APPENDIX B

Forms

EVIDENCE TAG		
Date	*Case Number*	*Evidence Tag Number*
Consent Required ☐ Yes ☐ No	*Signature of Consenting Person*	*Evidence Bar Code*
Description of Item(s) (include custodian)		
Description of Container		
Person Receiving Evidence	*Signature*	

CHAIN OF CUSTODY			
Relinquished By *Location*	*Date/Time*	*Reason*	*Received By* *Location*
From *Location*	*Date/Time*	*Reason*	*To* *Location*
From *Location*	*Date/Time*	*Reason*	*To* *Location*
From *Location*	*Date/Time*	*Reason*	*To* *Location*
From *Location*	*Date/Time*	*Reason*	*To* *Location*
From *Location*	*Date/Time*	*Reason*	*To* *Location*
Final Disposition of Evidence		*Date* *Signature*	

CLIENT SYSTEM DESCRIPTION

Date:	Case Number:	Evidence Tag Number:
Project Manager:		

CPU / CASE INFORMATION

Make/Model:
Serial Number:

NOTES

EVIDENCE SYSTEM DESCRIPTION

Date:	Case Number:	Evidence Tag Number:
Custodian:	Location:	

BIOS INFORMATION

BIOS Type/Version:	BIOS Date/Time:
Configured Boot Sequence:	Calibrated Date/Time:

CPU / CASE INFORMATION

Make/Model:	Memory:
Serial Number:	Processor:
Remarks:	

STORAGE

DRIVE 0

Jumper Settings	Make/Model:	Capacity:
	Serial Number:	
	Remarks:	
	Image Type: ( ) EnCase ( ) dd/raw ( ) Other:	

Acquisition Time:	Start:	End:	Duration:
Original Drive Hash:			
Encase Hash:			

DRIVE 1

Jumper Settings	Make/Model:	Capacity:
	Serial Number:	
	Remarks:	
	Image Type: ( ) EnCase ( ) dd/raw ( ) Other:	

Acquisition Time:	Start:	End:	Duration:
Original Drive Hash:			
Encase Hash:			

NOTES

REVIEWER INFORMATION

Name:	Date:	Signature:

SECURITY CONTAINER CHECK SHEET

TO (if required)	THRU (if required)

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

FOLD HERE - REVERSE FOLD FOR FULL USE OF BOTH SIDES - FOLD HERE

SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.

CERTIFICATION

I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME

Reset

STANDARD FORM 702 (8-85) (EG)
Prescribed by GSA/ISOO
32 CFR 2003
Designed using Perform Pro, WHS/DIOR, Jul 94

Incident Detection Worksheet

CASE#: _____ DATE: _____

Contact Information	
☐	**Person Completing this Form** **Name:** _____ **Phone:** _____ **Other:** _____

Detection Source	
☐	**Date of Detection:** _____
☐	**Detection Type: Automated / Human / Other**
☐	**Name of Source:** _____

Detection Details	
☐	**Detection Peer Reviewed? Yes / No** **Name of Reviewer:** _____ **Raw Alert/Data Viewed? Yes / No** **Detection Appears Valid? Yes / No / Uncertain**

Incident Detection Worksheet

CASE#: _____ DATE: _____

Data Source	
☐	Installation Date: _____
☐	Date of Most Recent Upgrade or Maintenance: _____
☐	Typical Error Rate: High / Medium / Low

Evidence/Data Retention	
☐	Normal Period of Data Retention: _____
☐	Is Detection Data Preserved? Yes / No Date Preserved: _____ Point of Contact: _____

Incident Summary Worksheet

CASE#: _____ DATE: _____

Date Information	
☐	Date Incident Was Reported: _____
☐	Date Incident Was Detected: _____

Contact Information	
☐	**Person Completing this Form** Name: _____ Phone: _____ Other: _____
☐	**Person Reporting the Incident** Name: _____ Phone: _____ Other: _____
☐	**Person Who Detected the Incident** Name: _____ Phone: _____ Other: _____

Incident Summary Worksheet

CASE#: _____ DATE: _____

Summary	
☐	**Incident Status:** _____
☐	**Type of Incident:** _____
☐	**Detection Method:** _____
☐	**Systems Affected**
☐	**Persons Aware of the Incident**
☐	**Dissemination Restrictions:** _____

Malware Details Worksheet

CASE#: _____ DATE: _____

Contact Information	
☐	**Person Completing this Form** **Name:** _____ **Phone:** _____ **Other:** _____

Detection	
☐	**Date Found:** _____ **System Discovered On:** _____ **Detection Method:** _____ **Detection Detail:** _____ **Is the Malware Active?** Yes / No / Unknown

File Properties	
☐	**File Name:** _____ **Size:** _____ **Directory:** _____ **Checksum (indicate type):** _____

Malware Details Worksheet

CASE#: _____ DATE: _____

Other Questions	
ANALYSIS The status of any analysis; has the malware been analyzed for network and host indicators of compromise	
DISTRIBUTION Was the malware was submitted to third parties, either through automated processes or direct action by an employee? If so, list each third party and the purpose.	
PRESERVATION Is a copy of the malware preserved, either manually or through a quarantine process?	

Network Details Worksheet

CASE#: _____ DATE: _____

Contact Information

Person Completing this Form

Name: _____

Phone: _____

Other: _____

Relevant IP Addresses and Domains

Attacker IP Addresses

#	Date Found	IP Address or Domain
1		
2		
3		
4		
5		
6		
7		
8		
9		

Actions Taken

#	Date	Monitor	Block	Blackhole	Other (describe)
1					
2					
3					
4					
5					
6					
7					
8					
9					

Network Details Worksheet

CASE#: _____ DATE: _____

Other Questions	
MONITORING Determine whether network monitoring is being conducted. If network administrators have set up network capture devices, determine who is performing it, where the capture is being performed at (physically and logically), where the data is being stored, and who has access to it. Clarify the filtering rules applied to the capture, whether the capture contains sessions' full content or only header (connection) information.	
PRESERVATION If any data is being preserved, what process is being used and where it is being stored. Similar to individual system details, be sure that any data related to network detection is being properly handled and tracked.	