Note Regarding NIST Special Publication 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Security Requirement 3.12.4, System Security Plan

While Revision 1 of the NIST SP 800-171 added the system security plan as an explicit requirement - the original version of the publication stated that the system security plan "is expected to be routinely satisfied by nonfederal organizations without specification...". Even without Revision 1 of the NIST SP 800-171 – the contractor may still document implementation of the security requirements with a system security plan.

Frequently Asked Questions (FAQs), dated January 27, 2017, regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 address this in FAQ 34 as follows: The “system security plan” is addressed in NIST 800-171 as “expected to be routinely satisfied by nonfederal organizations without specification” as part of an overall risk-based information security program (see footnote 16, page 6 and Table E-12, PL-2). The system security plan should be used to describe how the system security protections are implemented, any exceptions to the requirements to accommodate issues such as those listed in the question above, and plans of action as provided by security requirement 3.12.2, to correct deficiencies and reduce or eliminate vulnerabilities. Elements of the security plan may be included with the contractor’s technical proposal (and may subsequently be incorporated as part of the contract).