FAQs

Version 3 (2021)

1. When is contract compliance due?

    a. Effective Immediately – as contracts are renewed.

2. Do all existing contracts need to be re-negotiated to become compliant?

    a.

ii. Section II: Independent Service Auditor’s Report

iii. Section III: Description of Services during the Examination Period

iv. Section IV: Description of Control Objectives, Controls, Tests, and Test Results

1. CC1.0 Control Environment
2. CC2.0 Communication and Information
3. CC3.0 Risk Assessment
4. CC4.0 Monitoring Activities
5. CC5.0 Control Activities
6. CC6.0 Logical and Physical Access Controls
7. CC7.0 System Operations
8. CC8.0 Change Management
9. CC9.0 Risk Mitigation
10. A.0 Availability Criteria
11. C.0 Confidentiality Criteria

v. Section V: Other Information Provided by Company

vi. Management Response(s) to items of note

16. What is an Incident Response Plan?

a. An incident response plan establishes and maintains processes to identify and report cybersecurity incidents affecting USG information and data assets.

17. What incident response roles does suppliers have?

a. 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.

18. How quickly should suppliers report an incident?

a. All cybersecurity incidents affecting the operation of mission-critical systems and categorized as “High” shall be reported to USG Cybersecurity **within one hour** of identification.

19. Are there specific types of incidents suppliers must report?

a. Yes – the incidents that suppliers must report to USG Cybersecurity include “type of cyber-attack, data breach, or use of malware” if these criteria are met:

i. Creates a life-safety event, or
ii. Substantially impacts the security of data and information systems, or
iii. Affects mission-critical systems, equipment, or service delivery.