The Enhanced Security Control Model was proposed by Dr. Choonghee Han in July 2019. The Enhanced Security Control Model is a methodology to block foreign cyber threats for web-based information systems. In the ESC model, there are BP process with six factors: FR (Foreign Relation), RL (Real Login), BC (Blocking Complexity), ST (Stop Tolerance), OR (Outer Relation) and SI (Stop Impact). By these six factors, we can decide BID (Blocking foreign IP ranges Impact Degree) to prioritize IT systems to block from foreign IP ranges. If BID is over the DOA (Degree of Assurance), we can decide not to block from foreign IP ranges. It means we can tell which IT systems should be concentrated with enhanced security operation. This ESC model is an effective approach to enhance cyber safety of critical infrastructures to help decision making in blocking prioritization. The ESC model can be used every SOC to improve security operation. The Blocking foreign IP ranges Impact Degree (BID) can be calculated by the summation of all six factors' evaluated points. The BID ranges from 0 to 12. A lower BID means that it is recommended to block foreign IP ranges.

Table 1 Operational definition & criteria about six factors

Factors	Definition	Criteria
Foreign Relation(FR)	Business relationship with foreign regular users	Purpose of HTTP service
Real Login(RL)	Frequency of real login	Real login counts for 6 month
Blocking Complexity(BC)	Additional consideration and efforts to unblock foreign IP ranges	Counts of exception handling
Stop Tolerance(SI)	Acceptable stop duration level of HTTP service	Acceptable stop time of HTTP service
Outer Relation(OR)	Outer connectivity level of HTTP service	Counts of outer IP systems connected with HTTP service
Stop Impact(SI)	Stop influence level of HTTP service	Size of stop influence

Table 2 Detailed criteria for the six factors

Factors	Detailed criteria	Score
Foreign Relation(FR)	Complete business purpose for foreign users	High(2)
	A certain degree business purpose for foreign users	Medium(1)
	No business purpose for foreign users	Low(0)
Real Login(RL)	More than 5 times real login for 6 months	High(2)
	From 1 to 4 times real login for 6 months	Medium(1)
	No real login for 6 months	Low(0)
Blocking Complexity(BC)	A lot of additional efforts expected to unblock foreign IP ranges	High(2)
	Some additional efforts expected to unblock foreign IP ranges	Medium(1)
	Few additional efforts expected to unblock foreign IP ranges	Low(0)
Stop Tolerance(ST)	More than 1 day of acceptable stop time	High(2)
	From 4 hours to 1 day of acceptable stop time	Medium(1)
	Less than 4 hours of acceptable stop time	Low(0)
Outer Relation(OR)	Less than 1 outer connected IT systems	Low(2)
	From 2 to 4 outer connected 1 day IT systems	Medium(1)
	More than 5 outer connected IT systems	High(0)
Stop Impact(SI)	Small amount of stop influence level	Low(2)
	Medium amount of stop influence level	Medium(1)
	Large amount of stop influence level	High(0)

From April to September 2019, 20 out of 28 web-based IT systems of Korea Power Exchange (KPX) completed overseas IP ranges blocking. Also, from March 18th to March 30th of 2020, 6 out of 8 web-based IT systems completed overseas IP ranges blocking. After blocking overseas IP ranges, there were six innovative benefits were observed. First, the cyber infringement risk decreased by 92.9% compared to 2018. The cyber threat attempts for the blocked 26 information systems became zero. Second, all high-risk cyber threat events, excluding simple information gathering events, have been significantly reduced. High-risk cyber threats in 2018 were around 79.4%, and as a result of continuous overseas IP band restriction work in 2019, they were decreased to around 29.9% in March 2020. Third, cyber threat events detected by IPS have decreased by about 60% compared to 2018. Fourth, the number of bad IPs generated in the process of detecting cyber threat events was

reduced by about 43%. Fifth, the SOC's activity time was reduced by 7.1 hours per day in the year 2020 compared to the year 2018. Sixth, the accountability for cyber threats has been enhanced by blocking overseas IP bands.