REQUEST FOR RECORDS DISPOSITION AUTHORITY	JOB NUMBER N1-65-10-35
To NATIONAL ARCHIVES & RECORDS ADMINISTRATION 8601 ADELPHI ROAD COLLEGE PARK, MD 20740-6001	Date received 8/17/10
1 FROM (Agency or establishment) **DEPARTMENT OF JUSTICE**	**NOTIFICATION TO AGENCY**
2 MAJOR SUBDIVISION **FEDERAL BUREAU OF INVESTIGATION**	In accordance with the provisions of 44 U S C 3303a, the disposition request, including amendments, is approved except for items that may be marked "disposition not approved" or "withdrawn" in column 10
3 MINOR SUBDIVISION **Operational Technology Division (OTD)**	

4 NAME OF PERSON WITH WHOM TO CONFER **Tammy J. Strickler**	5 TELEPHONE NUMBER **540-868-4363**	DATE 1 June 11	ARCHIVIST OF THE UNITED STATES

6 AGENCY CERTIFICATION

I hereby certify that I am authorized to act for this agency in matters pertaining to the disposition of its records and that the records proposed for disposal on the attached ___2___ page(s) are not needed now for the business for this agency or will not be needed after the retention periods specified, and that written concurrence from the General Accounting Office, under the provisions of Title 8 of the GAO Manual for Guidance of Federal Agencies,

☒ is not required ☐ is attached, or ☐ has been requested

DATE 8/16/2010	SIGNATURE OF AGENCY REPRESENTATIVE	TITLE Chief, Records Automation Section (for) Agency Records Officer

7 ITEM NO	8 DESCRIPTION OF ITEM AND PROPOSED DISPOSITION	9 GRS OR SUPERSEDED JOB CITATION	10 ACTION TAKEN (NARA USE ONLY)
	Malware Repository The Malware Repository is housed on the Analysis Secure Computing Network (ASCNet), and contains the following information relative to each piece of malware seized/collected in FBI intelligence or criminal investigations • Malware Name • IP addresses • Hash Values • Metadata (i e , file names, registry keys) • Submitted data • Associated File (if files are created during the analysis)		

Malware Repository

Background:

As the FBI conducted more and more intrusion investigations where software applications were used to facilitate a criminal act or terrorist plot, there was an increasing need for a repository of information about the software applications encountered   The Malware Repository improves case turnaround time, thus making the analysis process more efficient   Additionally, the repository helps agents and/or analysts make associations with other cases where similar technical methods were used

The Malware Repository serves the same role as a reference library, providing ready access to information from a variety of sources This repository is maintained on ASCNet, which is an isolated network environment in which an analyst/engineer may conduct deep technical analysis of potentially malicious software

Disposition:

1. **Inputs:** A copy of the data to be analyzed is provided from case agents and imported from CD-ROM/DVD's, USB, and other such media devices   The evidentiary copy is managed in the case file for legal, fiscal, administrative, and accountability purposes

   Disposition Return/destroy input sources to the appropriate case file within 60 days after verification of successful entry into the Malware Repository. GRS 20, item 2

2. **Master Data Files:** The malware repository contains copies of evidence which document the
   - Malware Name
   - IP Addresses
   - Hash Values
   - Known Metadata (i e file names, registry keys)
   - Submitted Data
   - Associated Files

Disposition DELETE/DESTROY when superseded by updated information or when no longer needed for analytical purposes, not to exceed the life of the system

3. **Outputs:** Malware Repository users may obtain responses to a query that provides information useful to a current investigation or intelligence gathering activity

   a Reports Analysis reports of a specific set of digital data provided from the OTD Digital Evidence Section (DES), Investigative Analysis Unit (IAU) to the case agent

   Disposition RETAIN/DESTROY within the related case file and managed under the records disposition for that classification   File instruction b Associative Analysis Reports. Analysts, using the Malware repository, make associations with other cases where similar technical methods were used The analysis may indicate malware associated with more than one case

Disposition Incorporate Associative Analysis reports into all affected case files RETAIN/DESTROY within the related case files and manage under the records disposition for those classifications File instruction

4. System Documentation: Specifications, design criteria, record layouts, user guides, search tools and their dates of usage, and related information

Disposition DELETE/DESTROY when superseded or obsolete, or upon authorized deletion of the related master file GRS20, item 11

5. Audit Records: The audit log contains information such as the date and time that records were imported into the system, when any updates occurred, any changes that were made to the data, who accessed the data, etc

Disposition DELETE/DESTROY when 25 years old N1-65-10-39, item 1

6. Policy, Usage Agreements, and Memoranda of Understanding:

Disposition DELETE/DESTROY when superseded or obsolete or upon termination of the system, whichever is sooner

7. Backups: Backups are maintained for potential system restoration in the event of a system failure or other unintentional loss of data

a Incremental backups DELETE/DESTROY incremental backups when superseded by a full backup, or when no longer needed for system restoration, whichever is later

b Full backups DELETE/DESTROY full backups when second subsequent backup is verified as successful or when no longer needed for system restoration, whichever is later. GRS 24, item 4