and IAN (Internet Access Network) is weakness strength relation.

Table 13 Improved criteria 3-B and Score

criteria	Evaluation contents & measure	
Relation of other infrastructur e - quality	Related type	Related quality
	Related – other infrastructures	Very High(5)
	Related – core service	High(4)
	Related – other services	Medium(3)
	Related – just linked	Low (2)
	Independence business	N/A(0)

3.4.3 Ripple effect when obstacle of infrastructure

Table 14 Improved criteria 3-C and Score

criteria	Evaluation contents & measure	
Ripple effect when obstacle of infrastructur e	Effect to other infrastructure	Ripple speed
	Effect - Full business	Very Fast(10), Fast(9), Medium(8), Slow(7), Very Slow(6)
	Effect - Core business	Very Fast(9), Fast(8), Medium(7), Slow(6), Very Slow(5)
	Effect – the others	Very Fast(8), Fast(7), Medium(6), Slow(5), Very Slow(4)
	Unrelated	N/A(0)

3.5 Improved criteria 4

3.5.1 Business continuing capability

Table 15 Improved criteria 4-A and Score

criteria	Evaluation contents & measure	
Business continuing capability	Business effect	Damage
	Loss – Full business	Very High(10)
	Loss – core business	High(9)
	Delay – core business	Some High(8)
	Loss - supporting biz	Medium(7)
	Delay – supporting biz	Low(5)
	Non Applicable	N/A(0)

3.5.2 Measuring national crisis – regional scope of damage

Table 16 Improved criteria 4-B and Score

criteria	Evaluation contents & measure	
Measuring national crisis – regional scope of damage	Extent of damage	Damage
	International	Very High(5)
	National	Very High(5)
	Administrative district	High(4)
	Organization, Enterprise	Medium(3)
	Relevant system	Restricted(2)
	Non Applicable	N/A(0)

3.5.3 Measuring national crisis - sensory scope of damage

Table 17 Improved criteria 4-C and Score

criteria	Evaluation contents & measure	
Damage scope of information leakage	Sensory damage	Domain
	Out of normal life	Very High(5)
	Make disorder	High(4)
	Inconvenience	Medium(3)
	Normal life	N/A(0)

3.5.4 Damage scope of information leakage

Table 18 Improved criteria 4-D and Score

criteria	Evaluation contents & measure	
Measuring national crisis – sensory scope of damage	Damage Level	Damage
	Nation, Society	All(10), majority (9), minority(8)
	Region	All(8), majority (7), minority(6)
	Organization, Enterprise	All(6), majority (5), minority(4)
	No information	N/A(0)

3.6 Improved criteria 5

3.6.1 Possibility of cyber incident

Table 19 Improved criteria 5-A and Score

criteria	Evaluation contents & measure	
Possibility of cyber incident	Service type	Connection type
	public	Internet(5), secure(4), closed(3), off-line(2)
	restricted area	Internet(4), secure(3), closed(2), off-line(1)
	restricted	Internet(3), secure(2), closed(1), off-line(1)

3.6.2 Required time for recovery

Table 20 Improved criteria 5-B and Score

criteria	Evaluation contents & measure	
Required time for recovery	Recovery type	Required level – real time recovery
	Full system	VH(10), H(9), M(8), L(7), VL(6)
	Core service	VH(9), H(8), M(7), L(6), VL(5)
	Supporting service	VH(8), H(7), M(6), L(5), VL(4)
	Unnecessary	N(0)

4 Simulation Result

We simulated using proposed criteria for apply of new criteria and validation of the point at issue and its effectiveness. Selected organizations are ISP (internet service provider) A and VoIP (Voice over Internet Protocol) service provider B. Below Fig 5 shows the result of simulation.

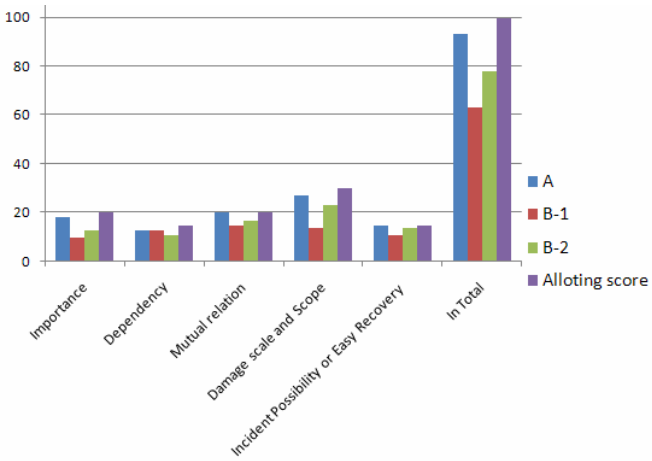

Fig 5 Simulation result using new criteria

In case of company A has high score because of business character that support Internet exchange or Internet connection. In case of company B has middle score because of VoIP service of low user of a member.

4 Conclusion

This research made a suggestion that detailed evaluation criteria for objectification and measuring for designation of CII in the field of information communication and broadcasting. We shall improved manage CII and CIIP using suggested criteria.

References:

[1] FERC, CIP Reliability Standards, **http://www.ferc.gov/industries/electric/indus-act/reliability/cip.asp**

[2] NERC, FAQ Cyber Security Standard CIP-002-1, **http://www.nerc.com/page.php?cid=2|20**

[3] The National Assembly of Korea, *Information Infrastructure Protection Act*, 2008