# Frequently Asked Questions - General Records Schedule 27

# Records of the Chief Information Officer

## 1. To whom does General Records Schedule 27 apply?

GRS 27 provides disposal authorization for certain records created and maintained by Federal Chief Information Officers (CIO). This schedule applies to the records of CIOs at agency or departmental headquarters as well as those of deputy and subordinate CIOs at the bureau or field office level.

## 2. Does this schedule describe all of the records of Federal CIOs?

Not necessarily. CIOs are often responsible for programs and activities whose records are covered by another General Records Schedule or approved agency records schedule.

## 3. How does this schedule differ from GRS 20, Electronic Records, and GRS 24, Information Technology (IT) Operations and Management Records?

GRS 20 and GRS 24 cover certain records associated with the day-to-day operation of individual information systems and related support services. GRS 27 provides disposal authority for records documenting the administration of the office of the CIO and its agency-wide information resources management.

## 4. How does GRS 27/4, "Legal and Regulatory Compliance Records," differ from GRS 24/1, "Oversight and Compliance Files"?

GRS 27/4 covers CIO records that document an agency's compliance with Federal laws and regulations governing information resources management. GRS 24/1 covers records that document an office's or a system's compliance with the IT policies, directives, and plans that are typically developed or issued by the agency CIO.

## 5. Does this schedule cover records related to IT security?

Insofar as they document agency-wide efforts to comply with the laws and regulations that govern IT security, such CIO records would be covered by 27/4, "Legal and Regulatory Compliance Records." However, records that document the security of individual IT systems – including vulnerability assessments, audits, risk management analyses, and security plans – are covered by GRS 24/5, "Files Related to Maintaining the Security of Systems and Data." Records related to specific security breaches or incidents are covered by GRS 24/7, "Computer Security Incident Handling, Reporting and Follow-up Records."

## 6. Does this schedule cover system data?

This schedule does not apply to the data or information content of IT systems. Records relating to specific systems that support or document the agency's mission must be scheduled individually by submission of an SF 115 to the National Archives.

**7. Do records have to be arranged in these categories?**
No. If records covered by more than one item in this schedule are maintained together in one file or recordkeeping system, keep the records for the longest retention period authorized for those items.

**8. Is this schedule only for paper records?**
No. This schedule applies to records regardless of their physical form or characteristics. Records may be maintained in any format on any medium.