FY21 - Cybersecurity Risk

Cybersecurity Risk **Targets and Thresholds**

1	2	3	4	5	6	7	8	9	10
0.00	**1.75**	**3.50**	**5.25**	**7.00**	**10.80**	**14.60**	**18.40**	**22.20**	**26.00**

Description

This performance indicator is a calculation that measures the reduction of the average heat score, by month, for the still-active and retired risks identified as of October 1, 2020. This calculation excludes any new risks identified after October 1, 2020, as well as excluding those risks that have since been rejected for reasons such as (but not limited to) being duplicative of another risk on the register or being based on un-founded assumptions.

Cybersecurity Risk is one portion (15%) of the HQ CIO Functional Effectiveness indicator.

Measurement Period -

This performance indicator will be measured each month at the begining of the month for the previous month. For instance a November 1st report will be pulled for the October period.

Data Source and Calculation

Source – Enterprise Cyber Risk Management System (ECRMS)

Indicator Value

$$\frac{\text{YTD Cybersecurity Risk Score}}{\text{Cybersecurity Risks Identified October 1, 2020} - 1}$$

Baseline Calculation: As of October 1, 2020, there were 49 active risks on the United States Postal Service Cyber Risk Register. The aggregate heat score (sum of the individual heat scores) for those risks was 290. The average heat score for those risks then computes to 290 / 49, or 5.92. This is the baseline average heat score against which progress is measured.

The Methodology to define the Population for monthly NPA calculation will include any still-active risks of the baseline 49 risks. "Still-active" is defined as those risks being actively tracked for awareness and address by the Enterprise Cyber Risk Management Team on the USPS Cyber Risk Register. “Retired” are retired risks of the baseline 49 and is defined as those risks that have mitigated to such a level (Heat Score 2 or 1) that the Enterprise Cyber Risk Management Team is no longer actively tracking them on the USPS Cyber Risk Register. An example of a retired risk is in December 2020, Risk #61 was retired. This risk will be counted as part of the continuing population.

Any new risks identified after October 1, 2020 are considered to be Excluded risks. Additionally, any of the baseline 49 risks that have since been rejected for reasons such as (but not limited to) being duplicative of another risk on the register or being based on un-founded assumptions. An example of an excluded risk is in December 2020, Risk #49 was rejected as a duplicative risk. This risk will not be counted as part of the continuing population.

Business Rule –

The calculations for the Cybersecurity Risk are an average. The monthly average heat score is the aggregate heat score of the still-active and retired risks (by summing the current heat scores of the still-active risks and the residual heat scores of the retired risks) and dividing that by the current population of still-active and retired risks.
The Numerator is the Sum of:

- Current Heat Scores of the still-active risks of the baseline 49 risks
- Residual Heat Scores of the retired risks of the baseline 49 risks

The Denominator is the current population of still-active and retired risks. An example of the denominator is in December 2020, there were 49 with an Aggregate Heat score of 272; the Average Risk Score for December 2020 was 5.55.

The percent (%) reduction of the Average Heat Score is represented as a positive percentage. The formula is:

1 - (Current Average / Baseline Average)

Alternatively written and mathematically equal:

(Baseline Average – Current Average) / Baseline Average

An example is December 2020 = 1 - (5.55/5.92) = 6.25% cumulative reduction of the Average Heat Score.

Decimal Precision – Two Decimals

Data Validation

The Enterprise Cyber Risk Management System (ECRMS) is the system of record for USPS Cyber Risks. A report is generated and pulled from the system by the Enterprise Cyber Risk Management team, and cleaned for limited distribution. The generation of this specific report is limited to the Enterprise Cyber Risk Management Team. The report is filtered so as to only include a static subset of the risks in the system (those baseline 49 risks), and further filtered to not include the rejected risks. The report is saved to the CIO Strategy Teams site for NPA validation and reporting.

Applicable Positions / Units, Measurement Depth and Weight:

Scorecard Name	Depth	Weight	Total Weight Towards Composite
HQ CIO	Nation	15.0%	4.5%