



- [Solutions](#)
- [Products](#)
- [Industries](#)
- [Customers](#)
- [Partners](#)
- [Support](#)
- [Company](#)
- [Contact Us](#)



Solutions

[Security & Log Management](#)

Compliance Auditing

- PCI DSS
- HIPAA
- Sarbanes-Oxley

NISPOM

- FISMA
- DCID
- NERC
- ISO 27002

[IT Operations & Risk Management](#)

[Business Data Intelligence](#)

Comply With NISPOM Security Audit Trail Analysis Standards

The National Industrial Security Program Operating Manual (NISPOM), developed by the Department of Defense, sets comprehensive standards for protecting classified data. All government agencies and commercial contractors who have access to classified data are required to implement system protection processes to ensure continued availability and integrity of this data, and prevent its unauthorized disclosure. These regulations apply to systems used in the capture, creation, storage, processing or distribution of restricted information.

Audit/Protect Level	Requirements Addressed by SenSage
Automated Audit Trail Creation	Granular activity records Successful and unsuccessful logon and logoffs Successful and unsuccessful accesses to files and directories (including creation, open, close, modification and deletion).
Audit Trail Protection	System activity log protection from unauthorized access, modification or deletion.
Automated Audit Trail Analysis	Scheduled analysis of activity logs using automated tools At least weekly review of audit log records Documentation and reporting of security relevant events
Audit Record Retention	At least 1 year

The Most Flexible And Cost Effective Solution for Meeting NISPOM Chapter 8 Log Auditing Requirements

NISPOM Chapter 8's provisions include the automated creation of audit trails on security-relevant activities and their analysis on a periodic basis. Audit logs must be retained for at least one year and protected against unauthorized access.

In today's complex computing environments consisting of interconnected hosts, network servers, routers, databases and applications, SenSage provides government agencies and commercial contractors with a unified data management platform. It consolidates all applications' audit trails and scales easily to handle the volumes of data to meet the changing needs of the enterprise.

Security in Your Hands

SenSage stores up to multiple terabytes of operating and security information in an efficient, super-compressed format, with full data backup. Flexible loading of any log type allows enterprises to integrate data from different devices and applications. This solution also supports ad hoc queries of historical data and flexible reporting. What's more, SenSage works with seamlessly with all common platforms and legacy systems to produce the exhaustive and unified audit trails mandated by NISPOM Chapter 8.

Resources

Gartner

- Gartner 2009 SIEM Magic Quadrant
- Critical Capabilities for SIEM Technology

Brochures

NISPOM

» [Contact Us](#)