SUPPLIER MANAGEMENT: A USG IT HANDBOOK COMPANION GUIDE

VERSION 1.0

10/28/2021

PUBLIC

Abstract: This guideline is classified as "Public" and was developed for internal use. The purpose of this guideline is to focus on the elements of supplier management that are directly associated with the management of technology pertaining to cybersecurity and privacy.

Protecting USG information and data assets and the systems that collect, process and maintain this data is of critical importance. As a result, USG organizations must implement and manage the security of systems, products and services, which includes control baselines or safeguards to offset possible threats. USG's data protection strategy also includes requirements to ensure the security of data protection controls, regardless of the location or the party responsible for those controls. Suppliers serve a crucial role in achieving this goal. All suppliers are expected to meet the baseline controls identified. If a USG organization permits suppliers to process, store or transmit USG information and data assets that is considered "confidential" or "sensitive," additional data protection controls may be required. Effective cybersecurity is a team effort involving the collaboration, participation and support of each USG organization and its suppliers who interact with USG information and data assets and/or systems.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Privacy Framework

(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 1-888-875-3e ( ) (o)4.3 (( ) (o)4.3 (( ) (o)4.37(( ) (.2 (27.8 T(e)-3 1.5 (G)

a) Continuous monitoring to identify and verify the effectiveness of implemented protective measures, e.g. vulnerability scanning, and

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. P -0.8 (.)-2 (P -0.870.8 (.) 0 Td(4Tf0 Tfp7 (b)-0.8 (l)-3.3 (a)-6 (n)-6 (s)6..6 (c