Cybersecurity Contract Checklist

Version 3 (2021)

USG requires suppliers that process, transmit, or store information and data on behalf of the USG to meet, at a minimum, the standards set forth in this document. Considering this, Contract Administrators must review the standard requirements for compliance. It is recognized that operational needs and the give-and-take nature of contract negotiations may preclude 100% compliance by suppliers with respect to these provisions. However, USG institutions and organizations are nevertheless responsible for ensuring adequate protection of USG data analyzed in light of the preponderance of the entire set of supplier and USG controls and measures protecting USG data.

1. **Verify Contracts** – Contract Owner shall identify contracts that may access USG data or that may provide systems, products, or services.
2. **Determine Risk Levels** – Based on the type of data or service, the Contract Owner shall assess the overall level of risk associated with access to that USG data or the service availability for those suppliers. Ultimately, the level of risk will be assessed as "None," "Low," "Moderate" or "High" as defined in USG's *Business Procedures Manual*[1], Section 3.4.4.
3. **Verify Contract Language** – If the risk level is "High," ensure that the new contract, or contract renewal, has been reviewed so that the contract includes language appropriate for the designated risk level and requires the supplier to protect USG data in a manner consistent with the risk level.
4. **Cybersecurity Awareness Training** – If the risk level is "High," ensure the contracts include language to address supplier management and staff annual cybersecurity awareness training.
5. **Review Cyber-Insurance Needs** – If the risk level is "High," determine if a need exists concerning cybersecurity insurance. Examples include protecting USG's interests in case the supplier compromises USG data or cannot provide the mission-critical service. Also consider if the cyber insurance coverage will cover potential risks.
6. **Request/Review Supplier Documentation** – If the risk level is "High," ensure supplier compliance is documented or otherwise addressed in the contract. Examples of appropriate documentation could include a SOC report, an assurance provider's assessment of the supplier's cybersecurity protocols, etc.
7. **Review Supplier's Cybersecurity Controls (Data Assets)** – The Contract Administrator must have the supplier's documented processes for the assessment and analysis of risks associated with USG information and data assets and the controls to mitigate identified risks reviewed and approved by appropriate cyber security USG personnel. Examples of the controls to review are:
    a. **Architecture** – If the risk level is "High," ensure supplier provided documentation supports network segmentation, or an equally effective measure, to isolate USG information and data assets.
    b. **Firewall/IPS** – If the risk level is "High," verify supplier provided documentation addresses intrusion prevent system (IPS) and firewall implementation to detect anomalous activity in a timely manner to understand potential impacts to USG information and data assets.

[1] https://www.usg.edu/business_procedures_manual/

c. **Data Encryption** – If the risk level is "High," verify supplier provided documentation addresses encryption, or an equally effective measures, as a required for all personal, sensitive or confidential information that is processed (in-use), transmitted (in-transit) and stored (at-rest).

d. **Data Integrity** – If the risk level is "Moderate or High," verify supplier provided documentation concerning data integrity and cybersecurity protective safeguards (e.g., user access, rights and privileges).

8. **Review Supplier's Cybersecurity Controls (Systems, Products or Services)** – The Contract Administrator must have the contract controls reviewed and approved by appropriate USG cyber security personnel to ensure that the supplier's documented processes for the assessment and analysis of risks associated with the systems, products, or services under contract adequately mitigate identified risks. Examples of the controls to review are:

    a. **Vulnerability Assessment** – If the risk level is "Low, Moderate or High," verify supplier provided documentation addresses vulnerability management that includes, but is not limited to, continuous monitoring;

    b. **Patch Management** – If the risk level is "Low, Moderate or High," verify supplier provided documentation addresses security patches and security upgrades, which include, but are not limited to, servers, routers, desktop computers, mobile devices and firewalls. Application and testing of the patches and/or security upgrades must be addressed; and,

    c. **Principles of Least Functions** – If the risk level is "Low, Moderate or High," verify supplier provided documentation addresses server hardening that includes principles of least functions on systems that manage USG information and data assets.

9. **Incident Response** – If the security risk level is Low, Moderate, or High, the Contract Administrator must ensure the contract has been reviewed by appropriate USG cybersecurity personnel to establish and maintain a procedure to identify and report cybersecurity incidents affecting USG information and data assets. Incident Response standards can be located in the USG's *IT Handbook,* Section 5.3.