USG Standard for Supplier Management: Cybersecurity Requirements

Version 7 (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. Suppliers may also refer to the USG *IT Handbook*[1], a standard that is modeled on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, for additional information.

HIGH RISK: Suppliers are required to protect the availability, integrity and confidentiality of USG information and data assets in the supplier's possession, particularly data classified as "High" risk as defined in USG's *Business Procedures Manual*, Section 3.4.4[2]. Examples of the information and data that trigger a "High" classification include but are not limited to USG's mission-critical systems, personally identifiable information ("PII") such as date of birth, social security number, names of minor children, health information, financial information (credit card numbers, bank account numbers), student records as defined by FERPA, etc. To ensure that USG suppliers provide for the integrity and cybersecurity of USG's "high risk" information and data assets as required, USG requires its suppliers to:

1. Implement and maintain management and staff accountability for the protection of USG information and data assets. As part of this program, the Supplier shall ensure management and staff receive annual cybersecurity awareness training.
2. Establish and maintain risk management practices to meet USG's program objectives in the event of the unavailability, loss or misuse of USG information and data assets. Also, the Supplier must:
    a) Establish and maintain processes for the assessment and analysis of risks associated with USG information and data assets;
    b) Implement Intrusion Prevent System (IPS)/firewall configurations to detect anomalous activity in a timely manner to understand potential impacts. The Supplier shall document the baseline configuration each IPS/firewall with dataflow diagrams, update the documentation with all authorized changes and conduct periodic verification of the configuration; and
    c) Architect network segmentation, or an equally effective measure, to isolate USG information and data assets as a cybersecurity safeguard.
3. Establish and maintain processes to identify and report cybersecurity incidents affecting USG information and data assets. Suppliers must promptly report all cybersecurity incidents or events of interest affecting systems or data for any of the cybersecurity objectives of confidentiality, integrity or availability to USG Cybersecurity through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1-888-875-3697 (Toll free within Georgia). Further, suppliers should also notify the USG point of contact as identified in their contract.
4. Develop and implement a vulnerability management plan that includes, but is not limited to:
    a) Continuous monitoring to identify and verify the effectiveness of implemented protective measures, e.g. vulnerability scanning, and

[1] https://www.usg.edu/information_technology_services/it_handbook/
[2] https://www.usg.edu/business_procedures_manual/

b) 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.

5. Technology upgrades, which include, but are not limited to, operating system upgrades on servers, routers and firewalls. Appropriate planning and testing of upgrades must be addressed.

    a) Server configurations includes all servers that have any interaction with the Internet (public facing) or intranet traffic that manages USG information and data assets. Document the baseline configuration for each server with dataflow diagrams, update the documentation with all authorized changes and conduct periodic verification of the configuration.

    b) Server hardening must cover all servers that manages USG information and data assets. The process for making changes based on newly published vulnerability information as it becomes available must be included. Principles of least functions must be implemented.

6. Software management and software licensing must address acquisition from reliable and safe sources and must clearly state that using pirated or unlicensed software is prohibited.

7. Data files that are downloaded/uploaded must meet information and data integrity and cybersecurity protective safeguards (e.g., user access, rights and privileges), which were established for the original data file and which must be applied in the new environment.

8. Encryption, or an equally effective measures, is required for all personal, sensitive or confidential information that is processed (in-use), transmitted (in-transit) and stored (at-rest).

MODERATE RISK: USG shall require suppliers to protect the availability and integrity of the information and data assets classified as "Moderate" risk as defined in USG's *Business Procedures Manual*, Section 3.4.4 that includes but are not limited to publicly available information, directory information, and non-confidential information. Additionally, incident reporting as stated in item three (of this document) is also required.

LOW RISK: USG shall require suppliers to protect the availability of the systems, products or services classified as "Low" risk as defined in USG's *Business Procedures Manual*, Section 3.4.4. Additionally, incident reporting as stated in item three (of this document) is also required.

NONE: No Cybersecurity review is required – no systems, products, services and/or USG data are being exchanged as part of the contract.