

AP2. APPENDIX 2

SAMPLE NOTIFICATION LETTER

Dear Mr. John Miller:

On January 1, 2006, a DoD laptop computer was stolen from the parked car of a DoD employee in Washington, D.C. after normal duty hours while the employee was running a personal errand. The laptop contained personally identifying information on 100 DoD employees who were participating in the xxx Program. The compromised information is the name, social security number, residential address, date of birth, office and home email address, office, and home telephone numbers of the Program participants.

The theft was immediately reported to local and DoD law enforcement authorities, who are now conducting a joint inquiry into the loss.

We believe that the laptop was the target of the theft as opposed to any information that the laptop might contain. Because the information in the laptop was password protected and encrypted, we also believe that the probability is low that the information will be acquired and used for an unlawful purpose. However, we cannot say with certainty that this might not occur. We therefore believe that you should consider taking such actions as are possible to protect against the potential that someone might use the information to steal your identity.

You should be guided by the actions recommended by the Federal Trade Commission (FTC) at its Web site at http://www.consumer.gov/idtheft/con_steps.htm. The FTC urges that you immediately place an initial fraud alert on your credit file. The Fraud alert is for a period of 90 days, during which, creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information that can be taken now or in the future if problems should develop.

The Department of Defense takes this loss very seriously and is reviewing its current policies and practices with a view of determining what must be changed to preclude a similar occurrence in the future. At a minimum, we will be providing additional training to personnel to ensure that they understand that personally identifiable information must at all times be treated in a manner that preserves and protects the confidentiality of the data.

We deeply regret and apologize for any inconvenience and concern this theft may cause you.

Should you have any questions, please call _____.

Sincerely,

Signature Block
(Directorate level or higher)