**Incident response report**

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-61, VERIS

Date:

**Contact Information for the Incident Reporter and Handler**

– Name

– Role

– Organizational unit (e.g., agency, department, division, team) and affiliation

– Email address

– Phone number

– Location (e.g., mailing address, office room number)

**Incident Category**

**[Cat 0 – Cat 6]**

**Incident Details**

– Status change date/timestamps (including time zone): when the incident started, when the incident was discovered/detected, when the incident was reported, when the incident was resolved/ended, etc.

– Physical location of the incident (e.g., city, state)

– Current status of the incident (e.g., ongoing attack)

– Source/cause of the incident (if known), including hostnames and IP addresses

– Description of the incident (e.g., how it was detected, what occurred)

– Description of affected resources (e.g., networks, hosts, applications, data), including systems’ hostnames, IP addresses, and function

– If known, incident category, vectors of attack associated with the incident, and indicators related to the incident (traffic patterns, registry keys, etc.)

– Prioritization factors (functional impact, information impact, recoverability, etc.)

– Mitigating factors (e.g., stolen laptop containing sensitive data was using full disk encryption)

– Response actions performed (e.g., shut off host, disconnected host from network)

– Other organizations contacted (e.g., software vendor)

**VERIS**

* **Actions [Hacking, Social, Malware, Misuse]**
* **Actors [Internal, External, Partner]**
* **Asset [Server, Network, User Device]**
* **Attribute [Confidentiality, Integrity, Availability]**

**General Comments**

COMPUTER SECURITY INCIDENT HANDLING GUIDE

**Current Status of the Incident Response**

**Summary of the Incident**

CISCO CyberOp

Who: What IP and Domain was associated with the malware?

What: What type of malware is on the system?

When: When did the event occur?

Where: Where is geolocation of the originating source of attack?

Why: Why was the malware designed for this intended purpose?

How: How did the malware get onto the system?

**Incident Handling Actions**

– Log of actions taken by all handlers

– Contact information for all involved parties

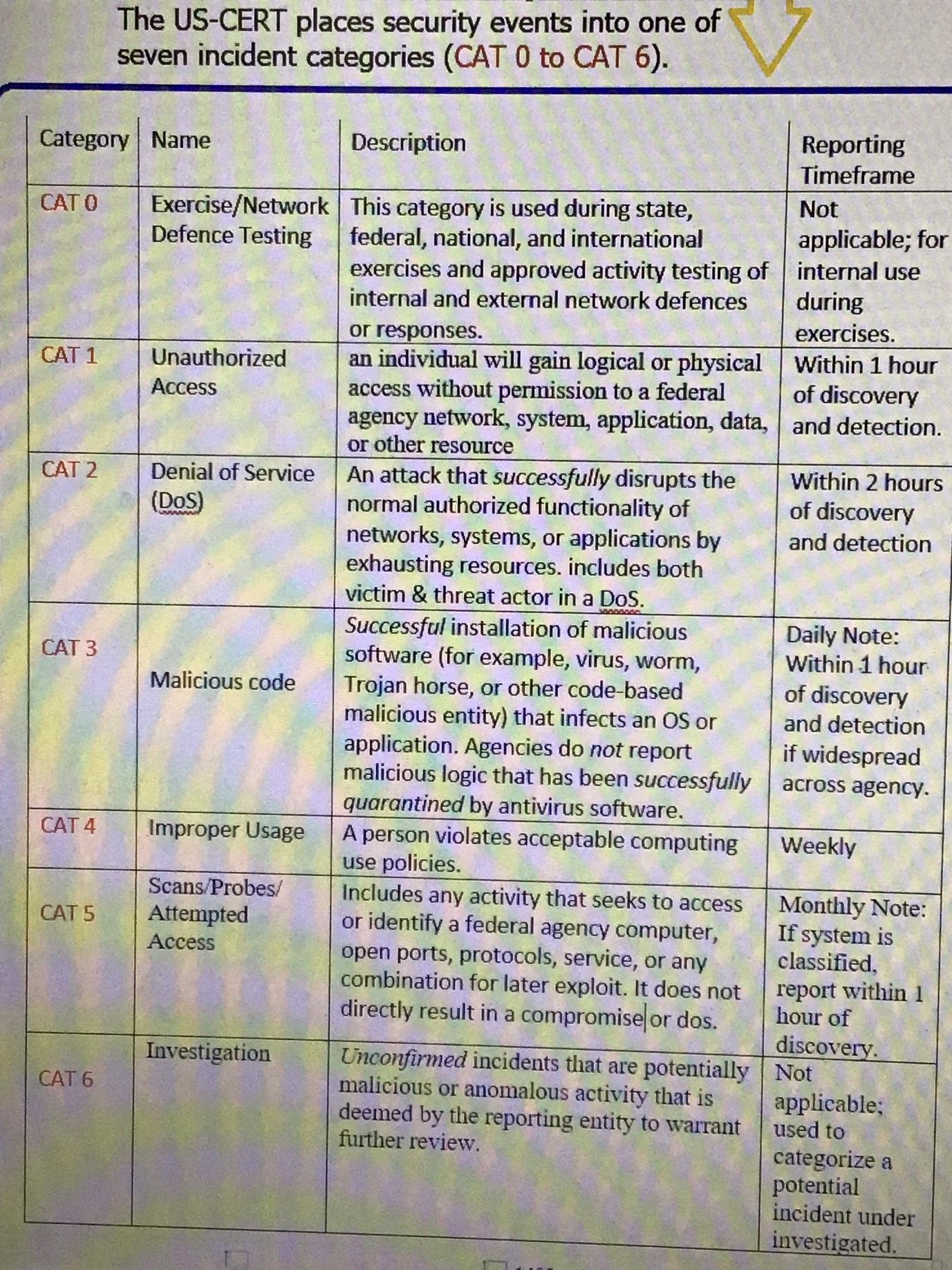
– List of evidence gathered

**Incident Handler Comments**

**Cause of the Incident (e.g., misconfigured application, unpatched host)**

**Cost of the Incident**

**Business Impact of the Incident**

**Appendix**