Possible Cybersecurity Control Measures for MARSEC Levels

MARSEC Level 1 Cybersecurity Controls for Consideration

- Annually exercise the organization's Incident Response Plan
- Conduct regular training for all users
- Maintain cyber threat situational awareness
- Report suspicious activity to the MTS-ISAC, DHS, and USCG
- Maintain baseline cybersecurity control measures for the organization (among other framework controls[1], the baseline controls should include multi-factor authentication for critical systems / applications, network segmentation, and continuous monitoring)

MARSEC Level 2 Cybersecurity Controls for Consideration (in addition to Level 1 controls)

- Review user accounts for unauthorized account creation and/or privilege escalation
- Limit remote access to essential services / personnel; terminate any remote access sessions which were initiated prior to the change in MARSEC Level
- Review critical system audit records for unauthorized configuration changes
- Scan network for unauthorized devices, prioritizing the review of wireless networks
- If email attachments or links are not scanned for malware, remove attachments / disable links
- Enact additional web browsing restrictions for users
- Adjust monitoring support requirements as needed (e.g. adjust normal SLA timeframes to mirror heightened security posture)
- Review network segmentation firewall rules for unauthorized changes
- Adjust configuration settings to disallow mobile phone connections to systems
- Test critical system backups for restoration capabilities
- If not using application whitelisting, adjust configurations to use whitelisting
- Add physical security controls to automated access control systems (e.g. physical checking of facility security badges instead of only electronic)
- Report suspicious activity to the MTS-ISAC, DHS, and USCG

MARSEC Level 3 Cybersecurity Controls for Consideration (in addition to Level 2 controls)

- All remote access sessions reviewed and authorized on an as needed basis
- Remove unpatched systems from direct internet access
- Report suspicious activity to the MTS-ISAC, DHS, and USCG

[1] Pick the reference that works for you – NIST, ISO, CIS Top 20, etc.