Attachment #1

Cybersecurity Readiness Factor Methodology

The Cybersecurity Readiness Factor methodology was developed by DHS based on a FY23 statistical analysis of the DHS Cyber Hygiene Assessment Instrument Questionnaire received by 400 small and other than small DHS contractors that handle DHS Controlled Unclassified Information (CUI). Using a calibrated secure assessment instrument, this analysis established the corresponding readiness assessment and objective baseline percentiles used to develop the Ratings for the Cybersecurity Readiness Factor. For FY24, the baseline is established at the 15th percentile and the mean at the 53rd percentile.

DHS will utilize statistical analysis to identify offerors' cybersecurity readiness in the pre-award stage. To accomplish this, DHS will analyze offerors' responses submitted via the secure assessment instrument questionnaire against the model developed by assessing existing DHS contractors. This secure assessment instrument enables DHS to consider how well an offeror is prepared to protect CUI on nonfederal information systems by assessing its implementation of the National Institute of Standards and Technology (NIST) security requirements in compliance with HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information clause.[1]

To enable DHS to measure offerors' cybersecurity readiness, an offeror must represent its level of fulfillment of security requirements from NIST SP 800-171r2 and NIST SP 800-172. These NIST publications outline federally recognized standards for protecting CUI on nonfederal information systems. The assessment includes a distribution of basic, derived, and enhanced security requirements from each of the 14 security requirement families. The assessment items for the basic and derived questions are from NIST SP 800-171r2, and the enhanced questions are drawn from NIST SP 800-172 security functions.[2]

The Cybersecurity Readiness Factor measures the Government's confidence that the offeror understands and has implemented the necessary technical controls to protect DHS CUI in accordance with NIST requirements. The offerors are assigned ratings based on its readiness result received in response to the standardized secure assessment instrument. The readiness result assigned to the ratings is based on the number of and type of security requirements indicated as fully satisfied, partially satisfied, or not satisfied by the offeror when completing the secure assessment instrument and subsequent statistical analysis as outlined in detail below.

High Likelihood of Cybersecurity Readiness	The Government assesses a High Likelihood that the offeror understands and has implemented the necessary technical controls to protect DHS CUI in accordance with National Institute of Standards and Technology requirements. A rating of High Likelihood indicates that the offeror assigned readiness against the secure assessment instrument is above the mean of the

[1] HSAR | Homeland Security (dhs.gov)

[2] SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC (nist.gov); SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171 | CSRC

	DHS contractor population that access, handle, process, store, manage, protect, or transmit CUI data.
Likelihood of Cybersecurity Readiness	The Government assesses a Likelihood that the offeror understands and has implemented the necessary technical controls to protect DHS controlled CUI in accordance with National Institute of Standards and Technology requirements. A rating of Likelihood indicates that the offeror assigned readiness against the secure assessment instrument falls between the fifteenth percentile (baseline) and up to the mean of the DHS contractor population that access, handle, process, store, manage, protect, or transmit CUI data.
Low Likelihood of Cybersecurity Readiness	The Government assesses a Low Likelihood that the Offeror understands and has implemented the necessary technical controls to protect DHS CUI in accordance with National Institute of Standards and Technology requirements. A rating of Low Likelihood indicates that the offeror assigned readiness against the secure assessment instrument falls below the fifteenth percentile (baseline) of the DHS contractor population that access, handle, process, store, manage, protect, or transmit CUI data.

As part of this Cybersecurity Readiness Factor, in addition to the ratings, the specific readiness result percentile for each offeror will be provided to the Contracting Officer (CO) and will aid the Source Selection Official in differentiating between contractor assigned readiness against this evaluation Factor. Since this is a comparative measure and not pass/fail, there is no percentile whereby offerors would be excluded from award eligibility.[3] At the present time, this Cybersecurity Readiness Factor will only be used for best value tradeoff award decisions for applicable solicitations. However, solicitation language may require a Plan of Action and Milestones as a post-award deliverable if an awardee's assessment result does not meet DHS's expectations of compliance with the applicable clauses upon award.

[3] The detailed statistical analysis and questionnaire responses used to formulate a vendor's specific readiness results will be considered proprietary and not be shared with any other vendor.