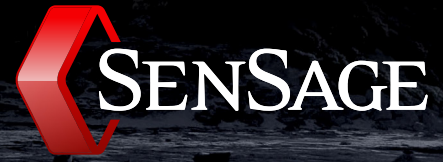


Compliance Auditing for DCID



Ease your DCID Compliance Efforts While Reducing Overall Costs

The US government imposes strict controls for the protection of information systems containing intelligence data. The Director of Central Intelligence 6/3 (DCID 6/3) applies to all organizations, including US Government and commercial contractors, that process, store, and communicate intelligence data. Information systems auditing and logging are required to ensure continued availability and integrity of this data, and prevent its unauthorized disclosure. The collection, retention and analysis of event and log data is a key requirement for compliance. SenSage helps organizations quickly implement Compliance Auditing for DCID solutions that uniquely deliver actionable results.

Covering DCID 6/3 Requirements

The Director of Central Intelligence Directive 6/3 Manual provides guidance and requirements for ensuring adequate protection of different categories of intelligence information that are stored or processed in an information system. The DCID 6/3 guidelines also specify monitoring, auditing, and reporting capabilities. Among them is the automated creation of audit trails on security-relevant activities and weekly analysis, as well as the secure retention of up to five years of audit log data.

Complying with DCID 6/3 rules raises many challenges. Information System Security Officers (ISSOs) and Facilities Security Officers (FSOs) must collect and review activity logs from a multitude of sources. Each of these sources can produce thousands or millions of records per day, which must be retained.

A Pragmatic Platform for Protecting Intelligence Data

SenSage understands the unique standards and controls to which government agencies are held. SenSage's compliance reporting and data storage efficiencies are catered specifically to DCID 6/3 mandates. Additionally, SenSage's real-time compliance monitoring empowers agencies to adhere to the DCID 6/3 guidelines for weekly analysis of security-related activity as well as unauthorized access activity.

SenSage offers a comprehensive IT auditing and analysis solution that provides complete visibility into information system activity. SenSage has the unique ability to store several years of log data online and with a "data forensics tool" it is instantly accessible. Tying this capability to SenSage's virtually limitless storage capacity, allows organizations to collect and analyze both "allowed" and "disallowed" access, and in this manner, uncover sophisticated "low and slow" insider abuse attacks.

SenSage's comprehensive surveillance capabilities also expedite return on investment as early detection, customized reporting of anomalous activity, and routine security queries across your entire data network facilitates detection of security events quickly. Furthermore, with SenSage, agencies can immediately review any associated historical log activity to help determine depth and breadth of impact when breaches and violations occur. Readily reviewing event logs and operational reports, as well as providing immediate investigation capabilities expedites the auditing process.

Taken altogether, SenSage not only meets government regulatory requirements, its collection, retention, reporting and analytical capabilities readily enable contractors and agencies to demonstrate that compliance, quickly, flexibly, and with minimum impact on resources.

Is SenSage able to support DCID 6/3's 5 year audit data retention requirement?

Yes. By leveraging an optimized data storage model, SenSage enables defense contractors and intelligence agencies to satisfy long-term data retention requirements – including storing multiple years worth of event data – all online and accessible. When storing event data, SenSage can compress it to as little as 10 percent of the original raw event log data volume, and 2.5 percent of the volume of data that must be stored when using an RDBMS-based solution for data retention.

How quickly can SenSage produce query results?

Our uniquely scalable repository and high performance features streamline reporting by delivering more immediate results, even within complex, iterative ad hoc queries. Specifically, SenSage can deliver a scan rate of 2 million records per second. This scan rate is based on a complex sub-string URL search with full data extraction. Because SenSage does not rely on an RDBMS architecture that produces an ever increasing amount of indices, these scan rates are not affected by increasing data volume or by the introduction of new sources.

DCID 6/3 Audit Trail Analysis - See <http://fas.org/irp/offdocs/dcid.htm>

Audit / Protect	Requirements Addressed by SenSage
Audit 1 / PL1, PL2, PL3, PL4, PL5	Collect audit logs from all security-relevant information systems. Protect all audit trails from tampering. Maintaining collected audit data at least 5 years and reviewing at least weekly.
Audit 2, Audit 5 / PL2, PL3, PL4	Support individual accountability, ability to audit user-level activity. Allow periodic IS security testing by the ISSO or ISSM via intrusion/attack detection and monitoring tools.
Audit 3 / PL2-55	Use audit reduction and analysis tools.
Audit 4 / PL3	Create and maintain an IS audit trail, recording changes to mechanism's list of user formal access permissions.
Audit 5 / PL3, PL4	Maintain individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual); support periodic IS security testing by the ISSO or ISSM via intrusion/attack detection and monitoring tools. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM in the monitoring and detection of suspicious, intrusive, or attack-like behavior patterns.
Audit 6 / PL4, PL5	Enforce the capability to audit changes in security labels; implement the capability to audit accesses or attempt accesses to objects or data whose labels are inconsistent with user privileges; enforce the capability to audit all program initiations, information downgrades and overrides, and all other security-relevant events (including identified events that may be used in the exploitation of covert channels); shutdown system in the event of an audit failure, unless an alternative audit capacity exists.
Audit 7 / PL4	Implement system capability to monitor occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies. Enforce system capability to notify the ISSO of suspicious events and take the least disruptive action to terminate the suspicious event.
Audit 8 / PL5	Maintain individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). Support at least monthly testing by the ISSO or ISSM via intrusion/attack detection and monitoring tools. These tools shall build upon audit reduction and analysis tools to aid the ISSO or ISSM monitor and detect suspicious, intrusive, or attack-like behavior patterns.
Audit 9 / PL5	Enforce system capability to monitor, in real-time, occurrences of, or accumulation of, auditable events that may indicate an imminent violation of security policies. Enforce system capability to notify the ISSO of suspicious events and take the least disruptive action to terminate the suspicious event.

SenSage, Inc. offers patented event data warehouse solutions that provide actionable results from massive amounts of log and event data. Hundreds of customers have deployed SenSage solutions to reduce security, fraud and compliance risks at a fraction of the cost of traditional data warehouses and log management solutions. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, Hitachi Data Systems, McAfee, Tokyo Electron Device and many others. Visit www.SenSage.com for more information.