Procedures for Agency Users to Gain Access to Networx Agency Pricer

Purpose. The Networx Agency Pricer is a secure Government web site that consists of an authenticated, secure web interface to Networx contract and Agency-specific data maintained in multiple databases. It is a Government provided collaborative component of the FAS Networx Hosting Center (HC), which provides ongoing support to Agencies and/or ordering entities in accessing Networx contracts prices for available products and services.

Agency Users will have the capability to browse and query the Networx Agency Pricer for current and future year contract prices (10-year prices) as part of the "fair opportunity" phase of the acquisition process. In addition, Agency Users can utilize agency-specific IT inventory information or upload new IT inventory information to be included in the pricing information processed by the Networx Agency Pricer. Information generated in response to queries can also be used for budgeting purposes and to determine Independent Government Cost Estimates (IGCEs).

The steps below describe the process and procedures for Agency Transition Managers and Agency Users designated by the Agency Transition Manager to gain access to the Networx Agency Pricer. If an Agency has not designated an Agency Transition Manager, an authorized Agency individual referred to as the Agency Administrator, will designate that Agency's Users.

1. **Agreement to Protect Sensitive But Unclassified (SBU) Government Information.** The Agency Transition Manager must certify that the Agency User is authorized to obtain the required authentication tokens and Agency User accounts by executing the "Agreement to Protect Sensitive But Unclassified (SBU) Government Information." This agreement is signed by the Agency Transition Manager/Agency Administrator and the Agency User.

2. **Nondisclosure and Conflict of Interest Agreement (NDA) for Agency Government/Contractor Personnel.** The Agency Transition Manager/Agency Administrator ensures that the Agency User reads and completes this form. If a support contractor individual is designated as Agency User, the NDA portion of the form must specify that individual's Company Name and the Agency supported by the contractor individual.

3. **Corporate Nondisclosure Agreement (NDA).** If a support contractor individual is designated as Agency User, the Agency Transition Manager/Agency Administrator ensures that this NDA is submitted on the support contractor's company letterhead and signed by a company individual who is authorized to contractually bind the company.

4. **Request for Account.** The Agency Transition Manager/Agency Administrator completes the "List of Designated Agency Users" (MS Excel format).

5. **Submit Documents.** The Agency Transition Manager/Agency Administrator submits the following four documents to the Networx Agency Pricer POC (hereafter referred to as AP POC):
    a. Signed **Agreement to Protect Sensitive But Unclassified (SBU) Government Information** – via Adobe .pdf image file of the original signed document as an e-mail attachment
    b. Signed **Nondisclosure and Conflict of Interest Agreement (NDA) for Agency Government/Contractor Personnel** – via Adobe .pdf image file of the original signed document as an e-mail attachment
    c. Signed **Corporate Nondisclosure Agreement (NDA) –** via Adobe .pdf image file of the original signed document as an e-mail attachment
    d. Completed **List of Agency Users** – MS Excel format as an e-mail attachment. ***See also Step 7 below. Agencies electing to pick up tokens from the AP POC (instead of having tokens delivered via secure postal service) will insert "Will Pick Up From AP POC" in the Mailing Address cell of the Agency User(s) who will pick up the token(s). Agency Users designated to pick up the tokens from the AP POC will be required to sign for all tokens received.***

    The above documents will be submitted to the following email addresses:
    paul.pimchaipong@gsa.gov
    winifred.kutz@gsa.gov
    nancy.rohde@gsa.gov
    cc: jack.braun@gsa.gov
    (Networx Universal Contracting Officer)
    or
    robert.abood@gsa.gov
    (Networx Enterprise Contracting Officer)

6. **RSA SecurID® Token and Unique Identifier Code Assigned.** For each Agency User, the AP POC will select an RSA SecurID® token, determine the Unique Identifier Code, and note the serial number of the token and the Unique Identifier Code in the List of Agency Users.

7. **Delivery of RSA SecurID® token.** The AP POC will deliver the RSA SecurID® token [in an inactive state] to the Agency User to the postal address provided by the Agency Transition Manager/Agency Administrator via secure delivery service [tracking with receipt signature required (i.e., FedEx, USPS, UPS)]. ***For Agencies where delivery via secure postal service is not feasible, alternative secure delivery arrangements will be made by the AP POC and***

Agency Transition Managers/Agency Administrators. A recommended delivery alternative is for Agency Transition Managers/Agency Administrators to receive the token(s) in person from the AP POC at the AP POC's location.

8. **E-Mail Notification.** The AP POC will send an e-mail to the e-mail address provided by the Agency Transition Manager/Agency Administrator indicating that the RSA SecurID® token has been sent and will include instructions and information necessary to activate the RSA SecurID® token to include:

    a. Date and/or range of dates for the Agency User to confirm receipt of the RSA SecurID® token.
    b. Time and date when AP POC will call Agency User to confirm receipt and activate the account
    c. Unique Identifier Code

    For Agencies where secure delivery via postal service is not feasible, the AP POC will send an e-mail to the e-mail address provided by the Agency Transition Manager/Agency Administrator indicating that the RSA SecurID® token is ready to be delivered at the AP POC's location. Tokens will only be delivered to a Transition Manager/Agency Administrator or Agency User.

9. **Authorization for Agency User Account.** At the time the e-mail notification and RSA SecurID® token are sent to the Agency User, the AP POC will send the completed List of Agency Users to the FAS Networx HC.

10. **User Account Set up.** After receiving the completed List of Agency Users, the FAS Networx HC will configure the Agency User account as requested within 48 hours.

11. **Agency User Confirmation.** The Agency User will confirm receipt of the e-mail in Step 8 above and the RSA SecurID® when the AP POC calls the Agency User.

12. **Set Personal Identification Number (PIN).** During the telephone call with the Agency User in Step 11, the AP POC will do the following:

    a. Verify that the Agency User is authorized and has the correct token
        (1) Verify the serial number on the back of the RSA SecurID® token by asking the Agency User to read the number from the token they received in Step 7
        (2) Verify the Unique Identifier Code by asking the Agency User to read it from the e-mail received in Step 8
    b. Logon to the RSA SecurID® token management device using AP POC RSA SecurID® token to authenticate to the management interface
        (1) Locate and activate the Agency User account

(2) Instruct the Agency User to read the first number code displayed on the RSA SecurID® token and enter that number where indicated in the user interface.

(3) Enter the information as indicated on the Agency Pricer web site.

(4) Instruct the Agency User to write down and remember the next number code displayed on the RSA SecurID® token. This number will be the Agency User's logon Personal Identity Number (PIN) to access the Networx Agency Pricer

(5) Agency Users may change the PIN at any time.

13. **Reactivation of Agency User Account.** Every Agency User is required to change his/her RSA SecurID® PIN every 90 days. If the PIN is not changed as required, the Agency User account and RSA SecurID® token are disabled for inactivity. The Agency User is required to contact the AP POC to reactivate the Agency User account. The AP POC will confirm the identity of the Agency User and logon to the RSA SecurID® token PIN management interface and reactivate the account and reset the PIN using the process described in Step 12.

14. **Replacement of RSA SecurID® token and Reactivation of Agency User Account.** If the Agency User loses his/her RSA SecurID® token or the token is compromised, the Agency User is required to immediately notify the FAS Networx HC helpdesk. The FAS Networx HC staff will immediately disable the Agency User account and RSA SecurID® token and notify the AP POC that the token has been lost and/or compromised. The Agency User will be required to contact the AP POC to request a replacement token. The AP POC will send an e-mail with a Unique Identifier Code and a replacement token as described in Steps 7 and 8. The Agency User and AP POC will then follow the procedure in Step 12.

15. **PIN Reset.** If the Agency User forgets their PIN or fails 5 times to logon successfully, the Agency User is required to contact the AP POC to request a PIN reset. The AP POC will confirm the identity of the Agency User and follow the procedures in Step 12.

16. **Failure to Activate.** If the Agency User has not contacted the AP POC to activate their RSA SecurID® token within 90 days, the Agency User account will be disabled and RSA SecurID® token will be deactivated.

17. **Return of Tokens to AP POC.** In the event that Agencies no longer need one or more of their tokens, Agency Transition Managers/Agency Administrators will send an email to the addresses in Step 5 above indicating same as well as specifying return method. If token(s) will be physically handed over to the AP

POC, the date and time of handover will be provided. If token(s) will be returned via secure postal service, relevant package identification information and mailing date will be provided.

18. **Audit and Accountability.** Audit records and logs will be maintained for all transactions related to these issuance and access control procedures.