INFORMATION ASSURANCE DIRECTORATE

"INFORMATION ASSURANCE LEADERSHIP FOR THE NATION"

INFORMATION ASSURANCE IA ALERT **Date: 8 June 2011**

SUBJECT: Replacement of RSA SecurID Tokens Strongly Recommended

1. New evidence has surfaced indicating that the risk of relying upon RSA SecurID tokens issued prior to April 2011 as a second form of authentication is greater than previously assessed. NSA's Information Assurance Directorate strongly advocates that enterprises employing RSA SecurID tokens replace these tokens. At the same time, it is critical to establish that local RSA Authentication Managers are hardened and not compromised; and to protect all information regarding RSA tokens and infrastructure.

2. To obtain replacement tokens, enterprises should contact RSA directly through their normal acquisition channels. Acquiring and implementing use of replacement tokens will not provide a complete mitigation by itself. The Information Assurance Directorate therefore recommends that, at a minimum, users take basic steps to harden their infrastructures and to heighten their awareness of proper security practices so they are less vulnerable to network intrusions. For specific guidance documents, see NSA's website at: http://www.nsa.gov/ia/guidance/index.shtml.

3. In addition to replacing tokens, it is of primary importance that enterprises ensure that local RSA Authentication Managers (AM) are hardened and not compromised. Follow the guidance in IAA-003-2011 (attached) for hardening the local AM. The Information Assurance Directorate strongly encourages, where possible, building a new AM system from known-good software distributions and using it to replace the existing AM as part of the upgrade process. Additionally, if the AM is on a Windows server, then the enterprise needs to assess the probability that a Domain Admin account has been compromised. If there is a reasonable probability, then the threat of a compromised domain exploiting the new SecurID seeds must be mitigated by the enterprise. This can be done through a combination of measures, including but not limited to: a global password reset, not joining the machine to the domain, or implementing the AM on a platform that can't be joined to the domain. (Alternatives include Red Hat Enterprise Linux and Solaris, which are officially supported by RSA).

4. Enterprises should also protect supporting information regarding RSA tokens and infrastructure, particularly spreadsheets and databases which correlate seed files, seed values, token serial numbers and users. This information should be maintained in offline systems or, at a minimum, be encrypted.

5. Until old tokens are replaced by new tokens, enterprises should restrict remote access for users with old tokens to the bare minimum needed for business operations. Remote logins using old tokens that are still permitted should be audited to the greatest extent possible to ensure they are authorized. In addition to scrutinizing SecurID logs for failed attempts, enterprises should thoroughly examine remote login times, locations, IP addresses, and the actions of users logged in remotely in order to detect a compromised SecurID token and PIN. Enterprises should also consider frequent PIN resets of tokens that were issued before April 2011.