**INSTRUCTIONS:** This report Section 1 shall be completed to the extent possible by the person reporting or involved in a security or privacy incident (or their manager/supervisor). The report should be sent by email to [*CMS\_IT\_Service\_desk@cms.hhs.gov*](mailto:CMS_IT_Service_desk@cms.hhs.gov)*.* The Reporting Individual should collaborate with the CMS Incident Management Team (IMT) to update this report as the incident is resolved.

If the Reporting Individual does not initially have enough information to complete the report at this time, fill out as much as possible. DO NOT DELAY reporting this or any other incident, even if the incident is not yet confirmed. All suspected information security and privacy incidents must be reported to the CMS IT Service Desk within one hour of initial detection.

**Section 1: Incident Information**

*(This section to be completed by the Reporting Individual to the extent possible at the time of the report.)*

**Date/Time of Initial Report:**

**Date/Time Activity First Detected:**

**Incident Tracking Number:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Reporting Individual Contact Information** | | | | | |
| **First Name** | | **Last Name** | | **Email** | |
|  | |  | |  | |
| **Office Number** | **Cell Number** | | **Dept/OPDIV** | | **UserID** |
|  |  | |  | |  |

|  |  |
| --- | --- |
| **PII/PHI Breach Information** | |
| **Is PII/PHI suspected to be compromised (Yes/No)?** |  |
| **(If Yes) Estimated Total Number of PII/PHI Records Impacted:** |  |
| **(If Yes) Estimated Total Number of Users Impacted:** |  |

|  |  |
| --- | --- |
| **Incident Description**  *(Please describe the incident. This section should be updated as the incident is handled.)* | **Last Update Date/Time** |
| **How was this incident detected/discovered?** |  |
|  | |
| **What triage/analysis has been performed?** |  |
|  | |
| **Is the incident contained? How?** |  |
|  | |
| **What recovery/remediation action has taken place?** |  |
|  | |

**Section 2: Estimated Incident Impact (Optional)**

*(This section is optional, intended for security personnel to complete where possible.)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impacted FISMA System Information**  *(If more than one FISMA system is impacted, fill out a copy of this table for each system)* | | | | | | |
| **FISMA System Name** | |  | | | | |
| **FISMA System Officials** | | | | | | |
| **Official** | **First Name** | | **Last Name** | **Email** | **Cell Number** | **Notified?** |
| Business Owner |  | |  |  |  |  |
| Information System Security Officer |  | |  |  |  |  |
| Other: |  | |  |  |  |  |

**Functional Impact**

No Impact  Significant Impact to Non-Critical Services

No Impact to Services  Denial of Non-Critical Services

Minimal Impact to Non-Critical Services  Significant Impact to Critical Services

Minimal Impact to Critical Services  Denial of Critical Services/Loss of Control

**Information Impact**

No Impact  Destruction of Non-Critical Systems

Suspected But Not Identified  Critical Systems Data Breach

Privacy Data Breach  Core Credential Compromise

Proprietary Information Breach  Destruction of Critical System

**Recoverability**

Regular  Extended

Supplemented  Not Recoverable

**Attack Vector**

Unknown  Impersonation/Spoofing  Other

External/Removable Media  Attrition

Improper Usage  Web

Loss or Theft of Equipment  Email/Phishing

**Location of Observed Activity**

L1 – Business Demilitarized Zone  L4 – Critical System DMZ  L7 – Safety Systems

L2 – Business Network  L5 – Critical System Mgmt  – Unknown

L3 – Business Network Mgmt  L6 – Critical Systems