INFORMATION ASSURANCE DIRECTORATE

"INFORMATION ASSURANCE LEADERSHIP FOR THE NATION"

INFORMATION ASSURANCE ADVISORY **Date: 28 March 2011**

SUBJECT: Recommended Actions for SecurID Users in Response to RSA Cyber Intrusion

RSA has publicly stated that information was extracted from its company network which could reduce the effectiveness of the SecurID two-factor authentication. On 18 March, an Information Assurance Alert – Mitigations for the RSA Cyber Intrusion was released providing up-front guidance to mitigate threats associated with this data loss. This advisory provides additional guidance on:

- The use of SecurID hard tokens and soft tokens
- Fortifying the security profile of SecurID's authentication factors
- Measures to harden SecurID's Authentication Manager

Users should evaluate these recommendations against their particular risk factors and operational considerations.

RSA has issued specific guidance which should also be reviewed. This includes the best practice guidelines, available at the following URL: www.rsa.com.

The Use of SecurID Hard Tokens and Soft Tokens

RSA is exploring a range of remediation strategies and best practices for its customers. However, implementation of these strategies may take some time. Customers, including USG agencies, should continue to work with RSA to develop short-term and long-term mitigations that are appropriate for their needs. Options include:

1. Continued use of hard tokens.

In some circumstances, the risk of continued use of hard tokens may be deemed minimal. For example, a system that is physically isolated from external networks might not be subject to significant threat. However, even if the continued use of hard tokens is deemed acceptable, customers should consider implementing some of the recommendations below to more fully harden their systems.

2. Replacing hard tokens with soft tokens.

An alternative to the use of hard tokens is to deploy soft tokens. For this option, an application is installed on a computing device to generate a one-time password. The downside of this approach is that all authentication information is then stored on that device. The effectiveness of soft token-based solutions depends on the type of device and means to integrate it into the authentication solution.

Soft tokens can be deployed via:

- A non-networked Personal Digital Assistant (PDA). One of the main benefits of an external token is that the seed value is not stored on the user's computer, which may be vulnerable to network intrusion. A non-networked PDA with soft token functionality could provide the same level of assurance. For this option, the end user would load the soft token on the device and then use it just like the original hard token. Two issues for USG customers would be the availability of these devices and the need to disable networking features. This solution may be more viable for the larger user community.

- A smartphone. A smartphone (e.g. BlackBerry, iPhone, Android) could be loaded with the soft-token functionality and used in the same manner as the hard token. This option might gain wider acceptance than the non-networked PDA option, as smartphones are routinely carried by both senior government officials and non-government personnel. The downside is that these devices are networked and thus more susceptible than the SecurID token or non-networked PDA to network intrusion. This may be the most viable option for many USG customers.

Fortifying the Authentication Factors

As a best practice, for critical applications, SecurID should not be used as the sole means of authentication. Recommendations and guidance on additional authentication measures and how to securely implement them are below.

1) Augment SecurID with usernames and passwords. A relatively simple way to augment SecurID is to also require a user to log in to the protected system/network. This forces the adversary to compromise additional user information in order to gain access. Specific measures include the following:

    - Enable Account Login Restrictions – Enclaves should establish standard working hours for users and disable remote logins outside of users' established working hours. This can be enforced by the Authentication Manager or many account authorization systems such as Active Directory or LDAP.

- Require users to phone-in before logging in – Require remote users to call in to system administrators in order to authorize remote logins for a period of time. Accounts should have remote login disabled by default and manually enabled by a system administrator when called by the user. The accounts should revert back to a disabled state automatically after a defined period of time.

2) Augment SecurID with the DoD Common Access Card (CAC) card. A DoD customer could choose to augment or replace its existing SecurID system with the DoD CAC card, which is widely used across the DoD. A downside of this is that an entirely new system would need to be integrated into the enterprise infrastructure and users and administrators would need to familiarize themselves with new procedures. Customers in other parts of the US Government could employ HSPD-12(PIV) cards in a similar manner.

3) Perform regular audits of remote login activity. Enclaves should regularly audit login activities in order to identify unauthorized activity. For U.S. Government users, any unusual or unauthorized activity should be immediately reported to DHS/US-CERT or USCYBERCOM. Specific steps include:

   - Verify remote logins with each user. Logs of remote access can be verified on a daily or weekly basis. This is especially critical for high-risk users and/or critical applications. At a minimum, verify remote logins for users associated with suspicious activity.

   - Analyze logs for unusual IP Addresses. This will help identify remote access from unknown IP addresses for a given user.

   - Analyze logs for failed login attempts. A spike in the number of failed login attempts may indicate adversarial activity.

   - Notify users of last logins. Users can be prompted with their last login date/time with each login. This will help users identify unauthorized activity on their accounts

4) Implement robust PIN policies – If it is not possible to integrate additional mechanisms, implement strong policies for PIN and password usage and selection. The following should be considered:

   - Enforce the selection of robust PINs and passwords (e.g. longer and more complex PINs). Implement a randomized pin capability in which the pin is randomly generated and issued to the user.

   - Have users select new PINs and passwords and increase the frequency at which this needs to be performed. If possible, positively confirm the identity of the user

requesting the PIN change (e.g. via face-to-face interaction) and review logs associated with that user to detect indications of unauthorized SecurID use.

- Implement quicker user lock-out after failed log-in attempts. Disable automatic re-enablement of locked-out accounts in the Authentication Manager.

Authentication Manager (AM) Hardening

1. Change default passwords. Many systems are installed with a default password. Often this value is not changed after installation is complete. This password should be changed immediately in accordance with robust password policies.

2. Install a system integrity checker. The integrity of critical network resources, such as the AM, should be maintained. Tools can be installed on a server to establish a system baseline and then monitor the system for changes to that baseline. For this to be truly effective, it is recommended that the AM be loaded on a clean server.

3. Only install valid software. The Windows operating system (OS) validates signatures on critical software, such as extensions of the OS or cryptographic subsystem. Windows informs the user of the results of the validity checks. If these checks fail, that software should not be loaded onto the system.

4. Do not co-locate the AM with other services. If possible, house the AM on its own server platform to minimize the potential of it being exploited via vulnerabilities from other services. Disable all unneeded services. In particular, file system sharing between the AM server and other servers should be prohibited.

5. Restrict Internet access from the AM. As stated above, the integrity of the AM is critical to the proper functioning of the SecurID system. To help maintain the integrity of the AM, access to the Internet from the AM should be restricted to the greatest extent possible. If access is not needed, prohibit it. If access is required but only to a finite set of machines or services, restrict access accordingly.

6. Limit user access to the AM. User access to the AM should be restricted to only those administrators requiring access.

7. Baseline the AM network communications. As part of normal operations, the AM must interface with other components on the network (e.g. domain server, end user host). Network traffic associated with those communications should be collected, analyzed, and baselined. Once this baseline is established, communications should be monitored to detect anomalous traffic.

8. Establish firewall rules to restrict network access to the AM. The AM should initiate connections with only a select set of devices and only a select set of devices should initiate connections with the AM. For example, the Agent initiates communications with the AM and the AM initiates communications with the Active Directory domain controller. Firewall rules should be defined to restrict data flow to only that which is required for the AM to function on the network. All other connections should be prohibited. Standard network security practices should also be considered to the network around the AM.

9. Limit user access to only a specific IP address or range of IP addresses. User access should be limited to only those IP addresses that are valid for that user or in the case of DHCP, for that network. Access from any other IP address should be prohibited. Network Access Control (NAC) and Trusted Network Connect (TNC) are two technologies that can be used for this. Similarly, hardware MAC address protection will aid in the prevention of unauthorized systems to administer or attack the AM.

10. Restrict remote access to the AM. It can be assumed that an adversary attempting to access an AM would do so from a remote computer. Therefore, it is critical that remote access be limited and monitored. Some suggestions are:

    - Only allow remote access to those users truly requiring it to perform their job duties.
    - Restrict remote access to certain times. This can be baselined based on users' typical access times and can be enforced by many account authorization systems like Active Directory and LDAP.
    - Require a remote user to call in prior to remote authentication and lock out that user's remote access at other times.