**Cyber 9-Line**

\*Note: All fields are mandatory unless “If Applicable” is listed in the description field.

|  |  |
| --- | --- |
| **Line 1 : Reporting Unit Information** | |
| Unit |  |
| Unit Location |  |
| Secure Phone / Email |  |
| **Line 2 : Location of Activity** | |
| Point of Contact |  |
| Secure Phone / E-mail |  |
| Victim Organization |  |
| Victim Location |  |
| **Line 3 : Technical Details** | |
| System / Application Affected |  |
| System Domain (SIPR, NIPR, etc.) |  |
| System Mission / Role |  |
| IP Address: Destination |  |
| MAC Address |  |
| System Name |  |
| Operating System |  |
| Malware / Suspicious Activity |  |
| File Name (If Applicable) |  |
| Mission Impact |  |
| Detection Method (HIPS, logs, email etc.) |  |
| Detection Date Time Group (DTG) |  |
| **Line 4 : Description of Event** | |
|  | |
| **Line 5 : Incident/Ticket/CAT # (If Applicable)** | |
|  | |
| **Line 6 : Reporting Unit Commander** | |
| **Name / Rank** |  |
| **Secure Phone / Email** |  |
| **Line 7 : Updates (If Applicable)** | |
|  | |
| **Line 8 : Recommendations (If Applicable)** | |
|  | |
| **Line 9 : Actions Taken (If Applicable)** | |
|  | |