ENSURING COMPLIANCE TO NIST 800-171 USING E-SAFE COMPLIANCE

Author: Rizwan Mahmood

Published: August 2018

What is Controlled Unclassified Information (CUI)?

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

What is NIST 800-171?

As computing platforms and technologies are ubiquitously deployed worldwide and systems and components are increasingly interconnected through wired and wireless networks, the susceptibility of Controlled Unclassified Information (CUI) to loss or compromise grows.

The purpose of NIST 800-171 is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI when the CUI is resident in a non-federal information system and with organizations such as contractors.

Who needs to follow NIST 800-171?

The standard is applicable to any prime contractor or sub-contractor who works on government projects, where it is highly likely they have access to CUI and therefore need to implement the necessary controls as per this standard.

What is e-Safe Compliance?

e-Safe Compliance is an information security solution that helps companies monitor and secure sensitive information such as CUI. The following are some of the key capabilities of this solution:

1. Discovers and classifies sensitive information from various sources including ERPs, databases and file-stores.
2. Protects sensitive documents and files from breach or loss using persistent encryption and access control. This ensures data remains:
   a) protected from unauthorised disclosure.
   b) protected in the event of a loss.
   c) secured from unauthorised access by both internal and external users.
   d) protected when shared with authorised third parties.
3. Provides data breach monitoring and alerting. Monitors the access, deletion, modification and movement of sensitive data (files and text) on all corporate and non-corporate channels and alerts if data breach occurs.
4. Pre-empt issues by monitoring possible malicious changes in user behaviour using advanced behaviour analytics and machine learning.
5. Automates risk and security assessment processes.
6. Monitors the organisational environment using configuration management features such as software auditing and highlights issues such as the use of malicious programs or out-of-date PC configurations.

How can e-Safe Compliance help companies comply with NIST 800-171?

NIST 800-171 organises the security requirements into fourteen families. The chart below lists the families and highlights in **red** each family that is either fully or partially managed by e-Safe Compliance. The chart also highlights the families where e-Safe Compliance is not applicable.

Note: Please refer to the next section for a detailed mapping of each requirement to the features of e-Safe Compliance.

SECURITY REQUIREMENT FAMILIES	**ENSURING COMPLIANCE USING E-SAFE COMPLIANCE**
Access Control	**Full Compliance.** e-Safe Compliance provides the required access control on CUI.
Awareness and Training	**Partial Compliance.** e-Safe Compliance helps to fulfil the required security risk awareness among staff.
Audit and Accountability	**Full Compliance.** e-Safe Compliance has powerful reporting and auditing capabilities, which provide clear forensic evidence to support an investigation.
Configuration Management	**Partial Compliance.** e-Safe Compliance fulfils the configuration baselining requirements; however, the requirement also relates to taking action when gaps are identified, which is a manual task.
Identification and Authentication	**Not Applicable.** The security control is about having an appropriate identity and access management system in place.
Incident Response	**Full Compliance.** e-Safe Compliance offers complete tracking of CUI and incident response capabilities, which includes case management workflow.
Maintenance	**Not Applicable.**
Media Protection	**Full Compliance.** e-Safe Compliance offers extensive media protection capabilities.
Personnel Security	**Partial Compliance.** e-Safe Compliance fulfils the requirement of monitoring the users.
Physical Protection	**Not Applicable.**
Risk Assessment	**Full Compliance.** e-Safe Compliance helps to automate many facets of risk and security assessment. It includes an automated risk register. The risk report from e-Safe Compliance becomes an integral part of closing any security gaps in the company.
Security Assessment	
System and Communications Protection	**Partial Compliance.** This security requirement is mostly related to network configuration and information flows within the network. e-Safe Compliance offers partial compliance to this requirement by fulfilling the cryptographic requirements for CUI.
System and Information Integrity	**Not applicable** – This requirement is mainly to do with correcting application flaws such as a vulnerability in a company's ERP system or having the appropriate anti-virus/anti-spam software installed.

1 DETAILED MAPPING OF NIST 800 – 171 SECURITY REQUIREMENTS TO E-SAFE COMPLIANCE

The chart below lists the fourteen NIST requirement families and highlights in **red** the individual requirements of each family that are fulfilled by e-Safe Compliance. The chart also highlights where e-Safe Compliance is partially or not applicable.

SECURITY REQUIREMENTS	ENSURING COMPLIANCE USING E-SAFE COMPLIANCE
Access Control Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). Limit system access to the types of transactions and functions that authorized users are permitted to execute.	**Full Compliance.** Secures sensitive CUI files using persistent and transparent encryption. Information remains encrypted when at rest, in use and in motion (flow). This secures the information from unauthorised access by any unauthorised external party. Implements access profiles on CUI files so that only authorised users within the company can have access to the information. Implements usage controls on who can edit, print and copy the information. Implements ownership controls to further restrict and control sensitive CUI information and to protect it from malicious authorised insiders. Secures access of CUI on mobile devices by keeping it encrypted so that it can be accessed only by authorised users using the e-Safe Mobile RMS app.
Awareness and Training Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	**Partial Compliance.** e-Safe Compliance helps to fulfil the requirement of security risk awareness among company staff. e-Safe Compliance's user behaviour analytics capabilities help to raise awareness among staff about the importance of securing sensitive information by monitoring their behaviour and producing alerts when they perform risky actions such as syncing CUI to personal mobile phone or sending it to the wrong person. The reports are sent not only to IT but also to the department heads, who can assist in raising awareness about the risky actions performed by their staff. Additionally, CUI files secured by e-Safe Compliance are displayed with a triangle (green, yellow or red) overlaying their icons to ensure that users know the files are sensitive and have to be handled with care.

Audit and Accountability Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	**Full Compliance** e-Safe Compliance has powerful reporting and auditing capabilities, which provide clear forensic evidence in the case of an investigation. All monitoring is done from a user's point of view. Hence it facilitates an investigation. The following information is available regarding each transgression: 1. User involved. 2. Information involved down to content level. 3. Device involved. 4. Date and time. 5. Exfiltration method used such as copying to USB, printing, etc. 6. Visual evidence in the form of screenshots. 7. Network or communication channel used. 8. User's action before and after the transgression. 9. Behaviour trends of the user.
Configuration Management Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. Establish and enforce security configuration settings for information technology products employed in organizational systems.	**Partial Compliance.** e-Safe Compliance fulfils the configuration baselining requirements; however, the requirements also relate to taking action on identified gaps, which is a manual task. e-Safe Compliance's offers hardware, software and network audit modules as part of the one-stop solution. These modules help to baseline the hardware and software configurations of a company's network and to report any unauthorised changes. For example, the software audit module highlights any unauthorised software installed in the devices or any non-standard configuration of installed software. e-Safe Compliance maintains a real-time full inventory of the location and usage of marked CUI documents within any given period of time. This includes documents maintained in network stores, PCs and mobile devices.
Identification and Authentication Identify system users, processes acting on behalf of users, and devices. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	**Not Applicable.** This security requirement is about having an appropriate identity and access management system in place.
Incident Response Establish an operational incident-handling capability for organizational systems that includes	**Full Compliance.** e-Safe Compliance offers complete incident response capabilities, including case management workflow. The process starts from the classification and securing of CUI, monitoring it, reporting incidents related to it, and entering positively-identified transgressions into the case management workflow.

preparation, detection, analysis, containment, recovery, and user response activities. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	Case management workflow automates the incident response process. Key processes include gathering additional information related to an incident, assigning appropriate non-technical users for investigative and action purposes, establishing the damage done, taking the appropriate containment actions and following the case until its closure. Sensitive CUI is tracked throughout its lifecycle. The tracking is not impacted even if a CUI file is renamed or edited. e-Safe Compliance is able to track the locations of all the copies of a particular CUI file within any given period of time regardless of whether it is in a local or external network or in a vendor's PC or user's personal mobile device. The tracking includes who has viewed the file and whether it has been deleted or edited.
Maintenance Perform maintenance on organizational systems. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	**Not Applicable.**
Media Protection Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. Limit access to CUI on system media to authorized users. Sanitize or destroy system media containing CUI before disposal or release for reuse.	**Full Compliance.** e-Safe Compliance secures CUI files using persistent and transparent encryption, and applies access control to ensure they are accessible by only authorised internal and external users. The information remains encrypted and secure throughout its lifecycle whether it is at rest, in use or in motion (flow). CUI remains encrypted and secure while stored in a company's network and devices and also when transferred using any online channel such as via cloud storage or email or offline channel such via USB or CDs. CUI files are marked with a green, yellow or red triangle overlaying their icons to depict their sensitivity. As the information is encrypted, it remains secure even if lost, stolen or hacked. Further, e-Safe Compliance allows information to be made completely inaccessible by deleting keys for devices that are no longer required, lost or stolen, and for users who have left an organisation. Key deletion can also be triggered based on time, for example, if a device does not reappear on a company's network within a preset period of time. Note that this feature continues to work even if the device is kept offline by a malicious person. e-Safe Compliance monitors the printing of CUI and also has the ability to prevent its printing based on who the user is and its sensitivity. Further, e-Safe Compliance also offers device control features such as blocking USB use by user, by PC or by type of information.

Personnel Security Screen individuals prior to authorizing access to organizational systems containing CUI. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	**Partial Compliance.** e-Safe Compliance fulfils the requirement of monitoring the users. e-Safe Compliance monitors user behaviour and uses machine learning and behaviour analytics to detect malicious actions by staff. All actions of users are monitored, which includes how they access, use and transfer CUI. This monitoring is not limited to just file-based monitoring but also covers textual content. As such, e-Safe Compliance is able to detect if a rogue user copies sensitive CUI and then pastes it into chat or free email. In the case of staff termination, e-Safe Compliance provides the ability to revoke user access centrally by deleting a user's key so that any data in his possession is no longer accessible to him.
Physical Protection Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. Protect and monitor the physical facility and support infrastructure for organizational systems.	**Not Applicable.**
Risk Assessment Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	**Full Compliance.** e-Safe Compliance helps to automate many facets of risk and security assessments. The risk report from e-Safe Compliance becomes an integral part of closing the security gaps in a company. e-Safe Compliance offers specialised capabilities and reports that help to test the security and risk posture of a company on an on-going basis. It does this by allowing users to define various risks, security controls and their severity levels in a digital risk register. Once defined, advanced analytics and machine learning are used to monitor the usage of CUI and the users' behaviour over a period of time against the defined risks. This includes monitoring the usage pattern against peer groups and also how changes in user behaviour occur over time. The system learns from these changes and highlights changes which are out of the ordinary. A risk score is calculated based on each user interaction, which helps to highlight the top risk-causing user in a company and the types of risky actions that result in a high-risk score. This can be fed back into user training and also into any security adjustments required within a company's environment. An overall security and risk assessment report is produced, which details the current risk posture of an entire company. The report allows the management to drill down on any particular identified risk and decide the appropriate actions to take to mitigate it.
Security Assessment Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	
System and Communications Protection Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	**Partial Compliance.** This security requirement is mostly related to network configuration and information flows within the network. e-Safe Compliance offers partial compliance to this requirement by fulfilling the cryptographic requirements for CUIs. e-Safe Compliance keeps CUI files encrypted using libraries that are FIPS 140-2 compliant. This encryption method is based on public and private key structure. They maintain the encryption of CUI files at rest, in use and in motion. This ensures they are protected from unauthorised disclosure.
System and Information Integrity Identify, report, and correct system flaws in a timely manner. Provide protection from malicious code at designated locations within organizational systems. Monitor system security alerts and advisories and take action in response.	**Not Applicable** – This requirement has mainly to do with correcting application flaws such as a vulnerability in a company's ERP system or having the appropriate anti-virus/anti-spam software installed.