Arizona Department Of Administration
Risk Management Division
CYBER LOSS REPORT

Please fill out as much of the loss report as possible.

AGENCY	DIVISION	SECTION
Loss Coverage: ☐ 1st Party Loss (direct loss to the agency) ☐		3rd Party Loss (harm to others)
Key Person(s) to Contact:		Position:
Email:		Phone Number:
Incident Lead Name:		Position:
Email:		Phone Number:
Name of the computer system affected:		Number of people affected:
Specifically what section or person in the division was affected:		
Location Address:		
Date/time loss was discovered/detected: Time: a.m. p.m. Date/time loss occurred: Time: a.m. p.m.		How was the event discovered:

PROVIDE THE INCIDENT TYPE	☐ Technology Asset* Outage	☐ DDoS**	☐ Ransomware
	☐ Technology Asset* Degradation/delay	☐ Insider Threat	☐ Unauthorized Access
	☐ ABM Jackpotting	☐ Malware - Other	☐ Loss/theft of Equipment
	☐ Account Take-over	☐ Malware Campaign	☐ Other (Specify below ↓)
	☐ Cyber Crime	☐ Online Extortion	
	☐ Data Breach/leak	☐ Phishing	

*A "Technology Asset" is something tangible (e.g., hardware, infrastructure) or intangible (e.g., software/application, data,information) that needs protection and supports the provision of technology services.
**Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks. A DDoS attack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic.

IMPACT OF THE INCIDENT/ SYSTEMS AFFECTED	IP Address(es):
	Hostname(s):
	Purpose of System(s):
	Operating System & Version:
	Ports of Communication Utilized:
	Physical Location:
	Attack Vector Utilized/Exploited:
	Evidence Discovered:
	Additional Details:

Arizona Department Of Administration
Risk Management Division
CYBER LOSS REPORT

Please fill out as much of the loss report as possible.

DESCRIPTION	Provide a description of what occurred and **include the Root Cause:**
	Direct and Indirect Impacts: Do we know threat actor and/or variant:
	Provide details on the tactics, techniques and procedures involved to respond/remedy:
	Timeline to address the remediation:
	Provide description of sensitive information compromised or at risk: (If no sensitive information is at risk please indicate N/A)
	Has a cyber company been called in to fix the problem: No Name of company:
	If this involves a ransom, who made the demand and how much is the ransom demand: Is there a ransom note: No Has there been any communication with the threat actor: No
	Does this involve a third party vendor: No **If yes**, Name of vendor:
	If yes, do you have a contract with them: No Do they have cyber insurance: No
NOTIFICATION	Have other regulators or supervisory agencies been notified: No Date: Time: a.m. p.m.
	Has senior management been notified: No Date: Time: a.m. p.m.
	Has your agency media person been notified: No Agency Media Person Notified:
	Has Homeland Security been notified: No Date: Time: a.m. p.m
	Has legal counsel been notified: No **If yes,** name of counsel:
	Has law enforcement been notified: No **If yes,** what agency: Report Number: Police Office/Contact Name: Have evidence logs and other forensic artifacts been preserved: No
	Has an external forensics firm been engaged: No Has a breach coach been engaged: No
	Were there any media reports: No **If yes,** who:
Remarks:	
Reported by:	Date:

Email Completed Form to: AZ Dept. of Homeland Security Operations Center at azsoc@azdohs.gov and plnewclaims@azdoa.gov

All cyber incidents and losses should be reported immediately to Arizona Department of Homeland Security's (AZDoHS) Security Operations Center at azsoc@azdohs.gov. This notification is required by A.R.S. section 18-105(E) and A.R.S. section 41-4282(E) which states that budget units and their contractors must identify and report security incidents to "the statewide information security and privacy office" - which resides with the Arizona Department of Homeland Security. AZDoHS will then notify ADOA Risk Management of those incidents they feel represent potential claims.