RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 2, was issued to address, in part, the protection of the design and development of safety systems from both malicious and non-malicious events. As a result of the issuance of 10 CFR 73.54, and the supporting RG 5.71, to address cyber security requirements, the staff has issued DG-1249 to clarify the guidance in RG 1.152, Revision 2 to remove guidance for malicious events. DG-1249 focuses on providing guidance on the establishment of a secure development and operational environment (SDOE), which is based on the requirements in 10 CFR 50.55a(h), 10 CFR Part 50, Appendix A, GDC 21, and Criterion III of 10 CFR Part 50, Appendix B. The establishment of a SDOE for digital safety systems refers to: (i) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications and (ii) protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

The information that should be provided for a SDOE review should demonstrate conformance to each regulatory position of RG 1.152 (as clarified in DG-1249). Some of this information may be in the form of commitments in the development process. For example, this includes:

1) An assessment of the development process, including the development environment for each phase of the software lifecycle (i.e., concepts through test phase) for both the MELTAC platform and the PSMS application software should be provided. The vulnerability assessment should cover steps in the development process that may allow for potential unauthorized or unintended changes to the system during the development process. The development controls used to mitigate the identified vulnerabilities should be described. For example, during the requirements specification phase there may be weaknesses in the development process that may allow for unauthorized or unintended changes to the requirements specifications documents (e.g., unintended addition, subtraction, or modification of requirements). In this particular example, the development control may include use of “a documents storage center” that is access controlled, all changes to documents in the storage center are tracked, all changes are reviewed and validated, etc. The vulnerability assessment of the development environment should provide a vulnerability analysis of development tools and networks and a description of secure development environment controls used to prevent unauthorized access to these tools and networks. The analysis should cover all interfaces to these development tools and networks and measures used to protect these interfaces.

2) An assessment of the design should be provided and the secure operational environment design controls used to mitigate these vulnerabilities should be identified. The analysis should include identification of interfaces that may allow for unintended access or modification to the safety system (e.g., maintenance terminals, and data communications links).

3) A description of the development process for the selected secure operational environment design controls for each phase of the software lifecycle should be provided. For example, a description the process used to ensure that the secure operating environment requirements are derived from the results of the vulnerability assessment and what process is used to ensure these requirements are correct, accurate, complete, testable, and consistent should be provided.

4) A description of measures taken to prevent the introduction of unnecessary requirements, design features, or functions that may result in inclusion of unwanted or unnecessary code as relevant to each lifecycle phase.

5) A discussion should be provided on how pre-developed or COTS software has been integrated into the system, including additional requirements to ensure the integrity of the COTS software and testing of the COTS software to validate the integrity of the system. Specifics of what measures are used to validate the COTS software should be discussed (e.g., source code analysis).

6) A description of how each secure operational environment design feature will be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access and/or the effects of undesirable behavior of connected systems and does not degrade the safety system's reliability.