GRS 3.2 Information Systems Security Records

This file contains two documents. The Draft Schedule contains the proposed text of the new GRS in publication format. The Draft Appraisal Memorandum provides additional background explanation and includes the appraiser's justification for the retention decisions proposed in the schedule.

THE SCHEDULE IS NOT APPROVED FOR USE.

National Archives and Records Administration
Office of the Chief Records Officer
GRS Team
January 2022

DRAFT

GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records

This schedule covers records created and maintained by Federal agencies related to protecting the security of information technology systems and data, and responding to computer security incidents. This schedule does not apply to system data or content.

Item	Records Title/Description		Disposition Instruction	Disposition Authority
010-031	**NO CHANGES**			
035	**Cybersecurity logging records.** For additional information about these records, see OMB Memo M-21-31.	**Full packet capture data.** Packet capture (PCAP) results from the interception and copying of a data packet that is crossing or moving over a specific computer network. **Legal citation:** OMB Memo M-21-31 **Not media neutral.** Applies to electronic records only.	**Temporary.** Destroy when 72 hours old. Longer retention is authorized for business use.	DAA-GRS-2022-000X-0001
036		**Cybersecurity event logs.** Logs required by OMB Memo M-21-31 to capture data used in the detection, investigation, and remediation of cyber threats. **Legal citation:** OMB Memo M-21-31 **Not media neutral.** Applies to electronic records only.	**Temporary.** Destroy when 30 months old. Longer retention is authorized for business use.	DAA-GRS-2022-000X-0002
040 - 062	**NO CHANGES**			

Date: November 22, 2021
Appraiser: Andrea Riley, ACRS
Agency: General Record Schedules (GRS) **DRAFT**
Subject: DAA-GRS-2022-000X

INTRODUCTION

Schedule Subject
GRS 3.2 Addition: Cybersecurity Logging Records

Additional Background Information
NARA is adding two new items to GRS 3.2, Information System Security Records, in response to issuance of OMB Memo M-21-31. The memo supports Executive Order 14028, Improving the Nation's Cybersecurity, and establishes retention requirements for cybersecurity logging records. These GRS items were developed to provide disposition authority in line with the new retention requirements. The logs described in the EO and the OMB Memo were not previously scheduled in the GRS.

Overall Recommendation
Approval of the attached schedule is recommended based on NARA Directive 1441 Appraisal Policy of the National Archives and Records Administration.

APPRAISAL

Item 0001 (GRS 3.2, item 035): Cybersecurity Logging Records – Full packet capture data
These records are data packets captured during the process of moving data across a network. The records are captured for the purposes identifying security threats, troubleshooting problems with the network, identifying data loss, and forensic network analysis. A full packet includes a payload and a header. The payload is the actual contents of the packet (the information being moved) and the header contains metadata, such as the packet's source and destination.
Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

* Records related to administrative housekeeping activities. These are routine records created by all agencies for the process of monitoring information system security. The actual data contained in the packet is not unique. The packets literally contain every bit that travels across the network.
* Similar records have been approved as temporary. (GRS 3.2, items 010, System and data security records, DAA-GRS2013-0006-0001; and 020, Computer security incident

handling, reporting and follow-up records, DAA-GRS2013-0006-0002). These items include other records involved in monitoring information system security and addressing cybersecurity incidents.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. The retention of the records comes directly from OMB Memo M-21-31 and is deemed reasonable given the volume and short-term usefulness of the records.
Media Neutrality: Not Approved. Applies to electronic records only.

Item 0002 (GRS 3.2, item 036): Cybersecurity Logging Records – Cybersecurity Event Logs

Proposed Disposition: Temporary
Appropriateness of Proposed Disposition: Appropriate
Appraisal Justification:

* Records related to administrative housekeeping activities. These are computer system logs that agencies are required to capture and retain per OMB Memo M-21-31 for system security monitoring and information sharing purposes in the event of a cybersecurity incident.
* Similar records have been approved as temporary. (GRS 3.2, items 010, System and data security records, DAA-GRS2013-0006-0001; and 020, Computer security incident handling, reporting and follow-up records, DAA-GRS2013-0006-0002). These items include other records involved in monitoring information system security and addressing cybersecurity incidents.

Adequacy of Proposed Retention Period: Adequate from the standpoint of legal rights and accountability. The retention of the records comes directly from OMB Memo M-21-31 and is deemed reasonable given the volume and short-term usefulness of the records. The guidance states that Cloud GCP records can be retained for only 24 months, while all other logs are retained for 30 months, with longer retention allowed. There is nothing in the guidance that explains why Cloud GCP records are shorter. We have decided to combine all event logs under a single disposition authority with a 30 month retention to reduce the number of disposition authorities agencies have to manage.
Media Neutrality: Not Approved. Applies to electronic records only.

Andrea M. Riley

ANDREA M. RILEY
Appraiser

Supervisor Concurrence: AMR 1/3/2022