## Contents

1 The OpenShift Compliance Guide
   1.1 About ................................................................. 3
   1.2 Table of Contents .................................................. 3
   1.3 Frequently Asked Questions ....................................... 3
   1.4 Contributing ........................................................ 4

2 Security CONOPS .................................................. 5
   2.1 Introduction ......................................................... 5
   2.2 Architecture ........................................................ 5

3 Security Controls .................................................. 23
   3.1 Overview ............................................................ 23
   3.2 AC-1 - Access Control Policy And Procedures .................. 24
   3.3 AC-12 - Session Termination ....................................... 25
   3.4 AC-14 - Permitted Actions Without Identification Or Authentication .................................................. 26
   3.5 AC-17 - Remote Access ............................................ 27
   3.6 AC-18 - Wireless Access ........................................... 28
   3.7 AC-18(5) - Wireless Access | Antennas / Transmission Power Levels .................................................. 28
   3.8 AC-19 - Access Control For Mobile Devices .................... 29
   3.9 AC-19(5) - Access Control For Mobile Devices | Full Device / Container-based Encryption .................................................. 30
   3.10 AC-2 - Account Management ....................................... 30
   3.11 AC-2(1) - Account Management | Automated System Account Management .................................................. 34
   3.12 AC-2(11) - Account Management | Usage Conditions .................. 35
   3.13 AC-2(2) - Account Management | Removal Of Temporary / Emergency Accounts .................................................. 36
   3.14 AC-2(3) - Account Management | Disable Inactive Accounts .................................................. 36
   3.15 AC-20 - Use Of External Information Systems .................. 37
   3.16 AC-21 - Information Sharing ....................................... 38
   3.17 AC-22 - Publicly Accessible Content ............................ 38
   3.18 AC-3 - Access Enforcement ......................................... 40
   3.19 AC-4 - Information Flow Enforcement ............................ 40
   3.20 AC-6(3) - Least Privilege | Network Access To Privileged Commands .................................................. 41
   3.21 AC-7 - Unsuccessful Logon Attempts ............................ 41
   3.22 AC-8 - System Use Notification .................................... 42
   3.23 AP-1 - Authority To Collect ....................................... 45
   3.24 AP-2 - Purpose Specification ...................................... 45
   3.25 AR-1 - Governance And Privacy Program .......................... 46
   3.26 AR-2 - Privacy Impact And Risk Assessment ..................... 48
<table>
<thead>
<tr>
<th>Section</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.27</td>
<td>AR-3 - Privacy Requirements For Contractors And Service Providers</td>
<td>49</td>
</tr>
<tr>
<td>3.28</td>
<td>AR-4 - Privacy Monitoring And Auditing</td>
<td>50</td>
</tr>
<tr>
<td>3.29</td>
<td>AR-5 - Privacy Awareness And Training</td>
<td>51</td>
</tr>
<tr>
<td>3.30</td>
<td>AR-6 - Privacy Reporting</td>
<td>52</td>
</tr>
<tr>
<td>3.31</td>
<td>AR-7 - Privacy-enhanced System Design And Development</td>
<td>53</td>
</tr>
<tr>
<td>3.32</td>
<td>AR-8 - Accounting Of Disclosures</td>
<td>53</td>
</tr>
<tr>
<td>3.33</td>
<td>AT-1 - Security Awareness And Training Policy And Procedures</td>
<td>55</td>
</tr>
<tr>
<td>3.34</td>
<td>AT-2 - Security Awareness Training</td>
<td>56</td>
</tr>
<tr>
<td>3.35</td>
<td>AT-3 - Role-based Security Training</td>
<td>57</td>
</tr>
<tr>
<td>3.36</td>
<td>AT-4 - Security Training Records</td>
<td>58</td>
</tr>
<tr>
<td>3.37</td>
<td>AU-1 - Audit And Accountability Policy And Procedures</td>
<td>59</td>
</tr>
<tr>
<td>3.38</td>
<td>AU-11 - Audit Record Retention</td>
<td>60</td>
</tr>
<tr>
<td>3.39</td>
<td>AU-12 - Audit Generation</td>
<td>61</td>
</tr>
<tr>
<td>3.40</td>
<td>AU-2 - Audit Events</td>
<td>62</td>
</tr>
<tr>
<td>3.41</td>
<td>AU-3(2) - Content Of Audit Records</td>
<td>64</td>
</tr>
<tr>
<td>3.42</td>
<td>AU-4 - Audit Storage Capacity</td>
<td>65</td>
</tr>
<tr>
<td>3.43</td>
<td>AU-5 - Response To Audit Processing Failures</td>
<td>65</td>
</tr>
<tr>
<td>3.44</td>
<td>AU-5(2) - Response To Audit Processing Failures</td>
<td>Real-time Alerts</td>
</tr>
<tr>
<td>3.45</td>
<td>AU-6 - Audit Review, Analysis, And Reporting</td>
<td>67</td>
</tr>
<tr>
<td>3.46</td>
<td>AU-6(5) - Audit Review, Analysis, And Reporting</td>
<td>Integration / Scanning And Monitoring Capabilities</td>
</tr>
<tr>
<td>3.47</td>
<td>AU-6(6) - Audit Review, Analysis, And Reporting</td>
<td>Correlation With Physical Monitoring</td>
</tr>
<tr>
<td>3.48</td>
<td>AU-7 - Audit Reduction And Report Generation</td>
<td>69</td>
</tr>
<tr>
<td>3.49</td>
<td>AU-7(1) - Audit Reduction And Report Generation</td>
<td>Automatic Processing</td>
</tr>
<tr>
<td>3.50</td>
<td>AU-8 - Time Stamps</td>
<td>70</td>
</tr>
<tr>
<td>3.51</td>
<td>AU-9 - Protection Of Audit Information</td>
<td>71</td>
</tr>
<tr>
<td>3.52</td>
<td>AU-9(2) - Protection Of Audit Information</td>
<td>Audit Backup On Separate Physical Systems / Components</td>
</tr>
<tr>
<td>3.53</td>
<td>AU-9(3) - Protection Of Audit Information</td>
<td>Cryptographic Protection</td>
</tr>
<tr>
<td>3.54</td>
<td>CA-1 - Security Assessment And Authorization Policy And Procedures</td>
<td>73</td>
</tr>
<tr>
<td>3.55</td>
<td>CA-2 - Security Assessments</td>
<td>74</td>
</tr>
<tr>
<td>3.56</td>
<td>CA-2(2) - Security Assessments</td>
<td>Specialized Assessments</td>
</tr>
<tr>
<td>3.57</td>
<td>CA-3 - System Interconnections</td>
<td>77</td>
</tr>
<tr>
<td>3.58</td>
<td>CA-4 - Baseline Configuration</td>
<td>78</td>
</tr>
<tr>
<td>3.59</td>
<td>CA-5 - Plan Of Action And Milestones</td>
<td>78</td>
</tr>
<tr>
<td>3.60</td>
<td>CA-6 - Security Authorization</td>
<td>79</td>
</tr>
<tr>
<td>3.61</td>
<td>CA-7 - Continuous Monitoring</td>
<td>80</td>
</tr>
<tr>
<td>3.62</td>
<td>CA-7(1) - Continuous Monitoring</td>
<td>Independent Assessment</td>
</tr>
<tr>
<td>3.63</td>
<td>CA-8 - Penetration Testing</td>
<td>83</td>
</tr>
<tr>
<td>3.64</td>
<td>CA-9 - Internal System Connections</td>
<td>83</td>
</tr>
<tr>
<td>3.65</td>
<td>CM-1 - Configuration Management Policy And Procedures</td>
<td>84</td>
</tr>
<tr>
<td>3.66</td>
<td>CM-10 - Software Usage Restrictions</td>
<td>86</td>
</tr>
<tr>
<td>3.67</td>
<td>CM-11 - User-installed Software</td>
<td>87</td>
</tr>
<tr>
<td>3.68</td>
<td>CM-2 - Baseline Configuration</td>
<td>88</td>
</tr>
<tr>
<td>3.69</td>
<td>CM-2(2) - Baseline Configuration</td>
<td>Automation Support For Accuracy / Currency</td>
</tr>
<tr>
<td>3.70</td>
<td>CM-2(3) - Baseline Configuration</td>
<td>Retention Of Previous Configurations</td>
</tr>
<tr>
<td>3.71</td>
<td>CM-2(7) - Baseline Configuration</td>
<td>Configure Systems, Components, Or Devices For High-risk Areas</td>
</tr>
<tr>
<td>3.72</td>
<td>CM-3(1) - Configuration Change Control</td>
<td>Automated Document / Notification / Prohibition Of Changes</td>
</tr>
<tr>
<td>3.73</td>
<td>CM-3(2) - Configuration Change Control</td>
<td>Test / Validate / Document Changes</td>
</tr>
<tr>
<td>3.74</td>
<td>CM-4 - Security Impact Analysis</td>
<td>92</td>
</tr>
<tr>
<td>3.75</td>
<td>CM-5(3) - Access Restrictions For Change</td>
<td>Signed Components</td>
</tr>
<tr>
<td>3.76</td>
<td>CM-6 - Configuration Settings</td>
<td>94</td>
</tr>
<tr>
<td>3.77</td>
<td>CM-6(2) - Configuration Settings</td>
<td>Respond To Unauthorized Changes</td>
</tr>
<tr>
<td>3.78</td>
<td>CM-7 - Least Functionality</td>
<td>96</td>
</tr>
<tr>
<td>3.79</td>
<td>CM-7(4) - Least Functionality</td>
<td>Unauthorized Software / Blacklisting</td>
</tr>
<tr>
<td>3.80</td>
<td>CM-8 - Information System Component Inventory</td>
<td>98</td>
</tr>
</tbody>
</table>
3.241 SA-9 - External Information System Services ................................................................. 251
3.242 SC-1 - System And Communications Protection Policy And Procedures .......................... 252
3.243 SC-10 - Network Disconnect ............................................................................................ 253
3.244 SC-12 - Cryptographic Key Establishment And Management .......................................... 254
3.245 SC-12(1) - Cryptographic Key Establishment And Management | Availability .................. 254
3.246 SC-13 - Cryptographic Protection .................................................................................... 255
3.247 SC-15 - Collaborative Computing Devices ...................................................................... 256
3.248 SC-2 - Application Partitioning ....................................................................................... 256
3.249 SC-20 - Secure Name / Address Resolution Service (authoritative Source) ..................... 257
3.250 SC-21 - Secure Name / Address Resolution Service (recursive Or Caching Resolver) .......... 258
3.251 SC-22 - Architecture And Provisioning For Name / Address Resolution Service .......... 258
3.252 SC-24 - Fail In Known State ............................................................................................ 259
3.253 SC-3 - Security Function Isolation .................................................................................... 260
3.255 SC-4 - Information In Shared Resources ......................................................................... 261
3.256 SC-42 - Sensor Capability And Data .................................................................................. 261
3.257 SC-42(3) - Sensor Capability And Data | Prohibit Use Of Devices ................................. 262
3.258 SC-5 - Denial Of Service Protection .................................................................................. 262
3.259 SC-7 - Boundary Protection .............................................................................................. 263
3.260 SC-7(18) - Boundary Protection | Fail Secure .................................................................. 264
3.261 SC-7(21) - Boundary Protection | Isolation Of Information System Components .......... 265
3.262 SE-1 - Inventory Of Personally Identifiable Information ................................................. 266
3.263 SE-2 - Privacy Incident Response .................................................................................... 266
3.264 SI-1 - System And Information Integrity Policy And Procedures ....................................... 267
3.265 SI-12 - Information Handling And Retention ................................................................. 269
3.266 SI-16 - Memory Protection ............................................................................................... 269
3.267 SI-2 - Flaw Remediation .................................................................................................... 270
3.268 SI-3 - Malicious Code Protection ..................................................................................... 271
3.269 SI-4 - Information System Monitoring ............................................................................. 273
3.270 SI-4(2) - Information System Monitoring | Automated Tools For Real-time Analysis .......... 275
3.271 SI-5 - Security Alerts, Advisories, And Directives ............................................................ 276
3.272 SI-5(1) - Security Alerts, Advisories, And Directives | Automated Alerts And Advisories ... 277
3.273 SI-6 - Security Function Verification .................................................................................. 278
3.274 SI-7 - Software, Firmware, And Information Integrity ...................................................... 279
3.275 SI-7(1) - Software, Firmware, And Information Integrity | Integrity Checks ...................... 280
3.276 SI-7(2) - Software, Firmware, And Information Integrity | Automated Notifications Of Integrity Violations .............................................................................................................. 281
3.277 SI-7(5) - Software, Firmware, And Information Integrity | Automated Response To Integrity Violations .............................................................................................................. 281
3.278 SI-7(7) - Software, Firmware, And Information Integrity | Integration Of Detection And Response .............................................................................................................. 282
3.279 SI-8 - Spam Protection ...................................................................................................... 282
3.280 SI-8(1) - Spam Protection | Central Management .............................................................. 283
3.281 SI-8(2) - Spam Protection | Automatic Updates ................................................................. 284
3.282 TR-1 - Privacy Notice ........................................................................................................ 284
3.283 TR-1(1) - Privacy Notice | Real-time Or Layered Notice ...................................................... 286
3.284 TR-2 - System Of Records Notices And Privacy Act Statements ...................................... 286
3.285 TR-2(1) - System Of Records Notices And Privacy Act Statements | Public Website Publication .............................................................................................................. 288
3.286 TR-3 - Dissemination Of Privacy Program Information ..................................................... 288
3.287 UL-1 - Internal Use ............................................................................................................ 289
3.288 UL-2 - Information Sharing With Third Parties ................................................................. 290

4 Customer Responsibility Matrix ................................................. 293

4.1 Overview .......................................................................................................................... 293
4.2 CM-8(4) - Information System Component Inventory | Accountability Information .......... 293
4.3 CP-10(2) - Information System Recovery And Reconstitution | Transaction Recovery .......... 294
4.4 DI-1 - Data Quality
4.5 DI-1(1) - Data Quality | Validate Pii
4.6 DI-1(2) - Data Quality | Re-validate Pii
4.7 DI-2 - Data Integrity And Data Integrity Board
4.8 DM-1 - Minimization Of Personally Identifiable Information
4.9 DM-2 - Data Retention And Disposal
4.10 DM-2(1) - Data Retention And Disposal | System Configuration
4.11 DM-3 - Minimization Of Pii Used In Testing, Training, And Research
4.12 IP-1 - Consent
4.13 IP-1(1) - Consent | Mechanisms Supporting Itemized Or Tiered Consent
4.14 IP-2 - Individual Access
4.15 IP-3 - Redress
4.16 IP-4 - Complaint Management
4.17 IP-4(1) - Complaint Management | Response Times
4.18 MA-1 - System Maintenance Policy And Procedures
4.19 PL-2 - System Security Plan
4.20 RA-1 - Risk Assessment Policy And Procedures
4.21 RA-3 - Risk Assessment
4.22 SA-11 - Developer Security Testing And Evaluation
4.23 SA-3 - System Development Life Cycle
4.24 SA-4(1) - Acquisition Process | Functional Properties Of Security Controls
4.25 SA-4(2) - Acquisition Process | Design / Implementation Information For Security Controls
4.26 SE-1 - Inventory Of Personally Identifiable Information
4.27 SI-1 - System And Information Integrity Policy And Procedures
4.28 TR-1 - Privacy Notice
4.29 TR-1(1) - Privacy Notice | Real-time Or Layered Notice
4.30 TR-2 - System Of Records Notices And Privacy Act Statements
4.31 TR-2(1) - System Of Records Notices And Privacy Act Statements | Public Website Publication
4.32 TR-3 - Dissemination Of Privacy Program Information
4.33 UL-1 - Internal Use
4.34 UL-2 - Information Sharing With Third Parties

5 Ansible
5.1 Reference Architecture
5.2 Manual Workarounds

6 Frequently Asked Questions
6.1 Is this guide complete?
6.2 Has OpenShift been accredited anywhere?
6.3 How can I help?
6.4 X is wrong, what’s up?
6.5 Who can I talk to about this?

7 Indices and tables
Contents:
CHAPTER 1

The OpenShift Compliance Guide

About

OpenShift is a container management platform based on Docker containers and the Kubernetes container cluster manager. OpenShift adds developer and operational centric tools to enable rapid application development, easy deployment and scaling, and long-term lifecycle maintenance for small and large teams and applications.

Built atop Red Hat Enterprise Linux (RHEL), OpenShift is very secure. For users who must comply with the Federal Information Security Management Act (FISMA), there is additional configuration burden.

This guide can help you secure your OpenShift cluster to comply with the FISMA moderate confidentiality, integrity, and availability requirements.

While the configurations and Security Control Traceability Matrix (SCTM) documented in this guide could be implemented in any environment, the reference architecture is Amazon Web Services.

Table of Contents

1. Security CONOPS
2. Security Controls
3. Customer Responsibility Matrix
4. Ansible

Frequently Asked Questions

Have questions? Visit our Frequently Asked Questions.
Contributing

Security is an ongoing effort, and we appreciate any feedback or recommendations that you may have. Please use this project’s GitHub page to submit issues or pull requests.

Authors

- Nick Sabine
- Ken Evensen
- Mark Shoger
- Mike Epley
- Durell Willoughby
- Tiffany Gray
- Matt Bagnara
- Jason Callaway
Introduction

The Security Concept of Operations (CONOPS) details, at various levels of abstraction, a deployment of Red Hat’s OpenShift Container Platform (OCP) deployed on Amazon Web Services (AWS). The NIST Definition of Cloud Computing (NIST 800-145) succinctly describes different cloud service models and the attributes of a cloud platform. The architecture described herein follows the definitions found in the NIST 800-145. For example, Red Hat’s OCP is a Platform as a Service (PaaS) under NIST 800-145. Similarly, AWS is an Infrastructure as a Service (IaaS) per the NIST definition.

Security Standards

The Federal Information Security Modernization Act (FISMA), originally enacted in 2002, directs United States Federal Agencies to develop and implement programs to implement information and information systems security. This reference architecture aims to describe an OCP deployment on AWS as FISMA high: high confidentiality, high integrity, high availability.

In order to demonstrate FISMA high, this architecture is traced to NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The NIST 800-53 provides a catalog of controls across multiple categories. Many controls relate to organizational processes. These controls will be mapped as appropriate. The controls that are technical in nature are addressed by this architecture.

Architecture

This architecture is divided into architectural views loosely mapped to the NIST 800-145 Definition of Cloud Computing. The nature of cloud computing affords the adoption of a Landlord/Tenant model. This model allows the Landlord to take responsibility for a set of controls under NIST 800-53, relieving the tenant of the need to address those controls. The following table lists the relationship of Landlord to Tenant in this reference architecture.
As stated previously, the IaaS in this architecture is AWS. Red Hat’s OCP is the PaaS. Tenant applications are deployed in containers, managed by OCP.

**Infrastructure View**

The infrastructure view describes the OCP components at the infrastructure level. These components are necessary to serve OCP in AWS and achieving FISMA high.

**IaaS Definition - NIST 800-145**

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

**Description**

AWS provides this capability. Amazon provides the underlying hardware infrastructure that supports the self-service provisioning into the cloud of what has traditionally been based in hardware. This includes, but is not limited to compute, storage, and networking services.

**Stakeholders**

**Cluster Administrators** require AWS console access and the ability to deploy and/or configure the following AWS components.

- VPC
- Elastic IP
- Elastic Cloud Compute (EC2)
- VPC Peering
- Route Tables

**Application Developers** do not have a role at the infrastructure level.

**Application Consumers** do not have a role at the infrastructure level.
Diagram

The following diagram illustrates the high level deployment of OCP in AWS and the necessary AWS components to support OCP.

Components

The following table describes each AWS component and relates it to the implementation in the OCP reference architecture.
### Network Architecture

The network views below assume that OCP is deployed on to an air-gapped network that is unable to route to the Internet.

The Staging Subnet provides an isolated area for platform administrators to apply regular patches and test configuration changes before applying these to the operations cluster. One cluster of OCP is deployed in this VPC.

The Operations Subnet contains a single deployment of OpenShift where tenants will deploy applications. OCP Nodes will be labeled and functionally grouped to support development, test, and production deployments of an application. This is described in detail in the Platform View.

The Management Subnet contains the Trusted Container Repository as well as the Package Repository. A route table allows the Management Subnet to communicate to the Staging Subnet, Operations Subnet. The Staging Subnet and Operations Subnet are not permitted to communicate with each other. A VPC peering connection allows the Management Subnet in the Red Hat VPC to communicate with any Dedicated VPC’s.

Dedicated VPC’s are VPC’s that are deployed to support specific isolation needs of a particular tenant. These may be created and destroyed per organizational needs.

The bastion host allows OCP Administrators and only OCP Administrators the ability to access the underlying hosts in each VPC.

Application Developers interact with OCP via a command line interface (CLI) and web user interface (WebUI). An application router, internal to OCP, handles application traffic. Therefore certain ports in a security group must be exposed on the Red Hat VPC to allow the traffic. The same is true of any Dedicated VPC’s. The following table details this information.
Communications internal to the nodes occur in the network address space defined by VPC subnets.

**Platform View**

The platform view describes the OCP architecture at the platform level. This view abstracts out the AWS components and focuses primarily on the functional components of OCP.

**PaaS Definition - NIST 800-145**

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

**Description**

The OpenShift Container Platform provides application developer’s the ability to rapidly deploy applications in a variety of application frameworks.

**Stakeholders**

**Cluster Administrators** are responsible for the operations and proper function of the platform. They have the ability to affect OCP security policies surrounding developer interaction and container function.

**Application Developers** have access to the OCP WebUI and CLI to deploy applications.

**Application Users** do not have a role at the platform level.

**Roles**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Administrator</td>
<td>Full administrative control over the OpenShift cluster</td>
</tr>
<tr>
<td>Cluster Auditor</td>
<td>Read-only access to all objects on the cluster</td>
</tr>
<tr>
<td>Project Administrator</td>
<td>Full administrative access to a project</td>
</tr>
<tr>
<td>Project Auditor</td>
<td>Read-only access to a project</td>
</tr>
<tr>
<td>Application Developer</td>
<td>Full access to build, deploy and terminate applications. Cannot modify access to the project.</td>
</tr>
</tbody>
</table>
Diagram

The following diagram details the minimum highly-available configuration of OCP to meet FISMA high at the platform level.
2.2. Architecture
Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>The OCP Master provides the API and WebUI entry points for Application Developers and OCP administrators. The OCP Master is also responsible for scheduling containers on each node.</td>
</tr>
<tr>
<td>ETCD</td>
<td>The ETCD servers are key-value stores used for maintaining information about the state of the OCP cluster.</td>
</tr>
<tr>
<td>Application Node</td>
<td>The Application Nodes handle executing application containers.</td>
</tr>
<tr>
<td>Infrastructure Node</td>
<td>In an OCP cluster, a containerized HA proxy routes application traffic. A containerized integrated container registry in OCP is a mechanism in the automated build and deployment flow. Both the application router and integrated container registry and only these components run on the Infrastructure Node.</td>
</tr>
</tbody>
</table>

Network Architecture

The network architecture in the platform view is broken into two parts. The first is the internal networking from between the EC2 instances supporting the platform. The second is the software defined networking layer enabling multi-tenant deployment of container based applications.

The following diagram illustrates the internetworking of the platform components of OCP.
The following table describes the port information of the internal platform components.
<table>
<thead>
<tr>
<th>From</th>
<th>To</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Traffic ELB</td>
<td>OCP Infrastructure Node</td>
<td>443/TCP</td>
<td></td>
</tr>
<tr>
<td>API Traffic ELB</td>
<td>HA and Authentication Proxy</td>
<td>8443/TCP</td>
<td></td>
</tr>
<tr>
<td>HA and Authentication Proxy</td>
<td>OCP Master</td>
<td>8443/TCP</td>
<td></td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Master and Loop</td>
<td>8053/TCP</td>
<td>Required for DNS resolution of clustered services.</td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Master and Loop</td>
<td>8053/UDP</td>
<td>Required for DNS resolution of clustered services.</td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Master</td>
<td>2379/TCP</td>
<td>Used for standalone etcd (clustered) to accept changes in state.</td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Master</td>
<td>2380/TCP</td>
<td>etcd requires this port be open between masters for leader election and peering connections when using standalone etcd (clustered).</td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Node</td>
<td>4789/UDP</td>
<td>Required for SDN communication between pods on separate hosts.</td>
</tr>
<tr>
<td>OCP Master</td>
<td>OCP Node</td>
<td>10250/TCP</td>
<td>The master proxies to node hosts via the Kubelet for oc commands.</td>
</tr>
<tr>
<td>OCP Node</td>
<td>OCP Master</td>
<td>4789/UDP</td>
<td>Required for SDN communication between pods on separate hosts.</td>
</tr>
<tr>
<td>OCP Node</td>
<td>OCP Master</td>
<td>8053/TCP</td>
<td>Required for DNS resolution of clustered services.</td>
</tr>
<tr>
<td>OCP Node</td>
<td>OCP Master</td>
<td>8053/UDP</td>
<td>Required for DNS resolution of clustered services.</td>
</tr>
<tr>
<td>All</td>
<td>Package Repository</td>
<td>443/TCP</td>
<td></td>
</tr>
<tr>
<td>OCP Node</td>
<td>Trusted Container Repository</td>
<td>443/TCP</td>
<td></td>
</tr>
<tr>
<td>Bastion</td>
<td>All</td>
<td>22/TCP</td>
<td>SSH</td>
</tr>
<tr>
<td>Ansible Tower</td>
<td>All</td>
<td>22/TCP</td>
<td>SSH used during Ansible Plays</td>
</tr>
<tr>
<td>OCP Node</td>
<td>Gluster Node</td>
<td>49152-49251/TCP</td>
<td>For client communication with Red Hat Gluster Storage 2.1 and for brick processes depending on the availability of the ports. The total number of ports required to be open depends on the total number of bricks exported on the machine.</td>
</tr>
<tr>
<td>Gluster Node</td>
<td>Gluster Node</td>
<td>24007/TCP</td>
<td>For glusterd (for management).</td>
</tr>
</tbody>
</table>

In order to achieve network traffic isolation between containers owned by different tenants running on the same node, the traffic must be encapsulated. This capability is provided by OpenVSwitch which encapsulates the OSI L2 traffic from the containers in the L3 traffic between the nodes. The packets are then tagged by an 24 bit value known as a VXLAN Network Identifier (VNID). A VNID corresponds to a project space in OCP and is transparent to both the **Application Developer** and **Application User**. In order to utilize this option the `redhat/openshift-ovs-multitenant` must be selected during the installation.

The L3 traffic between nodes is sent as UDP packets to port 4789.

More information on the software defined network in OCP can be found in the online documentation.

### Platform Security - Platform Users

Regardless of the user role, all users are subject to authorization policies managed in the OCP cluster. Authorization policies dictate what a user can and cannot do. Policies are enforce at the project (local) level, and separately at the cluster level.

---

**OpenShift Compliance Guide, Release 1.0 beta**

---

**Chapter 2. Security CONOPS**
The following table describes the elements comprising an authorization role.

<table>
<thead>
<tr>
<th>Rules</th>
<th>Sets of permitted verbs on a set of objects. For example, whether something can create pods.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles</td>
<td>Collections of rules. Users and groups can be associated with, or bound to, multiple roles at the same time.</td>
</tr>
<tr>
<td>Bindings</td>
<td>Associations between users and/or groups with a role.</td>
</tr>
</tbody>
</table>

**Platform Security - Container Security**

Container security occurs at multiple levels. At the platform level, OCP applies security context constraints (SCC’s) to manage what a container can and cannot do. OCP provides a number of SCC’s out of the box. The default SCC is highly restrictive to unprivileged containers.

Unprivileged containers are containers deployed in a tenant application. Specific action is required on the part of the **Cluster Administrator** to allow an **Application Developer** the ability to deploy a container with escalated privileges.

A notable attribute of SCC’s is the user ID enforcement. When a container executes, the entry process runs in the container as a specified user ID. The **restricted SCC** forces the container to be run as a very high UID. This prevents a container from being deployed where the internal user ID is set to 0 (root).

**Storage Architecture**

Managing storage is a distinct problem from managing compute resources. OpenShift Container Platform leverages the Kubernetes persistent volume (PV) framework to allow administrators to provision persistent storage for a cluster. Using persistent volume claims (PVCs), developers can request PV resources without having specific knowledge of the underlying storage infrastructure.

In this reference architecture, storage services are provided through a managed storage tier, implemented by Red Hat Gluster Storage (Gluster). Gluster provides a fault-tolerant and highly available network storage resource, efficiently rationed to tenant applications as PVs. Since the storage interface to developers is managed by the Kubernetes PVC resource, the details of the underlying storage implementation are abstracted.

PVCs are specific to a project and are created and used by developers as a means to use a PV. PV resources on their own are not scoped to any single project; they can be shared across the entire OpenShift Container Platform cluster and claimed from any project. After a PV has been bound to a PVC, however, that PV cannot then be bound to additional PVCs. This has the effect of scoping a bound PV to a single namespace (that of the binding project).

The Gluster storage services are provided through a dedicated cluster of AWS instances within the scope of the platform VPC. Administrators allocate storage resources, creating a pool of available PVs in standard sizes, and monitor the capacity of the underlying storage resources. As PVs are released, administrators ensure the deletion and reclamation of storage resources, returning capacity to the pool of available PVs.

**Platform Security - Storage Security**

Gluster complies with data protection requirements through secure configuration of the storage resources and transport protocols. At rest, data is protected by LUKS encryption of the of the AWS EBS devices. This ensures that access to EBS volumes or snapshots by unauthorized mechanisms are unable to extract any usable information from the storage tier. Configuration of LUKS encryption in Red Hat Enterprise Linux 7 is configured according to the Encryption chapter of the RHEL 7 Security Guide.

During transit, information is protected through configuration of SSL connections, and enforcement of mutually authenticated TLS connections. For more information, refer to Configuring Network Encryption in Red Hat Gluster Storage.
The following diagram depicts the mapping of storage devices to application resources within OCP. The LUKS encryption is enabled at the EBS device, ensuring that all data is encrypted prior to writing to disk. This architecture is designed to be compatible with the OCP and Kubernetes roadmaps, specifically with reference to upcoming dynamic provisioning features.

In this view, the synchronous replication is shown between availability zones of the IaaS tier. This ensures high availability and integrity of data stored within the platform.
Application View

Definition

The application view describes the OCP architecture at the application level. This view focuses on the services and interfaces available to project tenants within the platform.

Description

Actors

Application Developers

OCP Administrators are responsible for the creation of tenant projects and assignment of proper roles of project administrators.

Project Administrators are responsible for assignment of proper roles within the scope of a single tenant project. They have the ability to affect security policies surrounding developer interaction and container function, including the ability to grant privileges to administer, edit, or view project level resources.

Application Developers have access to the OCP WebUI and CLI to create, build, deploy, and delete applications within the scope of a project, subject to the roles and privileges assigned by the Project Administrators.

Application Users do not have a role at the application level.
Application Security - Sensitive Configuration Data

There is often a need to provide sensitive data for the proper configuration of the application or service component. For instance, it may be necessary to provide encryption keys, passwords, configuration files, private source repository credentials, and other data considered sensitive. This data often varies between environments, such as database passwords or SSL server certificates. Secrets provide a mechanism to decouple sensitive content from the pods that use it, removing the necessity of storing this data on the filesystem or within the container image itself. This mechanism promotes best practices for abstracting environment-specific configuration data away from the build process, as well as provides an encrypted storage mechanism. For more information on this topic, refer to the Secrets documentation.

Diagram

The following diagram details the conceptual use of project resources to build and deploy applications within a project.
Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dev</td>
<td>Application Developers interact with the platform by creating project resource definitions, and by pushing application code revisions to the enterprise hosted git service.</td>
</tr>
<tr>
<td>App Code</td>
<td>The source code artifacts implementing the business logic of an application service or component.</td>
</tr>
<tr>
<td>git</td>
<td>The source code configuration management system. For this architecture, the git service is assumed to be provided externally, as a corporate or project team resource.</td>
</tr>
<tr>
<td>Build Config</td>
<td>A build configuration describes a single build definition and a set of triggers for when a new build should be created. For in-depth description of builds and OCP build configurations, refer to the Build documentation.</td>
</tr>
<tr>
<td>Integrated Registry</td>
<td>The OCP integrated registry is a controlled container image registry for storing OCP container images and completed application builds. For more information regarding the integrated registry, refer to the Image Registry documentation.</td>
</tr>
<tr>
<td>Builder Image</td>
<td>A builder image is a pre-defined container image that stores the build process for compilation and assembly of application source code. It houses the compiler binaries required for interpretation of source code, and the tools necessary for building application images.</td>
</tr>
<tr>
<td>builder</td>
<td>The builder is a container derived from the builder image. It produces an application image using the defined build process using the compiler binaries.</td>
</tr>
<tr>
<td>App Image</td>
<td>An Application Image is produced as a result of the application build process. It is composed of a certified base image, application server components, required configurations, and finally, the compiled application source code.</td>
</tr>
<tr>
<td>Deployment Config</td>
<td>The deployment config defines the requirements and configuration of resources necessary for operations of the application component. For more information regarding the deployment config, refer to the Deployment documentation.</td>
</tr>
<tr>
<td>Deployer</td>
<td>The deployer is a container responsible for setting up the operational environment of the application container.</td>
</tr>
<tr>
<td>Pod</td>
<td>OpenShift Container Platform leverages the Kubernetes concept of a pod, which is one or more containers deployed together on one host, and the smallest compute unit that can be defined, deployed, and managed. For more information regarding Pods, refer to the Pod documentation.</td>
</tr>
<tr>
<td>App Container</td>
<td>The application container is the running instance of an application image, as defined by the deployment configuration.</td>
</tr>
<tr>
<td>etcd</td>
<td>EtcD is the key-value database for OCP state and configuration information.</td>
</tr>
<tr>
<td>Secret</td>
<td>Secrets provide a mechanism to hold information such as encryption keys, passwords, config files, private source repository credentials, and other data considered sensitive. Secrets decouple sensitive content from the pods that use it and can be mounted into containers using a volume plug-in or used by the system to perform actions on behalf of a pod. For more information regarding Secrets, refer to the Secrets documentation.</td>
</tr>
<tr>
<td>Persistent Volume</td>
<td>A Persistent Volume is a storage resource in OCP. Storage is provisioned by the cluster administrators by creating PersistentVolume objects from the storage infrastructure system. Application Developers utilize Persistent Volumes by creating a Persistent Volume Claim within the scope of the project. For more information regarding persistent storage, refer to the Storage documentation.</td>
</tr>
<tr>
<td>Log Aggregation</td>
<td>In OCP, Log Aggregation is implemented as the integrated deployment of Elastic Search, FluentD, and Kibana (EFK). This stack aggregates logs for a range of OCP services, including project resources deployed on the platform. Application developers can view the logs of the projects for which they have view access. The EFK stack aggregates logs from hosts and applications, whether coming from multiple containers or even deleted pods. For more information regarding log aggregation in OCP, refer to the Aggregate Logging documentation.</td>
</tr>
<tr>
<td>Replication Controller</td>
<td>A replication controller ensures that a specified number of replicas of a pod are running at all times. If pods exit or are deleted, the replication controller acts to instantiate more up to the defined number. Likewise, if there are more running than desired, it deletes as many as necessary to match the defined amount. For more information regarding replication controllers, refer to the Replication Controller documentation.</td>
</tr>
<tr>
<td>Services</td>
<td>A service serves as an internal load balancer. It identifies a set of replicated pods in order to proxy connections it receives to them. Balking pods can be added to or removed from a service arbitrarily while the service remains consistently available, enabling anything that depends on the service to refer to it at a consistent internal address. For more information regarding services, refer to the Services documentation.</td>
</tr>
</tbody>
</table>

2.2. Architecture

Routing

The OpenShift Container Platform supports two types of routing. First, all traffic is routed through a

**Container View**

**Definition**

A container in the context of an information system is an operating system level virtualization method, provided by kernel constructs, for isolating processes using a single kernel.

Due to the value of containers to the information technology field, the definition for both the container image specification and runtime are managed by a community of interested parties: Open Container Initiative (OCI). The technical definition is divided into an Image Specification (image-spec) and Runtime Specification (runtime-spec).

**Description**

The container view describes the constructs used in OCIF and runc process isolation. This view addresses a single container regardless of being run in the OCP cluster.

**Actors**

**Platform Administrators** are responsible for two specific container processes in the OCP cluster. The first is an integrated container registry. The second is an application traffic HAProxy router, running in a container. While these nominally operate without intervention, their continued operation falls under the responsibility of the Platform Administrators.

**Application Developers** do not necessarily need to be aware of the container construct in OCP. An Application Developer can deploy a containerized application inside OCP simply by providing OCP a source code repository. At this point OCP automatically builds the source into and deploys a containerized application.

**Container Filesystem**

A single container as it exists on the host’s filesystem is actually a multi-layer filesystem: UnionFS. Each container image consists of a Kernel library layer, bootfs, and Base Image. Additional layers may contain application libraries and binaries. Once this container image is built, it is immutable. This has implications:

1. Any patches to a lower layer of the container (e.g. the base image) require the container to be rebuilt from that level up.

2. Without an externally mounted persistent storage share, any data written to the container's file system is lost when that container is destroyed.

The following graphic presents a simplified view of a layered container image.
External storage can be provided to the container and mounted as a file system in the container for data persistence. The platform layer abstracts the Persistent Volume from the container. The container has no knowledge of the nature of the underlying storage share; only that it has a file system to which it can write.

**Kernel Components**

A container is constructed using Linux kernel mechanisms, some of which have existed for over 10 years. The following table describes these kernel mechanisms and their role in isolating processes.

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SELinux</td>
<td>SELinux, a core component of Red Hat Enterprise Linux, labels processes and filesystems, enforcing mandatory access control. Each containerized process receives a unique SELinux category.</td>
</tr>
<tr>
<td>CGroups</td>
<td>CGroups provide resource constraints preventing run-away processes.</td>
</tr>
<tr>
<td>Kernel Namespaces</td>
<td>Namespaces allow resources to have identical names in the context of that resource, but unique names from perspective of the host. For example, the PID namespace allows for PID 0 in each container, but be PID N on the host.</td>
</tr>
<tr>
<td>Kernel Capabilities</td>
<td>Capabilities are process permission controls that group system calls in different categories. By default, all capabilities are removed for unprivileged containers.</td>
</tr>
<tr>
<td>Secomp</td>
<td>Secure computing assists with creating sandboxes by defining which system calls should be blocked.</td>
</tr>
</tbody>
</table>
The criticality of protecting the platform in a multi-tenant environment cannot be understated. As a result, the protection offered by SELinux Multi-Category Security (MCS) as an integral component of the layered security model within the Red Hat Enterprise Linux Docker Security Policy is indispensable. RHEL's Container MCS policy is derived and extended from sVirt, the SELinux policy for isolating virtual machine hypervisor processes. sVirt policy has been developed, refined, and continuously tested since 2009, and offers a mature and validated model for infrastructure protection. It is the gold standard of preventing a compromised process from gaining additional privileges or access to components of the system that have not been specifically allowed by policy.

In a SELinux-labeled file or process, there multiple fields that affect how the policy is evaluated. Most critical for interpretation of the container MCS policy are the type and category fields. In the case of a container process, the type will be `svirt_lxc_net_t`. This indicates that the process will only be allowed to invoke system actions that have been explicitly whitelisted in the policy. On the other hand, the category fields will be uniquely assigned for each process. This ensures that container processes on the same physical system are not permitted to interact at the system level, and that tenants in the multi-tenant system are unable to access or affect other tenants.
Overview

These security controls comply with FISMA Low, Moderate, and High requirements as defined by NIST SP800-53r4. Each control indicates the role responsible for implementing that control. The defined roles are based on those identified in the FedRAMP SSP Template, but have been modified to make sense in the context of Security CONOPS.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
<th>Number Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>A control that is satisfied by the hosting organization. This includes enterprise services such as LDAP, the Audit and Logging solution, etc.</td>
<td>423</td>
</tr>
<tr>
<td>IaaS</td>
<td>A control that is satisfied by the Organization’s Infrastructure as a Service implementation. In the Security CONOPS reference architecture, this is AWS, or the Landlord’s Landlord.</td>
<td>11</td>
</tr>
<tr>
<td>OpenShift Landlord</td>
<td>Container Platform’s implementation. This includes tools such as Ansible Tower and OpenSCAP.</td>
<td>187</td>
</tr>
<tr>
<td>OpenShift Tenant</td>
<td>Controls that need to be implemented by the programs hosted on the OpenShift Container Platform. These controls are listed in the Customer Responsibility Matrix.</td>
<td>73</td>
</tr>
<tr>
<td>Total unique controls</td>
<td>All unique technical controls tracked by this guide.</td>
<td>658</td>
</tr>
</tbody>
</table>

Procedural Generation

This chapter is automatically generated from the master_sctm.xlsx spreadsheet on this project’s GitHub. Do not edit it directly. If you’d like to change how this chapter is rendered, refer to the following:
AC-1 - Access Control Policy And Procedures

Requirement ACCESS CONTROL POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and b. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and 2. Access control procedures [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AC-1 What is the solution and how is it implemented?

Part a

Requirement ACCESS CONTROL POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role Organization
Status Inherited
Details Developed and maintained by the Organization. OCP framework administrators with the policy as published.
References SP 800-12; SP 800-100;

Part b

Requirement

2. Procedures to facilitate the implementation of the access control policy and associated access controls; and

Role Organization
Part c

Requirement

2. Reviews and updates the current: 1. Access control policy [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Developed and maintained by the Organization. OCP framework administrators with the policy as published.

References SP 800-12; SP 800-100;

Part d

Requirement

2. Access control procedures [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Developed and maintained by the Organization. OCP framework administrators with the policy as published.

References SP 800-12; SP 800-100;

AC-12 - Session Termination

Requirement SESSION TERMINATION Control: The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Control Summary Information

Role OpenShift Landlord

Status Planned

Origin OpenShift Landlord SSP
AC-12 What is the solution and how is it implemented?

Part a

Requirement  SESSION TERMINATION Control: The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

Role  OpenShift Landlord

Status  Planned

Details  Access to the OpenShift API endpoints is granted via token that can only be acquired by a user with an X.509 certificate who's DN is in the proper OU. The tokens expire at the organizationally defined interval.

AC-14 - Permitted Actions Without Identification Or Authentication

Requirement  PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control: The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Control Summary Information

Role  Organization, OpenShift Landlord

Status  Implemented

Origin  OpenShift Landlord SSP

AC-14 What is the solution and how is it implemented?

Part a

Requirement  PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION Control: The organization: a. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and

Role  Organization, OpenShift Landlord

Status  Implemented

Details  All actions (OpenShift user & admins) require prior authentication and authorization

Part b

Requirement

2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.
Role Organization, OpenShift Landlord
Status Implemented
Details See AC-14a

AC-17 - Remote Access

Requirement REMOTE ACCESS Control: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorizes remote access to the information system prior to allowing such connections.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AC-17 What is the solution and how is it implemented?

Part a

Requirement REMOTE ACCESS Control: The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

Role Organization
Status Inherited
Details Inherited from organizational policies.
References SP 800-46; SP 800-77; SP 800-113; SP 800-114; SP 800-121;

Part b

Requirement
2. Authorizes remote access to the information system prior to allowing such connections.

Role Organization
Status Inherited
Details All users must be authorized via organizational request which requires staff approval for access to the system.
References SP 800-46; SP 800-77; SP 800-113; SP 800-114; SP 800-121;
AC-18 - Wireless Access

Requirement WIRELESS ACCESS Control: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and b. Authorizes wireless access to the information system prior to allowing such connections.

Control Summary Information

Role OpenShift Landlord
Status Not implemented
Origin OpenShift Landlord SSP

AC-18 What is the solution and how is it implemented?

Part a

Requirement WIRELESS ACCESS Control: The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

Role OpenShift Landlord
Status Not implemented
Details Tailored out - there are no wireless components to the system.
References SP 800-48; SP 800-94; SP 800-97;

Part b

Requirement 2. Authorizes wireless access to the information system prior to allowing such connections.

Role OpenShift Landlord
Status Not implemented
Details See AC-18a
References SP 800-48; SP 800-94; SP 800-97;

AC-18(5) - Wireless Access | Antennas / Transmission Power Levels

Requirement WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.
Control Summary Information

Role  OpenShift Landlord
Status  Not implemented
Origin  OpenShift Landlord SSP

AC-18(5) What is the solution and how is it implemented?

Part a

Requirement  WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

Role  OpenShift Landlord
Status  Not implemented
Details  See AC-18a

AC-19 - Access Control For Mobile Devices

Requirement  ACCESS CONTROL FOR MOBILE DEVICES Control: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and b. Authorizes the connection of mobile devices to organizational information systems.

Control Summary Information

Role  OpenShift Landlord
Status  Not implemented
Origin  OpenShift Landlord SSP

AC-19 What is the solution and how is it implemented?

Part a

Requirement  ACCESS CONTROL FOR MOBILE DEVICES Control: The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and

Role  OpenShift Landlord
Status  Not implemented
Details  Tailored out - there are no Mobile components to the system.
References  OMB M-06-16; SP 800-114; SP 800-124; SP 800-164;
Part b

Requirement

2. Authorizes the connection of mobile devices to organizational information systems.

Role OpenShift Landlord

Status Not implemented

Details Reference AC-19a

References OMB M-06-16; SP 800-114; SP 800-124; SP 800-164;

AC-19(5) - Access Control For Mobile Devices | Full Device / Container-based Encryption

Requirement ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

Control Summary Information

Role OpenShift Landlord

Status Not implemented

Origin OpenShift Landlord SSP

AC-19(5) What is the solution and how is it implemented? Part a

Requirement ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

Role OpenShift Landlord

Status Not implemented

Details Reference AC-19a

AC-2 - Account Management

Requirement ACCOUNT MANAGEMENT Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types]; b. Assigns account managers for information system accounts; c. Establishes conditions for group and role membership; d. Specifies authorized users of the information system, group and role membership, and access
authorizations (i.e., privileges) and other attributes (as required) for each account; e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts; f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions]; g. Monitors the use of, information system accounts; h. Notifies account managers: 1. When accounts are no longer required; 2. When users are terminated or transferred; and 3. When individual information system usage or need-to-know changes; i. Authorizes access to the information system based on: 1. A valid access authorization; 2. Intended system usage; and 3. Other attributes as required by the organization or associated missions/business functions; j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

AC-2 What is the solution and how is it implemented?

Part a

Requirement ACCOUNT MANAGEMENT Control: The organization: a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

Role Organization

Status Inherited

Details Developed and maintained by the Organization. OCP framework administrators with the policy as published.

Part b

Requirement

2. Assigns account managers for information system accounts;

Role Organization

Status Inherited

Details Developed and maintained by the Organization. OCP framework administrators with the policy as published.

Part c

Requirement

3. Establishes conditions for group and role membership;

Role Organization
### Part d

**Requirement**

4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

**Role** Organization, OpenShift Landlord

**Status** Implemented

**Details** Users - delegated to enterprise Admins - user credentials deployed via Ansible Tower

### Part e

**Requirement**

5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

**Role** IaaS

**Status** Inherited

**Details** Inherited from IaaS user policy.

### Part f

**Requirement**

6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

**Role** IaaS

**Status** Inherited

**Details** Inherited from IaaS user policy.

### Part g

**Requirement**

7. Monitors the use of, information system accounts;

**Role** Organization, IaaS

**Status** Inherited

**Details** Inherited from organization desktop policy and IaaS user policy.
Part h

Requirement
8. Notifies account managers: 1. When accounts are no longer required;

Role Organization
Status Inherited
Details Inherited from organizational policy and user directory. OpenShift authenticates against X.509 certificates, and is configured to check the corporate OCSP responder.

Part i

Requirement
2. When users are terminated or transferred; and

Role Organization
Status Inherited
Details Inherited from organizational policy and user directory. OpenShift authenticates against X.509 certificates, and is configured to check the corporate OCSP responder.

Part j

Requirement
3. When individual information system usage or need-to-know changes;

Role Organization, OpenShift Landlord
Status Implemented
Details Access to OpenShift is controled by the user’s X.509 DN being in an Organizational Unit in the user directory. If the user no longer requires access, the organization removes the user’s DN from the OU. Cluster admin access is managed by SSH keys via Ansible Tower and can be easily removed from all systems when employees leave or when directed to do so by the COR.

Part k

Requirement
1. Authorizes access to the information system based on: 1. A valid access authorization;

Role Organization, OpenShift Landlord
Status Implemented
Details Inherited from organizational policy and user directory. OpenShift authenticates against X.509 certificates, and is configured to check the corporate OCSP responder.
Part I

Requirement
2. Intended system usage; and
Role Organization, OpenShift Landlord
Status Implemented
Details Inherited from organizational policy and user directory. OpenShift authenticates against X.509 certificates, and is configured to check the corporate OCSP responder.

Part m

Requirement
3. Other attributes as required by the organization or associated missions/business functions;
Role Organization, OpenShift Landlord
Status Implemented
Details Inherited from organizational policy and user directory. OpenShift authenticates against X.509 certificates, and is configured to check the corporate OCSP responder.

Part n

Requirement
10. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
Role Organization, OpenShift Landlord
Status Implemented
Details Users - inherited from to organization user directory Admins - continuous CM by Ansible Tower

Part o

Requirement
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
Role OpenShift Landlord
Status Not implemented
Details No shared credentials

AC-2(1) - Account Management | Automated System Account Management

Requirement ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT
The organization employs automated mechanisms to support the management of information system accounts.
Control Summary Information

**Role**  Organization, OpenShift Landlord

**Status**  Implemented

**Origin**  OpenShift Landlord SSP

**AC-2(1) What is the solution and how is it implemented?**

Part a

**Requirement**  ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT

The organization employs automated mechanisms to support the management of information system accounts.

**Role**  Organization, OpenShift Landlord

**Status**  Implemented

**Details**  Users - delegated to enterprise Admins - user credentials deployed via puppet/ansible

**AC-2(11) - Account Management | Usage Conditions**

**Requirement**  ACCOUNT MANAGEMENT | USAGE CONDITIONS

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

Control Summary Information

**Role**  Organization

**Status**  Inherited

**Origin**  Inherited from pre-existing ATO

**AC-2(11) What is the solution and how is it implemented?**

Part a

**Requirement**  ACCOUNT MANAGEMENT | USAGE CONDITIONS

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

**Role**  Organization

**Status**  Inherited

**Details**  Dependent on implementing organization.
AC-2(2) - Account Management | Removal Of Temporary / Emergency Accounts

**Requirement** ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

**Control Summary Information**

- **Role** OpenShift Landlord
- **Status** Not implemented
- **Origin** OpenShift Landlord SSP

AC-2(2) What is the solution and how is it implemented?

**Part a**

**Requirement** ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

- **Role** OpenShift Landlord
- **Status** Not implemented
- **Details** No emergency accounts

AC-2(3) - Account Management | Disable Inactive Accounts

**Requirement** ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

**Control Summary Information**

- **Role** Organization, OpenShift Landlord
- **Status** Implemented
- **Origin** OpenShift Landlord SSP

AC-2(3) What is the solution and how is it implemented?

**Part a**

**Requirement** ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

- **Role** Organization, OpenShift Landlord
- **Status** Implemented
Details  Users - delegated to enterprise Admins - not subject to automatic disabling, accounts which are no longer necessary will be detected during review detailed in AC-2j

AC-20 - Use Of External Information Systems

Requirement  USE OF EXTERNAL INFORMATION SYSTEMS Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and b. Process, store, or transmit organization-controlled information using external information systems.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from a pre-existing ATO

AC-20 What is the solution and how is it implemented?

Part a

Requirement  USE OF EXTERNAL INFORMATION SYSTEMS Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from external information systems; and

Role  Organization
Status  Inherited
Details  undefined
References  FIPS Pub 199;

Part b

Requirement

2. Process, store, or transmit organization-controlled information using external information systems.

Role  Organization
Status  Inherited
Details  undefined
References  FIPS Pub 199;
AC-21 - Information Sharing

**Requirement** INFORMATION SHARING Control: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and b. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Inherited from a pre-existing ATO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**AC-21 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION SHARING Control: The organization: a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>undefined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>undefined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**AC-22 - Publicly Accessible Content**

**Requirement** PUBLICLY ACCESSIBLE CONTENT Control: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and d. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.
AC-22 What is the solution and how is it implemented?

Part a

Requirement  PUBLICLY ACCESSIBLE CONTENT Control: The organization: a. Designates individuals authorized to post information onto a publicly accessible information system;

Role  Organization
Status  Inherited
Details  Not responsible

Part b

Requirement  
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

Role  Organization
Status  Inherited
Details  Not responsible

Part c

Requirement  
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and

Role  Organization
Status  Inherited
Details  Not responsible

Part d

Requirement  
4. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

Role  Organization
Status  Inherited
Details  Not responsible
AC-3 - Access Enforcement

**Requirement** ACCESS ENFORCEMENT Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

**Control Summary Information**

- **Role** Organization, OpenShift Landlord
- **Status** Implemented
- **Origin** OpenShift Landlord SSP

**AC-3 What is the solution and how is it implemented?**

**Part a**

**Requirement** ACCESS ENFORCEMENT Control: The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- **Role** Organization, OpenShift Landlord
- **Status** Implemented

- **Details** Users - Access control capabilities implemented through OpenShift tenant applications. Administrators - access control to virtual machines implemented via ssh with key deployment controlled via Ansible Tower.

AC-4 - Information Flow Enforcement

**Requirement** INFORMATION FLOW ENFORCEMENT Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

**Control Summary Information**

- **Role** OpenShift Landlord
- **Status** Implemented
- **Origin** OpenShift Landlord SSP

**AC-4 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION FLOW ENFORCEMENT Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].
Role OpenShift Landlord
Status Implemented
Details All OpenShift infrastructure resources (i.e., user database, message bus, Ansible Tower) are housed within a VPC which can only be externally accessed through a tightly controlled bastion host which will be configured to be compliant with organization specified controls.

References Web: ucdmo.gov;

AC-6(3) - Least Privilege | Network Access To Privileged Commands

Requirement LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AC-6(3) What is the solution and how is it implemented?

Part a

Requirement LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS The organization authorizes network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

Role Organization
Status Inherited
Details Dependent on implementing organization.

AC-7 - Unsuccessful Logon Attempts

Requirement UNSUCCESSFUL LOGON ATTEMPTS Control: The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.
Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

AC-7 What is the solution and how is it implemented?

Part a

Requirement UNSUCCESSFUL LOGON ATTEMPTS Control: The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and

Role OpenShift Landlord
Status Implemented
Details Logins are done via PKI certificates and/or SSH keys. Invalid logins consist of the user not being authorized to login to the target gear, system or console and result in a rejected connection attempt. All rejected attempts are logged for review and provided to the continuous monitoring branch for review.

Part b

Requirement

2. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

Role OpenShift Landlord
Status Implemented
Details See AC-7a

AC-8 - System Use Notification

Requirement SYSTEM USE NOTIFICATION Control: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for
such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system.

Control Summary Information

- **Role**: Organization, OpenShift Landlord
- **Status**: Implemented
- **Origin**: OpenShift Landlord SSP

AC-8 What is the solution and how is it implemented?

Part a

**Requirement** SYSTEM USE NOTIFICATION Control: The information system: a. Displays to users [Assignment: organization-defined system use notification message or banner] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system;

- **Role**: Organization, OpenShift Landlord
- **Status**: Implemented
- **Details**: For non-privileged access the user has already acknowledged the required banner upon login to the organization’s workstation. A non-privileged user cannot escalate privileges in the WebGUI context. For administrators or privileged access, only SSH login is supported and a banner will be presented in compliance with organizational policy.

Part b

**Requirement**

2. Information system usage may be monitored, recorded, and subject to audit;

- **Role**: Organization, OpenShift Landlord
- **Status**: Implemented
- **Details**: see AC-8a

Part c

**Requirement**

3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

- **Role**: Organization, OpenShift Landlord
- **Status**: Implemented
- **Details**: see AC-8a
Part d

Requirement

4. Use of the information system indicates consent to monitoring and recording;

Role  Organization, OpenShift Landlord
Status  Implemented
Details  see AC-8a

Part e

Requirement

2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

Role  Organization, OpenShift Landlord
Status  Implemented
Details  see AC-8a

Part f

Requirement

3. For publicly accessible systems: 1. Displays system use information [Assignment: organization-defined conditions], before granting further access;

Role  Organization, OpenShift Landlord
Status  Implemented
Details  see AC-8a

Part g

Requirement

2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and

Role  Organization, OpenShift Landlord
Status  Implemented
Details  see AC-8a

Part h

Requirement

3. Includes a description of the authorized uses of the system.

Role  Organization, OpenShift Landlord
Status  Implemented
Details see AC-8a

AP-1 - Authority To Collect

Requirement AUTHORITY TO COLLECT Control: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AP-1 What is the solution and how is it implemented?

Part a

Requirement AUTHORITY TO COLLECT Control: The organization determines and documents the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

Role Organization
Status Inherited
Details Inherited from organizational policies.
References The Privacy Act of 1974, 5 U.S.C. § 552a (e); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB Circular A-130, Appendix I;

AP-2 - Purpose Specification

Requirement PURPOSE SPECIFICATION Control: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
AP-2 What is the solution and how is it implemented?

Part a

Requirement PURPOSE SPECIFICATION Control: The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.

Role Organization

Status Inherited

Details Inherited from organizational policies.

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B); Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347);

AR-1 - Governance And Privacy Program

Requirement GOVERNANCE AND PRIVACY PROGRAM Control: The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; b. Monitors federal privacy laws and policy for changes that affect the privacy program; c. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program; d. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; e. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and f. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

AR-1 What is the solution and how is it implemented?

Part a

Requirement GOVERNANCE AND PRIVACY PROGRAM Control: The organization: a. Appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems;

Role Organization

Status Inherited
Part b

Requirement

2. Monitors federal privacy laws and policy for changes that affect the privacy program;

Role Organization

Status Inherited

Details Inherited from organizational policies.


Part c

Requirement

3. Allocates [Assignment: organization-defined allocation of budget and staffing] sufficient resources to implement and operate the organization-wide privacy program;

Role Organization

Status Inherited

Details Inherited from organizational policies.


Part d

Requirement

4. Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures;

Role Organization

Status Inherited

Details Inherited from organizational policies.

Part e

Requirement

5. Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and

Role Organization

Status Inherited

Details Inherited from organizational policies.


Part f

Requirement

6. Updates privacy plan, policies, and procedures [Assignment: organization-defined frequency, at least biennially].

Role Organization

Status Inherited

Details Inherited from organizational policies.


AR-2 - Privacy Impact And Risk Assessment

Requirement PRIVACY IMPACT AND RISK ASSESSMENT Control: The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO
AR-2 What is the solution and how is it implemented?

Part a

**Requirement** PRIVACY IMPACT AND RISK ASSESSMENT Control: The organization: a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational policies.


Part b

**Requirement**

2. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational policies.


AR-3 - Privacy Requirements For Contractors And Service Providers

**Requirement** PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS Control: The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.

**Control Summary Information**

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

AR-3 What is the solution and how is it implemented?
Part a

**Requirement** PRIVACY REQUIREMENTS FOR CONTRACTORS AND SERVICE PROVIDERS

Control: The organization: a. Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational policies.

**References** The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130;

Part b

**Requirement**

2. Includes privacy requirements in contracts and other acquisition-related documents.

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational policies.

**References** The Privacy Act of 1974, 5 U.S.C. § 552a(m); Federal Acquisition Regulation, 48 C.F.R. Part 24; OMB Circular A-130;

AR-4 - Privacy Monitoring And Auditing

**Requirement** PRIVACY MONITORING AND AUDITING Control: The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.

Control Summary Information

**Role** Organization, OpenShift Landlord

**Status** Implemented

**Origin** OpenShift Landlord SSP

AR-4 What is the solution and how is it implemented?

Part a

**Requirement** PRIVACY MONITORING AND AUDITING Control: The organization monitors and audits privacy controls and internal privacy policy [Assignment: organization-defined frequency] to ensure effective implementation.

**Role** Organization, OpenShift Landlord

**Status** Implemented
Details  Partly inherited; information system auditing satisfied by OpenSCAP scans and Ansible configuration/compliance management.


AR-5 - Privacy Awareness And Training

Requirement  PRIVACY AWARENESS AND TRAINING Control: The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; b. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and c. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].

Control Summary Information

Role  Organization, OpenShift Landlord
Status  Implemented
Origin  OpenShift Landlord SSP

AR-5 What is the solution and how is it implemented?

Part a

Requirement  PRIVACY AWARENESS AND TRAINING Control: The organization: a. Develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures;

Role  Organization, OpenShift Landlord
Status  Implemented
Details  Partly inherited; role based training provided by training template required prior to access.

References  The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

Part b

Requirement

2. Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually]; and

Role  Organization, OpenShift Landlord
Status  Implemented
Part c

Requirement

3. Ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements [Assignment: organization-defined frequency, at least annually].

Role Organization
Status Inherited
Details Inherited from organizational policies. Landlord can provide training template but the organization must provide acceptance and tracking methods.

References The Privacy Act of 1974, 5 U.S.C. § 552a(e); Section 208, E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

AR-6 - Privacy Reporting

Requirement PRIVACY REPORTING Control: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AR-6 What is the solution and how is it implemented?

Part a

Requirement PRIVACY REPORTING Control: The organization develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

Role Organization
Status Inherited
Details Inherited from organizational policies.

**AR-7 - Privacy-enhanced System Design And Development**

**Requirement** PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT Control: The organization designs information systems to support privacy by automating privacy controls.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>

**AR-7 What is the solution and how is it implemented?**

**Part a**

**Requirement** PRIVACY-ENHANCED SYSTEM DESIGN AND DEVELOPMENT Control: The organization designs information systems to support privacy by automating privacy controls.

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Details</td>
<td>We will implement related controls with OpenSCAP and Ansible.</td>
</tr>
<tr>
<td>References</td>
<td>The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10); Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22;</td>
</tr>
</tbody>
</table>

**AR-8 - Accounting Of Disclosures**

**Requirement** ACCOUNTING OF DISCLOSURES Control: The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made; b. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and c. Makes the accounting of disclosures available to the person named in the record upon request.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization, OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>
AR-8 What is the solution and how is it implemented?

Part a

Requirement ACCOUNTING OF DISCLOSURES Control: The organization: a. Keeps an accurate accounting of disclosures of information held in each system of records under its control, including:
   (1) Date, nature, and purpose of each disclosure of a record; and

Role Organization, OpenShift Landlord

Status Implemented

Details Partly inherited; fulfilled by OpenShift logging subsystem and the submission of those logs to organizationally required entities and organizational enterprise A&L services.

References The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k);

Part b

Requirement
   2. Name and address of the person or agency to which the disclosure was made;

Role Organization

Status Inherited

Details See AR-8a

References The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k);

Part c

Requirement
   2. Retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and

Role Organization

Status Inherited

Details See AR-8a

References The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k);

Part d

Requirement
   3. Makes the accounting of disclosures available to the person named in the record upon request.

Role Organization

Status Inherited

Details See AR-8a

References The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k);
AT-1 - Security Awareness And Training Policy And Procedures

Requirement SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES Control:
The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and 2. Security awareness and training procedures [Assignment: organization-defined frequency].

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

AT-1 What is the solution and how is it implemented?

Part a

Requirement SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES Control:
The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References SP 800-12; SP 800-16; SP 800-50; SP 800-100;

Part b

Requirement
2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References SP 800-12; SP 800-16; SP 800-50; SP 800-100;
Part c

Requirement
2. Reviews and updates the current: 1. Security awareness and training policy [Assignment: organization-defined frequency]; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References SP 800-12; SP 800-16; SP 800-50; SP 800-100;

Part d

Requirement
2. Security awareness and training procedures [Assignment: organization-defined frequency].

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References SP 800-12; SP 800-16; SP 800-50; SP 800-100;

AT-2 - Security Awareness Training

Requirement SECURITY AWARENESS TRAINING Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

AT-2 What is the solution and how is it implemented?

Part a

Requirement SECURITY AWARENESS TRAINING Control: The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users;
Part b

Requirement
2. When required by information system changes; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); EO 13587; SP 800-50;

Part c

Requirement
3. [Assignment: organization-defined frequency] thereafter.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References C.F.R. Part 5 Subpart C (5 C.F.R. 930.301); EO 13587; SP 800-50;

AT-3 - Role-based Security Training

Requirement ROLE-BASED SECURITY TRAINING Control: The organization provides role-based
security training to personnel with assigned security roles and responsibilities: a. Before authorizing
access to the information system or performing assigned duties; b. When required by information
system changes; and c. [Assignment: organization-defined frequency] thereafter.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

AT-3 What is the solution and how is it implemented?

Part a

Requirement ROLE-BASED SECURITY TRAINING Control: The organization provides role-based
security training to personnel with assigned security roles and responsibilities: a. Before authorizing
access to the information system or performing assigned duties;

Role OpenShift Landlord
Status Planned
Part b

Requirement

2. When required by information system changes; and

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

References C.F.R. Part Subpart C (C.F.R. 930.301); SP 800-16; SP 800-50;

Part c

Requirement

3. [Assignment: organization-defined frequency] thereafter.

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

References C.F.R. Part Subpart C (C.F.R. 930.301); SP 800-16; SP 800-50;

AT-4 - Security Training Records

Requirement SECURITY TRAINING RECORDS Control: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [Assignment: organization-defined time period].

Control Summary Information

Role OpenShift Landlord

Status Planned

Origin OpenShift Landlord SSP

AT-4 What is the solution and how is it implemented?

Part a

Requirement SECURITY TRAINING RECORDS Control: The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

Role OpenShift Landlord
Part b

Requirement

2. Retains individual training records for [Assignment: organization-defined time period].

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

AU-1 - Audit And Accountability Policy And Procedures

Requirement AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and 2. Audit and accountability procedures [Assignment: organization-defined frequency].

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

AU-1 What is the solution and how is it implemented?

Part a

Requirement AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role Organization

Status Inherited

Details Inherited from organizational audit policies.

References SP 800-12; SP 800-100;
Part b

Requirement

2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and

Role Organization
Status Inherited
Details See AU-1a
References SP 800-12; SP 800-100;

Part c

Requirement

2. Reviews and updates the current: 1. Audit and accountability policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details See AU-1a
References SP 800-12; SP 800-100;

Part d

Requirement

2. Audit and accountability procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details See AU-1a
References SP 800-12; SP 800-100;

AU-11 - Audit Record Retention

Requirement AUDIT RECORD RETENTION Control: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
AU-11 What is the solution and how is it implemented?

Part a

Requirement AUDIT RECORD RETENTION Control: The organization retains audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Role Organization

Status Inherited

Details Inherited from organizational A&L service

AU-12 - Audit Generation

Requirement AUDIT GENERATION Control: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP

AU-12 What is the solution and how is it implemented?

Part a

Requirement AUDIT GENERATION Control: The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components];

Role OpenShift Landlord

Status Implemented

Details Generation of audit records for events described in AU-2 is handled by two separate subsystems. Audit records related to administrative actions are generated by auditd and related system tools while generation of user audit events is performed by the OpenShift software.

Part b

Requirement

2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
Part c

Requirement

3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

Role OpenShift Landlord
Status Implemented
Details See response to AU-3

AU-2 - Audit Events

Requirement AUDIT EVENTS Control: The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines that the following events are to be audited within the information system: [Assignment: organization-defined audited events (the subset of the auditable events defined in AU-2 a.) along with the frequency of (or situation requiring) auditing for each identified event].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

AU-2 What is the solution and how is it implemented?

Part a

Requirement AUDIT EVENTS Control: The organization: a. Determines that the information system is capable of auditing the following events: [Assignment: organization-defined auditable events];

Role Organization
Status Inherited
Details Auditable events are split into two compartments based on their source: (1) administrative events performed by system administrators and (2) user events performed by application developers.

A wide variety of administrative events are captured including user logins via ssh and all actions performed as a super-user.
User events include actions taken through the OpenShift API and audited events include: the cre-
ation, update and destruction of applications and component gears.

References  SP 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov;

Part b

Requirement

2. Coordinates the security audit function with other organizational entities requiring audit-related
information to enhance mutual support and to help guide the selection of auditable events;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  SP 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov;

Part c

Requirement

3. Provides a rationale for why the auditable events are deemed to be adequate to support after-
the-fact investigations of security incidents; and

Role  Organization

Status  Inherited

Details  Auditing of administrative events is designed to capture all actions taken by superusers on the
systems housing the OSO environment. This is intended to capture any attempt to modify the oper-
ating environment for hosted applications.

Likewise auditing of application developers is designed to capture all “change” events committed
through the OSO API.

References  SP 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov;

Part d

Requirement

4. Determines that the following events are to be audited within the information system: [Assign-
ment: organization-defined audited events (the subset of the auditable events defined in AU-2
a.) along with the frequency of (or situation requiring) auditing for each identified event].

Role  Organization

Status  Inherited

Details  Auditable events documented in section AU-2a are captured in near-real-time and shared with
appropriate stakeholders.

References  SP 800-92; Web: csrc.nist.gov/pcig/cig.html, idmanagement.gov;
AU-3 - Content Of Audit Records

Requirement CONTENT OF AUDIT RECORDS Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

AU-3 What is the solution and how is it implemented?

Part a

Requirement CONTENT OF AUDIT RECORDS Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Role OpenShift Landlord
Status Implemented
Details Audit records collected for both administrative and user events follow standard, accepted formats.


In the case of user events the data formats and standards provided by relevant stakeholders are followed.

AU-3(2) - Content Of Audit Records | Centralized Management Of Planned Audit Record Content

Requirement CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP
AU-3(2) What is the solution and how is it implemented?

Part a

Requirement CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT The information system provides centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined information system components].

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

AU-4 - Audit Storage Capacity

Requirement AUDIT STORAGE CAPACITY Control: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP

AU-4 What is the solution and how is it implemented?

Part a

Requirement AUDIT STORAGE CAPACITY Control: The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

Role OpenShift Landlord

Status Implemented

Details Implemented by auditing subsystem and stored on system storage for the organizationally mandated length of time.

AU-5 - Response To Audit Processing Failures

Requirement RESPONSE TO AUDIT PROCESSING FAILURES Control: The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>

AU-5 What is the solution and how is it implemented?

Part a

**Requirement**  RESPONSE TO AUDIT PROCESSING FAILURES Control: The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>NEED TO ADDRESS</td>
</tr>
</tbody>
</table>

Part b

**Requirement**

2. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Details</td>
<td>The system will archive the current log entries to alternate storage to create adequate storage for current logs.</td>
</tr>
</tbody>
</table>

AU-5(2) - Response To Audit Processing Failures | Real-time Alerts

**Requirement**  RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>
AU-5(2) What is the solution and how is it implemented?

Part a

Requirement  RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS The information system provides an alert in [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].

Role  OpenShift Landlord
Status  Planned
Details  NEED TO ADDRESS

AU-6 - Audit Review, Analysis, And Reporting

Requirement  AUDIT REVIEW, ANALYSIS, AND REPORTING Control: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and b. Reports findings to [Assignment: organization-defined personnel or roles].

Control Summary Information

Role  OpenShift Landlord
Status  Planned
Origin  OpenShift Landlord SSP

AU-6 What is the solution and how is it implemented?

Part a

Requirement  AUDIT REVIEW, ANALYSIS, AND REPORTING Control: The organization: a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and

Role  OpenShift Landlord
Status  Planned
Details  NEED TO ADDRESS

Part b

Requirement

2. Reports findings to [Assignment: organization-defined personnel or roles].

Role  OpenShift Landlord
Status  Planned
Details  NEED TO ADDRESS
**AU-6(5) - Audit Review, Analysis, And Reporting | Integration / Scanning And Monitoring Capabilities**

**Requirement** AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

**Control Summary Information**

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Origin**: OpenShift Landlord SSP

**AU-6(5) What is the solution and how is it implemented?**

**Part a**

**Requirement** AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES The organization integrates analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Details**: NEED TO ADDRESS

**AU-6(6) - Audit Review, Analysis, And Reporting | Correlation With Physical Monitoring**

**Requirement** AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

**Control Summary Information**

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Origin**: OpenShift Landlord SSP
AU-6(6) What is the solution and how is it implemented?

Part a

Requirement AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

AU-7 - Audit Reduction And Report Generation

Requirement AUDIT REDUCTION AND REPORT GENERATION Control: The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

Role OpenShift Landlord

Status Planned

Origin OpenShift Landlord SSP

AU-7 What is the solution and how is it implemented?

Part a

Requirement AUDIT REDUCTION AND REPORT GENERATION Control: The information system provides an audit reduction and report generation capability that: a. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

Part b

Requirement

2. Does not alter the original content or time ordering of audit records.

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS
AU-7(1) - Audit Reduction And Report Generation | Automatic Processing

**Requirement**  
AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

**Control Summary Information**

- **Role**: OpenShift Landlord  
- **Status**: Planned  
- **Origin**: OpenShift Landlord SSP

**AU-7(1) What is the solution and how is it implemented?**

**Part a**

**Requirement**  
AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING
The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

- **Role**: OpenShift Landlord  
- **Status**: Planned  
- **Details**: NEED TO ADDRESS

AU-8 - Time Stamps

**Requirement**  
TIME STAMPS Control: The information system: a. Uses internal system clocks to generate time stamps for audit records; and b. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

**Control Summary Information**

- **Role**: OpenShift Landlord  
- **Status**: Implemented  
- **Origin**: OpenShift Landlord SSP

**AU-8 What is the solution and how is it implemented?**

**Part a**

**Requirement**  
TIME STAMPS Control: The information system: a. Uses internal system clocks to generate time stamps for audit records; and
Role: OpenShift Landlord
Status: Implemented
Details: Both administrative and user audit events are timestamped based on the internal clock of the machine from which they were generated.

Part b

Requirement
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: organization-defined granularity of time measurement].

Role: OpenShift Landlord
Status: Implemented
Details: Timestamps are accurate to the millisecond and time zone information is recorded to support conversion to UTC/GMT.

AU-9 - Protection Of Audit Information

Requirement: PROTECTION OF AUDIT INFORMATION Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Control Summary Information

Role: OpenShift Landlord
Status: Planned
Origin: OpenShift Landlord SSP

AU-9 What is the solution and how is it implemented?

Part a

Requirement: PROTECTION OF AUDIT INFORMATION Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Role: OpenShift Landlord
Status: Planned
Details: NEED TO ADDRESS

AU-9(2) - Protection Of Audit Information | Audit Backup On Separate Physical Systems / Components

Requirement: PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS The information system backs up audit records [Assignment:
organization-defined frequency] onto a physically different system or system component than the system or component being audited.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

AU-9(2) What is the solution and how is it implemented?

Part a

Requirement PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS The information system backs up audit records [Assignment: organization-defined frequency] onto a physically different system or system component than the system or component being audited.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Implemented</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

AU-9(3) - Protection Of Audit Information | Cryptographic Protection

Requirement PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>

AU-9(3) What is the solution and how is it implemented?

Part a

Requirement PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>NEED TO ADDRESS</td>
</tr>
</tbody>
</table>
CA-1 - Security Assessment And Authorization Policy And Procedures

Requirement  SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
Control:  The organization:  a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and b. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and 2. Security assessment and authorization procedures [Assignment: organization-defined frequency].

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Inherited from pre-existing ATO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CA-1 What is the solution and how is it implemented?

Part a

Requirement  SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES
Control:  The organization:  a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Inherited from organizational IA policy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References  SP 800-12; SP 800-37; SP 800-53A; SP 800-100;

Part b

Requirement
2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>Inherited from organizational IA policy.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References  SP 800-12; SP 800-37; SP 800-53A; SP 800-100;
Part c

Requirement

2. Reviews and updates the current: 1. Security assessment and authorization policy [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Inherited from organizational IA policy.

References SP 800-12; SP 800-37; SP 800-53A; SP 800-100;

Part d

Requirement

2. Security assessment and authorization procedures [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Inherited from organizational IA policy.

References SP 800-12; SP 800-37; SP 800-53A; SP 800-100;

CA-2 - Security Assessments

Requirement SECURITY ASSESSMENTS Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

CA-2 What is the solution and how is it implemented?
Part a

**Requirement** SECURITY ASSESSMENTS Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment;

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational IA policy.

**References** EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;

Part b

**Requirement**

2. Assessment procedures to be used to determine security control effectiveness; and

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational IA policy.

**References** EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;

Part c

**Requirement**

3. Assessment environment, assessment team, and assessment roles and responsibilities;

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational IA policy.

**References** EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;

Part d

**Requirement**

2. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

**Role** Organization

**Status** Inherited

**Details** Inherited from organizational IA policy.

**References** EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;
Part e

Requirement

3. Produces a security assessment report that documents the results of the assessment; and

Role Organization

Status Inherited

Details Inherited from organizational IA policy.

References EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;

Part f

Requirement

4. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles].

Role Organization

Status Inherited

Details Inherited from organizational IA policy.

References EO 13587; FIPS Pub 199; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137;

**CA-2(2) - Security Assessments | Specialized Assessments**

Requirement SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

**CA-2(2) What is the solution and how is it implemented?**

Part a

Requirement SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

Role Organization
Status Inherited

Details The framework will comply with the recommendations of the assessment by addressing the PoAMs created as a result of the assessment.

CA-3 - System Interconnections

Requirement SYSTEM INTERCONNECTIONS Control: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CA-3 What is the solution and how is it implemented?

Part a

Requirement SYSTEM INTERCONNECTIONS Control: The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;

Role OpenShift Landlord
Status Implemented

Details Interconnection Security Agreements (ISAs) are documented in the System Security Plan (SSP) for the OpenShift system and are updated as required or as changes, additions or deletions occur to the ISAs.

References FIPS Pub 199; SP 800-47;

Part b

Requirement 2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and

Role OpenShift Landlord
Status Implemented
Details See CA-3a
References FIPS Pub 199; SP 800-47;
Part c

Requirement
3. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].

Role OpenShift Landlord
Status Implemented
Details See CA-3a
References FIPS Pub 199; SP 800-47;

CA-5 - Plan Of Action And Milestones

Requirement PLAN OF ACTION AND MILESTONES Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

CA-5 What is the solution and how is it implemented?

Part a

Requirement PLAN OF ACTION AND MILESTONES Control: The organization: a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

Role OpenShift Landlord
Status Planned
Details Upon delivery of the report from the security assessor(s), a POA&M document will be created and each item will be addressed with the: a) deficiency b) party responsible for remediation c) the estimated time to remediation and d) the current progress/status of the remediation.

References OMB M-02-01; SP 800-37;
Part b

Requirement
2. Updates existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Role OpenShift Landlord
Status Planned
Details The POAMs (as described in the response to CA-5a) will be updated as progress is made or on/before predetermined milestone.
References OMB M-02-01; SP 800-37;

CA-6 - Security Authorization

Requirement SECURITY AUTHORIZATION Control: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CA-6 What is the solution and how is it implemented?

Part a

Requirement SECURITY AUTHORIZATION Control: The organization: a. Assigns a senior-level executive or manager as the authorizing official for the information system;

Role Organization
Status Inherited
Details Inherited from organizational IA policy.
References OMB Circular A-130; OMB M-11-33; SP 800-37; SP 800-137;

Part b

Requirement
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

Role Organization
Status Inherited
Part c

Requirement

3. Updates the security authorization [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Inherited from organizational IA policy.

References OMB Circular A-130; OMB M-11-33; SP 800-37; SP 800-137;

CA-7 - Continuous Monitoring

Requirement CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored; b. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Control Summary Information

Role OpenShift Landlord

Status Planned

Origin OpenShift Landlord SSP

CA-7 What is the solution and how is it implemented?

Part a

Requirement CONTINUOUS MONITORING Control: The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes: a. Establishment of [Assignment: organization-defined metrics] to be monitored;

Role OpenShift Landlord

Status Planned

Details NEED TO ADDRESS

References OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;
Part b

Requirement

2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;

Part c

Requirement

3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;

Part d

Requirement

4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;

Part e

Requirement

5. Correlation and analysis of security-related information generated by assessments and monitoring;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;
Part f

Requirement

6. Response actions to address results of the analysis of security-related information; and

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;

Part g

Requirement

7. Reporting the security status of organization and the information system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  OMB M-11-33; SP 800-37; SP 800-39; SP 800-53A; SP 800-115; SP 800-137; US-CERT Technical Cyber Security Alerts; DoD Information Assurance Vulnerability Alerts;

CA-7(1) - Continuous Monitoring | Independent Assessment

Requirement  CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

Control Summary Information

Role  OpenShift Landlord

Status  Planned

Origin  OpenShift Landlord SSP

CA-7(1) What is the solution and how is it implemented?

Part a

Requirement  CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.
CA-8 - Penetration Testing

Requirement PENETRATION TESTING Control: The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CA-8 What is the solution and how is it implemented?

Part a

Requirement PENETRATION TESTING Control: The organization conducts penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined information systems or system components].

Role Organization
Status Inherited
Details Inherited from organizational IA team

CA-9 - Internal System Connections

Requirement INTERNAL SYSTEM CONNECTIONS Control: The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and b. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP
CA-9 What is the solution and how is it implemented?

Part a

**Requirement**  INTERNAL SYSTEM CONNECTIONS Control: The organization: a. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and

**Role**  OpenShift Landlord

**Status**  Planned

**Details**  NEED TO ADDRESS

Part b

**Requirement**

2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

**Role**  OpenShift Landlord

**Status**  Planned

**Details**  NEED TO ADDRESS

CM-1 - Configuration Management Policy And Procedures

**Requirement**  CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and b. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and 2. Configuration management procedures [Assignment: organization-defined frequency].

**Control Summary Information**

**Role**  OpenShift Landlord

**Status**  Planned

**Origin**  OpenShift Landlord SSP

CM-1 What is the solution and how is it implemented?

Part a

**Requirement**  CONFIGURATION MANAGEMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A configuration management policy that addresses purpose, scope, roles, respon-
sibilities, management commitment, coordination among organizational entities, and compliance; and

**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS  
**References** SP 800-12; SP 800-100;

**Part b**

**Requirement**

2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and

**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS  
**References** SP 800-12; SP 800-100;

**Part c**

**Requirement**

2. Reviews and updates the current: 1. Configuration management policy [Assignment: organization-defined frequency]; and

**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS  
**References** SP 800-12; SP 800-100;

**Part d**

**Requirement**

2. Configuration management procedures [Assignment: organization-defined frequency].

**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS  
**References** SP 800-12; SP 800-100;
CM-10 - Software Usage Restrictions

**Requirement** SOFTWARE USAGE RESTRICTIONS Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CM-10 What is the solution and how is it implemented?**

**Part a**

**Requirement** SOFTWARE USAGE RESTRICTIONS Control: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>undefined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
<th>Status</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>undefined</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Part c**

**Requirement**

3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
<th>Status</th>
<th>Not implemented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details</td>
<td>OCP does not user peer-to-peer file-sharing technology</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CM-11 - User-installed Software


Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CM-11 What is the solution and how is it implemented?

Part a


Role Organization
Status Inherited
Details Dependent on implementing organization.

Part b

Requirement

2. Enforces software installation policies through [Assignment: organization-defined methods]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part c

Requirement

3. Monitors policy compliance at [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
CM-2 - Baseline Configuration

Requirement BASELINE CONFIGURATION Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-2 What is the solution and how is it implemented?

Part a

Requirement BASELINE CONFIGURATION Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Role OpenShift Landlord
Status Implemented
Details Configuration management enforced through Ansible playbooks.
References SP 800-128;

CM-2(2) - Baseline Configuration | Automation Support For Accuracy / Currency

Requirement BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-2(2) What is the solution and how is it implemented?

Part a

Requirement BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Role OpenShift Landlord
CM-2(3) - Baseline Configuration | Retention Of Previous Configurations

**Requirement** BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS
The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.

**Control Summary Information**

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Origin**: OpenShift Landlord SSP

**CM-2(3) What is the solution and how is it implemented?**

**Part a**

- **Requirement** BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS
  The organization retains [Assignment: organization-defined previous versions of baseline configurations of the information system] to support rollback.
  
  - **Role**: OpenShift Landlord
  - **Status**: Implemented
  - **Details**: Ansible playbooks are revision controlled through Git.

CM-2(7) - Baseline Configuration | Configure Systems, Components, Or Devices For High-risk Areas

**Requirement** BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS
The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and (b) Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO
CM-2(7) What is the solution and how is it implemented?

Part a

Requirement BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS The organization: (a) Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and

Role Organization

Status Inherited

Details Inherited from organizational policy.

Part b

Requirement

2. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

Role Organization

Status Inherited

Details See CM-2(7)

CM-3(1) - Configuration Change Control | Automated Document / Notification / Prohibition Of Changes

Requirement CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval; (c) Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period]; (d) Prohibit changes to the information system until designated approvals are received; (e) Document all changes to the information system; and (f) Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP
CM-3(1) What is the solution and how is it implemented?

Part a

Requirement CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES The organization employs automated mechanisms to: (a) Document proposed changes to the information system;

Role OpenShift Landlord

Status Implemented

Details Proposed changes to be submitted via the organization’s CRM tool.

Part b

Requirement

2. Notify [Assignment: organized-defined approval authorities] of proposed changes to the information system and request change approval;

Role OpenShift Landlord

Status Implemented

Details See CM-3(1)a

Part c

Requirement

3. Highlight proposed changes to the information system that have not been approved or disapproved by [Assignment: organization-defined time period];

Role OpenShift Landlord

Status Implemented

Details See CM-3(1)a

Part d

Requirement

4. Prohibit changes to the information system until designated approvals are received;

Role OpenShift Landlord

Status Implemented

Details By policy and practice, administrators will not implement proposed changes without organizational approval.

Part e

Requirement

5. Document all changes to the information system; and
Part f

Requirement

6. Notify [Assignment: organization-defined personnel] when approved changes to the information system are completed.

Role OpenShift Landlord
Status Implemented
Details See CM-3(1)a

CM-3(2) - Configuration Change Control | Test / Validate / Document Changes

Requirement CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-3(2) What is the solution and how is it implemented?

Part a

Requirement CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Role OpenShift Landlord
Status Implemented
Details See CM-3b

CM-4 - Security Impact Analysis

Requirement SECURITY IMPACT ANALYSIS Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-4 What is the solution and how is it implemented?

Part a

Requirement SECURITY IMPACT ANALYSIS Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
Role OpenShift Landlord
Status Implemented
Details See CM-3(1)a
References SP 800-128;

CM-5(3) - Access Restrictions For Change | Signed Components

Requirement ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

Control Summary Information

Role IaaS
Status Inherited
Origin Inherited from pre-existing ATO

CM-5(3) What is the solution and how is it implemented?

Part a

Requirement ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
Role IaaS
Status Inherited
Details Inherited from IaaS - we are unable to impact lower level IaaS systems.
CM-6 - Configuration Settings

Requirement CONFIGURATION SETTINGS Control: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Control Summary Information

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Origin**: OpenShift Landlord SSP

CM-6 What is the solution and how is it implemented?

Part a

Requirement CONFIGURATION SETTINGS Control: The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Details**: Ansible and OpenSCAP enforce continuous security control compliance and auditing.
- **References**: OMB M-07-11; OMB M-07-18; OMB M-08-22; SP 800-70; SP 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov;

Part b

Requirement

2. Implements the configuration settings;

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Details**: See CM-6a
- **References**: OMB M-07-11; OMB M-07-18; OMB M-08-22; SP 800-70; SP 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov;
Part c

Requirement

3. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and

Role OpenShift Landlord

Status Implemented

Details See CM-3(1)a

References OMB M-07-11; OMB M-07-18; OMB M-08-22; SP 800-70; SP 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov;

Part d

Requirement

4. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Role OpenShift Landlord

Status Implemented

Details See CM-3c

References OMB M-07-11; OMB M-07-18; OMB M-08-22; SP 800-70; SP 800-128; Web: nvd.nist.gov, checklists.nist.gov, www.nsa.gov;

CM-6(2) - Configuration Settings | Respond To Unauthorized Changes

Requirement CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP

CM-6(2) What is the solution and how is it implemented?

Part a

Requirement CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].

Role OpenShift Landlord
OpenShift Compliance Guide, Release 1.0 beta

Status Implemented
Details Ansible Tower with email notification to the administrator users.

CM-7 - Least Functionality

Requirement LEAST FUNCTIONALITY Control: The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-7 What is the solution and how is it implemented?

Part a

Requirement LEAST FUNCTIONALITY Control: The organization: a. Configures the information system to provide only essential capabilities; and

Role OpenShift Landlord
Status Implemented
Details Dependent on the individual deployment / project / scope of the project.
References DoD Instruction 8551.01;

Part b

Requirement

2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services].

Role OpenShift Landlord
Status Implemented
Details OpenShift infrastructure components communicate with each other using ports, which are communication endpoints that are identifiable for specific processes or services. Ensure the following ports required by OpenShift are open between hosts, for example if you have a firewall in your environment. Some ports are optional depending on your configuration and usage.

Node to Node - 4789 - Required for SDN communication between pods on separate hosts.
Nodes to Master - 53 - Required for SDN communication between pods on separate hosts. - 4789 - Required for SDN communication between pods on separate hosts. - 443 or 8443 - Required for
node hosts to communicate to the master API, for the node hosts to post back status, to receive tasks, and so on.

Master to Node - 4789 - Required for SDN communication between pods on separate hosts. - 10250 - The master proxies to node hosts via the Kubelet for oc commands.

Master to Master - 53 - Provides DNS services. - 2379 - Used for standalone etcd (clustered) to accept changes in state. - 2380 - etcd requires this port be open between masters for leader election and peering connections when using standalone etcd (clustered). - 4001 - Used for embedded etcd (non-clustered) to accept changes in state. - 4789 - Required for SDN communication between pods on separate hosts.

External to Master - 443 or 8443 - Required for node hosts to communicate to the master API, for node hosts to post back status, to receive tasks, and so on.

IaaS Deployments - 22 - Required for SSH by the installer or system administrator. - 53 - For SkyDNS use. Only required to be internally open on master hosts. - 80 or 443 - For HTTP/HTTPS use for the router. Required to be externally open on node hosts, especially on nodes running the router. - 1936 - For router statistics use. Required to be open when running the template router to access statistics, and can be open externally or internally to connections depending on if you want the statistics to be expressed publicly. - 4001 - For embedded etcd (non-clustered) use. Only required to be internally open on the master host. 4001 is for server-client connections. - 2379 and 2380 - For standalone etcd use. Only required to be internally open on the master host. 2379 is for server-client connections. 2380 is for server-server connections, and is only required if you have clustered etcd. - 4789 - For VxLAN use (OpenShift SDN). Required only internally on node hosts. - 8443 - For use by the OpenShift web console, shared with the API server. - 10250 - For use by the Kubelet. Required to be externally open on nodes. - 24224 - For use by Fluentd. Required to be open on master hosts for internal connections to node hosts.

References DoD Instruction 8551.01;

CM-7(4) - Least Functionality | Unauthorized Software / Blacklisting

Requirement LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING The organization: (a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system]; (b) Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and (c) Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CM-7(4) What is the solution and how is it implemented?

Part a

Requirement LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING The organization: (a) Identifies [Assignment: organization-defined software programs not authorized to execute on the information system];
Part b

Requirement

2. Employs an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system; and

Role Organization
Status Inherited
Details undefined

Part c

Requirement

3. Reviews and updates the list of unauthorized software programs [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details undefined

CM-8 - Information System Component Inventory

Requirement INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system; 2. Includes all components within the authorization boundary of the information system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and b. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP
CM-8 What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM COMPONENT INVENTORY Control: The organization: a. Develops and documents an inventory of information system components that: 1. Accurately reflects the current information system;

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-128;

Part b

Requirement

2. Includes all components within the authorization boundary of the information system;

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-128;

Part c

Requirement

3. Is at the level of granularity deemed necessary for tracking and reporting; and

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-128;

Part d

Requirement

4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-128;
Part e

Requirement

2. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Role OpenShift Landlord

Status Implemented

Details undefined

References SP 800-128;

CM-8(1) - Information System Component Inventory | Updates During Installations / Removals

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP

CM-8(1) What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Role OpenShift Landlord

Status Implemented

Details undefined

CM-8(4) - Information System Component Inventory | Accountability Information

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.
Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

CM-8(4) What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.

Role OpenShift Tenant
Status Planned
Details Specified in the individual project / program’s System Security Plan.

CM-8(5) - Information System Component Inventory | No Duplicate Accounting Of Components

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

CM-8(5) What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

Role OpenShift Landlord
Status Implemented
Details undefined
CP-1 - Contingency Planning Policy And Procedures

Requirement CONTINGENCY PLANNING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and b. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and 2. Contingency planning procedures [Assignment: organization-defined frequency].

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

CP-1 What is the solution and how is it implemented?

Part a

Requirement CONTINGENCY PLANNING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>Federal Continuity Directive 1; SP 800-12; SP 800-34; SP 800-100;</td>
</tr>
</tbody>
</table>

Part b

Requirement

2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>Federal Continuity Directive 1; SP 800-12; SP 800-34; SP 800-100;</td>
</tr>
</tbody>
</table>

Part c

Requirement
2. Reviews and updates the current: 1. Contingency planning policy [Assignment: organization-defined frequency]; and
   
   **Role** Organization
   **Status** Inherited
   **Details** Dependent on implementing organization.
   **References** Federal Continuity Directive 1; SP 800-12; SP 800-34; SP 800-100;

**Part d**

**Requirement**

2. Contingency planning procedures [Assignment: organization-defined frequency].

   **Role** Organization
   **Status** Inherited
   **Details** Dependent on implementing organization.
   **References** Federal Continuity Directive 1; SP 800-12; SP 800-34; SP 800-100;

**CP-10 - Information System Recovery And Reconstitution**

**Requirement** INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

**Control Summary Information**

   **Role** Organization
   **Status** Implemented
   **Origin** Inherited from pre-existing ATO

**CP-10 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION SYSTEM RECOVERY AND RECONSTITUTION Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

   **Role** Organization
   **Status** Implemented
   **Details** Inherited from the organization’s enterprise backup service
   **References** Federal Continuity Directive 1; SP 800-34;
CP-10(2) - Information System Recovery And Reconstitution | Transaction Recovery

**Requirement** INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY The information system implements transaction recovery for systems that are transaction-based.

Control Summary Information

- **Role:** OpenShift Tenant
- **Status:** Planned
- **Origin:** Tenant SSP

CP-10(2) What is the solution and how is it implemented?

**Part a**

**Requirement** INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY The information system implements transaction recovery for systems that are transaction-based.

- **Role:** OpenShift Tenant
- **Status:** Planned
- **Details:** undefined

CP-10(4) - Information System Recovery And Reconstitution | Restore Within Time Period

**Requirement** INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD The organization provides the capability to restore information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Control Summary Information

- **Role:** Organization
- **Status:** Inherited
- **Origin:** Inherited from pre-existing ATO
CP-10(4) What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD The organization provides the capability to restore information system components within [Assignment: organization-defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Role Organization

Status Inherited

Details undefined

CP-2 - Contingency Plan

Requirement CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

CP-2 What is the solution and how is it implemented?

Part a

Requirement CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements;

Role Organization
Part b

Requirement

2. Provides recovery objectives, restoration priorities, and metrics;

Role Organization

Status Inherited

Details undefined

References Federal Continuity Directive 1; SP 800-34;

Part c

Requirement

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

Role Organization

Status Inherited

Details undefined

References Federal Continuity Directive 1; SP 800-34;

Part d

Requirement

4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

Role Organization

Status Inherited

Details undefined

References Federal Continuity Directive 1; SP 800-34;

Part e

Requirement

5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and

Role Organization

Status Inherited

Details undefined
Part f

Requirement

6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

Role  Organization
Status  Inherited
Details  undefined
References  Federal Continuity Directive 1; SP 800-34;

Part g

Requirement

2. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];

Role  Organization
Status  Inherited
Details  undefined
References  Federal Continuity Directive 1; SP 800-34;

Part h

Requirement

3. Coordinates contingency planning activities with incident handling activities;

Role  Organization
Status  Inherited
Details  undefined
References  Federal Continuity Directive 1; SP 800-34;

Part i

Requirement

4. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];

Role  Organization
Status  Inherited
Details  undefined
References  Federal Continuity Directive 1; SP 800-34;
Part j

Requirement

5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-34;

Part k

Requirement

6. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-34;

Part l

Requirement

7. Protects the contingency plan from unauthorized disclosure and modification.

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-34;

CP-2(1) - Contingency Plan | Coordinate With Related Plans

Requirement CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan development with organizational elements responsible for related plans.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
CP-2(1) What is the solution and how is it implemented?

Part a

**Requirement** CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan development with organizational elements responsible for related plans.

**Role** Organization

**Status** Inherited

**Details** undefined

CP-2(2) - Contingency Plan | Capacity Planning

**Requirement** CONTINGENCY PLAN | CAPACITY PLANNING The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

CP-2(2) What is the solution and how is it implemented?

Part a

**Requirement** CONTINGENCY PLAN | CAPACITY PLANNING The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

**Role** Organization

**Status** Inherited

**Details** undefined

CP-2(3) - Contingency Plan | Resume Essential Missions / Business Functions

**Requirement** CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.
Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

CP-2(3) What is the solution and how is it implemented?

Part a

Requirement  CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS
The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

Role  Organization
Status  Inherited
Details  undefined

CP-2(4) - Contingency Plan | Resume All Missions / Business Functions

Requirement  CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS
The organization plans for the resumption of all missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

CP-2(4) What is the solution and how is it implemented?

Part a

Requirement  CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS
The organization plans for the resumption of all missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

Role  Organization
Status  Inherited
Details  undefined
**CP-2(5) - Contingency Plan | Continue Essential Missions / Business Functions**

**Requirement** CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**CP-2(5) What is the solution and how is it implemented?**

**Part a**

**Requirement** CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined

**CP-2(8) - Contingency Plan | Identify Critical Assets**

**Requirement** CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS The organization identifies critical information system assets supporting essential missions and business functions.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**CP-2(8) What is the solution and how is it implemented?**

**Part a**

**Requirement** CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS The organization identifies critical information system assets supporting essential missions and business functions.
Role Organization
Status Inherited
Details undefined

CP-3 - Contingency Training

Requirement CONTINGENCY TRAINING Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CP-3 What is the solution and how is it implemented?

Part a

Requirement CONTINGENCY TRAINING Control: The organization provides contingency training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-16; SP 800-50;

Part b

Requirement

2. When required by information system changes; and

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-16; SP 800-50;
Part c

Requirement
3. [Assignment: organization-defined frequency] thereafter.

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; SP 800-16; SP 800-50;

CP-3(1) - Contingency Training | Simulated Events

Requirement CONTINGENCY TRAINING | SIMULATED EVENTS The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CP-3(1) What is the solution and how is it implemented?

Part a

Requirement CONTINGENCY TRAINING | SIMULATED EVENTS The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Role Organization
Status Inherited
Details undefined

CP-4 - Contingency Plan Testing

Requirement CONTINGENCY PLAN TESTING Control: The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan; b. Reviews the contingency plan test results; and c. Initiates corrective actions, if needed.
Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

CP-4 What is the solution and how is it implemented?

Part a

Requirement CONTINGENCY PLAN TESTING Control: The organization: a. Tests the contingency plan for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; FIPS Pub 199; SP 800-34; SP 800-84;

Part b

Requirement
2. Reviews the contingency plan test results; and

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; FIPS Pub 199; SP 800-34; SP 800-84;

Part c

Requirement
3. Initiates corrective actions, if needed.

Role Organization
Status Inherited
Details undefined
References Federal Continuity Directive 1; FIPS Pub 199; SP 800-34; SP 800-84;

CP-4(1) - Contingency Plan Testing | Coordinate With Related Plans

Requirement CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan testing with organizational elements responsible for related plans.
**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**CP-4(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS The organization coordinates contingency plan testing with organizational elements responsible for related plans.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

**CP-4(2) - Contingency Plan Testing | Alternate Processing Site**

**Requirement** CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE The organization tests the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and (b) To evaluate the capabilities of the alternate processing site to support contingency operations.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**CP-4(2) What is the solution and how is it implemented?**

**Part a**

**Requirement** CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE The organization tests the contingency plan at the alternate processing site: (a) To familiarize contingency personnel with the facility and available resources; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>
Part b

Requirement

2. To evaluate the capabilities of the alternate processing site to support contingency operations.

Role  Organization
Status  Inherited
Details  undefined

CP-6 - Alternate Storage Site

Requirement  ALTERNATE STORAGE SITE Control: The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and b. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

CP-6 What is the solution and how is it implemented?

Part a

Requirement  ALTERNATE STORAGE SITE Control: The organization: a. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and

Role  Organization
Status  Inherited
Details  undefined
References  SP 800-34;

Part b

Requirement

2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

Role  Organization
Status  Inherited
Details  undefined
References  SP 800-34;
CP-6(1) - Alternate Storage Site | Separation From Primary Site

**Requirement** ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

Control Summary Information

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

CP-6(1) What is the solution and how is it implemented?

**Part a**

**Requirement** ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats. Supplemental Guidance: Threats that affect alternate storage sites are typically defined in organizational assessments of risk and include, for example, natural disasters, structural failures, hostile cyber attacks, and errors of omission/commission. Organizations determine what is considered a sufficient degree of separation between primary and alternate storage sites based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber attack), the degree of separation between sites is less relevant. Related control: RA-3.

- **Role** Organization
- **Status** Inherited
- **Details** undefined

CP-6(2) - Alternate Storage Site | Recovery Time / Point Objectives

**Requirement** ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Control Summary Information

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO
CP-6(2) What is the solution and how is it implemented?

Part a

Requirement  ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Role  Organization
Status  Inherited
Details  undefined

CP-6(3) - Alternate Storage Site | Accessibility

Requirement  ALTERNATE STORAGE SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

CP-6(3) What is the solution and how is it implemented?

Part a

Requirement  ALTERNATE STORAGE SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Role  Organization
Status  Inherited
Details  undefined

CP-7 - Alternate Processing Site

Requirement  ALTERNATE PROCESSING SITE Control: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and c. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

CP-7 What is the solution and how is it implemented?

Part a

**Requirement** ALTERNATE PROCESSING SITE Control: The organization: a. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

Part b

**Requirement**

2. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

Part c

**Requirement**

3. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>
CP-7(1) - Alternate Processing Site | Separation From Primary Site

**Requirement** ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**CP-7(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

- **Role** Organization
- **Status** Inherited
- **Details** undefined

CP-7(2) - Alternate Processing Site | Accessibility

**Requirement** ALTERNATE PROCESSING SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**CP-7(2) What is the solution and how is it implemented?**

**Part a**

**Requirement** ALTERNATE PROCESSING SITE | ACCESSIBILITY The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

- **Role** Organization
**CP-7(3) - Alternate Processing Site | Priority Of Service**

**Requirement** ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

**Control Summary Information**
- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**CP-7(3) What is the solution and how is it implemented?**

**Part a**

**Requirement** ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

**Role** Organization
- **Status** Inherited
- **Details** undefined

**CP-7(4) - Alternate Processing Site | Preparation For Use**

**Requirement** ALTERNATE PROCESSING SITE | PREPARATION FOR USE The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

**Control Summary Information**
- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO
CP-7(4) What is the solution and how is it implemented?

Part a

Requirement ALTERNATE PROCESSING SITE | PREPARATION FOR USE The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

Role Organization

Status Inherited

Details undefined

CP-8 - Telecommunications Services

Requirement TELECOMMUNICATIONS SERVICES Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

CP-8 What is the solution and how is it implemented?

Part a

Requirement TELECOMMUNICATIONS SERVICES Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Role Organization

Status Inherited

Details undefined

References SP 800-34; National Communications Systems Directive 3-10; Web: tsp.ncs.gov;

CP-8(1) - Telecommunications Services | Priority Of Service Provisions

Requirement TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS The organization: (a) Develops primary and alternate telecommunications service agreements that con-
tain priority-of-service provisions in accordance with organizational availability requirements (includ-
ing recovery time objectives); and (b) Requests Telecommunications Service Priority for all
telecommunications services used for national security emergency preparedness in the event that the
primary and/or alternate telecommunications services are provided by a common carrier.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

CP-8(1) What is the solution and how is it implemented?

Part a

**Requirement** TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS The
organization: (a) Develops primary and alternate telecommunications service agreements that con-
tain priority-of-service provisions in accordance with organizational availability requirements (in-
cluding recovery time objectives); and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

Part b

**Requirement**

2. Requests Telecommunications Service Priority for all telecommunications services used for na-
tional security emergency preparedness in the event that the primary and/or alternate telecom-
munications services are provided by a common carrier.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

CP-8(2) - Telecommunications Services | Single Points Of Failure

**Requirement** TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE The organiza-
tion obtains alternate telecommunications services to reduce the likelihood of sharing a single point
of failure with primary telecommunications services.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
</tbody>
</table>
Origin  Inherited from pre-existing ATO

CP-8(2) What is the solution and how is it implemented?

Part a

Requirement  TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Role  Organization

Status  Inherited

Details  undefined

CP-8(3) - Telecommunications Services | Separation Of Primary / Alternate Providers

Requirement  TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

CP-8(3) What is the solution and how is it implemented?

Part a

Requirement  TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Role  Organization

Status  Inherited

Details  undefined

CP-8(4) - Telecommunications Services | Provider Contingency Plan

Requirement  TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN The organization: (a) Requires primary and alternate telecommunications service providers to have contingency plans; (b) Reviews provider contingency plans to ensure that the plans meet organizational
contingency requirements; and (c) Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency].

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

CP-8(4) What is the solution and how is it implemented?

Part a

Requirement  TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN The organization: (a) Requires primary and alternate telecommunications service providers to have contingency plans;

Role  Organization
Status  Inherited
Details  undefined

Part b

Requirement

2. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and

Role  Organization
Status  Inherited
Details  undefined

Part c

Requirement

3. Obtains evidence of contingency testing/training by providers [Assignment: organization-defined frequency].

Role  Organization
Status  Inherited
Details  undefined
CP-9 - Information System Backup

**Requirement** INFORMATION SYSTEM BACKUP Control: The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d. Protects the confidentiality, integrity, and availability of backup information at storage locations.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**CP-9 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION SYSTEM BACKUP Control: The organization: a. Conducts backups of user-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Conducts backups of system-level information contained in the information system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives];

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

**Part c**

**Requirement**
3. Conducts backups of information system documentation including security-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

Part d

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Protects the confidentiality, integrity, and availability of backup information at storage locations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-34;</td>
</tr>
</tbody>
</table>

**CP-9(1) - Information System Backup | Testing For Reliability / Integrity**

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION SYSTEM BACKUP</td>
</tr>
<tr>
<td>The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.</td>
</tr>
</tbody>
</table>

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**CP-9(1) What is the solution and how is it implemented?**

Part a

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>INFORMATION SYSTEM BACKUP</td>
</tr>
<tr>
<td>The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>
CP-9(2) - Information System Backup | Test Restoration Using Sampling

**Requirement** INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**CP-9(2) What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined

CP-9(3) - Information System Backup | Separate Storage For Critical Information

**Requirement** INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**CP-9(3) What is the solution and how is it implemented?**
Part a

**Requirement** INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.

**Role** Organization

**Status** Inherited

**Details** undefined

**DI-1 - Data Quality**

**Requirement** DATA QUALITY Control: The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

**Control Summary Information**

**Role** OpenShift Tenant

**Status** Planned

**Origin** OpenShift Tenant SSP

**DI-1 What is the solution and how is it implemented?**

Part a

**Requirement** DATA QUALITY Control: The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;
Part b

Requirement

2. Collects PII directly from the individual to the greatest extent practicable;

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;

Part c

Requirement

3. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;

Part d

Requirement

4. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;
DI-1(1) - Data Quality | Validate Pii

**Requirement** DATA QUALITY | VALIDATE PII The organization requests that the individual or individual’s authorized representative validate PII during the collection process.

Control Summary Information

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Origin**: OpenShift Tenant SSP

**DI-1(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** DATA QUALITY | VALIDATE PII The organization requests that the individual or individual’s authorized representative validate PII during the collection process.

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined

DI-1(2) - Data Quality | Re-validate Pii

**Requirement** DATA QUALITY | RE-VALIDATE PII The organization requests that the individual or individual’s authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].

Control Summary Information

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Origin**: OpenShift Tenant SSP

**DI-1(2) What is the solution and how is it implemented?**

**Part a**

**Requirement** DATA QUALITY | RE-VALIDATE PII The organization requests that the individual or individual’s authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
DI-2 - Data Integrity And Data Integrity Board

**Requirement** DATA INTEGRITY AND DATA INTEGRITY BOARD Control: The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

**Control Summary Information**

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Origin**: OpenShift Tenant SSP

**DI-2 What is the solution and how is it implemented?**

**Part a**

**Requirement** DATA INTEGRITY AND DATA INTEGRITY BOARD Control: The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
- **References**: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I;

**Part b**

**Requirement**

2. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined
- **References**: The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I;
DI-2(1) - Data Integrity And Data Integrity Board | Publish Agreements On Website

**Requirement**  DATA INTEGRITY AND DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE The organization publishes Computer Matching Agreements on its public website.

**Control Summary Information**

- **Role**  Organization
- **Status**  Inherited
- **Origin**  Inherited from pre-existing ATO

**DI-2(1) What is the solution and how is it implemented?**

**Part a**

**Requirement**  DATA INTEGRITY AND DATA INTEGRITY BOARD | PUBLISH AGREEMENTS ON WEBSITE The organization publishes Computer Matching Agreements on its public website.

- **Role**  Organization
- **Status**  Inherited
- **Details**  undefined

**DM-1 - Minimization Of Personally Identifiable Information**

**Requirement**  MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

**Control Summary Information**

- **Role**  Organization
- **Status**  Inherited
- **Origin**  Inherited from pre-existing ATO
DM-1 What is the solution and how is it implemented?

Part a

Requirement MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

Role Organization
Status Inherited
Details undefined

References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

Part b

Requirement 2. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

Part c

Requirement 3. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Role Organization
Status Inherited
Details undefined

References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

DM-1(1) - Minimization Of Personally Identifiable Information | Locate / Remove / Redact / Anonymize Pii

Requirement MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-
identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

DM-1(1) What is the solution and how is it implemented?

Part a

Requirement MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION | LOCATE / REMOVE / REDACT / ANONYMIZE PII The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

DM-2 - Data Retention And Disposal

Requirement DATA RETENTION AND DISPOSAL Control: The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Tenant SSP</td>
</tr>
</tbody>
</table>

DM-2 What is the solution and how is it implemented?

Part a

Requirement DATA RETENTION AND DISPOSAL Control: The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law;
Part b

Requirement

2. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB M-07-16; OMB Circular A-130; SP 800-88;

Part c

Requirement

3. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB M-07-16; OMB Circular A-130; SP 800-88;

DM-2(1) - Data Retention And Disposal | System Configuration

Requirement DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP
DM-2(1) What is the solution and how is it implemented?

Part a

Requirement DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Role OpenShift Tenant

Status Planned

Details undefined

DM-3 - Minimization Of PII Used In Testing, Training, And Research

Requirement MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH Control: The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

DM-3 What is the solution and how is it implemented?

Part a

Requirement MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH Control: The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

Role Organization

Status Inherited

Details undefined

References SP 800-122

Part b

Requirement

2. Implements controls to protect PII used for testing, training, and research.

Role OpenShift Tenant

Status Planned

Details undefined
DM-3(1) - Minimization Of PII Used In Testing, Training, And Research | Risk Minimization Techniques

**Requirement** MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**DM-3(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH | RISK MINIMIZATION TECHNIQUES The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

- **Role** Organization
- **Status** Inherited
- **Details** undefined

**IA-1 - Identification And Authentication Policy And Procedures**

**Requirement** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and b. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and 2. Identification and authentication procedures [Assignment: organization-defined frequency].

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO
### IA-1 What is the solution and how is it implemented?

#### Part a

**Requirement** IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES Control:
The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**References** FIPS Pub 201; SP 800-12; SP 800-63; SP 800-73; SP 800-76; SP 800-78; SP 800-100;

#### Part b

**Requirement**
2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**References** FIPS Pub 201; SP 800-12; SP 800-63; SP 800-73; SP 800-76; SP 800-78; SP 800-100;

#### Part c

**Requirement**
2. Reviews and updates the current: 1. Identification and authentication policy [Assignment: organization-defined frequency]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**References** FIPS Pub 201; SP 800-12; SP 800-63; SP 800-73; SP 800-76; SP 800-78; SP 800-100;

#### Part d

**Requirement**
2. Identification and authentication procedures [Assignment: organization-defined frequency].

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**References** FIPS Pub 201; SP 800-12; SP 800-63; SP 800-73; SP 800-76; SP 800-78; SP 800-100;
IA-2 - Identification And Authentication (organizational Users)

**Requirement** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Control:
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Control Summary Information

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

IA-2 What is the solution and how is it implemented?

**Part a**

**Requirement** IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) Control:
The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

- **Role**: Organization
- **Status**: Inherited

**Details** OpenShift has the ability to utilize 3rd party authentication sources such as LDAP and Active Directory. These have the ability to fulfill this control, thus if used with OpenShift this control is satisfied.

**References** HSPD 12; OMB M-04-04; OMB M-06-16; OMB M-11-11; FIPS Pub 201; SP 800-63; SP 800-73; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

IA-2(1) - Identification And Authentication | Network Access To Privileged Accounts

**Requirement** IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to privileged accounts.

Control Summary Information

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Origin**: OpenShift Landlord SSP
IA-2(1) What is the solution and how is it implemented?

Part a

**Requirement** IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for network access to privileged accounts.

**Role** OpenShift Landlord

**Status** Planned

**Details** NEED TO ADDRESS

IA-2(12) - Identification And Authentication | Acceptance Of Piv Credentials

**Requirement** IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

IA-2(12) What is the solution and how is it implemented?

Part a

**Requirement** IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

**Role** Organization

**Status** Inherited

**Details** OpenShift has the ability to utilize 3rd party authentication sources such as LDAP and Active Directory. These have the ability to fulfill this control, thus if used with OpenShift this control is satisfied.

IA-2(3) - Identification And Authentication | Local Access To Privileged Accounts

**Requirement** IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to privileged accounts.
**Control Summary Information**

**Role** OpenShift Landlord  
**Status** Planned  
**Origin** OpenShift Landlord SSP

**IA-2(3) What is the solution and how is it implemented?**

**Part a**

**Requirement** IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS The information system implements multifactor authentication for local access to privileged accounts.  
**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS

**IA-4 - Identifier Management**

**Requirement** IDENTIFIER MANAGEMENT Control: The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier; b. Selecting an identifier that identifies an individual, group, role, or device; c. Assigning the identifier to the intended individual, group, role, or device; d. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and e. Disabling the identifier after [Assignment: organization-defined time period of inactivity].

**Control Summary Information**

**Role** Organization  
**Status** Inherited  
**Origin** Inherited from pre-existing ATO

**IA-4 What is the solution and how is it implemented?**

**Part a**

**Requirement** IDENTIFIER MANAGEMENT Control: The organization manages information system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;  
**Role** Organization  
**Status** Inherited  
**Details** Dependent on implementing organization.  
**References** FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78;
Part b

Requirement

2. Selecting an identifier that identifies an individual, group, role, or device;

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78;

Part c

Requirement

3. Assigning the identifier to the intended individual, group, role, or device;

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78;

Part d

Requirement

4. Preventing reuse of identifiers for [Assignment: organization-defined time period]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78;

Part e

Requirement

5. Disabling the identifier after [Assignment: organization-defined time period of inactivity].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78;
IA-5 - Authenticator Management

**Requirement** AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**IA-5 What is the solution and how is it implemented?**

**Part a**

**Requirement** AUTHENTICATOR MANAGEMENT Control: The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

**References** OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

**Part b**

**Requirement**

2. Establishing initial authenticator content for authenticators defined by the organization;

- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

**References** OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;
Part c

Requirement

3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part d

Requirement

4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part e

Requirement

5. Changing default content of authenticators prior to information system installation;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part f

Requirement

6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;
Part g

Requirement

7. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];

Role Organization
Status Inherited
Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part h

Requirement

8. Protecting authenticator content from unauthorized disclosure and modification;

Role Organization
Status Inherited
Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part i

Requirement

1. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;

Part j

Requirement

10. Changing authenticators for group/role accounts when membership to those accounts changes.

Role Organization
Status Inherited
Details Dependent on implementing organization.

References OMB M-04-04; OMB M-11-11; FIPS Pub 201; SP 800-73; SP 800-63; SP 800-76; SP 800-78; FICAM Roadmap and Implementation Guidance; Web: idmanagement.gov;
IA-5(1) - Authenticator Management | Password-based Authentication

**Requirement**  AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]; (b) Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]; (c) Stores and transmits only encrypted representations of passwords; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; (e) Prohibits password reuse for [Assignment: organization-defined number] generations; and (f) Allows the use of a temporary password for system logons with an immediate change to a permanent password.

**Control Summary Information**

- **Role**  OpenShift Landlord
- **Status**  Planned
- **Origin**  OpenShift Landlord SSP

**IA-5(1) What is the solution and how is it implemented?**

**Part a**

** Requirement**  AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

- **Role**  OpenShift Landlord
- **Status**  Planned
- **Details**  NEED TO ADDRESS

**Part b**

**Requirement**

2. Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number];

- **Role**  OpenShift Landlord
- **Status**  Planned
- **Details**  NEED TO ADDRESS
Part c

Requirement
3. Stores and transmits only encrypted representations of passwords;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

Part d

Requirement
4. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum];

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

Part e

Requirement
5. Prohibits password reuse for [Assignment: organization-defined number] generations; and

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

Part f

Requirement
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

IA-5(11) - Authenticator Management | Hardware Token-based Authentication

Requirement  AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].
Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IA-5(11) What is the solution and how is it implemented?

Part a

Requirement AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

Role Organization
Status Inherited
Details undefined

IA-5(2) - Authenticator Management | PKI-based Authentication

Requirement AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; (b) Enforces authorized access to the corresponding private key; (c) Maps the authenticated identity to the account of the individual or group; and (d) Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

IA-5(2) What is the solution and how is it implemented?

Part a

Requirement AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION The information system, for PKI-based authentication: (a) Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
Part b

Requirement
2. Enforces authorized access to the corresponding private key;

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part c

Requirement
3. Maps the authenticated identity to the account of the individual or group; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part d

Requirement
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

IA-5(3) - Authenticator Management | In-person Or Trusted Third-party Registration

Requirement AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
IA-5(3) What is the solution and how is it implemented?
Part a

Requirement AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION The organization requires that the registration process to receive [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted third party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

Role Organization
Status Inherited
Details undefined

IA-6 - Authenticator Feedback

Requirement AUTHENTICATOR FEEDBACK Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

IA-6 What is the solution and how is it implemented?
Part a

Requirement AUTHENTICATOR FEEDBACK Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

IA-7 - Cryptographic Module Authentication

Requirement CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

IA-7 What is the solution and how is it implemented?

Part a

Requirement CRYPTOGRAPHIC MODULE AUTHENTICATION Control: The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References FIPS Pub 140; Web: csrc.nist.gov/groups/STM/cmvp/index.html;

IA-8 - Identification And Authentication (non-organizational Users)

Requirement IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

IA-8 What is the solution and how is it implemented?

Part a

Requirement IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References OMB M-04-04; OMB M-11-11; OMB Memoranda 10-06-2011; FICAM Roadmap and Implementation Guidance; FIPS Pub 201; SP 800-63; SP 800-116; National Strategy for Trusted Identities in Cyberspace; Web: idmanagement.gov;

IA-8(1) - Identification And Authentication | Acceptance Of Piv Credentials From Other Agencies

Requirement IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

IA-8(1) What is the solution and how is it implemented?

Part a

Requirement IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

IA-8(2) - Identification And Authentication | Acceptance Of Third-party Credentials

Requirement IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS The information system accepts only FICAM-approved third-party credentials.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
IA-8(2) What is the solution and how is it implemented?
Part a

Requirement IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF THIRD-PARTY CREDENTIALS The information system accepts only FICAM-approved third-party credentials.

Role Organization
Status Inherited
Details undefined

IA-8(3) - Identification And Authentication | Use Of Ficam-approved Products

Requirement IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IA-8(3) What is the solution and how is it implemented?
Part a

Requirement IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-APPROVED PRODUCTS The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

Role Organization
Status Inherited
Details undefined

IA-8(4) - Identification And Authentication | Use Of Ficam-issued Profiles

Requirement IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES The information system conforms to FICAM-issued profiles.
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

IA-8(4) What is the solution and how is it implemented?

Part a

**Requirement** IDENTIFICATION AND AUTHENTICATION | USE OF FICAM-ISSUED PROFILES
The information system conforms to FICAM-issued profiles.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

IP-1 - Consent

**Requirement** CONSENT Control: The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Tenant SSP</td>
</tr>
</tbody>
</table>

IP-1 What is the solution and how is it implemented?

Part a

**Requirement** CONSENT Control: The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>
**References** The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

**Part b**

**Requirement**

2. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII;

**Role** OpenShift Tenant  
**Status** Planned  
**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

**Part c**

**Requirement**

3. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and

**Role** OpenShift Tenant  
**Status** Planned  
**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

**Part d**

**Requirement**

4. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

**Role** OpenShift Tenant  
**Status** Planned  
**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

**IP-1(1) - Consent | Mechanisms Supporting Itemized Or Tiered Consent**

**Requirement** CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT The organization implements mechanisms to support itemized or tiered consent for specific uses of data.
### IP-1(1) What is the solution and how is it implemented?

**Part a**

**Requirement** CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Tenant SSP</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

### IP-2 - Individual Access

**Requirement** INDIVIDUAL ACCESS Control: The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in System of Records Notices (SORNs); and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

### Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Tenant SSP</td>
</tr>
</tbody>
</table>

### IP-2 What is the solution and how is it implemented?

**Part a**

**Requirement** INDIVIDUAL ACCESS Control: The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

**References** The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;
Part b

Requirement

2. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

Part c

Requirement

3. Publishes access procedures in System of Records Notices (SORNs); and

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

Part d

Requirement

4. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

IP-3 - Redress

Requirement REDRESS Control: The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.
Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

IP-3 What is the solution and how is it implemented?

Part a

Requirement REDRESS Control: The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130;

Part b

Requirement

2. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130;

IP-4 - Complaint Management

Requirement COMPLAINT MANAGEMENT Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP
IP-4 What is the solution and how is it implemented?

Part a

Requirement  COMPLAINT MANAGEMENT Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  OMB Circular A-130; OMB M-07-16; OMB M-08-09;

IP-4(1) - Complaint Management | Response Times

Requirement  COMPLAINT MANAGEMENT | RESPONSE TIMES The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].

Control Summary Information

Role  OpenShift Tenant

Status  Planned

Origin  OpenShift Tenant SSP

IP-4(1) What is the solution and how is it implemented?

Part a

Requirement  COMPLAINT MANAGEMENT | RESPONSE TIMES The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].

Role  OpenShift Tenant

Status  Planned

Details  undefined

IR-1 - Incident Response Policy And Procedures

Requirement  INCIDENT RESPONSE POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency].
Control Summary Information

Role: Organization
Status: Inherited
Origin: Inherited from pre-existing ATO

IR-1 What is the solution and how is it implemented?

Part a

Requirement: INCIDENT RESPONSE POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role: Organization
Status: Inherited
Details: Dependent on implementing organization.
References: SP 800-12; SP 800-61; SP 800-83; SP 800-100;

Part b

Requirement
2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and

Role: Organization
Status: Inherited
Details: Dependent on implementing organization.
References: SP 800-12; SP 800-61; SP 800-83; SP 800-100;

Part c

Requirement
2. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and

Role: Organization
Status: Inherited
Details: Dependent on implementing organization.
References: SP 800-12; SP 800-61; SP 800-83; SP 800-100;
Part d

Requirement
2. Incident response procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-61; SP 800-83; SP 800-100;

IR-2 - Incident Response Training

Requirement INCIDENT RESPONSE TRAINING Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IR-2 What is the solution and how is it implemented?

Part a

Requirement INCIDENT RESPONSE TRAINING Control: The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-16; SP 800-50;

Part b

Requirement
2. When required by information system changes; and

Role Organization
Status Inherited
Details  Dependent on implementing organization.

References  SP 800-16; SP 800-50;

Part c

Requirement

3. [Assignment: organization-defined frequency] thereafter.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-16; SP 800-50;

IR-2(1) - Incident Response Training | Simulated Events

Requirement  INCIDENT RESPONSE TRAINING | SIMULATED EVENTS The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

IR-2(1) What is the solution and how is it implemented?

Part a

Requirement  INCIDENT RESPONSE TRAINING | SIMULATED EVENTS The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

IR-2(2) - Incident Response Training | Automated Training Environments

Requirement  INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.
IR-2(2) What is the solution and how is it implemented?

Part a

**Requirement** INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

**Role** Organization

**Status** Inherited

**Details** undefined

IR-3(2) - Incident Response Testing | Coordination With Related Plans

**Requirement** INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

The organization coordinates incident response testing with organizational elements responsible for related plans.

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

IR-3(2) What is the solution and how is it implemented?

Part a

**Requirement** INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS

The organization coordinates incident response testing with organizational elements responsible for related plans.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.
IR-4 - Incident Handling

Requirement INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IR-4 What is the solution and how is it implemented?

Part a

Requirement INCIDENT HANDLING Control: The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
Role Organization
Status Inherited
Details Dependent on implementing organization.
References EO 13587; SP 800-61;

Part b

Requirement
2. Coordinates incident handling activities with contingency planning activities; and
Role Organization
Status Inherited
Details Dependent on implementing organization.
References EO 13587; SP 800-61;

Part c

Requirement
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.
Role Organization
Status Inherited
**IR-4(1) - Incident Handling | Automated Incident Handling Processes**

**Requirement** INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**IR-4(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES The organization employs automated mechanisms to support the incident handling process.

- **Role**: Organization
- **Status**: Inherited
- **Details**: Dependent on implementing organization.

**IR-5 - Incident Monitoring**

**Requirement** INCIDENT MONITORING Control: The organization tracks and documents information system security incidents.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**IR-5 What is the solution and how is it implemented?**

**Part a**

**Requirement** INCIDENT MONITORING Control: The organization tracks and documents information system security incidents.

- **Role**: Organization
IR-5(1) - Incident Monitoring | Automated Tracking / Data Collection / Analysis

Requirement INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IR-6 - Incident Reporting

Requirement INCIDENT REPORTING Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b. Reports security incident information to [Assignment: organization-defined authorities].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
IR-6 What is the solution and how is it implemented?

Part a

Requirement INCIDENT REPORTING Control: The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61; Web: www.us-cert.gov;

Part b

Requirement

2. Reports security incident information to [Assignment: organization-defined authorities].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61; Web: www.us-cert.gov;

IR-6(1) - Incident Reporting | Automated Reporting

Requirement INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

IR-6(1) What is the solution and how is it implemented?

Part a

Requirement INCIDENT REPORTING | AUTOMATED REPORTING The organization employs automated mechanisms to assist in the reporting of security incidents.

Role Organization
Status Inherited
Details Dependent on implementing organization.
IR-7 - Incident Response Assistance

**Requirement** INCIDENT RESPONSE ASSISTANCE Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**IR-7 What is the solution and how is it implemented?**

**Part a**

**Requirement** INCIDENT RESPONSE ASSISTANCE Control: The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

- **Role**: Organization
- **Status**: Inherited
- **Details**: Dependent on implementing organization.

**IR-7(1) - Incident Response Assistance | Automation Support For Availability Of Information / Support**

**Requirement** INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**IR-7(1) What is the solution and how is it implemented?**
Part a

Requirement INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Role Organization

Status Inherited

Details Dependent on implementing organization.

IR-8 - Incident Response Plan

Requirement INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

IR-8 What is the solution and how is it implemented?

Part a

Requirement INCIDENT RESPONSE PLAN Control: The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61:
Part b

Requirement
2. Describes the structure and organization of the incident response capability;
Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61;

Part c

Requirement
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61;

Part d

Requirement
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61;

Part e

Requirement
5. Defines reportable incidents;
Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-61;
Part f

Requirement

6. Provides metrics for measuring the incident response capability within the organization;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61;

Part g

Requirement

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61;

Part h

Requirement

8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61;

Part i

Requirement

2. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61;
Part j

**Requirement**

3. Reviews the incident response plan [Assignment: organization-defined frequency];

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-61;

Part k

**Requirement**

4. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-61;

Part l

**Requirement**

5. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-61;

Part m

**Requirement**

6. Protects the incident response plan from unauthorized disclosure and modification.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-61;
MA-1 - System Maintenance Policy And Procedures

Requirement  SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization:
  a. develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
     1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management
        commitment, coordination among organizational entities, and compliance; and
     2. Procedures to facilitate the implementation of the system maintenance policy and associated system
        maintenance controls; and
  b. Reviews and updates the current:
     1. System maintenance policy [Assignment: organization-defined frequency]; and
     2. System maintenance procedures [Assignment: organization-defined frequency].

Control Summary Information

Role  OpenShift Tenant
Status  Not implemented
Origin  Tenant SSP

MA-1 What is the solution and how is it implemented?

Part a

Requirement  SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization:
  a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
     1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management
        commitment, coordination among organizational entities, and compliance; and

Role  OpenShift Tenant
Status  Not implemented
Details  Documented in the individual project / program’s System Design Specification document and
        System Security Plan.

References  SP 800-12; SP 800-100;

Part b

Requirement
  2. Procedures to facilitate the implementation of the system maintenance policy and associated
     system maintenance controls; and

Role  OpenShift Tenant
Status  Not implemented
Details  Documented in the individual project / program’s System Design Specification document and
        System Security Plan.

References  SP 800-12; SP 800-100;
Part c

Requirement
2. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

Part d

Requirement
2. System maintenance procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

MA-2 - Controlled Maintenance

Requirement CONTROLLED MAINTENANCE Control: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and f. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
MA-2 What is the solution and how is it implemented?

Part a

**Requirement** CONTROLLED MAINTENANCE Control: The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

Part b

**Requirement**

1. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

Part c

**Requirement**

2. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

Part d

**Requirement**

3. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.
Part e

Requirement
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part f

Requirement

Role Organization
Status Inherited
Details Dependent on implementing organization.

MA-2(2) - Controlled Maintenance | Automated Maintenance Activities

Requirement CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (b) Produces up-to-date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

MA-2(2) What is the solution and how is it implemented?

Part a

Requirement CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES The organization: (a) Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
Part b

Requirement

2. Produces up-to-date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

Role Organization
Status Inherited
Details Dependent on implementing organization.

MA-3(1) - Maintenance Tools | Inspect Tools

Requirement MAINTENANCE TOOLS | INSPECT TOOLS The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

MA-3(1) What is the solution and how is it implemented?

Part a

Requirement MAINTENANCE TOOLS | INSPECT TOOLS The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Role Organization
Status Inherited
Details undefined

MA-4 - Nonlocal Maintenance

Requirement NONLOCAL MAINTENANCE Control: The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities; b. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d. Maintains records for nonlocal maintenance and diagnostic activities; and e. Terminates session and network connections when nonlocal maintenance is completed.
Control Summary Information

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

MA-4 What is the solution and how is it implemented?

**Part a**

**Requirement** NONLOCAL MAINTENANCE Control: The organization: a. Approves and monitors nonlocal maintenance and diagnostic activities;

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined
- **References** FIPS Pub 140-2; FIPS Pub 197; FIPS Pub 201; SP 800-63; SP 800-88; CNSS Policy 15;

**Part b**

**Requirement**

2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined
- **References** FIPS Pub 140-2; FIPS Pub 197; FIPS Pub 201; SP 800-63; SP 800-88; CNSS Policy 15;

**Part c**

**Requirement**

3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined
- **References** FIPS Pub 140-2; FIPS Pub 197; FIPS Pub 201; SP 800-63; SP 800-88; CNSS Policy 15;

**Part d**

**Requirement**

4. Maintains records for nonlocal maintenance and diagnostic activities; and

- **Role**: Organization
Part e

Requirement
5. Terminates session and network connections when nonlocal maintenance is completed.

Role Organization
Status Inherited
Details undefined
References FIPS Pub 140-2; FIPS Pub 197; FIPS Pub 201; SP 800-63; SP 800-88; CNSS Policy 15;

MA-4(2) - Nonlocal Maintenance | Document Nonlocal Maintenance

Requirement NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

MA-4(2) What is the solution and how is it implemented?

Part a

Requirement NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

Role Organization
Status Inherited
Details undefined

MA-5 - Maintenance Personnel

Requirement MAINTENANCE PERSONNEL Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; b. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and c. Designates organizational personnel with required
access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

**Control Summary Information**

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

**MA-5 What is the solution and how is it implemented?**

**Part a**

- **Requirement** MAINTENANCE PERSONNEL Control: The organization: a. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

**Part b**

- **Requirement**
  2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

**Part c**

- **Requirement**
  3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.
MA-5(1) - Maintenance Personnel | Individuals Without Appropriate Access

**Requirement** MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

The organization: (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; (2) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and (b) Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**MA-5(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS

The organization: (a) Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: (1) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
</tbody>
</table>
Part c

Requirement

2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

Role Organization

Status Inherited

Details Dependent on implementing organization.

MA-6 - Timely Maintenance

Requirement TIMELY MAINTENANCE Control: The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

Control Summary Information

Role IaaS

Status Implemented

Origin Inherited from pre-existing ATO

MA-6 What is the solution and how is it implemented?

Part a

Requirement TIMELY MAINTENANCE Control: The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

Role IaaS

Status Implemented

Details Inherited from IaaS.

MP-1 - Media Protection Policy And Procedures

Requirement MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]; 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and b. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and 2. Media protection procedures [Assignment: organization-defined frequency].
Control Summary Information

Role  Organization  
Status Inherited  
Origin Inherited from pre-existing ATO  

MP-1 What is the solution and how is it implemented?

Part a

Requirement MEDIA PROTECTION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  Organization  
Status Inherited  
Details Dependent on implementing organization.  
References SP 800-12; SP 800-100;  

Part b

Requirement  
2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and

Role  Organization  
Status Inherited  
Details Dependent on implementing organization.  
References SP 800-12; SP 800-100;  

Part c

Requirement  
2. Reviews and updates the current: 1. Media protection policy [Assignment: organization-defined frequency]; and

Role  Organization  
Status Inherited  
Details Dependent on implementing organization.  
References SP 800-12; SP 800-100;
Part d

**Requirement**

2. Media protection procedures [Assignment: organization-defined frequency].

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-12; SP 800-100;

---

**MP-2 - Media Access**

**Requirement** MEDIA ACCESS Control: The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

---

**Control Summary Information**

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

---

**MP-2 What is the solution and how is it implemented?**

Part a

**Requirement** MEDIA ACCESS Control: The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** FIPS Pub 199; SP 800-111;

---

**MP-3 - Media Marking**

**Requirement** MEDIA MARKING Control: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].
Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

MP-3 What is the solution and how is it implemented?

Part a

Requirement  MEDIA MARKING Control: The organization: a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  FIPS Pub 199;

Part b

Requirement  2. Exempts [Assignment: organization-defined types of information system media] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  FIPS Pub 199;

MP-4 - Media Storage

Requirement  MEDIA STORAGE Control: The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO
**MP-4 What is the solution and how is it implemented?**

**Part a**

**Requirement** MEDIA STORAGE Control: The organization: a. Physically controls and securely stores [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** FIPS Pub 199; SP 800-56; SP 800-57; SP 800-111;

**Part b**

**Requirement**

2. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** FIPS Pub 199; SP 800-56; SP 800-57; SP 800-111;

**MP-5 - Media Transport**

**Requirement** MEDIA TRANSPORT Control: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards]; b. Maintains accountability for information system media during transport outside of controlled areas; c. Documents activities associated with the transport of information system media; and d. Restricts the activities associated with the transport of information system media to authorized personnel.

**Control Summary Information**

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

**MP-5 What is the solution and how is it implemented?**

**Part a**

**Requirement** MEDIA TRANSPORT Control: The organization: a. Protects and controls [Assignment: organization-defined types of information system media] during transport outside of controlled areas using [Assignment: organization-defined security safeguards];
Part b

Requirement

2. Maintains accountability for information system media during transport outside of controlled areas;

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 199; SP 800-60;

Part c

Requirement

3. Documents activities associated with the transport of information system media; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 199; SP 800-60;

Part d

Requirement

4. Restricts the activities associated with the transport of information system media to authorized personnel.

Role Organization
Status Inherited
Details Dependent on implementing organization.
References FIPS Pub 199; SP 800-60;

MP-5(4) - Media Transport | Cryptographic Protection

Requirement MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
Control Summary Information

Role  Organization  
Status  Inherited  
Origin  Inherited from pre-existing ATO

**MP-5(4) What is the solution and how is it implemented?**

**Part a**

**Requirement** MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION  The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Role  Organization  
Status  Inherited  
Details  Dependent on implementing organization.

**MP-6 - Media Sanitization**

**Requirement** MEDIA SANITIZATION  Control: The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Control Summary Information

Role  Organization  
Status  Inherited  
Origin  Inherited from pre-existing ATO

**MP-6 What is the solution and how is it implemented?**

**Part a**

**Requirement** MEDIA SANITIZATION  Control: The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and

Role  Organization  
Status  Inherited  
Details  Dependent on implementing organization.

References  FIPS Pub 199; SP 800-60; SP 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.html
Part b

Requirement

2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 199; SP 800-60; SP 800-88; Web: www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

MP-6(1) - Media Sanitization | Review / Approve / Track / Document / Verify

Requirement MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

MP-6(1) What is the solution and how is it implemented?

Part a

Requirement MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY
The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

Role Organization

Status Inherited

Details Dependent on implementing organization.

MP-6(2) - Media Sanitization | Equipment Testing

Requirement MEDIA SANITIZATION | EQUIPMENT TESTING The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.
Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

MP-6(2) What is the solution and how is it implemented?

Part a

Requirement  MEDIA SANITIZATION | EQUIPMENT TESTING The organization tests sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.

MP-6(3) - Media Sanitization | Nondestructive Techniques

Requirement  MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

MP-6(3) What is the solution and how is it implemented?

Part a

Requirement  MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
MP-7 - Media Use

**Requirement** MEDIA USE Control: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

Control Summary Information

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

MP-7 What is the solution and how is it implemented?

Part a

**Requirement** MEDIA USE Control: The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.
- **References** FIPS Pub 199; SP 800-111;

PE-1 - Physical And Environmental Protection Policy And Procedures

**Requirement** PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and b. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and 2. Physical and environmental protection procedures [Assignment: organization-defined frequency].

Control Summary Information

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO
PE-1 What is the solution and how is it implemented?

Part a

**Requirement** PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part b

**Requirement**
2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part c

**Requirement**
2. Reviews and updates the current: 1. Physical and environmental protection policy [Assignment: organization-defined frequency]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part d

**Requirement**
2. Physical and environmental protection procedures [Assignment: organization-defined frequency].

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>
References  SP 800-12; SP 800-100;

PE-10 - Emergency Shutoff

Requirement  EMERGENCY SHUTOFF Control: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

PE-10 What is the solution and how is it implemented?

Part a

Requirement  EMERGENCY SHUTOFF Control: The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

Role  Organization
Status  Inherited
Details  undefined

Part b

Requirement

2. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and

Role  Organization
Status  Inherited
Details  undefined

Part c

Requirement

3. Protects emergency power shutoff capability from unauthorized activation.

Role  Organization
Status  Inherited
Details  undefined
PE-11 - Emergency Power

**Requirement** EMERGENCY POWER Control: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

Control Summary Information

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

PE-11 What is the solution and how is it implemented?

Part a

**Requirement** EMERGENCY POWER Control: The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

- **Role**: Organization
- **Status**: Inherited
- **Details**: undefined

PE-11(1) - Emergency Power | Long-term Alternate Power Supply - Minimal Operational Capability

**Requirement** EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Control Summary Information

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

PE-11(1) What is the solution and how is it implemented?
Part a

**Requirement** EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

*Role* Organization  
*Status* Inherited  
*Details* undefined

**PE-12 - Emergency Lighting**

**Requirement** EMERGENCY LIGHTING Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

**Control Summary Information**

*Role* Organization  
*Status* Inherited  
*Origin* Inherited from pre-existing ATO

**PE-12 What is the solution and how is it implemented?**

Part a

**Requirement** EMERGENCY LIGHTING Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

*Role* Organization  
*Status* Inherited  
*Details* undefined

**PE-13 - Fire Protection**

**Requirement** FIRE PROTECTION Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**Control Summary Information**

*Role* Organization  
*Status* Inherited
PE-13 What is the solution and how is it implemented?

Part a

**Requirement** FIRE PROTECTION Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

**Role** Organization

**Status** Inherited

**Details** undefined

PE-13(1) - Fire Protection | Detection Devices / Systems

**Requirement** FIRE PROTECTION | DETECTION DEVICES / SYSTEMS The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

PE-13(1) What is the solution and how is it implemented?

Part a

**Requirement** FIRE PROTECTION | DETECTION DEVICES / SYSTEMS The organization employs fire detection devices/systems for the information system that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.

**Role** Organization

**Status** Inherited

**Details** undefined

PE-13(2) - Fire Protection | Suppression Devices / Systems

**Requirement** FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].
Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

PE-13(2) What is the solution and how is it implemented?

Part a

Requirement  FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].

Role  Organization
Status  Inherited
Details  undefined

PE-13(3) - Fire Protection | Automatic Fire Suppression

Requirement  FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

PE-13(3) What is the solution and how is it implemented?

Part a

Requirement  FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

Role  Organization
Status  Inherited
Details  undefined
PE-14 - Temperature And Humidity Controls

Requirement TEMPERATURE AND HUMIDITY CONTROLS Control: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and b. Monitors temperature and humidity levels [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-14 What is the solution and how is it implemented?

Part a

Requirement TEMPERATURE AND HUMIDITY CONTROLS Control: The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [Assignment: organization-defined acceptable levels]; and

Role Organization
Status Inherited
Details undefined

Part b

Requirement

2. Monitors temperature and humidity levels [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details undefined

PE-15 - Water Damage Protection

Requirement WATER DAMAGE PROTECTION Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
PE-15 What is the solution and how is it implemented?

Part a

Requirement WATER DAMAGE PROTECTION Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Role Organization
Status Inherited
Details undefined

PE-15(1) - Water Damage Protection | Automation Support

Requirement WATER DAMAGE PROTECTION | AUTOMATION SUPPORT The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [Assignment: organization-defined personnel or roles].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-15(1) What is the solution and how is it implemented?

Part a

Requirement WATER DAMAGE PROTECTION | AUTOMATION SUPPORT The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [Assignment: organization-defined personnel or roles].

Role Organization
Status Inherited
Details undefined

PE-16 - Delivery And Removal

Requirement DELIVERY AND REMOVAL Control: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.
Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-16 What is the solution and how is it implemented?

Part a

Requirement DELIVERY AND REMOVAL Control: The organization authorizes, monitors, and controls [Assignment: organization-defined types of information system components] entering and exiting the facility and maintains records of those items.

Role Organization
Status Inherited
Details Dependent on implementing organization.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-17 - Alternate Work Site

Requirement ALTERNATE WORK SITE Control: The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-17 What is the solution and how is it implemented?

Part a

Requirement ALTERNATE WORK SITE Control: The organization: a. Employs [Assignment: organization-defined security controls] at alternate work sites;

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-46;
Part b

Requirement

2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-46;

Part c

Requirement

3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-46;

PE-18 - Location Of Information System Components

Requirement LOCATION OF INFORMATION SYSTEM COMPONENTS Control: The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

PE-18 What is the solution and how is it implemented?

Part a

Requirement LOCATION OF INFORMATION SYSTEM COMPONENTS Control: The organization positions information system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.

Role Organization

Status Inherited
Details  undefined

PE-2 - Physical Access Authorizations

Requirement  PHYSICAL ACCESS AUTHORIZATIONS Control: The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides; b. Issues authorization credentials for facility access; c. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d. Removes individuals from the facility access list when access is no longer required.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

PE-2 What is the solution and how is it implemented?

Part a

Requirement  PHYSICAL ACCESS AUTHORIZATIONS Control: The organization: a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
Role  Organization
Status  Inherited
Details  Dependent on implementing organization.

Part b

Requirement

2. Issues authorization credentials for facility access;
Role  Organization
Status  Inherited
Details  Dependent on implementing organization.

Part c

Requirement

3. Reviews the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
Part d

Requirement

4. Removes individuals from the facility access list when access is no longer required.

Role Organization

Status Inherited

Details Dependent on implementing organization.

PE-3 - Physical Access Control

Requirement PHYSICAL ACCESS CONTROL Control: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards]; b. Maintains physical access audit logs for [Assignment: organization-defined exit/exit points]; c. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible; d. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e. Secures keys, combinations, and other physical access devices; f. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

PE-3 What is the solution and how is it implemented?

Part a

Requirement PHYSICAL ACCESS CONTROL Control: The organization: a. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by; 1. Verifying individual access authorizations before granting access to the facility; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References

FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;
Part b

Requirement

2. Controlling ingress/egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;

Part c

Requirement

2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;

Part d

Requirement

3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;

Part e

Requirement

4. Escorts visitors and monitors visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring];

Role Organization

Status Inherited
Part f

Requirement

5. Secures keys, combinations, and other physical access devices;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;

Part g

Requirement

6. Inventories [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;

Part h

Requirement

7. Changes combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Role Organization

Status Inherited

Details Dependent on implementing organization.

References FIPS Pub 201; SP 800-73; SP 800-76; SP 800-78; SP 800-116; ICD 704; ICD 705; DoDI 5200.39; Personal Identity Verification (PIV) in Enterprise Physical Access Control System (EPACS); Web: idmanagement.gov, fips201ep.cio.gov;
PE-4 - Access Control For Transmission Medium

**Requirement** ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**PE-4 What is the solution and how is it implemented?**

**Part a**

**Requirement** ACCESS CONTROL FOR TRANSMISSION MEDIUM Control: The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

- **Role**: Organization
- **Status**: Inherited
- **Details**: Dependent on implementing organization.
- **References**: NSTISSI No. 7003;

PE-5 - Access Control For Output Devices

**Requirement** ACCESS CONTROL FOR OUTPUT DEVICES Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Control Summary Information**

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**PE-5 What is the solution and how is it implemented?**
Part a

**Requirement** ACCESS CONTROL FOR OUTPUT DEVICES Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

PE-6 - Monitoring Physical Access

**Requirement** MONITORING PHYSICAL ACCESS Control: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and c. Coordinates results of reviews and investigations with the organizational incident response capability.

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

PE-6 What is the solution and how is it implemented?

Part a

**Requirement** MONITORING PHYSICAL ACCESS Control: The organization: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

Part b

**Requirement**

2. Reviews physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.
Part c

Requirement
3. Coordinates results of reviews and investigations with the organizational incident response capability.
Role Organization
Status Inherited
Details Dependent on implementing organization.

PE-6(1) - Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment

Requirement MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT The organization monitors physical intrusion alarms and surveillance equipment.

Control Summary Information
Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-6(1) What is the solution and how is it implemented?

Part a

Requirement MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT The organization monitors physical intrusion alarms and surveillance equipment.
Role Organization
Status Inherited
Details Dependent on implementing organization.

PE-6(4) - Monitoring Physical Access | Monitoring Physical Access To Information Systems

Requirement MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].
Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-6(4) What is the solution and how is it implemented?

Part a

Requirement MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].

Role Organization
Status Inherited
Details Dependent on implementing organization.

PE-8 - Visitor Access Records

Requirement VISITOR ACCESS RECORDS Control: The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and b. Reviews visitor access records [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-8 What is the solution and how is it implemented?

Part a

Requirement VISITOR ACCESS RECORDS Control: The organization: a. Maintains visitor access records to the facility where the information system resides for [Assignment: organization-defined time period]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
Part b

Requirement

2. Reviews visitor access records [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.

PE-8(1) - Visitor Access Records | Automated Records Maintenance / Review

Requirement VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PE-8(1) What is the solution and how is it implemented?

Part a

Requirement VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

Role Organization
Status Inherited
Details Dependent on implementing organization.

PE-9 - Power Equipment And Cabling

Requirement POWER EQUIPMENT AND CABLEING Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
PE-9 What is the solution and how is it implemented?

Part a

Requirement  POWER EQUIPMENT AND CABLELING Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Role  Organization

Status  Inherited

Details  undefined

PL-1 - Security Planning Policy And Procedures

Requirement  SECURITY PLANNING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy [Assignment: organization-defined frequency]; and 2. Security planning procedures [Assignment: organization-defined frequency].

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

PL-1 What is the solution and how is it implemented?

Part a

Requirement  SECURITY PLANNING POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-12; SP 800-18; SP 800-100;

Part b

Requirement

2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-18; SP 800-100;

Part c

Requirement
2. Reviews and updates the current:
   1. Security planning policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-18; SP 800-100;

Part d

Requirement
2. Security planning procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-18; SP 800-100;

PL-2 - System Security Plan

Requirement SYSTEM SECURITY PLAN Control: The organization: a. Develops a security plan for
   the information system that: 1. Is consistent with the organization’s enterprise architecture; 2. Ex-
   plicitly defines the authorization boundary for the system; 3. Describes the operational context of
   the information system in terms of missions and business processes; 4. Provides the security cat-
   egorization of the information system including supporting rationale; 5. Describes the operational
   environment for the information system and relationships with or connections to other information
   systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any
   relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting
   those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is
   reviewed and approved by the authorizing official or designated representative prior to plan imple-
   mentation; b. Distributes copies of the security plan and communicates subsequent changes to the
   plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the
   information system [Assignment: organization-defined frequency]; d. Updates the plan to address
   changes to the information system/environment of operation or problems identified during plan im-
   plementation or security control assessments; and e. Protects the security plan from unauthorized
disclosure and modification.
Control Summary Information

Role OpenShift Tenant
Status Not implemented
Origin Tenant SSP

PL-2 What is the solution and how is it implemented?

Part a

Requirement SYSTEM SECURITY PLAN Control: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization’s enterprise architecture;

Role OpenShift Tenant
Status Not implemented
Details Documented in the individual project / program’s System Security Plan.
References SP 800-18;

Part b

Requirement

2. Explicitly defines the authorization boundary for the system;

Role OpenShift Tenant
Status Not implemented
Details Documented in the individual project / program’s System Security Plan.
References SP 800-18;

Part c

Requirement

3. Describes the operational context of the information system in terms of missions and business processes;

Role OpenShift Tenant
Status Not implemented
Details Documented in the individual project / program’s System Security Plan.
References SP 800-18;

Part d

Requirement

4. Provides the security categorization of the information system including supporting rationale;

Role OpenShift Tenant
5. Describes the operational environment for the information system and relationships with or connections to other information systems;

Role: OpenShift Tenant
Status: Not implemented
Details: Documented in the individual project / program’s System Security Plan.
References: SP 800-18;

6. Provides an overview of the security requirements for the system;

Role: OpenShift Tenant
Status: Not implemented
Details: Documented in the individual project / program’s System Security Plan.
References: SP 800-18;

7. Identifies any relevant overlays, if applicable;

Role: OpenShift Tenant
Status: Not implemented
Details: Documented in the individual project / program’s System Security Plan.
References: SP 800-18;

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

Role: OpenShift Tenant
Status: Not implemented
Details: Documented in the individual project / program’s System Security Plan.
Part i

Requirement

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-18;

Part j

Requirement

2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-18;

Part k

Requirement

3. Reviews the security plan for the information system [Assignment: organization-defined frequency];

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-18;

Part l

Requirement

4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-18;
Part m

Requirement

5. Protects the security plan from unauthorized disclosure and modification.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-18;

PL-2(3) - System Security Plan | Plan / Coordinate With Other Organizational Entities

Requirement  SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

PL-2(3) What is the solution and how is it implemented?

Part a

Requirement  SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

PL-4 - Rules Of Behavior

Requirement  RULES OF BEHAVIOR Control: The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; b. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and
the information system; c. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and d. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

PL-4 What is the solution and how is it implemented?

Part a

Requirement RULES OF BEHAVIOR Control: The organization: a. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-18;</td>
</tr>
</tbody>
</table>

Part b

Requirement

2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-18;</td>
</tr>
</tbody>
</table>

Part c

Requirement

3. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-18;</td>
</tr>
</tbody>
</table>
Part d

Requirement

4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-18;

PL-4(1) - Rules Of Behavior | Social Media And Networking Restrictions

Requirement RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PL-4(1) What is the solution and how is it implemented?

Part a

Requirement RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS
The organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Role Organization
Status Inherited
Details Dependent on implementing organization.

PS-1 - Personnel Security Policy And Procedures

Requirement PERSONNEL SECURITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and b. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and 2. Personnel security procedures [Assignment: organization-defined frequency].
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

PS-1 What is the solution and how is it implemented?

Part a

Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part b

Requirement
2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part c

Requirement
2. Reviews and updates the current: 1. Personnel security policy [Assignment: organization-defined frequency]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>
Part d

Requirement
2. Personnel security procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

PS-2 - Position Risk Designation

Requirement POSITION RISK DESIGNATION Control: The organization: a. Assigns a risk designation to all organizational positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and updates position risk designations [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PS-2 What is the solution and how is it implemented?

Part a

Requirement POSITION RISK DESIGNATION Control: The organization: a. Assigns a risk designation to all organizational positions;

Role Organization
Status Inherited
Details Dependent on implementing organization.
References 5 C.F.R. 731.106(a);

Part b

Requirement
2. Establishes screening criteria for individuals filling those positions; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References 5 C.F.R. 731.106(a);
Part c

Requirement
3. Reviews and updates position risk designations [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References 5 C.F.R. 731.106(a);

PS-3 - Personnel Screening

Requirement PERSONNEL SCREENING Control: The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PS-3 What is the solution and how is it implemented?

Part a

Requirement PERSONNEL SCREENING Control: The organization: a. Screens individuals prior to authorizing access to the information system; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References 5 C.F.R. 731.106; FIPS Pub 199; FIPS Pub 201; SP 800-60; SP 800-73; SP 800-76; SP 800-78; ICD 704;

Part b

Requirement
2. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

Role Organization
Status Inherited
Details Dependent on implementing organization.
PS-4 - Personnel Termination

Requirement PERSONNEL TERMINATION Control: The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period]; b. Terminates/revokes any authenticators/credentials associated with the individual; c. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieves all security-related organizational information system-related property; e. Retains access to organizational information and information systems formerly controlled by terminated individual; and f. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

PS-4 What is the solution and how is it implemented?

Part a

Requirement PERSONNEL TERMINATION Control: The organization, upon termination of individual employment: a. Disables information system access within [Assignment: organization-defined time period];

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part b

Requirement
2. Terminates/revokes any authenticators/credentials associated with the individual;

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part c

Requirement
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];

References 5 C.F.R. 731.106; FIPS Pub 199; FIPS Pub 201; SP 800-60; SP 800-73; SP 800-76; SP 800-78; ICD 704;
Role Organization
Status Inherited
Details Dependent on implementing organization.

Part d

Requirement
4. Retrieves all security-related organizational information system-related property;

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part e

Requirement
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part f

Requirement
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Role Organization
Status Inherited
Details Dependent on implementing organization.

PS-4(2) - Personnel Termination | Automated Notification

Requirement PERSONNEL TERMINATION | AUTOMATED NOTIFICATION The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
PS-4(2) What is the solution and how is it implemented?

Part a

**Requirement** PERSONNEL TERMINATION | AUTOMATED NOTIFICATION The organization employs automated mechanisms to notify [Assignment: organization-defined personnel or roles] upon termination of an individual.

- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

PS-5 - Personnel Transfer

**Requirement** PERSONNEL TRANSFER Control: The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Control Summary Information

- **Role** Organization
- **Status** Inherited
- **Origin** Inherited from pre-existing ATO

PS-5 What is the solution and how is it implemented?

Part a

**Requirement** PERSONNEL TRANSFER Control: The organization: a. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;

- **Role** Organization
- **Status** Inherited
- **Details** Dependent on implementing organization.

Part b

**Requirement**

2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
Part c

Requirement

3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part d

Requirement

4. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

Role Organization
Status Inherited
Details Dependent on implementing organization.

PS-6 - Access Agreements

Requirement ACCESS AGREEMENTS Control: The organization: a. Develops and documents access agreements for organizational information systems; b. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and c. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO
PS-6 What is the solution and how is it implemented?

Part a

Requirement ACCESS AGREEMENTS Control: The organization: a. Develops and documents access agreements for organizational information systems;

Role Organization

Status Inherited

Details Dependent on implementing organization.

Part b

Requirement

2. Reviews and updates the access agreements [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

Part c

Requirement

3. Ensures that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

Part d

Requirement

2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Dependent on implementing organization.

PS-7 - Third-party Personnel Security

Requirement THIRD-PARTY PERSONNEL SECURITY Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires
third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and e. Monitors provider compliance.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

PS-7 What is the solution and how is it implemented?

Part a

Requirement THIRD-PARTY PERSONNEL SECURITY Control: The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-35;</td>
</tr>
</tbody>
</table>

Part b

Requirement

2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-35;</td>
</tr>
</tbody>
</table>

Part c

Requirement

3. Documents personnel security requirements;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-35;</td>
</tr>
</tbody>
</table>
Part d

Requirement

4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [Assignment: organization-defined time period]; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-35;

Part e

Requirement

5. Monitors provider compliance.

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-35;

PS-8 - Personnel Sanctions

Requirement  PERSONNEL SANCTIONS Control: The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

PS-8 What is the solution and how is it implemented?

Part a

Requirement  PERSONNEL SANCTIONS Control: The organization: a. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.

Part b

Requirement

2. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.

RA-1 - Risk Assessment Policy And Procedures

Requirement  RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].

Control Summary Information

Role  OpenShift Tenant
Status  Not implemented
Origin  Tenant SSP

RA-1 What is the solution and how is it implemented?

Part a

Requirement  RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  OpenShift Tenant
Status  Not implemented
Details  Documented in the individual project / program’s System Security Plan.
References  SP 800-12; SP 800-30; SP 800-100;
Part b

Requirement

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-12; SP 800-30; SP 800-100;

Part c

Requirement

2. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-12; SP 800-30; SP 800-100;

Part d

Requirement

2. Risk assessment procedures [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-12; SP 800-30; SP 800-100;

RA-2 - Security Categorization

Requirement SECURITY CATEGORIZATION Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

RA-2 What is the solution and how is it implemented?

Part a

Requirement SECURITY CATEGORIZATION Control: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>FIPS Pub 199; SP 800-30; SP 800-39; SP 800-60;</td>
</tr>
</tbody>
</table>

Part b

Requirement

2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>FIPS Pub 199; SP 800-30; SP 800-39; SP 800-60;</td>
</tr>
</tbody>
</table>

Part c

Requirement

3. Ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>FIPS Pub 199; SP 800-30; SP 800-39; SP 800-60;</td>
</tr>
</tbody>
</table>
RA-3 - Risk Assessment

Requirement RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Summary Information

Role OpenShift Tenant
Status Not implemented
Origin Tenant SSP

RA-3 What is the solution and how is it implemented?

Part a

Requirement RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

Role OpenShift Tenant
Status Not implemented
Details Documented in the individual project / program’s System Security Plan.
References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part b

Requirement

2. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

Role OpenShift Tenant
Status Not implemented
Details Documented in the individual project / program’s System Security Plan.
References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;
Part c

**Requirement**
3. Reviews risk assessment results [Assignment: organization-defined frequency];

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Security Plan.

**References** OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part d

**Requirement**
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Security Plan.

**References** OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part e

**Requirement**
5. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

**RA-5 - Vulnerability Scanning**

**Requirement** VULNERABILITY SCANNING Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the
vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Control Summary Information

**Role**  Organization

**Status**  Inherited

**Origin**  Inherited from pre-existing ATO

**RA-5 What is the solution and how is it implemented?**

**Part a**

**Requirement**  VULNERABILITY SCANNING Control: The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

**Role**  Organization

**Status**  Inherited

**Details**  Dependent on implementing organization.

**References**  SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;

**Part b**

**Requirement**

2. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations;

**Role**  Organization

**Status**  Inherited

**Details**  Dependent on implementing organization.

**References**  SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;

**Part c**

**Requirement**

2. Formatting checklists and test procedures; and

**Role**  Organization

**Status**  Inherited

**Details**  Dependent on implementing organization.

**References**  SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;
Part d

**Requirement**

3. Measuring vulnerability impact;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;

Part e

**Requirement**

3. Analyzes vulnerability scan reports and results from security control assessments;

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;

Part f

**Requirement**

4. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and

**Role** OpenShift Landlord

**Status** Planned

**Details** Documented in the POAM created as a result of vulnerability scanning.

**References** SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;

Part g

**Requirement**

5. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-40; SP 800-70; SP 800-115; Web: cwe.mitre.org, nvd.nist.gov;
SA-1 - System And Services Acquisition Policy And Procedures

Requirement  SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and b. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and 2. System and services acquisition procedures [Assignment: organization-defined frequency].

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

SA-1 What is the solution and how is it implemented?

Part a

Requirement  SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-12; SP 800-100;

Part b

Requirement

2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-12; SP 800-100;
Part c

Requirement
2. Reviews and updates the current: 1. System and services acquisition policy [Assignment: organization-defined frequency]; and

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-12; SP 800-100;

Part d

Requirement
2. System and services acquisition procedures [Assignment: organization-defined frequency].

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-12; SP 800-100;

SA-11 - Developer Security Testing And Evaluation

Requirement DEVELOPER SECURITY TESTING AND EVALUATION Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

SA-11 What is the solution and how is it implemented?

Part a

Requirement DEVELOPER SECURITY TESTING AND EVALUATION Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan;

Role Organization
Status  Inherited
Details  Documented in the project’s System Test Plan.
References  ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part b

Requirement
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at
[Assignment: organization-defined depth and coverage];

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part c

Requirement
3. Produce evidence of the execution of the security assessment plan and the results of the security
testing/evaluation;

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part d

Requirement
4. Implement a verifiable flaw remediation process; and

Role  OpenShift Landlord, OpenShift Tenant
Status  Planned
Details  Documented in the POAM created as a result of vulnerability scanning.
References  ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part e

Requirement
5. Correct flaws identified during security testing/evaluation.

Role  OpenShift Landlord, OpenShift Tenant
**SA-16 - Developer-provided Training**

**Requirement** DEVELOPER-PROVIDED TRAINING Control: The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

**Control Summary Information**

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Origin**: OpenShift Landlord SSP

**SA-16 What is the solution and how is it implemented?**

**Part a**

**Requirement** DEVELOPER-PROVIDED TRAINING Control: The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Details**: NEED TO ADDRESS

**SA-17 - Developer Security Architecture And Design**

**Requirement** DEVELOPER SECURITY ARCHITECTURE AND DESIGN Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture; b. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and c. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.
Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

SA-17 What is the solution and how is it implemented?

Part a

Requirement DEVELOPER SECURITY ARCHITECTURE AND DESIGN Control: The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: a. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part b

Requirement

2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part c

Requirement

3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

SA-2 - Allocation Of Resources

Requirement ALLOCATION OF RESOURCES Control: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment
control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

SA-2 What is the solution and how is it implemented?

Part a

**Requirement** ALLOCATION OF RESOURCES Control: The organization: a. Determines information security requirements for the information system or information system service in mission/business process planning;

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-65;</td>
</tr>
</tbody>
</table>

Part b

**Requirement**

2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-65;</td>
</tr>
</tbody>
</table>

Part c

**Requirement**

3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-65;</td>
</tr>
</tbody>
</table>
SA-3 - System Development Life Cycle

**Requirement** SYSTEM DEVELOPMENT LIFE CYCLE Control: The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>Tenant SSP</td>
</tr>
</tbody>
</table>

**SA-3 What is the solution and how is it implemented?**

**Part a**

**Requirement** SYSTEM DEVELOPMENT LIFE CYCLE Control: The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-37; SP 800-64;</td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Defines and documents information security roles and responsibilities throughout the system development life cycle;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-37; SP 800-64;</td>
</tr>
</tbody>
</table>

**Part c**

**Requirement**

3. Identifies individuals having information security roles and responsibilities; and

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
</tbody>
</table>
Details  Documented in the individual project / program’s System Security Plan.

References  SP 800-37; SP 800-64;

Part d

Requirement

4. Integrates the organizational information security risk management process into system development life cycle activities.

Role  OpenShift Tenant

Status  Not implemented

Details  Documented in the individual project / program’s System Security Plan.

References  SP 800-37; SP 800-64;

SA-4 - Acquisition Process

Requirement  ACQUISITION PROCESS Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements; b. Security strength requirements; c. Security assurance requirements; d. Security-related documentation requirements; e. Requirements for protecting security-related documentation; f. Description of the information system development environment and environment in which the system is intended to operate; and g. Acceptance criteria.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

SA-4 What is the solution and how is it implemented?

Part a

Requirement  ACQUISITION PROCESS Control: The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs: a. Security functional requirements;

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.
Part b

Requirement

2. Security strength requirements;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References HSPD-12; ISO/IEC 15408; FIPS Pub 140-2; FIPS Pub 201; SP 800-23; SP 800-35; SP 800-36; SP 800-37; SP 800-64; SP 800-70; SP 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far;

Part c

Requirement

3. Security assurance requirements;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References HSPD-12; ISO/IEC 15408; FIPS Pub 140-2; FIPS Pub 201; SP 800-23; SP 800-35; SP 800-36; SP 800-37; SP 800-64; SP 800-70; SP 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far;

Part d

Requirement

4. Security-related documentation requirements;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References HSPD-12; ISO/IEC 15408; FIPS Pub 140-2; FIPS Pub 201; SP 800-23; SP 800-35; SP 800-36; SP 800-37; SP 800-64; SP 800-70; SP 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far;

Part e

Requirement

5. Requirements for protecting security-related documentation;

Role Organization
OpenShift Compliance Guide, Release 1.0 beta

**Part f**

**Requirement**

6. Description of the information system development environment and environment in which the system is intended to operate; and

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** HSPD-12; ISO/IEC 15408; FIPS Pub 140-2; FIPS Pub 201; SP 800-23; SP 800-35; SP 800-36; SP 800-37; SP 800-64; SP 800-70; SP 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far;

---

**Part g**

**Requirement**

7. Acceptance criteria.

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** HSPD-12; ISO/IEC 15408; FIPS Pub 140-2; FIPS Pub 201; SP 800-23; SP 800-35; SP 800-36; SP 800-37; SP 800-64; SP 800-70; SP 800-137; Federal Acquisition Regulation; Web: www.niap-ccevs.org, fips201ep.cio.gov, www.acquisition.gov/far;

---

**SA-4(1) - Acquisition Process | Functional Properties Of Security Controls**

**Requirement** ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

**Control Summary Information**

**Role** OpenShift Tenant

**Status** Not implemented

**Origin** Tenant SSP
SA-4(1) What is the solution and how is it implemented?

Part a

Requirement  ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Role  OpenShift Tenant

Status  Not implemented

Details  Documented in the individual project / program’s System Design Specification document and System Security Plan.

SA-4(10) - Acquisition Process | Use Of Approved Piv Products

Requirement  ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS
The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO

SA-4(10) What is the solution and how is it implemented?

Part a

Requirement  ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS
The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

SA-4(2) - Acquisition Process | Design / Implementation Information For Security Controls

Requirement  ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS
The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external
Control Summary Information

**Role**  OpenShift Tenant  
**Status**  Not implemented  
**Origin**  Tenant SSP

**SA-4(2) What is the solution and how is it implemented?**

**Part a**

**Requirement**  ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].  
**Role**  OpenShift Tenant  
**Status**  Not implemented  
**Details**  Documented in the individual project / program’s System Design Specification document and System Security Plan.

**SA-5 - Information System Documentation**

**Requirement**  INFORMATION SYSTEM DOCUMENTATION Control: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; b. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and 3. User responsibilities in maintaining the security of the system, component, or service; c. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response; d. Protects documentation as required, in accordance with the risk management strategy; and e. Distributes documentation to [Assignment: organization-defined personnel or roles].

Control Summary Information

**Role**  OpenShift Landlord  
**Status**  Implemented
Origin  
OpenShift Landlord SSP

SA-5 What is the solution and how is it implemented?

Part a

Requirement  
INFORMATION SYSTEM DOCUMENTATION Control: The organization: a. Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service;

Role  OpenShift Landlord

Status  Implemented

Details  Documentation available from the OSE vendor, Red Hat.

Part b

Requirement  
2. Effective use and maintenance of security functions/mechanisms; and

Role  OpenShift Landlord

Status  Implemented

Details  Documentation available from the OSE vendor, Red Hat.

Part c

Requirement  
3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

Part d

Requirement  
2. Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;

Role  OpenShift Landlord

Status  Implemented

Details  Documentation available from the OSE vendor, Red Hat.
Part e

Requirement

2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part f

Requirement

3. User responsibilities in maintaining the security of the system, component, or service;

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part g

Requirement

3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

Part h

Requirement

4. Protects documentation as required, in accordance with the risk management strategy; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

Part i

Requirement

5. Distributes documentation to [Assignment: organization-defined personnel or roles].

Role Organization
Status Inherited
Dependent on implementing organization.

SA-9 - External Information System Services

Requirement EXTERNAL INFORMATION SYSTEM SERVICES Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

Control Summary Information

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-35;

SA-9 What is the solution and how is it implemented?

Part a

Requirement EXTERNAL INFORMATION SYSTEM SERVICES Control: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-35;

Part b

Requirement

2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

Role Organization
Status Inherited
Details Dependent on implementing organization.

References SP 800-35;
Part c

Requirement
3. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-35;

SC-1 - System And Communications Protection Policy And Procedures

Requirement SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and b. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and 2. System and communications protection procedures [Assignment: organization-defined frequency].

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

SC-1 What is the solution and how is it implemented?

Part a

Requirement SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;
Part b

Requirement
2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

Part c

Requirement
2. Reviews and updates the current: 1. System and communications protection policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

Part d

Requirement
2. System and communications protection procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

SC-10 - Network Disconnect

Requirement NETWORK DISCONNECT Control: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP
SC-10 What is the solution and how is it implemented?

Part a

**Requirement** NETWORK DISCONNECT Control: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

**Role** OpenShift Landlord

**Status** Planned

**Details** NEED TO ADDRESS

SC-12 - Cryptographic Key Establishment And Management

**Requirement** CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

Control Summary Information

**Role** Organization

**Status** Inherited

**Origin** Inherited from pre-existing ATO

SC-12 What is the solution and how is it implemented?

Part a

**Requirement** CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

**Role** Organization

**Status** Inherited

**Details** Dependent on implementing organization.

**References** SP 800-56; SP 800-57;

SC-12(1) - Cryptographic Key Establishment And Management | Availability

**Requirement** CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY The organization maintains availability of information in the event of the loss of cryptographic keys by users.
Control Summary Information

**Role** Organization, OpenShift Landlord  
**Status** Implemented  
**Origin** OpenShift Landlord SSP

**SC-12(1) What is the solution and how is it implemented?**

**Part a**

**Requirement** CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY The organization maintains availability of information in the event of the loss of cryptographic keys by users.

**Role** Organization, OpenShift Landlord  
**Status** Implemented  
**Details** Inherited from the organizational user directory

**SC-13 - Cryptographic Protection**

**Requirement** CRYPTOGRAPHIC PROTECTION Control: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Control Summary Information

**Role** Organization  
**Status** Inherited  
**Origin** Inherited from pre-existing ATO

**SC-13 What is the solution and how is it implemented?**

**Part a**

**Requirement** CRYPTOGRAPHIC PROTECTION Control: The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**Role** Organization  
**Status** Inherited  
**Details** Dependent on implementing organization.  
**References** FIPS Pub 140-2; Web: csrc.nist.gov/cryptval, www.cnss.gov;
SC-15 - Collaborative Computing Devices

**Requirement**  COLLABORATIVE COMPUTING DEVICES Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**SC-15 What is the solution and how is it implemented?**

**Part a**

**Requirement**  COLLABORATIVE COMPUTING DEVICES Control: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Provides an explicit indication of use to users physically present at the devices.

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>NEED TO ADDRESS</td>
</tr>
</tbody>
</table>

**SC-2 - Application Partitioning**

**Requirement**  APPLICATION PARTITIONING Control: The information system separates user functionality (including user interface services) from information system management functionality.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Landlord</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Landlord SSP</td>
</tr>
</tbody>
</table>
SC-2 What is the solution and how is it implemented?

Part a

Requirement  APPLICATION PARTITIONING  Control: The information system separates user functionality (including user interface services) from information system management functionality.

Role  OpenShift Landlord
Status  Planned
Details  NEED TO ADDRESS

SC-20 - Secure Name / Address Resolution Service (authoritative Source)

Requirement  SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)  Control: The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Control Summary Information

Role  Organization
Status  Inherited
Origin  Inherited from pre-existing ATO

SC-20 What is the solution and how is it implemented?

Part a

Requirement  SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)  Control: The information system: a. Provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

Role  Organization
Status  Inherited
Details  undefined
References  OMB M-08-23; SP 800-81;

Part b

Requirement
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
<tr>
<td>References</td>
<td>OMB M-08-23; SP 800-81;</td>
</tr>
</tbody>
</table>

**SC-21 - Secure Name / Address Resolution Service (recursive Or Caching Resolver)**

**Requirement** SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

**SC-21 What is the solution and how is it implemented?**

**Part a**

**Requirement** SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) Control: The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-81;</td>
</tr>
</tbody>
</table>

**SC-22 - Architecture And Provisioning For Name / Address Resolution Service**

**Requirement** ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.
Control Summary Information

**Role** OpenShift Landlord  
**Status** Not implemented  
**Origin** OpenShift Landlord SSP

**SC-22 What is the solution and how is it implemented?**

**Part a**

**Requirement** ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

**Role** OpenShift Landlord  
**Status** Not implemented  
**Details** OSE systems are clients of DNS services and do not provide name resolution capabilities.  
**References** SP 800-81;

**SC-24 - Fail In Known State**


**Control Summary Information**

**Role** OpenShift Landlord  
**Status** Planned  
**Origin** OpenShift Landlord SSP

**SC-24 What is the solution and how is it implemented?**

**Part a**


**Role** OpenShift Landlord  
**Status** Planned  
**Details** NEED TO ADDRESS
SC-3 - Security Function Isolation

Requirement SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from nonsecurity functions.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

SC-3 What is the solution and how is it implemented?

Part a

Requirement SECURITY FUNCTION ISOLATION Control: The information system isolates security functions from nonsecurity functions.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

SC-39 - Process Isolation

Requirement PROCESS ISOLATION Control: The information system maintains a separate execution domain for each executing process.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

SC-39 What is the solution and how is it implemented?

Part a

Requirement PROCESS ISOLATION Control: The information system maintains a separate execution domain for each executing process.

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
**SC-4 - Information In Shared Resources**

**Requirement** INFORMATION IN SHARED RESOURCES Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

**Control Summary Information**

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Origin**: OpenShift Landlord SSP

**SC-4 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION IN SHARED RESOURCES Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

- **Role**: OpenShift Landlord
- **Status**: Planned
- **Details**: NEED TO ADDRESS

**SC-42 - Sensor Capability And Data**

**Requirement** SENSOR CAPABILITY AND DATA Control: The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

**Control Summary Information**

- **Role**: IaaS
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

**SC-42 What is the solution and how is it implemented?**

**Part a**

**Requirement** SENSOR CAPABILITY AND DATA Control: The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and

- **Role**: IaaS
- **Status**: Inherited
Details  Implemented by IaaS provider, OpenShift does not need access to the underlying hardware

Part b

Requirement

2. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users].

Role  IaaS

Status  Inherited

Details  Implemented by IaaS provider, OpenShift does not need access to the underlying hardware

SC-42(3) - Sensor Capability And Data | Prohibit Use Of Devices

Requirement  SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES The organization prohibits the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems].

Control Summary Information

Role  IaaS

Status  Inherited

Origin  Inherited from pre-existing ATO

SC-42(3) What is the solution and how is it implemented?

Part a

Requirement  SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES The organization prohibits the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems].

Role  IaaS

Status  Inherited

Details  Implemented by IaaS provider, OpenShift does not need access to the underlying hardware

SC-5 - Denial Of Service Protection

Requirement  DENIAL OF SERVICE PROTECTION Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].
Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

SC-5 What is the solution and how is it implemented?

Part a

Requirement DENIAL OF SERVICE PROTECTION Control: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS

SC-7 - Boundary Protection

Requirement BOUNDARY PROTECTION Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Control Summary Information

Role OpenShift Landlord
Status Planned
Origin OpenShift Landlord SSP

SC-7 What is the solution and how is it implemented?

Part a

Requirement BOUNDARY PROTECTION Control: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system;

Role OpenShift Landlord
Status Planned
Details NEED TO ADDRESS
References FIPS Pub 199; SP 800-41; SP 800-77;
Part b

Requirement

2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  FIPS Pub 199; SP 800-41; SP 800-77;

Part c

Requirement

3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS

References  FIPS Pub 199; SP 800-41; SP 800-77;

SC-7(18) - Boundary Protection | Fail Secure

Requirement  BOUNDARY PROTECTION | FAIL SECURE The information system fails securely in the event of an operational failure of a boundary protection device.

Control Summary Information

Role  OpenShift Landlord

Status  Planned

Origin  OpenShift Landlord SSP

SC-7(18) What is the solution and how is it implemented?

Part a

Requirement  BOUNDARY PROTECTION | FAIL SECURE The information system fails securely in the event of an operational failure of a boundary protection device.

Role  OpenShift Landlord

Status  Planned

Details  NEED TO ADDRESS
SC-7(21) - Boundary Protection | Isolation Of Information System Components

**Requirement** BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Origin</td>
<td>Inherited from pre-existing ATO</td>
</tr>
</tbody>
</table>

SC-7(21) What is the solution and how is it implemented?

Part a

**Requirement** BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined missions and/or business functions].

<table>
<thead>
<tr>
<th>Role</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Inherited</td>
</tr>
<tr>
<td>Details</td>
<td>Dependent on implementing organization.</td>
</tr>
</tbody>
</table>

SE-1 - Inventory Of Personally Identifiable Information

**Requirement** INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Origin</td>
<td>OpenShift Tenant SSP</td>
</tr>
</tbody>
</table>
SE-1 What is the solution and how is it implemented?

Part a

Requirement  INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION  Control: The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Pub 199; SP 800-37; SP 800-122;

Part b

Requirement

2. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Pub 199; SP 800-37; SP 800-122;

SE-2 - Privacy Incident Response

Requirement  PRIVACY INCIDENT RESPONSE  Control: The organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Control Summary Information

Role  Organization

Status  Inherited

Origin  Inherited from pre-existing ATO
SE-2 What is the solution and how is it implemented?

Part a

Requirement PRIVACY INCIDENT RESPONSE Control: The organization: a. Develops and implements a Privacy Incident Response Plan; and

Role Organization
Status Inherited
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB M-06-19; OMB M-07-16; SP 800-37;

Part b

Requirement
2. Provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan.

Role Organization
Status Inherited
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m); Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541; OMB M-06-19; OMB M-07-16; SP 800-37;

SI-1 - System And Information Integrity Policy And Procedures

Requirement SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].

Control Summary Information

Role OpenShift Tenant
Status Not implemented
Origin Tenant SSP
SI-1 What is the solution and how is it implemented?

Part a

Requirement  SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control:
The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  OpenShift Tenant

Status  Not implemented

Details  Documented in the individual project / program’s System Design Specification document and System Security Plan.

References  SP 800-12; SP 800-100;

Part b

Requirement

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

Role  Shared

Status  Shared

Details  Documented in the individual project / program’s System Design Specification document and System Security Plan.

References  SP 800-12; SP 800-100;

Part c

Requirement

2. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and

Role  Shared

Status  Shared

Details  Documented in the individual project / program’s System Design Specification document and System Security Plan.

References  SP 800-12; SP 800-100;

Part d

Requirement

2. System and information integrity procedures [Assignment: organization-defined frequency].

Role  Shared

Status  Shared
Details Documented in the individual project / program’s System Design Specification document and System Security Plan.

References SP 800-12; SP 800-100;

SI-12 - Information Handling And Retention

Requirement INFORMATION HANDLING AND RETENTION Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Control Summary Information

Role Organization
Status Inherited
Origin Inherited from pre-existing ATO

SI-12 What is the solution and how is it implemented?

Part a

Requirement INFORMATION HANDLING AND RETENTION Control: The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Role Organization
Status Inherited
Details Dependent on implementing organization.

SI-16 - Memory Protection

Requirement MEMORY PROTECTION Control: The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP
SI-16 What is the solution and how is it implemented?

Part a

Requirement MEMORY PROTECTION Control: The information system implements [Assignment: organization-defined security safeguards] to protect its memory from unauthorized code execution.

Role OpenShift Landlord
Status Implemented
Details undefined

SI-2 - Flaw Remediation

Requirement FLAW REMEDIATION Control: The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporates flaw remediation into the organizational configuration management process.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

SI-2 What is the solution and how is it implemented?

Part a

Requirement FLAW REMEDIATION Control: The organization: a. Identifies, reports, and corrects information system flaws;

Role OpenShift Landlord
Status Implemented
Details undefined

References SP 800-40; SP 800-128;

Part b

Requirement

2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40; SP 800-128;

Part c

Requirement

3. Installs security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40; SP 800-128;

Part d

Requirement

4. Incorporates flaw remediation into the organizational configuration management process.

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40; SP 800-128;

SI-3 - Malicious Code Protection

Requirement MALICIOUS CODE PROTECTION Control: The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP
SI-3 What is the solution and how is it implemented?

Part a

**Requirement** MALICIOUS CODE PROTECTION Control: The organization: 

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;

**Role** OpenShift Landlord

**Status** Implemented

**Details** undefined

**References** SP 800-83;

Part b

**Requirement**

2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;

**Role** OpenShift Landlord

**Status** Implemented

**Details** undefined

**References** SP 800-83;

Part c

**Requirement**

3. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and

**Role** OpenShift Landlord

**Status** Implemented

**Details** undefined

**References** SP 800-83;

Part d

**Requirement**

2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and

**Role** OpenShift Landlord

**Status** Implemented

**Details** undefined
Part e

Requirement

4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Role OpenShift Landlord

Status Implemented

Details undefined

References SP 800-83;

SI-4 - Information System Monitoring

Requirement INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

SI-4 What is the solution and how is it implemented?

Part a

Requirement INFORMATION SYSTEM MONITORING Control: The organization: a. Monitors the information system to detect: 1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and

Role Organization
Part b

Requirement

2. Unauthorized local, network, and remote connections;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

Part c

Requirement

2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

Part d

Requirement

3. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

Part e

Requirement

4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

Role Organization

Status Inherited
Part f

Requirement

5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

Part g

Requirement

6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

Part h

Requirement

7. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-61; SP 800-83; SP 800-92; SP 800-94; SP 800-137;

SI-4(2) - Information System Monitoring | Automated Tools For Real-time Analysis

Requirement  INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS The organization employs automated tools to support near real-time analysis of events.
Control Summary Information

- **Role**: Organization
- **Status**: Inherited
- **Origin**: Inherited from pre-existing ATO

SI-4(2) What is the solution and how is it implemented?

**Part a**

**Requirement** INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS The organization employs automated tools to support near real-time analysis of events.

- **Role**: Organization
- **Status**: Inherited
- **Details**: Dependent on implementing organization.

SI-5 - Security Alerts, Advisories, And Directives

**Requirement** SECURITY ALERTS, ADVISORIES, AND DIRECTIVES Control: The organization:

a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;  
b. Generates internal security alerts, advisories, and directives as deemed necessary;  
c. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and  
d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Control Summary Information

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Origin**: OpenShift Landlord SSP

SI-5 What is the solution and how is it implemented?

**Part a**

**Requirement** SECURITY ALERTS, ADVISORIES, AND DIRECTIVES Control: The organization:

a. Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;

- **Role**: OpenShift Landlord
- **Status**: Implemented
- **Details**: undefined
- **References**: SP 800-40;
Part b

Requirement

2. Generates internal security alerts, advisories, and directives as deemed necessary;

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40;

Part c

Requirement

3. Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40;

Part d

Requirement

4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-40;

SI-5(1) - Security Alerts, Advisories, And Directives | Automated Alerts And Advisories

Requirement SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

Control Summary Information

Role Organization
Status Inherited
SI-5(1) What is the solution and how is it implemented?

Part a

**Requirement** SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

**Role** Organization

**Status** Inherited

**Details** undefined

SI-6 - Security Function Verification

**Requirement** SECURITY FUNCTION VERIFICATION Control: The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions]; b. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and d. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

Control Summary Information

**Role** OpenShift Landlord

**Status** Implemented

**Origin** OpenShift Landlord SSP

SI-6 What is the solution and how is it implemented?

Part a

**Requirement** SECURITY FUNCTION VERIFICATION Control: The information system: a. Verifies the correct operation of [Assignment: organization-defined security functions];

**Role** OpenShift Landlord

**Status** Implemented

**Details** Implemented with Ansible Tower CM and OpenSCAP scans

Part b

**Requirement**
2. Performs this verification [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];

Role OpenShift Landlord
Status Implemented
Details undefined

Part c

Requirement
3. Notifies [Assignment: organization-defined personnel or roles] of failed security verification tests; and

Role OpenShift Landlord
Status Implemented
Details undefined

Part d

Requirement
4. [Selection (one or more): shuts the information system down; restarts the information system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.

Role OpenShift Landlord
Status Implemented
Details undefined

SI-7 - Software, Firmware, And Information Integrity

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY Control: The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP
SI-7 What is the solution and how is it implemented?

Part a

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY Control: The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

Role OpenShift Landlord
Status Implemented
Details undefined
References SP 800-147; SP 800-155;

SI-7(1) - Software, Firmware, And Information Integrity | Integrity Checks

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

SI-7(1) What is the solution and how is it implemented?

Part a

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

Role OpenShift Landlord
Status Implemented
Details undefined
SI-7(2) - Software, Firmware, And Information Integrity | Automated Notifications Of Integrity Violations

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP

SI-7(2) What is the solution and how is it implemented?

Part a

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS The organization employs automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.

Role OpenShift Landlord
Status Implemented
Details undefined

SI-7(5) - Software, Firmware, And Information Integrity | Automated Response To Integrity Violations

Requirement SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.

Control Summary Information

Role OpenShift Landlord
Status Implemented
Origin OpenShift Landlord SSP
SI-7(5) What is the solution and how is it implemented?

Part a

Requirement  SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguards]] when integrity violations are discovered.

Role  OpenShift Landlord

Status  Implemented

Details  undefined

SI-7(7) - Software, Firmware, And Information Integrity | Integration Of Detection And Response

Requirement  SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

Control Summary Information

Role  OpenShift Landlord

Status  Implemented

Origin  OpenShift Landlord SSP

SI-7(7) What is the solution and how is it implemented?

Part a

Requirement  SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

Role  OpenShift Landlord

Status  Implemented

Details  undefined

SI-8 - Spam Protection

Requirement  SPAM PROTECTION Control: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and b. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
Control Summary Information

Role  OpenShift Landlord
Status  Implemented
Origin  OpenShift Landlord SSP

SI-8 What is the solution and how is it implemented?

Part a

Requirement  SPAM PROTECTION Control: The organization: a. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and

Role  OpenShift Landlord
Status  Implemented
Details  undefined
References  SP 800-45;

Part b

Requirement

2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Role  OpenShift Landlord
Status  Implemented
Details  undefined
References  SP 800-45;

SI-8(1) - Spam Protection | Central Management

Requirement  SPAM PROTECTION | CENTRAL MANAGEMENT The organization centrally manages spam protection mechanisms.

Control Summary Information

Role  OpenShift Landlord
Status  Implemented
Origin  OpenShift Landlord SSP
SI-8(1) What is the solution and how is it implemented?

Part a

Requirement SPAM PROTECTION | CENTRAL MANAGEMENT The organization centrally manages spam protection mechanisms.

Role OpenShift Landlord

Status Implemented

Details undefined

SI-8(2) - Spam Protection | Automatic Updates

Requirement SPAM PROTECTION | AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms.

Control Summary Information

Role OpenShift Landlord

Status Implemented

Origin OpenShift Landlord SSP

SI-8(2) What is the solution and how is it implemented?

Part a

Requirement SPAM PROTECTION | AUTOMATIC UPDATES The information system automatically updates spam protection mechanisms.

Role OpenShift Landlord

Status Implemented

Details undefined

TR-1 - Privacy Notice

Requirement PRIVACY NOTICE Control: The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to
reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Control Summary Information

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Origin**: OpenShift Tenant SSP

**TR-1 What is the solution and how is it implemented?**

**Part a**

**Requirement** PRIVACY NOTICE Control: The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16; OMB M-10-22; OMB M-10-23; ISE Privacy Guidelines;

**Part b**

**Requirement**

2. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16; OMB M-10-22; OMB M-10-23; ISE Privacy Guidelines;
Part c

Requirement
3. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16; OMB M-10-22; OMB M-10-23; ISE Privacy Guidelines;

TR-1(1) - Privacy Notice | Real-time Or Layered Notice

Requirement PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE The organization provides real-time and/or layered notice when it collects PII.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

TR-1(1) What is the solution and how is it implemented?

Part a

Requirement PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE The organization provides real-time and/or layered notice when it collects PII.

Role OpenShift Tenant
Status Planned
Details undefined

TR-2 - System Of Records Notices And Privacy Act Statements

Requirement SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS Control: The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.
Control Summary Information

Role  OpenShift Tenant
Status  Planned
Origin  OpenShift Tenant SSP

TR-2 What is the solution and how is it implemented?

Part a

Requirement  SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS Control: The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

Role  OpenShift Tenant
Status  Planned
Details  undefined
References  The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;

Part b

Requirement
2. Keeps SORNs current; and

Role  OpenShift Tenant
Status  Planned
Details  undefined
References  The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;

Part c

Requirement
3. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Role  OpenShift Tenant
Status  Planned
Details  undefined
References  The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;
TR-2(1) - System Of Records Notices And Privacy Act Statements | Public Website Publication

Requirement SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION The organization publishes SORNs on its public website.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

TR-2(1) What is the solution and how is it implemented?

Part a

Requirement SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION The organization publishes SORNs on its public website.

Role OpenShift Tenant
Status Planned
Details undefined

TR-3 - Dissemination Of Privacy Program Information

Requirement DISSEMINATION OF PRIVACY PROGRAM INFORMATION Control: The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

TR-3 What is the solution and how is it implemented?

Part a

Requirement DISSEMINATION OF PRIVACY PROGRAM INFORMATION Control: The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and
Role: OpenShift Tenant
Status: Planned
Details: undefined

Part b

Requirement
2. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Role: OpenShift Tenant
Status: Planned
Details: undefined

UL-1 - Internal Use

Requirement INTERNAL USE Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Control Summary Information

Role: OpenShift Tenant
Status: Planned
Origin: OpenShift Tenant SSP

UL-1 What is the solution and how is it implemented?

Part a

Requirement INTERNAL USE Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Role: OpenShift Tenant
Status: Planned
Details: undefined
References: The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1);
UL-2 - Information Sharing With Third Parties

**Requirement** INFORMATION SHARING WITH THIRD PARTIES Control: The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

**Control Summary Information**

- **Role** OpenShift Tenant
- **Status** Planned
- **Origin** OpenShift Tenant SSP

**UL-2 What is the solution and how is it implemented?**

**Part a**

**Requirement** INFORMATION SHARING WITH THIRD PARTIES Control: The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

- **Role** OpenShift Tenant
- **Status** Planned
- **Details** undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;

**Part b**

- **Requirement**

  2. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

- **Role** OpenShift Tenant
- **Status** Planned
- **Details** undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;
Part c

Requirement

3. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

Role  OpenShift Tenant
Status  Planned
Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;

Part d

Requirement

4. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Role  OpenShift Tenant
Status  Planned
Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;
Overview

The following controls have been down-selected from the complete list in *Security Controls*.

Procedural Generation

Like the last chapter, this chapter is automatically generated from the `master_sctm.xlsx` spreadsheet on this project’s GitHub. Do not edit it directly. If you’d like to change how this chapter is rendered, refer to the following:

<table>
<thead>
<tr>
<th>File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>master_sctm_parser.py</code></td>
<td>Python program that parses the <code>master_sctm.xlsx</code> spreadsheet using the openpyxl module. When editing this sheet do not change the existing column headers. Column order does not matter. New columns can be added. Only visible rows are processed, so auto-filters can be used to modify which controls are rendered.</td>
</tr>
<tr>
<td><code>security_control.j2</code></td>
<td>Jinja2 template that is used to render this chapter.</td>
</tr>
<tr>
<td><code>crm.j2</code></td>
<td>Jinja2 template that is used to generate the <em>Customer Responsibility Matrix</em>.</td>
</tr>
</tbody>
</table>

CM-8(4) - Information System Component Inventory | Accountability Information

**Requirement** INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.
Control Summary Information

Role  OpenShift Tenant
Status  Planned
Origin  OpenShift Tenant SSP

CM-8(4) What is the solution and how is it implemented?

Part a

Requirement  INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION
The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible/accountable for administering those components.

Role  OpenShift Tenant
Status  Planned
Details  Specified in the individual project / program’s System Security Plan.

CP-10(2) - Information System Recovery And Reconstitution | Transaction Recovery

Requirement  INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY
The information system implements transaction recovery for systems that are transaction-based.

Control Summary Information

Role  OpenShift Tenant
Status  Planned
Origin  Tenant SSP

CP-10(2) What is the solution and how is it implemented?

Part a

Requirement  INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY
The information system implements transaction recovery for systems that are transaction-based.

Role  OpenShift Tenant
Status  Planned
Details  undefined
DI-1 - Data Quality

**Requirement** DATA QUALITY Control: The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; b. Collects PII directly from the individual to the greatest extent practicable; c. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and d. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

**Control Summary Information**

- **Role**: OpenShift Tenant
- **Status**: Planned
- **Origin**: OpenShift Tenant SSP

**DI-1 What is the solution and how is it implemented?**

**Part a**

- **Requirement** DATA QUALITY Control: The organization: a. Confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information;
- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;

**Part b**

- **Requirement**
  2. Collects PII directly from the individual to the greatest extent practicable;
- **Role**: OpenShift Tenant
- **Status**: Planned
- **Details**: undefined
- **References** The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;
Part c

Requirement
3. Checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems [Assignment: organization-defined frequency]; and

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;

Part d

Requirement
4. Issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Role OpenShift Tenant
Status Planned
Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e); Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4; Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001); OMB M-07-16;

DI-1(1) - Data Quality | Validate PII

Requirement DATA QUALITY | VALIDATE PII The organization requests that the individual or individual’s authorized representative validate PII during the collection process.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

DI-1(1) What is the solution and how is it implemented?
Part a

**Requirement** DATA QUALITY | VALIDATE PII The organization requests that the individual or individual’s authorized representative validate PII during the collection process.

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**DI-1(2) - Data Quality | Re-validate Pii**

**Requirement** DATA QUALITY | RE-VALIDATE PII The organization requests that the individual or individual’s authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].

**Control Summary Information**

**Role** OpenShift Tenant

**Status** Planned

**Origin** OpenShift Tenant SSP

**DI-1(2) What is the solution and how is it implemented?**

Part a

**Requirement** DATA QUALITY | RE-VALIDATE PII The organization requests that the individual or individual’s authorized representative revalidate that PII collected is still accurate [Assignment: organization-defined frequency].

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**DI-2 - Data Integrity And Data Integrity Board**

**Requirement** DATA INTEGRITY AND DATA INTEGRITY BOARD Control: The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and b. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

**Control Summary Information**

**Role** OpenShift Tenant

**Status** Planned
DI-2 What is the solution and how is it implemented?

Part a

Requirement DATA INTEGRITY AND DATA INTEGRITY BOARD Control: The organization: a. Documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I;

Part b

Requirement

2. Establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

Role Organization

Status Inherited

Details undefined

References The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u); OMB Circular A-130, Appendix I;

DM-1 - Minimization Of Personally Identifiable Information

Requirement MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; b. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and c. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO
DM-1 What is the solution and how is it implemented?

Part a

Requirement MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection;

Role Organization
Status Inherited
Details undefined
References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

Part b

Requirement

2. Limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

Part c

Requirement

3. Conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings [Assignment: organization-defined frequency, at least annually] to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.

Role Organization
Status Inherited
Details undefined
References The Privacy Act of 1974, 5 U.S.C. §552a (e); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16;

DM-2 - Data Retention And Disposal

Requirement DATA RETENTION AND DISPOSAL Control: The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law; b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized
access; and c. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Control Summary Information

**Role** OpenShift Tenant  
**Status** Planned  
**Origin** OpenShift Tenant SSP

### DM-2 What is the solution and how is it implemented?

#### Part a

**Requirement** DATA RETENTION AND DISPOSAL Control: The organization: a. Retains each collection of personally identifiable information (PII) for [Assignment: organization-defined time period] to fulfill the purpose(s) identified in the notice or as required by law;

**Role** OpenShift Tenant  
**Status** Planned  
**Details** undefined  
**References** The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB M-07-16; OMB Circular A-130; SP 800-88;

#### Part b

**Requirement**

2. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

**Role** OpenShift Tenant  
**Status** Planned  
**Details** undefined  
**References** The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2); Section 208 (e), E-Government Act of 2002 (P.L. 107-347); 44 U.S.C. Chapters 29, 31, 33; OMB M-07-16; OMB Circular A-130; SP 800-88;

#### Part c

**Requirement**

3. Uses [Assignment: organization-defined techniques or methods] to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

**Role** OpenShift Tenant  
**Status** Planned
DM-2(1) - Data Retention And Disposal | System Configuration

Requirement  DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Control Summary Information

Role  OpenShift Tenant  
Status  Planned  
Origin  OpenShift Tenant SSP

DM-2(1) What is the solution and how is it implemented?

Part a

Requirement  DATA RETENTION AND DISPOSAL | SYSTEM CONFIGURATION The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

Role  OpenShift Tenant  
Status  Planned  
Details  undefined

DM-3 - Minimization Of PII Used In Testing, Training, And Research

Requirement  MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH Control: The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and b. Implements controls to protect PII used for testing, training, and research.

Control Summary Information

Role  Organization  
Status  Inherited  
Origin  Inherited from pre-existing ATO
DM-3 What is the solution and how is it implemented?

Part a

Requirement  MINIMIZATION OF PII USED IN TESTING, TRAINING, AND RESEARCH Control: The organization: a. Develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and

Role  Organization
Status  Inherited
Details  undefined
References  SP 800-122

Part b

Requirement

2. Implements controls to protect PII used for testing, training, and research.

Role  OpenShift Tenant
Status  Planned
Details  undefined
References  SP 800-122

IP-1 - Consent

Requirement  CONSENT Control: The organization: a. Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; b. Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; c. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and d. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.

Control Summary Information

Role  OpenShift Tenant
Status  Planned
Origin  OpenShift Tenant SSP

IP-1 What is the solution and how is it implemented?
Part a

**Requirement**  CONSENT Control: The organization:  
a. Provides means, where feasible and appropriate,  
for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable  
information (PII) prior to its collection;

**Role**  OpenShift Tenant  
**Status**  Planned  
**Details**  undefined  

**References**  The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of  
2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

Part b

**Requirement**  
  2. Provides appropriate means for individuals to understand the consequences of decisions to ap-
  prove or decline the authorization of the collection, use, dissemination, and retention of PII;

**Role**  OpenShift Tenant  
**Status**  Planned  
**Details**  undefined  

**References**  The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of  
2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

Part c

**Requirement**  
  3. Obtains consent, where feasible and appropriate, from individuals prior to any new uses or  
disclosure of previously collected PII; and

**Role**  OpenShift Tenant  
**Status**  Planned  
**Details**  undefined  

**References**  The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3); Section 208(c), E-Government Act of  
2002 (P.L. 107-347); OMB M-03-22; OMB M-10-22;

Part d

**Requirement**  
  4. Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially  
described in the public notice that was in effect at the time the organization collected the PII.

**Role**  OpenShift Tenant  
**Status**  Planned  
**Details**  undefined
IP-1(1) - Consent | Mechanisms Supporting Itemized Or Tiered Consent

Requirement CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

IP-1(1) What is the solution and how is it implemented?

Part a

Requirement CONSENT | MECHANISMS SUPPORTING ITEMIZED OR TIERED CONSENT The organization implements mechanisms to support itemized or tiered consent for specific uses of data.

Role OpenShift Tenant
Status Planned
Details undefined

IP-2 - Individual Access

Requirement INDIVIDUAL ACCESS Control: The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; b. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; c. Publishes access procedures in System of Records Notices (SORNs); and d. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP
IP-2 What is the solution and how is it implemented?

Part a

**Requirement** INDIVIDUAL ACCESS Control: The organization: a. Provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records;

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

Part b

**Requirement**

2. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records;

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

Part c

**Requirement**

3. Publishes access procedures in System of Records Notices (SORNs); and

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

Part d

**Requirement**

4. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined
References The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4), (j), (k), (t); OMB Circular A-130;

IP-3 - Redress

Requirement REDRESS Control: The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and b. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

IP-3 What is the solution and how is it implemented?

Part a

Requirement REDRESS Control: The organization: a. Provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130;

Part b

Requirement

2. Establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended.

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4); OMB Circular A-130;
IP-4 - Complaint Management

Requirement COMPLAINT MANAGEMENT Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

IP-4 What is the solution and how is it implemented?

Part a

Requirement COMPLAINT MANAGEMENT Control: The organization implements a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices.

Role OpenShift Tenant
Status Planned
Details undefined
References OMB Circular A-130; OMB M-07-16; OMB M-08-09;

IP-4(1) - Complaint Management | Response Times

Requirement COMPLAINT MANAGEMENT | RESPONSE TIMES The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

IP-4(1) What is the solution and how is it implemented?

Part a

Requirement COMPLAINT MANAGEMENT | RESPONSE TIMES The organization responds to complaints, concerns, or questions from individuals within [Assignment: organization-defined time period].
<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Planned</td>
</tr>
<tr>
<td>Details</td>
<td>undefined</td>
</tr>
</tbody>
</table>

### MA-1 - System Maintenance Policy And Procedures

**Requirement** SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

b. Reviews and updates the current:

1. System maintenance policy [Assignment: organization-defined frequency]; and
2. System maintenance procedures [Assignment: organization-defined frequency].

### Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>Tenant SSP</td>
</tr>
</tbody>
</table>

### MA-1 What is the solution and how is it implemented?

**Part a**

**Requirement** SYSTEM MAINTENANCE POLICY AND PROCEDURES Control: The organization:

a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:

1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Design Specification document and System Security Plan.

**References** SP 800-12; SP 800-100;

**Part b**

**Requirement**

2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Design Specification document and System Security Plan.
Part c

Requirement

2. Reviews and updates the current: 1. System maintenance policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

Part d

Requirement

2. System maintenance procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-100;

PL-2 - System Security Plan

Requirement SYSTEM SECURITY PLAN Control: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization’s enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles]; c. Reviews the security plan for the information system [Assignment: organization-defined frequency]; d. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protects the security plan from unauthorized disclosure and modification.

Control Summary Information

Role OpenShift Tenant
Status Not implemented
**PL-2 What is the solution and how is it implemented?**

**Part a**

**Requirement** SYSTEM SECURITY PLAN Control: The organization: a. Develops a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture;

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program's System Security Plan.

**References** SP 800-18;

**Part b**

**Requirement**

2. Explicitly defines the authorization boundary for the system;

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Security Plan.

**References** SP 800-18;

**Part c**

**Requirement**

3. Describes the operational context of the information system in terms of missions and business processes;

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Security Plan.

**References** SP 800-18;

**Part d**

**Requirement**

4. Provides the security categorization of the information system including supporting rationale;

**Role** OpenShift Tenant

**Status** Not implemented

**Details** Documented in the individual project / program’s System Security Plan.

**References** SP 800-18;
Part e

Requirement

5. Describes the operational environment for the information system and relationships with or connections to other information systems;

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-18;

Part f

Requirement

6. Provides an overview of the security requirements for the system;

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-18;

Part g

Requirement

7. Identifies any relevant overlays, if applicable;

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-18;

Part h

Requirement

8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-18;
Part i

Requirement

9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-18;

Part j

Requirement

2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-18;

Part k

Requirement

3. Reviews the security plan for the information system [Assignment: organization-defined frequency];

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-18;

Part l

Requirement

4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

Role  Organization
Status  Inherited
Details  Dependent on implementing organization.
References  SP 800-18;
Part m

Requirement

5. Protects the security plan from unauthorized disclosure and modification.

Role  Organization

Status  Inherited

Details  Dependent on implementing organization.

References  SP 800-18;

RA-1 - Risk Assessment Policy And Procedures

Requirement  RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and b. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and 2. Risk assessment procedures [Assignment: organization-defined frequency].

Control Summary Information

Role  OpenShift Tenant

Status  Not implemented

Origin  Tenant SSP

RA-1 What is the solution and how is it implemented?

Part a

Requirement  RISK ASSESSMENT POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

Role  OpenShift Tenant

Status  Not implemented

Details  Documented in the individual project / program’s System Security Plan.

References  SP 800-12; SP 800-30; SP 800-100;

Part b

Requirement

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
Part c

Requirement

2. Reviews and updates the current: 1. Risk assessment policy [Assignment: organization-defined frequency]; and

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-30; SP 800-100;

Part d

Requirement

2. Risk assessment procedures [Assignment: organization-defined frequency].

Role Organization
Status Inherited
Details Dependent on implementing organization.
References SP 800-12; SP 800-30; SP 800-100;

RA-3 - Risk Assessment

Requirement RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]]; c. Reviews risk assessment results [Assignment: organization-defined frequency]; d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Control Summary Information

Role OpenShift Tenant
Status Not implemented
Origin Tenant SSP
RA-3 What is the solution and how is it implemented?

Part a

Requirement RISK ASSESSMENT Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part b

Requirement

2. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part c

Requirement

3. Reviews risk assessment results [Assignment: organization-defined frequency];

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

Part d

Requirement

4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;
Part e

Requirement

5. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Role Organization

Status Inherited

Details Dependent on implementing organization.

References OMB M-04-04; SP 800-30; SP 800-39; Web: idmanagement.gov;

SA-11 - Developer Security Testing And Evaluation

Requirement DEVELOPER SECURITY TESTING AND EVALUATION Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation.

Control Summary Information

Role Organization

Status Inherited

Origin Inherited from pre-existing ATO

SA-11 What is the solution and how is it implemented?

Part a

Requirement DEVELOPER SECURITY TESTING AND EVALUATION Control: The organization requires the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan;

Role Organization

Status Inherited

Details Documented in the project’s System Test Plan.

References ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

316 Chapter 4. Customer Responsibility Matrix
Part b

Requirement

2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];

Role Organization

Status Inherited

Details Dependent on implementing organization.

References ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part c

Requirement

3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;

Role Organization

Status Inherited

Details Dependent on implementing organization.

References ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part d

Requirement

4. Implement a verifiable flaw remediation process; and

Role OpenShift Landlord, OpenShift Tenant

Status Planned

Details Documented in the POAM created as a result of vulnerability scanning.

References ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;

Part e

Requirement

5. Correct flaws identified during security testing/evaluation.

Role OpenShift Landlord, OpenShift Tenant

Status Planned

Details Documented in the POAM created as a result of vulnerability scanning.

References ISO/IEC 15408; SP 800-53A; Web: nvd.nist.gov, cwe.mitre.org, cve.mitre.org, capec.mitre.org;
SA-3 - System Development Life Cycle

**Requirement** SYSTEM DEVELOPMENT LIFE CYCLE Control: The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations; b. Defines and documents information security roles and responsibilities throughout the system development life cycle; c. Identifies individuals having information security roles and responsibilities; and d. Integrates the organizational information security risk management process into system development life cycle activities.

**Control Summary Information**

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>Tenant SSP</td>
</tr>
</tbody>
</table>

**SA-3 What is the solution and how is it implemented?**

**Part a**

**Requirement** SYSTEM DEVELOPMENT LIFE CYCLE Control: The organization: a. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-37; SP 800-64;</td>
</tr>
</tbody>
</table>

**Part b**

**Requirement**

2. Defines and documents information security roles and responsibilities throughout the system development life cycle;

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-37; SP 800-64;</td>
</tr>
</tbody>
</table>

**Part c**

**Requirement**

3. Identifies individuals having information security roles and responsibilities; and

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
</tbody>
</table>
Part d

Requirement

4. Integretes the organizational information security risk management process into system development life cycle activities.

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Security Plan.

References SP 800-37; SP 800-64;

SA-4(1) - Acquisition Process | Functional Properties Of Security Controls

Requirement ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Control Summary Information

Role OpenShift Tenant

Status Not implemented

Origin Tenant SSP

SA-4(1) What is the solution and how is it implemented?

Part a

Requirement ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS
The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

Role OpenShift Tenant

Status Not implemented

Details Documented in the individual project / program’s System Design Specification document and System Security Plan.
SA-4(2) - Acquisition Process | Design / Implementation Information For Security Controls

**Requirement** ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].

**Control Summary Information**

- **Role** OpenShift Tenant
- **Status** Not implemented
- **Origin** Tenant SSP

**SA-4(2) What is the solution and how is it implemented?**

**Part a**

**Requirement** ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design/implementation information]] at [Assignment: organization-defined level of detail].

- **Role** OpenShift Tenant
- **Status** Not implemented
- **Details** Documented in the individual project / program’s System Design Specification document and System Security Plan.

**SE-1 - Inventory Of Personally Identifiable Information**

**Requirement** INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and b. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

**Control Summary Information**

- **Role** OpenShift Tenant
**SE-1 What is the solution and how is it implemented?**

**Part a**

**Requirement** INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION Control: The organization: a. Establishes, maintains, and updates [Assignment: organization-defined frequency] an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Pub 199; SP 800-37; SP 800-122;

**Part b**

**Requirement** 2. Provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII.

**Role** OpenShift Tenant

**Status** Planned

**Details** undefined

**References** The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10); Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB Circular A-130, Appendix I; FIPS Pub 199; SP 800-37; SP 800-122;

**SI-1 - System And Information Integrity Policy And Procedures**

**Requirement** SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and b. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and 2. System and information integrity procedures [Assignment: organization-defined frequency].
Control Summary Information

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Origin</td>
<td>Tenant SSP</td>
</tr>
</tbody>
</table>

SI-1 What is the solution and how is it implemented?

Part a

**Requirement** SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES Control: The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

<table>
<thead>
<tr>
<th>Role</th>
<th>OpenShift Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Not implemented</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Design Specification document and System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part b

**Requirement**

2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shared</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Design Specification document and System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>

Part c

**Requirement**

2. Reviews and updates the current: 1. System and information integrity policy [Assignment: organization-defined frequency]; and

<table>
<thead>
<tr>
<th>Role</th>
<th>Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Shared</td>
</tr>
<tr>
<td>Details</td>
<td>Documented in the individual project / program’s System Design Specification document and System Security Plan.</td>
</tr>
<tr>
<td>References</td>
<td>SP 800-12; SP 800-100;</td>
</tr>
</tbody>
</table>
Part d

Requirement

2. System and information integrity procedures [Assignment: organization-defined frequency].

Role Shared

Status Shared

Details Documented in the individual project / program’s System Design Specification document and System Security Plan.

References SP 800-12; SP 800-100;

TR-1 - Privacy Notice

Requirement PRIVACY NOTICE Control: The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Control Summary Information

Role OpenShift Tenant

Status Planned

Origin OpenShift Tenant SSP

TR-1 What is the solution and how is it implemented?

Part a

Requirement PRIVACY NOTICE Control: The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary;

Role OpenShift Tenant

Status Planned

Details undefined
Part b

Requirement

2. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16; OMB M-10-22; OMB M-10-23; ISE Privacy Guidelines;

Part c

Requirement

3. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change.

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4); Section 208(b), E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-07-16; OMB M-10-22; OMB M-10-23; ISE Privacy Guidelines;

TR-1(1) - Privacy Notice | Real-time Or Layered Notice

Requirement PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE The organization provides real-time and/or layered notice when it collects PII.

Control Summary Information

Role OpenShift Tenant

Status Planned

Origin OpenShift Tenant SSP
TR-1(1) What is the solution and how is it implemented?

Part a

Requirement PRIVACY NOTICE | REAL-TIME OR LAYERED NOTICE The organization provides real-time and/or layered notice when it collects PII.

Role OpenShift Tenant

Status Planned

Details undefined

TR-2 - System Of Records Notices And Privacy Act Statements

Requirement SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS Control: The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); b. Keeps SORNs current; and c. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Control Summary Information

Role OpenShift Tenant

Status Planned

Origin OpenShift Tenant SSP

TR-2 What is the solution and how is it implemented?

Part a

Requirement SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS Control: The organization: a. Publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII);

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;

Part b

Requirement

2. Keeps SORNs current; and

Role OpenShift Tenant

Status Planned
Details  undefined
References  The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;

Part c

Requirement

3. Includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

Role  OpenShift Tenant
Status  Planned
Details  undefined
References  The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3); OMB Circular A-130;

TR-2(1) - System Of Records Notices And Privacy Act Statements | Public Website Publication

Requirement  SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION The organization publishes SORNs on its public website.

Control Summary Information

Role  OpenShift Tenant
Status  Planned
Origin  OpenShift Tenant SSP

TR-2(1) What is the solution and how is it implemented?

Part a

Requirement  SYSTEM OF RECORDS NOTICES AND PRIVACY ACT STATEMENTS | PUBLIC WEBSITE PUBLICATION The organization publishes SORNs on its public website.

Role  OpenShift Tenant
Status  Planned
Details  undefined

TR-3 - Dissemination Of Privacy Program Information

Requirement  DISSEMINATION OF PRIVACY PROGRAM INFORMATION Control: The organization: a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO);
and b. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Control Summary Information

Role OpenShift Tenant
Status Planned
Origin OpenShift Tenant SSP

TR-3 What is the solution and how is it implemented?

Part a

Requirement DISSEMINATION OF PRIVACY PROGRAM INFORMATION Control: The organization:

a. Ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-23;

Part b

Requirement

2. Ensures that its privacy practices are publicly available through organizational websites or otherwise.

Role OpenShift Tenant
Status Planned
Details undefined
References The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347); OMB M-03-22; OMB M-10-23;

UL-1 - Internal Use

Requirement INTERNAL USE Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Control Summary Information

Role OpenShift Tenant
Status Planned
UL-1 What is the solution and how is it implemented?

Part a

Requirement  INTERNAL USE Control: The organization uses personally identifiable information (PII) internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices.

Role  OpenShift Tenant

Status  Planned

Details  undefined

References  The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1);

UL-2 - Information Sharing With Third Parties

Requirement  INFORMATION SHARING WITH THIRD PARTIES Control: The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; b. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; c. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and d. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Control Summary Information

Role  OpenShift Tenant

Status  Planned

Origin  OpenShift Tenant SSP

UL-2 What is the solution and how is it implemented?

Part a

Requirement  INFORMATION SHARING WITH THIRD PARTIES Control: The organization: a. Shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes;

Role  OpenShift Tenant

Status  Planned

Details  undefined
Part b

Requirement

2. Where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used;

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;

Part c

Requirement

3. Monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;

Part d

Requirement

4. Evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Role OpenShift Tenant

Status Planned

Details undefined

References The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o); ISE Privacy Guidelines;
This chapter describes how OCP 3.3 can be deployed according to the FISMA High security controls listed in this guide. Further, the deployed reference architecture is air-gapped in a private AWS VPC with not direct access to the Internet.

Reference Architecture

The Security CONOPS chapter describes the OpenShift FISMA High reference architecture. That architecture can be implemented in AWS with the openshift-disconnected project.

openshift-disconnected is implemented with Ansible. It can be deployed automatically, kept compliant with its CM baseline, and audited with OpenSCAP. The AWS VPC layout replicates an air-gapped deployment that is unable to access the Internet. This requires many services that are typically taken for granted like DNS to be deployed into the private VPC.

openshift-disconnected automatically deploys all of the required services to run OCP 3.3 in the private VPC. Many of the functions implemented by openshift-disconnected are pluggable and can be added to your Ansible project with Ansible Galaxy from the RHTPS organization.

Some of the most reusable roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>800-53</td>
<td>Implements RHEL FISMA compliance and scans the resultant configuration with OpenSCAP.</td>
</tr>
<tr>
<td>bind</td>
<td>Deploys DNS services into the private VPC</td>
</tr>
<tr>
<td>private-aws</td>
<td>Sets up the public and private VPCs and deploys the EC2 instances.</td>
</tr>
<tr>
<td>registry</td>
<td>Sets up a private docker registry and populates it with all of the images required by OpenShift.</td>
</tr>
<tr>
<td>yum</td>
<td>Sets up a yum server with all of the RPM content required for the OpenShift deployment.</td>
</tr>
</tbody>
</table>

For instructions on how to use the openshift-disconnected project, refer to the README.
Manual Workarounds

Some aspects of the reference architecture expressed in the Security CONOPS have not yet been implemented in the openshift-disconnected project. Those missing components are being tracked in the Issues page for that repo. As a workaround, manual implementation instructions are below.

User Authentication

Cluster Admins and Application developers gain access to OCP through a WebUI or CLI. In order to authenticate with the CLI, the user must first log in to the WebUI and obtain a CLI token. The following details how to enable PKI authentication in the WebUI.

Request Header Authentication

The request header authentication passes the authentication request to another Apache process. If that process successfully authenticates (and authorizes if desired) the user, then it passes the username back to the OpenShift master in an HTTP header.

This Apache process may be run on the OpenShift master or separate host. This example assumes the Apache process is on a separate host.

1. OpenShift Master – master.example.com
2. Apache proxy for authentication – proxy.example.com

OpenShift Master – Creating Certificates

OpenShift manages its own certificates to encrypt inter-nodal communication. This is beneficial in another way. We don’t want someone to spoof our proxy and authenticate by passing in a remote header from some random host. Therefore, we will create a certificate for the Apache proxy using the CA on the OpenShift master.

SSH to the OpenShift master and elevate your privileges to root.

```
# oadm ca create-signer-cert
--cert='/etc/origin/master/proxyca.crt'
--key='/etc/origin/master/proxyca.key'
--name='openshift-proxy-signer@1432232228'
--serial='/etc/origin/master/proxyca.serial.txt'

# oadm create-api-client-config
--certificate-authority='/etc/origin/master/proxyca.crt'
--client-dir='/etc/origin/master/proxy'
--signer-cert='/etc/origin/master/proxyca.crt'
--signer-key='/etc/origin/master/proxyca.key'
--signer-serial='/etc/origin/master/proxyca.serial.txt'
--user='system:proxy'

# pushd /etc/origin/master
# cp ca.crt /root/authproxyca.crt
# cp proxy/system/proxy.crt /root/authproxy.crt
# popd
```
Using your favorite file transfer method, copy the authproxy.crt and authproxyca.crt from the OpenShift Master to the Apache proxy host.

**Apache Proxy**

SSH into the Apache Proxy and install some basic packages as root.

```
# yum install -y httpd mod_ssl mod_session apr-util-openssl
```

Also, as root, create a new Apache configuration file with the following content in /etc/httpd/conf.d/

```
# vi /etc/httpd/conf.d/ose-proxy.conf

LoadModule session_module modules/mod_session.so
LoadModule request_module modules/mod_request.so

# Nothing needs to be served over HTTP. This virtual host simply redirects to HTTPS.
<VirtualHost *:80>
DocumentRoot /var/www/html
RewriteEngine On
RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R,L]
</VirtualHost>

<VirtualHost *:443>
# This needs to match the certificates you generated. See the CN and X509v3
# Subject Alternative Name in the output of:
# openssl x509 -text -in /etc/pki/tls/certs/localhost.crt
ServerName proxy.example.com

DocumentRoot /var/www/html
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/tls/private/localhost.key

# This is the CA against which your user’s certificates will be checked.
SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt

SSLProtocol ALL -SSLv2 -SSLv3
SSLCipherSuite ECDHE-RSA-AES256-SHA384:AES256-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH:!EXP:!SSLV2:!eNULL
SSLUserName SSL_CLIENT_S_DN_CN
SSLOptions +StdEnvVars +ExportCertData

#For PKI
SSLVerifyClient require

SSLPayloadEngine on

#These were created per the instructions in the OSE installation docs
SSLPayloadCAcertificateFile /etc/pki/CA/certs/authproxyca.crt
SSLPayloadMachineCertificateFile /etc/pki/tls/certs/authproxy.crt

ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel debug
CustomLog logs/ssl_request_log "\"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

5.2. Manual Workarounds
# Send all requests to the console
RewriteEngine On
RewriteRule ^/console(.*)$ https://%{HTTP_HOST}:8443/console$1 [R,L]

# In order to using the challenging-proxy an X-Csrf-Token must be present.
RewriteCond %{REQUEST_URI} ^/challenging-proxy
RewriteCond %{HTTP:X-Csrf-Token} ^$ [NC]
RewriteRule ^.* - [F,L]

<Location /challenging-proxy/oauth/authorize>
# Insert your backend server name/ip here.
AuthName openshift
ProxyPass https://master.example.com:8443/oauth/authorize
</Location>

<Location /login-proxy/oauth/authorize>
# Insert your backend server name/ip here.
AuthName openshift
ProxyPass https://master.example.com:8443/oauth/authorize
</Location>

<ProxyMatch /oauth/authorize>
#This require directive is very important
require valid-user
RequestHeader set X-Remote-User %{SSL_CLIENT_S_DN_CN}s
</ProxyMatch>

</VirtualHost>
RequestHeader unset X-Remote-User

Please note the SSLCACertificateFile directive. This is the CA against which the clients (your users) will be validated. Out of the box, the specified file won’t work. Please replace this will the valid CA file or chain.

**OpenShift Master - Auth Configuration**

Now that we have Apache configured, we need to configure the authentication provider for the OpenShift Master. SSH into the OpenShift Master and elevate your privileges to root. Then edit the Master’s configuration file.

```
# vi /etc/origin/master/master-config.yaml
```

Now, in the oauthConfig section, enter the following

```
oauthConfig:
  ...
  identityProviders:
  - name: requestheader
    challenge: true
    login: true
    provider:
      apiVersion: v1
      kind: RequestHeaderIdentityProvider
      challengeURL: "https://proxy.example.com/challenging-proxy/oauth/authorize?$\{query\}"  
      loginURL: "https://proxy.example.com/login-proxy/oauth/authorize?$\{query\}"  
      clientCA: /etc/origin/master/proxyca.crt
      headers:
        - X-Remote-User
```
YAML is delimited by spaces. Please ensure you have the correct spacing.

Once you have saved the file, go ahead and restart your master.

```
# systemctl restart atomic-openshift-master.service
```

Now navigate to your OpenShift master in a web browser. If you have a valid client certificate, you should just be authenticated.
Is this guide complete?

No. As of version 1.0 beta it is still under construction. There are several efforts under way to accredit OpenShift at FISMA High. During that process this guide will be updated, probably a lot.

Has OpenShift been accredited anywhere?

Yes, at variants of FISMA Moderate in several places in the US Department of Defense.

How can I help?

If you’d like to get involved, fork the project and send us pull requests.
If you’re not sure where to start, or if you’ve found a mistake or problem, take a look at the project Issues page for this version (1.0beta).

X is wrong, what’s up?

Found a mistake? Great! Open an Issue.

Who can I talk to about this?

Jason Callaway would be happy to talk your ear off about this. Or you could talk to your Red Hat account team.
CHAPTER 7

Indices and tables

• genindex
• modindex
• search