**APPENDIX E—FedRAMP *Tailored* Self-Attestation Requirements**

Cloud Service Providers (CSPs) must attest to meeting the intent of the implementations of the security controls below. CSPs are not required to implement the security controls as explicitly stated in the security controls statement, however vendors must attest to meeting the intent of the controls.

For example, for AT-2, a CSP would attest to the fact that CSP staff are appropriate trained on security awareness issues. The details of the training and an assessment of the training are not required as a part of the assessment and authorization under FedRAMP *Tailored*.

If a vendor does not meet the intent of any of the security controls below, a vendor must identify that security control in their attestation to state that they do not implement that control and agency Authorizing Officials must be aware when making a risk based determination to authorize that system for use.

**CSP ATTESTATION**

[CSP] attests to meeting the intent of all of the security controls in table E-1 below. Any details about the security controls agency Authorizing Officials should be aware of are noted in the last column of Table E-1.

/ x / [CSP System Owner Signature] (date)

TABLE E-1

| **No** | **Control ID** | **Control Name** | **Additional Control Information and Comments** | **CSP Implementation Notes** |
| --- | --- | --- | --- | --- |
|  | AC-1 | Access Control Policy and Procedures |  |  |
|  | AC-7 | Unsuccessful Login Attempts | NSO - for non-privileged users; Attestation - for privileged users related to multi-factor identification and authentication |  |
|  | AC-20 | Use of External Information Systems |  |  |
|  | AT-1 | Security Awareness and Training Policy and Procedures |  |  |
|  | AT-2 | Security Awareness Training |  |  |
|  | AT-3 | Role-Based Security Training |  |  |
|  | AT-4 | Security Training Records |  |  |
|  | AU-1 | Audit and Accountability Policy and Procedures |  |  |
|  | AU-2 | Audit Events |  |  |
|  | AU-8 | Time Stamps |  |  |
|  | AU-9 | Protection of Audit Information |  |  |
|  | AU-12 | Audit Generation |  |  |
|  | CA-1 | Security Assessment and Authorization Policies and Procedures |  |  |
|  | CA-2 (1) | Security Assessments | Independent Assessors |  |  |
|  | CA-3 | System Interconnections |  |  |
|  | CA-5 | Plan of Action and Milestones | Attestation - for compliance with *FedRAMP Tailored LISaaS Continuous Monitoring Requirements* |  |
|  | CM-1 | Configuration Management Policy and Procedures |  |  |
|  | CM-2 | Baseline Configuration |  |  |
|  | CM-7 | Least Functionality |  |  |
|  | CP-1 | Contingency Planning Policy and Procedures |  |  |
|  | IA-1 | Identification and Authentication Policy and Procedures |  |  |
|  | IA-2 | Identification and Authentication (Organizational Users) | NSO -for non-privileged users; Attestation - for privileged users related to multi-factor identification and authentication - specifically include description of management of service accounts |  |
|  | IA-4 | Identifier Management |  |  |
|  | IA-5 | Authenticator Management |  |  |
|  | IA-5 (1) | Authenticator Management | Password-Based Authentication |  |  |
|  | IA-7 | Cryptographic Module Authentication |  |  |
|  | IA-8 | Identification and Authentication (NonOrganizational Users) |  |  |
|  | IA-8 (3) | Identification and Authentication (NonOrganizational Users) | Acceptance of FICAM-Approved Products |  |  |
|  | IA-8 (4) | Identification and Authentication (NonOrganizational Users) | Use of FICAM-Issued Profiles |  |  |
|  | IR-1 | Incident Response Policy and Procedures |  |  |
|  | IR-2 | Incident Response Training |  |  |
|  | IR-5 | Incident Monitoring |  |  |
|  | IR-7 | Incident Response Assistance |  |  |
|  | IR-8 | Incident Response Plan | Attestation - Specifically attest to US-CERT compliance |  |
|  | IR-9 | Information Spillage Response | Attestation - Specifically describe information spillage response processes |  |
|  | MA-1 | System Maintenance Policy and Procedures |  |  |
|  | MA-2 | Controlled Maintenance | CSP includes inherited controls in self-attestation |  |
|  | MA-4 | Nonlocal Maintenance |  |  |
|  | MA-5 | Maintenance Personnel | CSP includes inherited controls in self-attestation |  |
|  | MP-1 | Media Protection Policy and Procedures |  |  |
|  | MP-2 | Media Access | CSP includes inherited controls in self-attestation |  |
|  | MP-6 | Media Sanitization | CSP includes inherited controls in self-attestation |  |
|  | MP-7 | Media Use | CSP includes inherited controls in self-attestation |  |
|  | PE-1 | Physical and Environmental Protection Policy and Procedures |  |  |
|  | PE-2 | Physical Access Authorizations | CSP includes inherited controls in self-attestation |  |
|  | PE-3 | Physical Access Control | CSP includes inherited controls in self-attestation |  |
|  | PE-6 | Monitoring Physical Access | CSP includes inherited controls in self-attestation |  |
|  | PE-8 | Visitor Access Records | CSP includes inherited controls in self-attestation |  |
|  | PE-12 | Emergency Lighting | CSP includes inherited controls in self-attestation |  |
|  | PE-13 | Fire Protection | CSP includes inherited controls in self-attestation |  |
|  | PE-14 | Temperature and Humidity Controls | CSP includes inherited controls in self-attestation |  |
|  | PE-15 | Water Damage Protection | CSP includes inherited controls in self-attestation |  |
|  | PE-16 | Delivery and Removal | CSP includes inherited controls in self-attestation |  |
|  | PL-1 | Security Planning Policy and Procedures |  |  |
|  | PL-4 | Rules of Behavior |  |  |
|  | PS-1 | Personnel Security Policy and Procedures |  |  |
|  | PS-4 | Personnel Termination |  |  |
|  | PS-5 | Personnel Transfer |  |  |
|  | PS-6 | Access Agreements |  |  |
|  | PS-7 | Third-Party Personnel Security | Attestation - Specifically stating that any third-party security personnel are treated as CSP employees |  |
|  | PS-8 | Personnel Sanctions |  |  |
|  | RA-1 | Risk Assessment Policy and Procedures |  |  |
|  | SA-1 | System and Services Acquisition Policy and Procedures |  |  |
|  | SA-2 | Allocation of Resources |  |  |
|  | SA-3 | System Development Life Cycle |  |  |
|  | SA-4 | Acquisition Process |  |  |
|  | SA-4 (10) | Acquisition Process | Use of Approved PIV Products |  |  |
|  | SA-5 | Information System Documentation |  |  |
|  | SC-1 | System and Communications Protection Policy and Procedures |  |  |
|  | SC-20 | Secure Name /Address Resolution Service (Authoritative Source) |  |  |
|  | SC-21 | Secure Name /Address Resolution Service (Recursive or Caching Resolver) |  |  |
|  | SC-22 | Architecture and Provisioning for Name/Address Resolution Service |  |  |
|  | SC-39 | Process Isolation |  |  |
|  | SI-1 | System and Information Integrity Policy and Procedures |  |  |
|  | SI-5 | Security Alerts, Advisories, and Directives |  |  |
|  | SI-12 | Information Handling and Retention | Attestation - Specifically related to US-CERT and FedRAMP communications procedures |  |