eFAACT Supports Government Contractor Compliance with DFARS 252.204-7008 / NIST SP 800-171

Background

Government contractors who store Controlled Unclassified Information (CUI) in non-Federal systems are required by DFARS 252.204-7012 to comply with NIST SP 800-171 by December 31, 2017.

DFARS clause 252.204-7012, Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting, was structured to ensure that unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes.

NIST Special Publication 800-171 is a set of security requirements that may be added or referenced in federal contracts with the goal of improving the protection of Controlled Unclassified Information (CUI).

eFAACT Compliance

The eFAACT 2017-2018 software design and development efforts are focused on system architecture enhancements, with security as the key component. The result is a sealed eFAACT environment that includes multi-factor authentication, user session locks and device specific controls. eFAACT's design and development requirements are based on NIST SP 800-171. See page two for **eFAACT NIST SP 800-171 Plan of Action and Milestones (POAM)**.

In the area of software system compliance, two key factors considered new additions to standard security policies include prompt cyber-incident reporting and the use of multi-factor authentication to access systems which contain CUI.

To safeguard covered defense information, multi-factor authentication is embedded in the eFAACT security protocol to protect CUI data and is activated through eFAACT company preferences. Multi-factor authentication may also be activated for each eFAACT GovCon Cloud login to provide additional security required for CUI data residing in both eFAACT and QuickBooks desktop applications.

Multifactor authentication uses two or more methods of authentication involving something you know; something you have; or something you are.

The reporting of cyber incidents is a standard eFAACT procedure. This procedure dictates reporting incidents which affect covered defense information or the contractor's ability to perform requirements designated as operationally critical support. As an eFAACT customer you will be notified of any unauthorized intrusion.

Summary

eFAACT complies with government contractor security requirements. Compliance with NIST SP 800-171 also relies on the government contractor's security policies and procedures. It is recommended that each contractor review their security documents for compliance to NIST SP 800-171. eFAACT software design, development, support, and all data centers reside within the United States.

eFAACT System 2017-2018 Plan of Action and Milestones (POAM)

Subject: DFARS 252.204-7012 / NIST SP 800-171 Compliance

Task	Purpose	Date Available
Multi Factor Authentication	Additional security option for CUI data residing in eFAACT and QuickBooks desktop applications	
eFAACT GovCon Cloud multi factor authentication	Company preference implemented by the contractor for each eFAACT GovCon Cloud login.	current
eFAACT Web multi factor authentication	Company preference implemented by the contractor.	current
eFAACT System multi factor authentication	Company preference, implemented by the contractor, allows for an additional 3rd level of authentication for all eFAACT System components.	current
NIST 800-171 Security Requirements	This section outlines NIST 800-171 Security Requirements as they pertain to the eFAACT System. A government contractor's compliance with NIST SP 800-171 relies on their overall security policies and procedures. It is recommended that each contractor review their security documents for compliance.	
3.1 Access Controls Basic Security Requirements	eFAACT provides user access security tools, implementation is the responsibility of the contractor.	current
3.2 Awareness and Training	eFAACT provides tools for reporting security incidents and training personnel, implementation is customer controlled.	
3.3 Audit and Accountability	eFAACT maintains an audit trail of user access and actions. See "eFAACT System Architecture Enhancements"	current and planned
3.4 Configuration Management	eFAACT System configuration models are regularly maintained.	
3.5 Identification and Authentication	eFAACT provides a multifaceted authentication process, implementation is implementation is customer controlled. See "eFAACT System Architecture Enhancements"	current and planned
3.6 Incident Response	eFAACT provides tools for reporting software incidents. Incidents are addressed upon receipt.	current
3.7 Maintenance	eFAACT System maintenance is monitored and performed by authorized personnel.	current
3.8 Media Protection	Media used to store eFAACT data is protected and access restricted.	current
3.9 Personnel Security	eFAACT provides personnel security tools, implementation is implementation is customer controlled.	current
3.10 Physical Protection	eFAACT data and facility access is protected and monitored, with access restricted to authorized eFAACT representatives.	current
3.11 Risk Assessment	eFAACT environment is continually scanned for vulnerabilities. If found, corrective and preventive actions are taken.	current
3.12 Security Assessment	eFAACT security controls are periodically monitored and assessed for effectiveness.	current
3.13 System and Communication Protection	eFAACT communications are currently monitored, controlled and protected, encryption is FIPS compliant. See "eFAACT System Architecture Enhancements"	current and planned
3.14 System And Information Security	eFAACT incident reports are tracked via the eF HelpDesk and addressed upon receipt. Measures are in place to protect from malicious code. See "eFAACT System Architecture Enhancements"	current and planned