National Aeronautics and
Space Administration
Goddard Space Flight Center

NO. 05-19	
DATE 11/22/2004	
DISTRIBUTION	
GREENBELT ONLY	* AA
WALLOPS ONLY	*
GSFC	*
CONTRACTORS	**

ANNOUNCEMENT

SUBJECT:

Holiday IT Security Preparation Guidance

With the holiday season arriving soon, Enterprise Information Technology Security Branch (EITSB), Code 297 would like to take this opportunity to thank each of you for the cooperation and hard work this year. Together we have accomplished some major milestones and overcome some impossible tasks. We look forward to working with all of you in the coming New Year and would like to wish you and yours a happy and safe Holiday Season.

Before leaving for the Holidays we would like to ask that you impart the following information to your organizations.

All Employees

- Don't forget to power off printers, copiers, computer peripherals, etc. Printers and other computer peripherals, even in "stand-by" mode, consume a fair amount of electricity.
- If a system needs to be left powered on, all idle users should be logged off or lock the screen with a password.
- Every year, a number of Holiday scams are perpetrated on businesses. Please use caution in responding to any phone, fax, or email solicitation. Legitimate fund-raising efforts should not be contacting employees at work, except through sanctioned channels.

In previous years, reports have been received of calls to employees to "verify a Holiday card mailing list". This is an example of social engineering, in which the caller is attempting to obtain a list of employees for an inappropriate use. Please use caution in providing information to unknown parties about your fellow employees.

PLEASE POST AND CIRCULATE THIS ANNOUNCEMENT

DISTRIBUTION CODES:
*A (Civil Service) – GSFC Employees
*B (Civil Service) – GSFC Section Level & Above
*C (Civil Service) – GSFC Branch Level & Above
*D (Civil Service) – GSFC Division Level & Above
**A (Contractor) – Contractor and Other Employees
**B (Contractor) – Contractor and Other Offices

System Administrators

- Power off as many systems as possible.
- Disable services that are infrequently used, or limit access to minimally required systems. Each service that is not available reduces the potential access methods an attacker can use to attack your system.
- Backup your systems before you leave. Be sure the back up are secured in a safe location.
- Ensure patches are all up to date before leaving on vacation or Holiday. Lack of patches is one of the most common weaknesses found in systems that have been compromised by a remote attacker.
- Ensure an alternate is available (and known to your local organization).
- Escrow your root/Administrator password with a trusted party. This could be an alternate administrator, an envelope in your manager's safe, etc. The escrowed password should be made available in case of an emergency when you (or your alternate) are not available.
- The end of year is a good time to perform account maintenance (expire unnecessary accounts) and inventory management (update the location of every piece of tagged hardware).

Webmasters

- Check with your systems administrators to ensure your server is up-to-date on patches and ready for the Holidays.

DCSO's/CSO's

- Notify Center IT Security Manager if the DCSO, CSO and Alternates will be absent for an extended period (>3 days).

Bernard V. Tomardy

Bernard V. Tomardy, Branch Head
Enterprise Information Technology Security Branch