SECURITY CONTROL CONSIDERATIONS

- Implement the basic controls that are required for Level 1 per the FAR clause 52.204-21.
- Limit information system access to authorized users.
- Ensure segregation of duties is in place.
- Sanitize/destroy info system media containing sensitive data (i.e. federal).
- Control and manage physical access.
- Monitor and control external/internal communication boundaries.
- Provide protection from malicious code.
- Provide privacy and security notices consistent with CUI rules.
- Employ the principle of least privileged.
- Monitor and control remote access sessions.
- Ensure the system is auditable.
- Ensure all staff are aware of security risks associated with their activities.
- Make sure passwords are in line with best practices.
- Regularly perform data backup testing.
- Scan for vulnerabilities.
- Identify unauthorized use.
- Implement the basic controls that are required for Level 3 per NIST SP 800-171 Rev 1.
- Ensure segregation of duties is in place.
- Protect wireless access using authentication and encryption.
- Define procedures for the handling of CUI data.
- Review and update logged events.
- Provide security awareness training.
- Enforce multi-factor authentication for all users.
- Test IR policy and procedure.
- Employ spam protection.
- Implement the basic controls that are required for Level 4 per NIST SP 800-171B.
- Control information flows between domains.
- Perform user access reviews.
- Automate analysis of audit logs.
- Perform practical security awareness exercises.
- Catalog and periodically update thread profiles/TTPs.
- Isolate administration of high-value network infrastructure and components.
- Identify and mitigate risk associated with wireless access points.
- Identify assets not reporting audit logs.
- Establish and maintain a 24-hour cyber IR team.
- Ensure info processing facilities meet defined continuity, redundancy, and availability requirements.
- Enforce port and protocol compliance.
- Monitor individuals and system components on an ongoing basis for suspicious behavior.