Information Sharing Report

Contact Information:

Name	
Title	
Telephone	
Email	
Internal Tracking Number	
Organization Name	

Type of Organization				
□ Federal Government	□ Private Sector	□ Critical Infrastructure	□ ISAO/ISAC	□ SLTT

Opt-In. This information may be shared with:			
□ Federal Government ○ CISA ○ IC3 ○ AIS ○ Other: __________	□ Law Enforcement ○ FBI ○ USSS ○ State law enforcement ○ Other: _________	□ Other ○ MS-ISAC ○ ISAO: _____________ ○ Partner: ___________ ○ Insurance: _________	□ Public

Incident Details:

Date/Time of Start	
Date/Time of Detected	
YYYY-MM-DD HH:MM:SS	

Time Zone	
□ Atlantic Standard Time (AST): UTC–4	□ Alaska Standard Time (AKT): UTC-9
□ Eastern Standard Time (ET): UTC–5	□ Hawaii-Aleutian Standard Time (HAT): UTC-10
□ Central Standard Time (CT): UTC–6	□ Samoa Standard Time (ST): UTC-11
□ Mountain Standard Time (MT): UTC–7	□ Chamorro Standard Time (ChT): UTC+10
□ Pacific Standard Time (PT): UTC–8	□ Wake Island Time Zone (WIT): UTC+12

Incident Title	
Description	

CIA Compromise: Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised?

□ Confidentiality: Was there potential or actual unauthorized access to protected or sensitive information?
□ Integrity: Was there intentional modification of information by unauthorized users?
□ Availability: Did authorized users have timely and uninterrupted access to information and systems?

Functional Impact: A measure of the impact to business functionality or ability to provide services.

□ No Impact – Event has no impact.
□ Impact to Non-Critical Services - Minimal or significant impact to non-critical systems and services.
□ Impact to Critical Services - Minimal or significant impact but to a critical system or service such as email or active directory.
□ Denial of Non-Critical Services - A non-critical system is denied or destroyed.
□ Denial of Critical Services or Loss of Control - A critical system has been rendered unavailable.

Information Impact: Describes the type of information lost, compromised, or corrupted.

□ Suspected – Data loss or impact to availability is suspected, but no direct confirmation exists.
□ Privacy Data Breach - The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
□ Proprietary Data Breach -The confidentiality of proprietary information like protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
□ Destruction of Non-Critical Systems - Destructive techniques, such as master boot record (MBR) overwrite; have been used against a non-critical system.
□ Critical Systems Data Breach - Data pertaining to a critical system has been exfiltrated.
□ Core Credential Compromise - Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
□ Destruction of Critical System - Destructive techniques, such as MBR overwrite; have been used against a critical system.

Recoverability: Identifies the scope of resources needed to recover from the incident

□ Regular – Time to recovery is predictable with existing resources.
□ Supplemented – Time to recovery is predictable with additional resources.
□ Extended – Time to recovery is unpredictable; additional resources and outside help are needed.
□ Not Recoverable – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).