SECURITY INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED WITHIN 24 HOURS OF DETECTING A SECURITY INCIDENT. (The affected individual is responsible for gathering pertinent information and completing this form.)

I. GENERAL INFORMATION [Section I, must be completed entirely]

Primary Contact: _____
E-Mail Address: _____
Telephone number: _____
Cell Phone Number: _____ FAX number: _____
Pager number: _____
Physical Location of Incident: _____

II. HOST INFORMATION [Section II, must be completed entirely]

Please provide information about all host(s) involved in the incident. Each host shall be listed separately.

Computer name: _____
IP Addresses: _____
Computer hardware: _____
Operating System and version: _____
Where on the network is the involved host? – (Home, Shared Lease space, Regional and Headquarters):_____
Nature of the information at risk on the involved host – NAD Case Files, Personnel, Financial, Privacy Act.

_____

Time zone of the involved host: _____
Was the host the source or victim of the attack or both:

_____

Was this host compromised as a result of the attack? ○Yes ○No
Hours system down_____

III. INCIDENT CATEGORIES

All categories applicable to the incident shall be documented.

Data Loss(es): _____

Hardware Loss(es): _____

Intruder gained "access" ○Yes ○No

Cracked password ○Yes ○No
Easily-guessable password ○Yes ○No
Misuse of host(s) resources ○Yes ○No

IV. SECURITY TOOLS

At the time of the Incident, was the individual using any of the following? ○Yes ○No

Authentication/Password tools: _____
Anti-Virus tools: _____
Other tools: data encryption, hardware encryption(s)

Were logs being maintained: If so, please describe.

_____

V. DETAILED INCIDENT DESCRIPTION

Detailed Incident Description: This should be as detailed as possible, especially when writing lesson learned or after the incident follow-up report. Please use separate sheets of paper to address the following:

A. Duration of Incident: _____

B. How was the incident discovered? _____

C. Method(s) used by intruders to gain access to host(s): _____

D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections:

_____

E. Hidden files/directories:

_____

G. Did system contain classified/sensitive information? What type?

_____

H. Was the information compromised?