Desktop Procedure for Establishment of Unclassified Internet Data Submission

1.0 Digital Signature and Encryption Support

- ❑ User must verify that **both** the client (i.e., workstation) and e-mail server support digital signatures and encryption. If the user's environment does not support this at both the client and server level, use of the Internet for unclassified data submission is not available. Three possible options are:
  - Lotus Notes R5/R6
  - Netscape Messenger
  - Microsoft Outlook 98/Express

Note: NMMSS falls under the requirement for encryption of unclassified data submitted via the Internet. The DOE owners of the data are not willing to assume the liability of processing unclassified data received from the Internet that may damage the data warehouse.

If the user does not send e-mail through a server, but through an Internet service provider (i.e., CompuServe, AOL, Mindspring, etc.), these service providers currently do not support the use of x.509 certificates.

2.0 Requesting x.509 Certificate from Third-Party Vendor

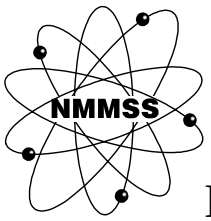
- ❑ The user must request an x.509 certificate from any third-party vendor. Several users have selected VeriSign. These users have been instructed to request a VeriSign Class 1 CA Individual Subscriber-Persona Not Validated certificate. This certificate is renewed annually for an estimated cost of $20.

Note: From VeriSign, you can purchase certificates individually or buy a set of tokens that can be distributed to individual end-users. These end-users can redeem the token for a certificate. This is a very basic certificate, only validating the e-mail address provided by the applicant. If more extensive authentication of the end-user is needed, more cost is incurred.

Each end-user must have a valid e-mail address that can receive e-mail from the Internet in order to receive a certificate from the third-party vendor.

Once the certificate is received, backing up the end-user's private key is critical. This will ensure that the end-user can continue to encrypt and de-encrypt any e-mail received or sent by the end-user.

- ❑ If a user would like to investigate alternatives to x.509 certificates, the alternative must meet the following Federal Information Processing Standards (FIPS):
  - 46-3 Data Encryption Standard (DES) – 99 Oct 25
  - 140-2 Security Requirements for Cryptographic Modules – 01 May 25 (Supercedes FIPS PUB 140-1, 1994 January 11)



Desktop Procedure for Establishment of Unclassified Internet Data Submission

- 180-1 Secure Hash Standard (SHS) – 95 Apr 17
- 185 Escrowed Encryption Standard (EES) – 94 Feb 09
- 186-2 Digital Signature Standard (DSS) – 00 January 27

http://www.itl.nist.gov/fipspubs/by-num.htm

3.0 Exchange of Public Keys

- ❑ The user will send a digitally signed e-mail message to data@nmmss.com. A digital signature should be a delivery option of the e-mail. In the case of Lotus Notes, the user would create the e-mail message and then select Delivery Options. Within Delivery Options, the user will find Security Options. There are check boxes for **Sign** and **Encrypt**. To digitally sign the message, the user would check the **Sign** box within these options.
- ❑ By sending a signed message that is "opened" by DATA, the ***public key of the user*** is sent to DATA.
- ❑ DATA will send its public key to the user. The subject will contain **My certified public key is included. You may cut and paste it into a Names database.** The contents of the e-mail message will be mixed numbers and letters. For Microsoft Outlook 98/Express users, DATA's public key should be pasted within the CONTACTS database.
- ❑ When the user reads the message sent by DATA (data@nmmss.com), the user must paste the ***public key of DATA*** in the appropriate database (i.e., Names, Addresses, or Contacts). The appropriate database varies according to the applicable software in use by the user.

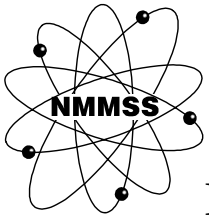
4.0 Unclassified Data Submission

- ❑ The user will generate an e-mail with the Reporting Identification Symbol as the first and only required entry.
- ❑ The user may send unclassified data as an attached file in the approved format to: data@nmmss.com
- ❑ The user must **Sign** and **Encrypt** the message each time data is submitted.

Notes:
When the user **Sign**s a message, the signature ensures that the recipient knows the sender.
When the user **Encrypt**s a message, the encryption ensures that any tampering will be detected.

5.0 Acknowledgement of Receipt

- ❑ DATA will reply to original message and acknowledge receipt of a signed and encrypted message.



Desktop Procedure for Establishment of Unclassified Internet Data Submission

Notes:

A simple analysis of the x.509 certificate follows:

When a user is issued the x.509 certificate, it contains two components - a private and public key. These keys are used to encrypt (or lock) and de-encrypt (or unlock). The user secures his/her private key. This key ensures that only the sender can encrypt the message. Through the exchange of public keys, the sender has authorized the recipient to de-encrypt a message the sender encrypts.