# Frequently Asked Questions (FAQs) about GRS 3.2, Information Systems Security Records

September 2014

## INTRODUCTION

### 1. What is the purpose of GRS 3.2?

This schedule provides disposition authority for records related to system and data security and access, reports on computer security incidents, and backup tapes and files.

### 2. From whom may I request more information about this schedule?

Please contact NARA's General Records Schedules Team at GRS_Team@nara.gov with questions about this schedule.

## CHANGES FROM THE OLD GRS

### 3. How does GRS 3.2 differ from the old General Records Schedules?

GRS 3.2 is comprised of updated items from GRS 24, Information Technology Operations and Management Records, that are related to information systems security. Public Key Infrastructure (PKI) Records schedules (GRS 24, items 13a1, 13a2, and 13b) are not rescheduled, but they are now part of this schedule (items 060, 061, and 062) under their existing authorities. GRS 3.2 also includes a few items relevant to this schedule that were in GRS 20, Electronic Records.

## DEFINITION OF TERMS USED IN THIS SCHEDULE

### 4. What are the definitions of terms used in GRS 3.2?

**Information system**

An information system means the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. (36 CFR 1220.18)

**Information systems security records**

GRS 3.2 defines these as records created and maintained by Federal agencies related to protecting the security of information technology systems and data and responding to computer security incidents.

**Information technology infrastructure (item 010)**

Information technology (IT) infrastructure means the basic systems and services used to supply the agency and its staff with access to computers and data communications. Components include hardware such as printers, desktop and laptop computers, network and web servers, routers, hubs, and network cabling, as well as software such as operating systems and shared applications (e.g., word processing).

The services necessary to design, implement, test, validate, and maintain such components are also considered part of an agency's IT infrastructure.

**Computer incident (item 020)**

A computer incident within the Federal Government as defined by NIST Special Publication 800-61, *Computer Security Incident Handling Guide, Revision 2* (August 2012), is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

**Significant computer incident (item 020)**

A significant computer incident that would require scheduling of records outside of this GRS would be defined as one that caused widespread system outage or denial of service, or gained notice by local news media, law enforcement, or the agency's Inspector General's office.

**System access records (items 030 and 031)**

GRS 3.2 defines these as records created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.

**System backups (items 040 and 041)**

Backup files maintained for potential system restoration in the event of a system failure or other unintentional loss of data.

**Master files (items 050 and 051)**

Master files are the actual content of the electronic records series or system, or in other words the recordkeeping copy of an electronic record or system. Master files may consist of data, scanned text, PDFs, digital images, or some other form of electronic information. They may include the information content of an entire system or that of a group of related files. Related records within a single master file are not always the same format.

**Electronic signature (items 060, 061, and 062)**

An electronic signature is a technologically neutral term indicating various methods of signing an electronic message that (a) identify and authenticate a particular person as source of the electronic message and (b) indicate such person's approval of the information contained in the electronic message (definition from Government Paperwork Elimination Act, Public Law 105-277). Examples of electronic signature technologies include PINs, user identifications and passwords, digital signatures, digitized signatures, and hardware and biometric tokens. (See Appendix A, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, NARA, October 18, 2000)

**QUESTION RELATED TO ITEMS 030 AND 031**

**5. Why don't Items 030 and 031 (system access records) include monitoring that is part of an agency's mission activities?**

Records associated with mission activities, such as law enforcement, wilderness preservation, and aeronautics engineering, are scheduled separately because the value of the records varies and they must be scheduled on agency-specific schedules. Items 030 and 031 cover internal administration of user access to systems and only records created as part of the user identification and authorization process.