NORTHROP GRUMMAN

September 1, 2021

Updates to Payment Clauses in Standard U.S. Terms and Conditions; and Reminder of Security Incident Reporting Obligations

---

Purpose:

The purpose of this Announcement is to notify our supplier chain partners of an important change to Northrop Grumman's Standard Terms and Conditions and remind our partners of their reporting obligations for any Information Security Incident.

Impacted Terms and Clauses:

CTM-P-ST-001, Clause 6, Invoicing & Payment (Subparagraph D)
CTM-P-ST-002, Clause 6, Invoicing and Payment (Subparagraph D)
CTM-P-ST-002, Clause 7, Service Rates, Invoicing, Payment (Subparagraph G)
CTM-P-ST-003, Clause 6, Invoicing and Payment (Subparagraph D)
CTM-P-ST-004, Clause 8, Allowable Cost, Fee, Invoicing, and Payment (Subparagraph J)
CTM-P-ST-005, Clause 6, Invoicing and Payment (Subparagraph D)
CTM-P-ST-006, Clause 6, Invoicing and Payment (Subparagraph D)
CTM-P-ST-007, Clause 6, Invoicing and Payment (Subparagraph D)

Link to Enterprise Standard Terms and Conditions on OASIS

New Subparagraph:

"Payments to Seller shall be made to the designated financial account at an office or branch of a regulated bank located in the United States. To prevent and detect fraudulent and unauthorized payment instructions, Seller shall implement and maintain multifactor authentication and other reasonable security measures on Seller's Ariba Network account and any Seller email accounts, including cloud based email accounts such as Microsoft 365, through which payment instructions could be transmitted to Buyer. Buyer shall not be responsible to pay Seller for any misdirected payments or other damages or losses attributable to Seller's failure to use multifactor authentication and other reasonable security measures."

Intent of the Change:

This updated subparagraph ensures that payments to our suppliers are made accurately and that suppliers take reasonable security measures to prevent fraudulent and unauthorized changes to their banking and financial information resulting in misdirected payments. The updated text requires all suppliers to implement multifactor authentication ("MFA") and other reasonable security measures on their Ariba Network accounts and company email accounts. If your company does not utilize the Ariba Network, please contact your Buyer/SCA regarding this updated text.

It is a general expectation of all Northrop Grumman suppliers to implement these minimal security measures to help ensure that no fraudulent activity occurs related to supplier payments. This change is intended to protect both Northrop Grumman and our valued supply chain partners.

Click here for a short video about MFA from Microsoft

How to Enable Multifactor Authentication in Ariba Network Accounts:

In the near future, MFA will be the default security setting when creating an Ariba Network account; however, MFA is currently an optional setting. Suppliers with existing Ariba Network accounts must update their account profile security settings as soon as possible to enable MFA; suppliers creating new Ariba Network accounts must select MFA as their account profile security setting.

Instructions on how to enable multifactor authentication in the Ariba Network account

Implementation Protocol:

Due to the significant risks associated with fraudulent payment instructions and to protect both Northrop Grumman and our suppliers:

(1) all RFPs/RFQs issued on or after September 1, 2021 will reference Northrop Grumman's updated Standard Terms and Conditions (Rev. 08/27/2021); and

(2) all current in-process negotiations (including for purchase orders, subcontracts, and agreements) will be updated to replace the impacted clauses referenced above with the updated 08/27/2021 revision.

Reminder – Information Security Incident Reporting:

Northrop Grumman reminds our suppliers of their obligation pursuant to Clause 57, Information Security, of Northrop Grumman's Standard Terms and Conditions to report any of the following within 72 hours of discovery:

(i) any actual or suspected incident involving supplier's information system that may involve Northrop Grumman's sensitive information; or
(ii) any actual or suspected unauthorized access, use, or disclosure of Northrop Grumman's sensitive information.

Both of the above are referred to as an "Information Security Incident." Notification of an Information Security Incident should be sent to Northrop Grumman's Authorized Representative (typically, the Buyer or Subcontracts Administrator) and Northrop Grumman's Cyber Security Operations Center (CSOC) at 877-615-3535.

For any questions regarding this Announcement or information contained herein, please contact your Northrop Grumman Buyer or Subcontracts Administrator.