



RTX Corporation
1000 Wilson Blvd.
Arlington, VA 22209
USA

October 14, 2024

Defense Acquisition Regulations System
ATTN: Ms. Heather Kitchens
OUSD(A&S) DPC/DARS
3060 Defense Pentagon
Washington, DC 20301-3060
osd.dfars@mail.mil

Subject: Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041) (RIN 0750-AK81)

RTX Corporation (RTX) is pleased to provide comments to help shape the subject final rule. Our comments are below along with our recommendations:

Notification of Lapses in Information Security

The proposed requirement at DFARS 252.204-7021(b)(4) regarding notifications is unclear, as is the Department's intent for when a contractor must notify the contracting officer of a lapse or change. Under the proposed requirement, contractors are to notify the contracting officer "when there are any lapses in information security or [emphasis added] changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract;" however, in the discussion and analysis of the proposed requirement, the Department indicates contractors are to notify the contracting officer "if there are any lapses or changes in CMMC certification levels that affect the requirements for information security during contract performance," without mention of notification of lapses in information security.

RTX believes the Department's intent is for contractors to only notify the contracting officer when there are any lapses or changes in the status or levels of CMMC certificates or CMMC self-assessments, but not any lapses or changes in information security.

If contractors were required to notify contracting officers of lapses in information security, it is likely the Department would receive many notifications that provide little to no security value while placing a high burden on contractors and the Department, particularly because the term "lapses in information security" is undefined and could be interpreted to include even minor lapses (e.g., a single security control failing) that have no adverse effect on an information system and/or the information residing therein. Further, because contractors implement common security controls across many systems, and systems are used across many contracts, a single lapse of information security could result in many

notifications. For contractors like RTX, such notifications could number in the hundreds if not thousands.

Recommendations

If the Department's intent is for contractors to only notify the contracting officer when there are any lapses or changes in the status or levels of CMMC certificates or CMMC self-assessments, RTX recommends the Department revise the proposed requirement by striking "in information security" so that it reads "Notify the Contracting Officer within 72 hours when there are any lapses or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract."

If the Department's intent is for contractors to notify the contracting officer when there are any lapses in information security, RTX recommends the Department define "lapses in information security" and exclude from such definition lapses that do not adversely affect information systems and/or the information residing therein," specify the information to be included in a notification, as well as how notifications are dispositioned, and consider a mechanism or central location that would allow contractors to make a single notification to many contracting officers.

Thank you for soliciting and considering our comments.

A handwritten signature in cursive script, reading "Brad Maiorino", is positioned above a horizontal line. To the left of the signature, there is a vertical line that extends from the top of the signature area down towards the bottom of the page.

Brad Maiorino
Vice President and Chief Information Security Officer
RTX Corporation