Incident Response Form

| **Breach Date and Time:**  MM/DD/20YY, H:M:S(:MS) | |
| --- | --- |
| **Affected IP/Hostname of Breached System(s):**  IP | Hostname | |
| **Source IP of Attacking System(s):**  (REQUIRED.) | |
| **Breach Narrative:**  (Provide information about the breach in detail here, including the type of incident.) | |
| **Impact on Services:**  Please highlight the designated impact below: | |
| None | No effect to the organization’s ability to provide all services to all users |
| Low | Minimal effect; the organization can still provide all critical services to all users but has lost efficiency |
| Medium | Organization has lost the ability to provide a critical service to a subset of system users |
| High | Organization is no longer able to provide some critical services to any users |
| **Impact on Information:**  Please highlight the designated impact below: | |
| None | No information was exfiltrated, changed, deleted, or otherwise compromised |
| Privacy Breach | Sensitive PII of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated |
| Proprietary Breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated |
| Integrity Loss | Sensitive or proprietary information was changed or deleted |
| Please highlight the applicable metrics below: | |
| **Attack Vector:**  Network Adjacent  Local Physical | **Attack Complexity:**    Low High |
| **Privileges Required:**  None Low High | **User Interaction:**  None Required |
| **Scope:**  Unchanged Changed | **Confidentiality:**  None Low High |
| **Integrity:**  None Low High | **Availability:**  None Low High |
| **Remediation/Mitigation Steps:**  (Steps to take in order to patch exploited machines and prevent further vulnerability.) | |
| **Extra Artifacts:**  (Additional artifacts related to the incident should be listed in this section. This can be text, code, or pictures.) | |

This template is modeled after the Forum of Incident Response and Security Teams (FIRST)’s Common Vulnerability Scoring System (CVSS) ([*https://www.first.org/cvss/calculator/3.1*](https://www.first.org/cvss/calculator/3.1)). This template is also copied over from our team members’ past engagements as it was customly developed to be applicable in all situations.