Security Incident Response Procedures

Version 2.2

PROCEDURE INFORMATION	
This table should be completed by the responsible office and IT Risk & Compliance, as it provides general information about the procedure.	
RESPONSIBLE OFFICES	IT Security Office (ITSO)
RELATED DOCUMENTS	▪ University Policy Number 1305, Reporting Electronic Security Incidents ▪ ITS.ITS-PRS004, Incident Management Process ▪ ITS.ITS-STD005, IR Plan for PCI DSS Incident ▪ DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
REFERENCE DOCUMENTS	SANS Security Incident Forms (https://www.sans.org/score/incident-forms)
DOCUMENT CONTROL NUMBER	ITS.ITSO-PROC004
LAST REVIEWED DATE	6/21/2024
INTENDED USERS	The intended user for this procedure is the Primary Forensic Investigator. The Primary Forensic Investigator is an ITSO Security Engineer or Analyst as defined by their position's Employee Work Profile (EWP). The Primary Forensic Investigator may work with the ITSO Analyst staff to assist with the analysis process.

NOTE TO ALL USERS

REVISION HISTORY

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
1.0	02/06/2020	ITSO / Mike Richardson	Initial release
2.0	02/05/2021	ITSO / Mike Richardson	Annual review with major revisions
2.1	06/23/2023	ITSO / Mike Richardson	Annual review with minor revision
2.2	6/21/2024	ITSO / Mike Richardson	Annual review with minor revisions - Correct grammatical errors throughout the document. - Update the Document Control Number (DCN) to reflect the current version. - Adjust the review frequency as per the latest organizational guidelines.

VERSION	DATE	ORGANIZATION/AUTHOR	DESCRIPTION OF CHANGES
			- Identify and update the responsible office for reporting cybersecurity breaches involving ITAR data

PROCEDURE'S PURPOSE AND SCOPE

Describe the purpose and scope of the procedure. Purpose describes what the procedure is about while scope outlines where the procedure starts and ends.

The purpose of this procedure:

This document outlines the general procedures for an incident response regarding a forensic investigation, including cybersecurity incidents impacting ITAR data in the CUI research environment. The Investigator may need to alter some aspects of their actions (mainly in the forensic capture of a device) based on best practices for the situation that presents itself in a particular case.

The scope of this procedure:

A request for forensic analysis can originate from several sources. A request may be generated internally from ITSO analyst staff based on log alerts (Splunk, FireEye, etc.), from an oversight department (Office of Institutional Research and Effectiveness), or from University Counsel.

DEFINITIONS

ACRONYM/TERM	DEFINITION
ORIA	Office of Research Integrity and Assurance
OSP	Office of Sponsored Programs

IR Go-Bag Contents

- SANS Security Incident Forms: https://www.sans.org/score/incident-forms
  - Incident Contact List
  - Incident Identification
  - Incident Survey
  - Incident Containment
  - Incident Eradication
  - Incident Communication Log
- GMU Chain of Custody Form
- Physical notebook for retention of case notes (preferably with serialized pages) – currently composition notebooks
- Laptop to serve as a capture device
- Forensic Write Blockers and associated cables
- Blank hard disks for image storage

- Disk carrier for image storage drives (capable of USB3, eSATA, or Firewire connectivity)
- Blank USB flash drive
- Blank DVDs, CD-Rs
- DVD and USB bootable images of current Forensic Linux Distributions, such as Kali Linux, Tsurugi Linux Acquire, or Sumuri Paladin
- Antistatic bags for media storage
- Tamper-proof Evidence bags
- Acquisition software (dd, Mandiant Memoryze)

INSTRUCTIONS

Reporting ITAR-related Incidents Procedure

In the event of a cybersecurity incident impacting the ITAR data in the CUI research environment,

1. ORIA must notify OSP by sending emails to export@gmu.edu and Lindsay Gilbreath (lgilbrea@gmu.edu) or the current contact for OSP, respectively
2. ORIA must report the incident to DoD within 72 hours of discovery to https://dibnet.dod.mil
3. When malicious software is discovered as being connected with the reported cyber incident, it is isolated, and ORIA submits the malicious software to the DoD Cyber Crime Center
4. ITSO can provide assistance to ORIA by preserving and protecting images of all known affected information systems and all relevant monitoring/packet capture data for at least 90 days from report submittal to DoD.
5. ORIA and OSP will have access to investigation updates and findings

Forensic Investigation Procedure for Compromised CUI/ITAR Virtual Machines

Once compromised CUI/ITAR Virtual Machine(s) is/are identified:

1. Record the following information:
    a. Responsible administrators, at least primary and secondary, including NetIDs and contact information
    b. Application and Data owner contact information
    c. External software vendor(s) with technical contact information, if available
    d. Hostname and any aliases
    e. vCPUs and Memory allocated
    f. Storage allocation
    g. Network or networks the virtual machine is attached to
    h. Cluster host, or individual hypervisor host
2. SUSPEND the virtual machine – DO NOT POWER OFF
3. Securely transfer the contents of the virtual machine directory to external storage media – this can be done through VMWare downloading from the data store or via SFTP.
    - include all files within the VM directory, including VMEM, VMDK files, and all restore points
4. If the external storage media is not hardware-encrypted (Aegis Padlock drive or similar), encrypt the individual files at rest.
5. Escrow a copy of the decryption key or Access PIN with the IT Security Office.

Forensic Investigation Procedure

Step 1 – Opening an Incident Response

1. Upon receipt of a request, a formal support ticket is created in the ITS ticketing system to track the incident.
2. The Forensic Investigator will reach out to the requestor to obtain more information regarding the background of the incident, contacts for the target system(s), location, and identification of the system under investigation.
    a. The SANS security forms for Contacts, Identification, and the Survey can be used for guidance on the questions to ask and to record the investigators' initial contact with the user(s) and the target(s) involved.

Step 2 – Obtaining Forensic Image(s) in the Field

1. The Forensic Investigator arrives on-site to identify the target system visually
    a. Photos of the location must be taken upon arrival
        i. Physical controls to the area where the system(s) is/are located
        ii. Pictures of the target systems in their existing state on-site, including connected cabling and storage media located nearby
    b. Record in the notebook a description of the location upon arrival
    c. The serial number or service code of the system(s) shall be recorded in the notebook and the Incident Forms
2. If the target is powered on and can be logged into (or is already logged in)
    a. Note the condition of the target in the notes
    b. Inventory currently running processes
    c. Attempt to obtain a live memory capture using the appropriate tool to an external USB device
        i. Windows machines – Mandiant Memoryze
        ii. Linux machines – may need a compiled module to allow full memory access – any changes to the filesystem have the potential to taint physical evidence
    d. Record current IP address, network MAC address, host name, and a list of filesystem and/or drive mounts.
    e. For Windows Machines: if the target disk is encrypted with BitLocker, record the Bitlocker recovery key.
    f. For windows machines: obtain the windows version and build number to faciliate faster analysis in Volatility.
    g. Once memory capture has been obtained, the system may be shut down
        i. For servers, indicate a reason for downtime e.g., "ITSO forensic investigation investigator: gunston"
3. Once the target is powered off (or if it already was powered off)
    a. Desktop or laptop computers with accessible internal HDDs
        i. Note the serial number of the disk(s) and connection(s) to the computer
            1. Enter the BIOS to determine the disk position in the IDE/SATA bus
        ii. If the drive can be attached to a forensic write blocker while in the chassis, attach the device to the source disk side of the write blocker hardware
        iii. If the drive must be removed, remove the disk and attach it to the source side of the write blocker hardware
    b. Server hardware or computers implementing RAID
        i. Start the machine, following prompts to enter the RAID configuration (per manufacturer documentation)

ii. Note the RAID configuration, serial numbers of participating disks, and any hotspares present in the chassis
    1. Some RAID controller software can blink the drive light to allow the identification of RAID members within the chassis. If possible, record physical disk positions in the investigation notebook
iii. Insert a Forensic Linux distribution USB or disc, booting in Live Forensic mode – this will disable the automatic mounting of disks and force all mounts to read-only

4. Capture the physical disks to a forensic disk image (including free space)
    a. Use a target disk that has been zeroed out or is brand new
    b. Using commercial software (FTK Imager) or software capable of creating EnCase or AFF forensic containers (E01, AFF)
        i. Whenever possible, capture the disk with the option to calculate MD5 and SHA-1 checksums during capture. Record capture times (start and finish), the hash values of the capture, and the filename used to store the captured image(s) in the Investigation Log
        ii. Record timestamps when the acquisition began and ended
        iii. As a last case resort, use dd (or ddfldd or dc3dd) to capture an uncompressed image
    c. For RAID arrays, the Investigator captures the array as presented to the operating system. Ideally, the capture should be on the RAID container, but individual partitions can be captured as separate forensic disk images
5. (OPTIONAL) Retain the original drive in a forensically sound manner
    a. Remove disk(s) from the chassis, record incident information and disk serial numbers on the outside of a tamper-proof evidence bag.
    b. Record disk serial number, system information, evidence bag number, and pertinent information on a GMU Chain of Custody Form
    c. Record retention action in an investigation notebook log
    d. Insert the disk into an antistatic bag
    e. Insert the antistatic bag into the evidence bag and seal
    f. Tear off the evidence bag tag and affix it to the appropriate page in an investigation notebook log
6. Reassemble the computer (if applicable), referring to photos for proper connectivity if cables were disturbed

Step 3 – Analyzing Forensic Image(s)

1. Copy field-captured disk and memory images to secure forensic workstation(s)
    a. Airgapped, fully updated Kali Linux with kali-forensic-all meta package installed
    b. Airgapped, fully updated Windows 10 with Autopsy or other Forensic Analysis tool installed
2. Live Memory Analysis
    a. Utilize the Volatility Framework (https://www.volatilityfoundation.org/) to process the memory image
        i. Assess currently active processes, looking for anomalies
        ii. Note results in the Investigation Log
3. Disk image analysis
    a. Basic filesystem analysis (file presence only)
        i. Mount filesystems read-only in Kali
    b. Semi-automated analysis (slack space, deleted files scanning)
        i. Import disk image(s) into Autopsy
4. All evidence should be recorded in the Investigation Log with the following metadata:
    a. date and time of discovery
    b. location

c. md5 and sha1 hash, if appropriate
d. summary of contents

Step 4 – Containment

1. Investigation workstation(s) must remain air-gapped when an investigation is in process or evidence is accessible on the drive
    a. In the Kali forensic workstation, the evidence drive is in a removable drive bay and can be detached physically before the system boots
2. Malicious binaries and/or documents retained on the investigation workstation should be stored with care

Step 5 – Eradication

1. The Investigator will make appropriate recommendations to remediate the workstation if necessary
    a. A general rule of thumb for infections or compromise is to rebuild the system from a known secure Gold Image or installation image, and any files to be returned from the infected system require screening to ensure the new install is not re-compromised

Step 6 – User Reporting

1. The Investigator will prepare a post-investigation report using a standard reporting template to include, at minimum
    a. An inventory of the device(s) involved and their physical location
    b. The timeline of the investigation, including the window of concern from the requestor
    c. Details on the acquisition of the image(s) involved
    d. One or more forensic results sections
        i. These should closely align with the requests from the requestor
    e. A section on post-action recommendations or remediations
        i. Recognized best practices to prevent future intrusions
        ii. User best practices to prevent reinfection

ARTIFACTS

ARTIFACT	PURPOSE
Forensic evidence	Examples include photos, notes, serial numbers, service codes, etc.
Incident Ticket	This is a record of an incident or problem reported in the ITS ticketing system.
Investigation Log with metadata	All evidence during a forensic investigation is recorded in this log which includes metadata on date and time of discovery, location, md5 and sha1 hash, and summary of contents.
Post-investigation Report	A report prepared by the Primary Forensic Investigator that includes the information described in Step 6 – User Reporting of Forensic Investigation Procedure.
Recommendations	Remediations to infected or compromised workstations that are recommended by the Primary Forensic Investigator during a forensic investigation. Can also provide suggestions to avoid compromise in the future, including changing user behavior or procedures.

SANS Security Incident Forms for Contacts, Identification, and Survey	The Primary Forensic Investigator uses these forms as a reference for the questions to ask and to document the initial interaction with users and targets.

TIMETABLE FOR REVIEW

This procedure will be reviewed on as-needed basis.

APPROVALS

ROLE	NAME & ORGANIZATION	SIGNATURE	DATE
Director, IT Security Office	Curtis McNay	DocuSigned by: Curtis McNay 6179577EE174479...	6/24/2024