snare

NIST SP 800 171 Requirements and Snare

This documents covers the NIST SP 800 171 requirements and how Snare agents and Snare Central Server complies with these requirements

snaresolutions.com

NIST SP 800 171 Requirements and Snare

This documents covers the NIST SP 800 171 requirements as listed on this site https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf and how Snare agents and Snare Central Server complies with these requirements.

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING CUI SECURITY REQUIREMENTS

This chapter describes: (i) the basic assumptions and methodology used to develop the security requirements to protect CUI in nonfederal information systems and organizations;

and (ii) the structure of the basic and derived CUI requirements and the tailoring criteria applied to the federal information security requirements and controls.

BASIC ASSUMPTIONS

The CUI security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are consistent, whether such information resides in federal information systems or nonfederal information systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are consistent in both federal and nonfederal information systems and organizations; and
- The confidentiality impact value for CUI is no lower than moderate14 in accordance with Federal Information Processing Standards (FIPS) Publication 199.15

The above assumptions reinforce the concept that federal information designated as CUI has the same intrinsic value and potential adverse impact if compromised—whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation. Additional assumptions also impacting the development of the CUI security requirements and the expectation of federal agencies in working with nonfederal entities include:

Nonfederal organizations have information technology infrastructures in place, and are not necessarily developing or acquiring information systems specifically for the purpose of processing, storing, or transmitting CUI;

- Nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the CUI security requirements;
- Nonfederal organizations can implement a variety of potential security solutions either directly or through the use of managed services, to satisfy CUI security requirements; and
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every CUI security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a particular requirement.

Requirement	Prophecy Controls and Applicability
Access Control	
Basic Security Requirements:	
3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Snare Agents and Snare Central all have password controls. Snare Central has role-based access controls in place to manage who has access to particular system functions.
3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute	Snare Agents and Snare Central all have password controls. Snare Central has role-based access controls in place to manage who has access to particular system functions.
Derived Security Requirements:	
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion	Snare Central has role-based access controls in place to manage who has access to particular system functions.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Snare Central has role-based access controls in place to manage who has access to particular system functions.
3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	Snare Agents can collect audit log information from the system to track what the commands that were executed by all users on that system.
3.1.8 Limit unsuccessful logon attempts.	Snare Agents can collect unsuccessful login attempts will result in account lockouts after the designated threshold is reached. Snare Central has standard out of the box reports to help report on this sort of user activity.
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	Snare Central has the option to provide a security login warning notice to users before they login.
3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity	Both Snare Agents and Snare Central have inactivity logout features included. Snare Agents can collect audit logs from systems that also implement this requirement.
3.1.11 Terminate (automatically) a user session after a defined condition.	Both Snare Agents and Snare Central have inactivity logout features included. Snare Central can be configured for specific time out periods. Snare Agents can collect audit logs from systems that also implement this requirement.
3.1.12 Monitor and control remote access sessions.	Snare agents can collect audit events for remote access to systems. Both Snare Agents and Snare Central will log remote access to the product and Snare Central has out of the box reports that can report on user remote access to systems
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions	Both Snare Agents and Snare Central can send logs over TLS syslog connections and also use HTTPS for remote access to protect information over remote networks.
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Snare Agents can collect the logs from systems for remote access and the execution of commands.

3.1.21 Limit use of organizational portable storage devices on external information systems	Snare Agents can collect logs from systems that use external or portable storage devices like DVD or USB media
3.3 AUDIT AND ACCOUNTABILITY	
Basic Security Requirements:	
3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	All system logs can be collected and stored centrally in our Snare Central system. Snare Central can securely store and protect all the log data for the defined period of time the customer needs for compliance.
3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	Snare agents can collect logs are collected from all systems that track all actions for an individual.
Derived Security Requirements:	
3.3.3 Review and update audited events.	The audit logs stored in Snare Central stored can be used to review all user and system activity. Snare Central contains around 300 objective report templates that customers can clone and tune to to suit their environment.
3.3.4 Alert in the event of an audit process failure	If there is an audit process failure then the relevant logs are generated with alerts from the Snare Agents. If there are specific events that need real time alerts then Snare Central can raise these alerts and send via email or SNMPTraps to the relevant systems. .

3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity	All system audit logs can be stored in Snare Central and correlated with other log data within our product to allow forensic investigations to occur. Snare Central contains many out of the box reports to assist with indications of compromise, inappropriate, suspicious and unusual system or user activity. There are also many objective reports that can assist with detecting security incidents.
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting	The Snare Central Server can filter the data as needed to allow reports to be generated for specific actions, systems, users, and date and time periods. The reporting system provides flexible and customizable reporting. There is also adhoc event and log searching for general review of log data and threat hunting using basic menu driven google style searching or advanced modes that allow complex regex for specific data matching.
3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records	All systems use a trusted NTP source for time so that audit logs all have the correct time. Snare agents will use the system clocks from the local host. Snare Central and sync its time using NTP from any trusted source for accurate log and timestamp tracking.
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	The Snare Central Server log collection systems has restricted access to the backend system to staff that have a job related need to know. All access is based on role based access for the UI.
3.3.9 Limit management of audit functionality to a subset of privileged users.	The customer can control who has access to the Snare Agents that can control the audit subsystem and logs collected. The Snare Central Server has role based access controls to limit which classes of users have access to data, system function and reports.
3.4 CONFIGURATION MANAGEMENT	

Derived Security Requirements:	
3.4.3 Track, review, approve/disapprove, and audit changes to information systems.	Snare Central and the Agents Management Console (AMC) can be used to ensure that the Snare Agents audit policy is kept in place and if it was tampered with then reports can be generated to show how the system was different to the master templates used for that group of systems.
3.4.9 Control and monitor user-installed software	Snare Agents can be used to log if new software is installed on systems. Snare Central can then be used to report on software that was installed on the systems using the out of the box objective reports.
3.6 INCIDENT RESPONSE	
Basic Security Requirements:	
3.6.1 Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities	Snare Agents and Snare Central can be used to assist with a customers incident management response. Snare Central as the long term storage of log data and with hundreds of out of the box objective report templates and adhoc dynamic searching to assist with any threat hunting and incident response.
3.12 SECURITY ASSESSMENT	
Basic Security Requirements:	
3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application	Snare Agents and Snare Central can be used to check on the changes to systems configuration, user configuration, system policy changes. Snare Central has many out of the box reports to report on system and user changes.

3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.	Snare Agents and Snare Central can be used to check on the changes to systems configuration, user configuration, system policy changes. Snare Central has many out of the box reports to report on system and user changes. If unauthorized changes were to occur then real time alerts can also be configured to report on system or user changes.
3.14 SYSTEM AND INFORMATION INTEGRITY	
Derived Security Requirements:	
3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Snare Agents can collect system audit logs that can have indicators of attacks over network connections. Snare Central can also take syslogs from any syslog device and can also report on indications of attack along with the Snare Agents log data.