

#	Finding Type	Topic	Code Reference	SED Finding	PG&E Response
1	Concerns	Gas Distribution Integrity Management: Identify Threats (GDIM.TH)	192.1007(b)	<p>SED discussed with PG&E the cybersecurity aspect of its distribution gas system. PG&E stated that its Gas Risk Management (Enterprise Risk Management group) evaluated the risk of cyber-attack on the "Loss of Containment on Gas Distribution Main or Service" (LOCDM) enterprise risk model. The conclusion was that a cyber-attack is not a risk driver, meaning it cannot cause a loss of containment event (major or minor leak), and it cannot significantly amplify the consequence for a loss of containment event on the gas distribution system. PG&E also apprised SED that TSA (Transportation Security Administration) has tentatively scheduled an on-site inspection for PG&E on June 21, 2022. It is not expected that this inspection includes gas distribution systems.</p> <p>SED recommends that PG&E's DIMP (Distribution Integrity Management Program) team evaluate cybersecurity as a potential threat for its distribution gas system. Furthermore, SED recommends that PG&E's DIMP team should complete a cybersecurity assessment of PG&E's gas distribution system to identify potential gaps or vulnerabilities in the system such as loss of service, loss of data, effect of cyber-attack on its transmission system etc. In addition, SED recommends PG&E designate a DIMP coordinator/Subject Matter Expert (SME) to serve on various teams of PG&E who work on cybersecurity threats and participate in the upcoming TSA field inspection.</p>	<p>PG&E's DIMP team will evaluate cybersecurity as a potential threat for its distribution gas system. DIMP will work with other stakeholders within PG&E to ensure a cybersecurity assessment of the gas distribution system includes a review of potential vulnerabilities which may lead to loss of service, loss of data and susceptibility of the distribution system to effects of cyber-attacks on the transmission system. Additionally, DIMP will designate a lead to serve on teams who work on the cybersecurity threat and inform the upcoming TSA field inspection.</p>
2	Concerns	Gas Distribution Integrity Management: Preventative and Mitigative Actions (GDIM.PM)	192.1007(b)	<p>PG&E's Distribution Integrity Management Program (DIMP) team identifies threats to its distribution gas system and the affected areas. The Mitigation Activities are developed by the PG&E's DIMP team, the projects are created to address each identified risk/threat and these projects are implemented for risk reduction. At the completion of projects, these projects go through the 'measurement in progress' phase.</p> <p>It is SED's understanding that PG&E's DIMP has no set criteria for certain projects to be designated as satisfactorily completed. For example, for project (2012-06 7001654 Tee Cap Unit Verification: Sacramento) completed on 07/16/2019, a number of addresses had comments such as inaccessible, no access to backyard, not located, new driveway, new patch etc. PG&E could not provide follow up information on how many attempts were made for inaccessible locations (or notes explaining what caused it to be inaccessible), or what percentage of missing locations are acceptable etc. for considering a project as 'closed'.</p> <p>SED recommends that PG&E should set acceptance criteria for completion of DIMP projects, where appropriate.</p>	<p>PG&E recognizes SED's concern and recommendation regarding implementing acceptance criteria for completion of DIMP mitigation activities. We will determine acceptance criteria for appropriate project types, with instructions for further review of projects that fall below acceptance criteria. Review will determine what, if any, additional mitigation activities are necessary. We intend to revise our DIMP documentation accordingly to implement this recommendation.</p>