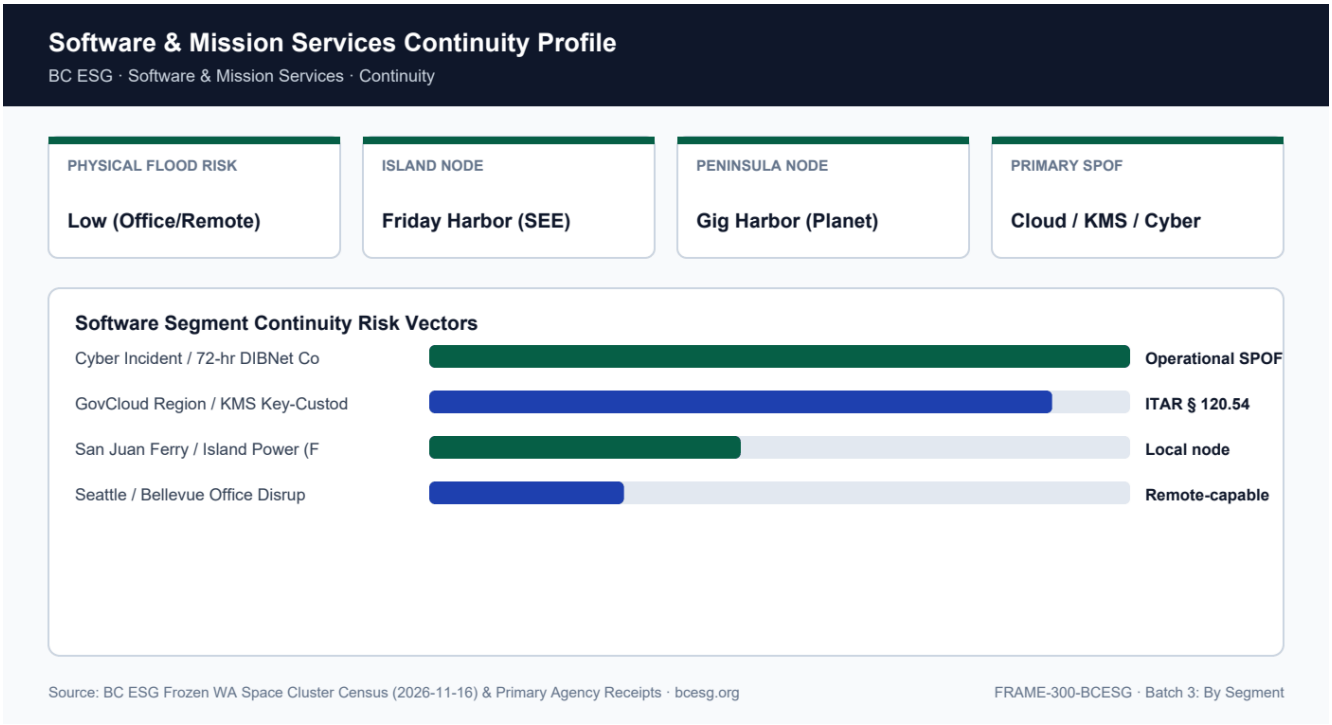
Software Continuity: Distributed Puget Sound/Island Nodes & Cloud/Cyber SPOFs

Published: November 16, 2026 · Canonical URL: https://bcesg.org/wa-space-software-mission-services-continuity/

Verification & Scope Baseline: Low physical flood/freight exposure across distributed offices; primary continuity single points are cloud GovCloud availability, HSM/KMS key custody, and 72-hr cyber containment.



Continuity Vector	Affected Firms	Mechanism	Resilience Control
FedRAMP / GovCloud Outage	Integrate, M42, Godel	Mission SaaS & C2 downtime	Multi-AZ / cross-region GovCloud failover
KMS / HSM Key Custody Loss	ITAR-controlled software	Decryption outage or compliance breach	Split-custody FIPS 140-3 HSM backups
San Juan / Peninsula Power	SEE (Friday Harbor), Planet (Gig Harbor)	Ferry/subsea cable & grid outage	Seattle dual-office & cellular/SATCOM backup

Why Physical Floodplains Matter Less Than Cloud & Key-Custody Continuity

Unlike hardware factories in Kent or Sedro-Woolley, Washington's 9 software and mission-services firms can shift engineering operations remotely during Puget Sound storms, ferry disruptions (affecting SEE in Friday Harbor or Planet Enterprises in Gig Harbor), or urban seismic events.

Their real continuity single points of failure are **FedRAMP Moderate / GovCloud region availability**, **customer-controlled KMS/HSM key custody** (required to preserve the ITAR § 120.54 encryption carve-out), and **72-hour cyber-incident containment** under DFARS 252.204-7012 without losing access to mission-planning or C2 pipelines.

Verified Primary Sources & Internal Bridges

- eCFR DFARS 252.204-7012: https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012
- eCFR 22 CFR § 120.54: https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/section-120.54