

Security Incident Notification

Agency _____ ORI: _____

Agency TAC: _____ Agency LASO: _____

Affected Systems and Locations: _____

Other Organizations Affected: _____

Date/Time of Incident: _____ Reported by: _____

Type of Incident: Malware/virus _____ Denial of Service _____ Network Intrusion _____ Other _____

What was happening at time of incident? (What applications were running, web sites visited, etc.)?

How was incident discovered?

Anti-Malware Software Alerted: During Real time Activity scans _____ During Scheduled Scan _____

Who received the alert? I.T./Administrator _____ Device End User _____

Manual scan using installed software _____ Manual Scan using alternate software _____

Give details why a manual scan was done or other details to how incident was discovered: _____

Name of infection as indicated by anti-malware software: _____

What Anti-Malware Application was running on the device(s) at time of incident?

Brand: _____ Date of Signature Definitions: _____

Damage Assessment: (include any indications if sensitive Data was lost or compromised) _____

Security Incident Notification

Notifications:

Date/Time LASO notified _____ By: _____

Date/Time I.T. notified _____ By: _____

Date/time KBI notified _____ KBI ticket # _____

Date/time KHP notified _____

Corrective / Resolution Measures:

Contact information of personnel performing corrective /restoration actions:

Name _____ phone: _____ email: _____

Agency employee _____ Government I.T. _____ Private Contractor _____

Name _____ phone: _____ email: _____

Agency employee _____ Government I.T. _____ Private Contractor _____

Was affected Device(s) Hard Drive erased and reformatted? Yes _____ No _____

If No, give details how malware was eradicated _____

Were files restored from a backup? N/A _____ NO _____

YES, from a: Network backup _____ Removable Storage Device _____

Operating System Restore Point/Recovery Disc _____

What Anti-Malware Application is currently running on the repaired device(s)?

Brand: _____ Date of Signature Definitions: _____

Actions being taken to minimize future incidents: _____
