(U//FOUO) Attention All Program Managers, Developers, and Website, Application and Database Owners:

FROM: Michael McNamee
Chief, SIGINT Systems Engineering (S01A)
Run Date: 06/21/2006

(U//FOUO) By next summer, externally accessible SIGINT databases and applications must be configured to use PKI certificates instead of usernames and passwords.

(U) If you maintain or own an external-facing SIGINT database or application that does not currently use PKI, this message affects you.

(U//FOUO) NSA takes seriously its obligation to share information with Second Party, Intelligence Community and DoD partners. We are also commited to enabling secure single sign-on to SIGINT systems. Both of these factors have led to the use of public key (PK) enabling of databases and applications accessed by users external to NSAW.

(U//FOUO) PK enabling:

- Positively identifies the user or recipient of information including nationality, organization and clearance level (when used with corporate authorization services) each time a connection is made;
- Reduces the use of multiple passwords to access multiple applications and databases;
- Expedites the granting of access to SIGINT databases to tactical military SIGINTers;
- Enables federated access to SIGINT applications and databases by Second Party and IC users external to NSANet via cross certification;
- Simplifies password management by system administrators, as secure channels are no longer required to inform users of new account names and passwords.

(U//FOUO) **Systems and applications must be configured to use PKI certificates for login in lieu of usernames and passwords.** This message provides advance notification of the requirement for PKI implementation. If you maintain or own an external-facing SIGINT database or application that does not currently use PKI, **you must re-configure your applications by 30 June 2007.**

(U//FOUO) Applications that currently use the PASSPORT system for password maintenance must be moved to CASPORT and must convert to PKI use by 31 December 2006. Owners and developers of these PASSPORT enabled systems have previously been individually notified of the need to migrate to the use of PKI and CASPORT the end of the calendar year.

(U) A draft of the policy mandating public key enabling of applications and databases is available here . Please address questions or comments to SID POCs: Brooks Emrick [redacted], [redacted]) or [redacted] ([redacted] [redacted]). Information on PKI is also available at go PKI and information on the corporate authorization service, CASPORT, is available at go CASPORT .

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid comms)."