



**IT Security Procedural Guide:
Security Engineering
Architecture Reviews
CIO-IT Security-19-95**

Revision 1


September 30, 2022

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – September 12, 2019		
N/A	ISE	New guide created.	N/A	N/A
1	Gillikin	Updates and comments.	Updates before initial publication.	Throughout
		Revision 1 – September 30, 2022		
1	ISE	Updated content throughout.	Scheduled update.	Throughout
2	McCormick/ Klemens	Edited content and updated format.	Align with current version of GSA Procedural Guide format.	Throughout

Approval

IT Security Procedural Guide: Security Engineering Architecture Reviews, CIO-IT Security 19-95, Revision 1, is hereby approved for distribution.

DocuSigned by:

FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Security Engineering Division (ISE) at SecEng@gsa.gov.

Table of Contents

1	Introduction	1
1.1	Purpose	1
1.2	Scope.....	1
1.3	Policy.....	2
1.4	Roles and Responsibilities.....	3
2	Security Architecture Review	3
2.1	Security Architecture Workflow	4
2.2	Security Architecture Workflow Steps.....	5
2.	Ongoing Security Consulting / Security Engineering Support	14
2.3	New Technology Review / Approval.....	14
	Appendix A AWS Architecture Best Practices	16
	Appendix B AWS Service Approvals Ready for Delivery to ISP.....	23
	Appendix C PostgreSQL Database Encryption.....	24
	Table 1-1. Roles and Responsibilities	3
	Table 2-1. Information System Components and Boundary Considerations.....	5
	Table 2-2. Use of Approved Software and Security Standards.....	8
	Table 2-3. Data Flow and Routing Paths.....	8
	Table 2-4. Technical Integration with Enterprise IT and Security Services.....	9
	Table 2-5. Key Technical Security Considerations	9
	Table 2-6. Other Considerations	11
	Table 2-7. AWS Specific Considerations	11
	Table A-1. Reliability Best Practices	16
	Table A-2. Performance Efficiency Best Practices	17
	Table A-3. Operational Excellence Best Practices.....	18
	Table A-4. Security Best Practices	20
	Table A-5. Cost Optimization Best Practices	21

Note:

- It may be necessary to copy and paste hyperlinks found in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

The development of increasingly complex information systems with new and emergent technologies and techniques requires focus on security activities throughout the system life cycle, ensuring systems are designed and built with security in mind from inception and remain dependable and secure in the face of ever-changing threats.

The Security Engineering Division (ISE) in the Office of the Chief Information Security Officer (OCISO) has developed the Security Engineering Framework described herein to facilitate a collaborative approach to the attainment of ubiquitous security adoption and compliant operations in the General Services Administration (GSA) information technology (IT) computing environment. The framework includes two loosely coupled security engineering services that when applied to systems development processes will further these goals. Specifically, ISE will seek to strengthen information systems and their supporting infrastructures by ensuring they are designed and built around their respective protection needs with proven security architectures; and that required protection mechanisms are addressed and implemented early and maintained throughout the life cycle of the system. ISE services include:

- Security Architecture Review – ISE will review and approve all proposed Security Architectures prior to assessment. The goal of the review is to ensure that any proposed security architecture or proposed changes to an existing architecture comply with GSA security requirements.
- Ongoing Security Consulting/Engineering Support- ISE will serve as a subject matter expert providing on-demand security consulting/engineering support to system and security staff.

ISE services are available to both new systems during the development/acquisition stage of the system life cycle; and, for operational systems undergoing a major change during the operation/maintenance stage of the system life cycle. The ensuing sections further detail the ISE security engineering services.

1.1 Purpose

This guide describes security engineering services provided by the OCISO ISE Division. It is designed to assist agency personnel with engaging the ISE Division with both formal and ad hoc security consulting services.

1.2 Scope

The security engineering architecture considerations described in this guide are applicable to all GSA information systems and the computing resources they provide to the GSA enterprise. These resources and services may consist of physical and virtual assets, hosted and services-based software, and the platforms that render or consume infrastructure as a service internally and externally by the GSA.

1.3 Policy

[GSA Order CIO 2100.1](#), GSA Information Technology (IT) Security Policy, contains the following policy statements regarding security engineering architecture.

Chapter 1, The GSA Information Technology Security Program

13. Cloud Services. No GSA user or SSOs including Regional Offices, shall conduct or acquire any type of pilot involving the use of GSA data or GSA logon credentials to a cloud service, platform, application, or tool without first consulting with the OCISO's Security Engineering Division (ISE). Such coordination can be made by contacting ISE representatives at SecEng@gsa.gov.

a. No procurement for such products/services shall be completed without coordination through the OCISO and having obtained a valid ATO granted by a GSA AO based on the processes defined in GSA CIO-IT Security-06-30 or a FedRAMP provisional ATO.

b. GSA users or SSOs may leverage GSA authorized Cloud Service Provider services reviewed by the GSA Security Engineering Division (ISE) and approved by the GSA CISO. Contact SecEng@gsa.gov for the current list of approved services.

Chapter 4, Policy for Protect Function

4. Information Protection Processes and Procedures.

g. ISE must approve all Security Architecture designs prior to implementation.

[CIO-IT Security-06-30](#): Managing Enterprise Cybersecurity Risk contains the following statements applicable to security engineering architecture.

Appendix F, Table F-1: GSA Showstopper Capabilities/Controls states:

1. Multi-Factor Authentication (MFA) for Privileged & User-level Access

All systems shall utilize a GSA-approved multi-factor authentication mechanism for both privileged and non-privileged user authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only username and password authentication.

Per NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, MFA methods involving the sending of PINS/passwords via email is prohibited and on public networks via SMS is restricted. Sending PINS/passwords to registered telephone numbers on GFE is allowed based on a risk analysis. MFA methods shall favor approaches that do not expose PINS/passwords to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn.

If an assessment identifies MFA has not been implemented, per policy requirements, then the system will not be approved for a 3-year ATO or OA, until MFA is implemented.

1.4 Roles and Responsibilities

The following table provides a general description of the roles and responsibilities for personnel involved in the Architecture Review as referenced in CIO-IT Security-06-30.

Table 1-1. Roles and Responsibilities

Role	Responsibilities
Information System Security Manager (ISSM)	<ul style="list-style-type: none"> Oversees and coordinates ISSO activities to ensure the architecture submission sufficiently addresses required artifacts and elements identified in this guide. Only ISSM can submit requests for security engineering architecture review.
Information Systems Security Officer (ISSO)	<ul style="list-style-type: none"> Coordinates security engineering and architecture reviews with relevant stakeholders. Works with the ISSM to conduct a review and provides attestation through the security engineering checklist that all items are addressed prior to the submission to Security Engineering for architecture review.
Security Engineer	<ul style="list-style-type: none"> Reviews system security architectures submitted by ISSOs, ensuring they are designed and built around their respective protection needs with proven security architectures in alignment with the security practices defined in this guide. Provides any findings or issues with the system in an official report sent to the ISSM and ISSO. ISSM and ISSOs are responsible for coordinating implementation of needed changes.

2 Security Architecture Review

GSA Security Engineering must review all Security Architectures prior to an assessment. The goal of the review is to ensure that any proposed security architecture or proposed changes to an existing architecture comply with GSA security requirements. In general, Security Engineering must perform a security architecture review as part of the Assessment and Authorization (A&A) process for *all* new systems and systems undergoing a major change. ISE will review architectures for:

- New Systems: During the system design phase of a new system before A&A.
- Re-Authorizations: Systems being re-authorized that have not previously had a security architecture review performed.
- Major Change: When substantive changes are made to an existing system, including but not limited to:
 - Addition of major components not previously authorized that expands the authorization to operate (ATO) boundary or significantly alters the systems risk profile.

- New integration points with external systems or services.
- Changes to the authentication or encryption subsystems.
- Migration to other environments, data centers, whereby the configurations change.
- Adoption of Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).
- Integration with third party services via API or making an API available for the purpose of third-party integration.

The GSA Security Engineering Division reviews and approves the security architecture of information systems undergoing the Security Assessment and Authorization Process. This requirement is described in section 3 of CIO-IT Security 06-30 and in section 2.3.2 of [CIO-IT Security 14-68](#): Lightweight Security Authorization Guide.

2.1 Security Architecture Workflow

This section summarizes the Architecture Review Process.

1. The ISSM/ISSO reviews and attests the [Security Architecture Checklist](#) items to ensure their supporting diagrams and System Security and Privacy Plan (SSPP) have the required items.
2. The ISSM submits their request through the [Security Engineer Architecture Review Request](#).
3. An ISE Security Engineer will triage the request for the following items:
 - a. To ensure key checklist items have been included. If they have not been addressed, the request will be rejected.
 - b. To determine the nature of the system and level of effort required to complete initial review.
4. Once accepted, an ISE engineer will be assigned to review supplied artifacts and will provide an estimated time frame to provide initial comments.
5. The ISE Security Engineer will review submitted architecture and provide feedback within the provided time frame. The ISE Security Engineer will meet with the ISSO and application teams to ensure sufficient understanding of requested updates. ISE will continue to work with the team until the documentation is sufficient.
6. ISSOs are responsible for coordinating implementation of needed changes to documentation and providing updates.
7. Once the review is complete, a final report noting any findings will be emailed to the ISSO, ISSM, and any relevant system points of contact (POCs).
8. If the system is in Archer, ISE will update Archer to note that a security architecture review was completed and the date on which it was completed. If the system is not in Archer, ISE will work with the ISSO to ensure it gets added.

2.2 Security Architecture Workflow Steps

Step 1: Review Security Architecture Checklist

The ensuing tables identify a series of checks, informed by existing requirements in [NIST SP 800-53, Revision 5](#) and/or GSA or Federal IT Security policy used by GSA Security Engineering in the performance of security architecture reviews. The checks are not all-inclusive and generally represent areas where GSA information systems have had implementation challenges. During the review of the security architecture documented in section 9-11 of the SSPP, GSA Security Engineering will use this checklist as guidance to ensure alignment of the proposed architecture to NIST Federal/GSA security requirements and/or GSA's security fabric (if internally hosted).

Information in the tables should not be construed as new requirements or superseding existing responsibilities for complying with information security and privacy requirements defined by existing Federal laws, Executive Orders, directives, standards, guidelines, or regulations.

Reference [Appendix A](#) for AWS security architecture best practices derived from the AWS Well Architected Framework.

Table 2-1. Information System Components and Boundary Considerations

#	Checklist Item	Control Reference
1	The ATO boundary must be well defined and include all assets, services and devices that constitute the information system. These shall include all physical and virtual resources. Using this checklist will ensure a well-defined architecture, facilitate ISE architecture approval, and ease control definitions in the SSPP.	CM-8 System Component Inventory
2	The system boundary contains all components, devices, services, communication paths (Virtual Private Networks [VPNs], Application Programming Interfaces [API] calls, etc.). Diagram(s) should be sufficiently detailed and identify flows with source/destination, ports/protocols, or whether the related traffic is encrypted or not. References to ports/protocols table(s) are acceptable (for large sets of ports). Tables identifying ports should reflect whether they are encrypted. Tables should easily be tracked to the architecture diagram.	CM-8 System Component Inventory AC-20 Use of External Systems
3	If shared assets or services are used, they must be appropriately defined and documented as a shared service within the ATO boundary of the system or within the corresponding ATO boundary of a relevant, authorized system. All components must be accounted for within an ATO boundary.	CM-8 System Component Inventory AC-20 Use of External Systems
4	If on-premise or cloud services are used to support operation, maintenance, management, security of the services in scope of the ATO, they should be reflected in the network architecture with related flows.	FedRAMP Policy Memo CA-6 Authorization AC-20 Use of External Systems

#	Checklist Item	Control Reference
	Depending on the nature and type of integration and sensitivity of the data, these dependent systems may also need to obtain an ATO; usage considered for risk acceptance; or, if not risk accepted, potentially removed from the architecture. All SaaS, IaaS or PaaS that support delivery of the system must have an ATO, approved by GSA or FedRAMP.	SA-9 External System Services
5	Integration points and network interconnections with external systems, networks, VPNs, APIs, and services must be well-defined in the architecture and securely implemented.	CA-3 Information Exchange AC-20 Use of External Systems SA-9 External System Services
6	A Trusted Internet Connection (TIC) as defined by FISMA and DHS must be utilized for all privileged, authenticated connections. Privileged access to external environments, including cloud environments shall route through the GSA MTIPs provider (when possible). Leveraging GSA's internet connection satisfies this item.	AC-17 Remote Access AC-17(3) Remote Access Managed Access Control Points TIC Reference Architecture requires all Cloud traffic to be routed through Trusted Internet Connections .
7	Any system that interconnects with GSA via physical or logical network connection shall obtain IP address provisioning from GSA Network Operations. This can be coordinated through the GSA NetOps teams (netops@gsa.gov). Classless Inter-Domain Routing (CIDR) block allocations will be provided for each team or tenant of Cloud Service Providers (CSPs) to prevent overlap of addressing across on premise and remote networks across CSPs. CIDR block allocations shall be coordinated through the GSA NetOps teams.	SC-22 Architecture and Provisioning for Name/Address Resolution Service
8	For public facing systems, integration with external systems including but not limited to other cloud assets via APIs or third-party enablers shall be appropriately secured. Reference GSA CIO-IT Security-19-93 : Application Programming Interface (API) Security for guidelines to secure APIs, GSA CIO-IT Security-07-35 : Web Application Security for securing web applications; and, GSA CIO-IT Security-14-69 : SSL/TLS Implementation for securely implementing SSL/TLS connections.	CA-3 Information Exchange AC-20 Use of External Systems SA-9 External System Services
9	All access control mechanisms, such as firewalls, router access control lists (ACLs), subnets, proxies, and cloud-based analogs, such as firewalls and network access controls configurations, shall be fully documented in the architecture diagram and supporting discussion in terms of specific access control rules, specifying source, destination, protocol, and other relevant attributes, as necessary.	SA-5 System Documentation SC-7 Boundary Protection

#	Checklist Item	Control Reference
10	<p>Ensure all authentication points (including but not limited to Amazon Web Services (AWS) console, jump, machine resources, application, API, enablers, etc. [as applicable]), in the architecture diagram and described in the supporting discussion. MFA should be for privileged, non-privileged, and/or Internet accessible logins within this system. All authentications shall be MFA; privileged authentication is required to be MFA for all Federal Information Processing Standards (FIPS) impact levels.</p> <p>Per NIST 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, MFA methods involving the sending of Personal Identification Numbers (PINs)/passwords via email is prohibited and on public networks via Short Message Service (SMS) is restricted. Sending PINs/passwords to registered telephone numbers on Government Furnished Equipment (GFE) is allowed based on a risk analysis. MFA methods shall favor approaches that do not expose PINs/passwords to intercept risk including but not limited to Hash-based One-time Password (HOTP), Time-based OTP (TOTP), Security Assertion Markup Language (SAML)/OpenID Connect (OIDC), Personal Identity Verification (PIV), Fast ID Online (FIDO)/WebAuthn.</p> <p>Note: System architectures must adhere to the considerations identified in the Admin Remote Access Guidance document. Contact SecEng@gsa.gov for the latest copy of this document.</p> <p>Note: GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy requires new or modernized applications to have ICAM portfolio approval. Any system in scope that has not gone through this process will need to contact icam-portfolio@gsa.gov.</p>	<p>IA-2(1) Identification and Authentication (Organizational Users) Multifactor Authentication to Privileged Accounts</p> <p>IA-2 (2) Identification and Authentication (Organizational Users) Multifactor Authentication to Non-Privileged Accounts</p>

Table 2-2. Use of Approved Software and Security Standards

#	Checklist Item	Control Reference
11	<p>Ensure that the proposed software stack aligns with approved IT Standards. Any proposed software which is not listed in GEAR must be reviewed following the GSA IT Standards process, prior to inclusion in the defined architecture. Proposed software will undergo a Security Review, 508 Accessibility Review, and Chief Technology Officer (CTO) review by multiple teams following the IT Standards process.</p> <p>The continued usage of End of Life (EOL) software requires a risk evaluation to be performed by the OCISO. An EOL software usage justification to include Plan of Action and Milestones (POA&M) tracking requirements or an approved Acceptance of Risk (AOR), are the possible documentation outcome requirements of the risk evaluation.</p>	<p>CM-2 Baseline Configuration</p> <p>CM-6 Configuration Settings</p> <p>SA-22 Unsupported System Components</p>
12	<p>The software stack, including operating system, application, database, etc. must be configured and hardened in accordance with GSA Enterprise Security Benchmarks (where they exist) or to a suitable hardening standard, such as ones provided by the Center for Internet Security (CIS).</p> <p>GSA information systems, including vendor owned/operated systems on behalf of GSA, must be configured in alignment with GSA security benchmark guidelines. Hardening Guides are available on the GSA Insite IT Security Technical Guides and Standards page. Automation content for the benchmarks is available on GitHub.</p>	<p>CM-6 Configuration Settings</p> <p>CIO 2100.1 GSA IT Security Policy</p>

Table 2-3. Data Flow and Routing Paths

#	Checklist Item	Control Reference
13	<p>Sections 9 and/or 10 of the SSPP shall document all data flows in both narrative and diagram versions.</p> <p>Diagram(s) in this section should be sufficiently detailed and identify flows to all components and support services with source/destination, ports/protocols, whether the related traffic is encrypted or not. References to the ports tables are acceptable (for large sets of ports). The tables identifying ports must reflect whether they are encrypted or not. Tables should easily be tracked to the architecture diagram. The ports, protocols, and services table should list whether the communication is encrypted. If not encrypted, there needs to be a description of the data contents, sensitivity, if the data is Government data, and which users have access to the data. This is so the ISSO/ISSM can make a risk-based decision regarding the use of unencrypted traffic.</p>	<p>SA-5 System Documentation</p> <p>AC-4 Information Flow Enforcement</p>

#	Checklist Item	Control Reference
14	Data flow through approved external or internal Continuous Integration systems (CI) and code repositories shall be documented in narrative and diagram versions in the SSPP.	SA-5 System Documentation AC-4 Information Flow Enforcement

Table 2-4. Technical Integration with Enterprise IT and Security Services

#	Checklist Item	Control Reference
15	Internal (on premise) and external (cloud) Federal systems must leverage and provide accessibility to existing GSA Enterprise IT and IT Security services such as Authentication, security information and event management (SIEM), Log Management, Security Scanning, OCISO Cloud Security Tooling, etc. Integration must be documented in prose and system diagrams.	RA-5 Vulnerability Monitoring and Scanning IR-5 Incident Monitoring AU-6 Audit Record Review, Analysis, and Reporting AU-6(1) Audit Record Review, Analysis, and Reporting Automated Process Integration AU-6(3) Audit Record Review, Analysis, and Reporting Correlate Audit Record Repositories

Table 2-5. Key Technical Security Considerations

#	Checklist Item	Control Reference
16	<p>All systems which require authentication, regardless of FIPS 199-impact level, shall implement multifactor authentication for user-level authentication. GSA systems with non-privileged users may integrate with GSA approved centralized authentication services using SAML 2.0 or OpenID Connect.</p> <p>Further, systems leveraging certificate-based authentication shall not be downgraded to only username and password authentication.</p> <p>Per NIST 800-63B, MFA methods involving the sending of pins via public networks via SMS or email are restricted; pin sending to registered telephone numbers to GFE as allowed on a risk basis. MFA methods shall favor approaches that do not expose pins to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn.</p>	<p>IA-2(1) Identification and Authentication (Organizational Users) Multifactor Authentication to Privileged Accounts</p> <p>IA-2 (2) Identification and Authentication (Organizational Users) Multifactor Authentication to Non-Privileged Accounts</p>

#	Checklist Item	Control Reference
17	The mechanisms for creating, storing, distributing, and signing any encryption keys or certificates in the system shall be fully documented in the security architecture. Additionally, all keys and certificates generated shall be reposed in a manner that supports a Business Continuity, Disaster Recovery, and Continuity of Operations planning consistent with NIST requirement per impact FIPS 199 impact level. For further details, see CIO-IT Security-09-43: Key Management .	SC-12 Cryptographic Key Establishment and Management
18	Systems that process personally identifiable information (PII) or other sensitive information shall employ encryption of data while at rest and while in transit. Authenticators (i.e., passwords), PII and Payment Card Industry (PCI) are required to be encrypted at rest, in files, and in databases, as applicable. If stored in databases, encryption can be implemented at the field, column, or table level, as appropriate. Ciphers shall be FIPS-approved.	SC-28 Protection of Information at Rest SC2-28(1) Protection of Information at Rest Cryptographic Protection
19	Ensure encryption for web services utilizes FIPS approved ciphers, FIPS validated encryption modules, at a minimum TLS 1.2 and up, HSTS, and HTTPS only. Complete details can be found in CIO-IT Security-14-69. <ul style="list-style-type: none"> • Digital signature encryption algorithms Reference: NIST Cryptographic Algorithm Validation Program (CAVP), CAVP Testing: Digital Signatures Algorithm Specifications • Block cypher encryption algorithms Reference: NIST CAVP, CAVP Testing: Block Ciphers • Secure hashing algorithms Reference: NIST CAVP: CAVP Testing: Secure Hashing. • Cybersecurity and Infrastructure Security Agency (CISA), Binding Operational Directive 18-01: Enhance Email and Web Security 	SC-8 Transmission Confidentiality and Integrity SC-8(1) Transmission Confidentiality and Integrity Cryptographic Protection SC-13 Cryptographic Protection
20	If high availability is a functional or security requirement, such as in the case of FIPS 199 Moderate or High Systems, the system shall utilize geographically separate infrastructure or availability zones to assure high availability. * A High Availability architecture is required for FedRAMP; but not a Limited ATO (LATO) based on CIO-IT Security-14-68: Lightweight Security Authorization Process .	CP-6 Alternate Storage Site CP-6 Alternate Storage Site Separation From Primary Site CP-7 Alternate Processing Site CP-7(1) Alternate Processing Site Separation from Primary Site
21	The network access controls shall be implemented in a least-permissive manner, assuring that only authorized and essential network communication occurs between elements of the system and across system boundaries.	AC-6 Least Privilege

Table 2-6. Other Considerations

#	Checklist Item	Control Reference
22	Ensure that the proposed architecture includes all applicable essential security controls as identified in CIO-IT Security-09-48 , Security and Privacy Requirements for IT Acquisition Efforts. Examples include multi-factor authentication, SIEM integration, and Vulnerability Scanning. Refer to the guide for a comprehensive list.	SA-4 Acquisition Process Applicable NIST 800-53 Control Baseline (i.e., Low, Moderate, or High)
23	Systems processing payment card information shall comply with the GSA PCI Guidelines guidance.	GSA PCI DSS Program Implementation Plan seceng@gsa.gov
24	Integration with GSA's Security Stack: System integration includes (where applicable). <ul style="list-style-type: none"> Enterprise Logging Platform (ELP) (AU-6(1)) BigFix (CM-6) Bit9 (CM-7) Tenable Security Center (TSC) & NetSparker Monthly Non-Auth Web Scans (RA-5) Endgame AV & (SI-3) FireEye (SI-4) OSEC (SI-7) Prisma Cloud Anchore StackRox 	AU-6(1) Audit Record Review, Analysis, and Reporting CM-6 Configuration Settings CM-7 Least Functionality RA-5 Vulnerability Monitoring and Scanning SI-3 Malicious Code Protection SI-4 System Monitoring SI-7 Software, Firmware, and Information Integrity

Table 2-7. AWS Specific Considerations

#	Checklist Item	Control Reference
25	Host backend database and services on private VPCs that are not visible on any public network.	SC-7 Boundary Protection PL-8: Security and Privacy Architectures
26	Enable encryption at rest for ALL Elastic Block Storage (EBS) volumes. Enable encryption at rest in other services (e.g., S3, RedShift, etc.) for sensitive data including but not limited to PII and PCI. Glacier, Redshift, and Storage Gateway encrypt data at rest by default.	SC-28 Protection of Information at Rest
27	Ensure all flows are documented in the architecture diagram. Further, encrypt all flows, including: <ul style="list-style-type: none"> Outbound traffic to the Internet Inbound traffic from the Internet; web traffic should enforce HTTPS only, with HSTS. All new domains should be pre-loaded. Communication to AWS services Flows to back-office networks (i.e., to GSA) 	PL-8: Security and Privacy Architectures SC-8(1): Transmission Confidentiality and Integrity Cryptographic Protection

#	Checklist Item	Control Reference
	<ul style="list-style-type: none"> Inter-VPC communication flows Intra-VPC flows when bridging public and private subnets and when transmitting sensitive traffic data (e.g., PCI, PII, security authenticators, other business sensitive information as identified by data owner). 	CISA BOD 18-01
28	Virtual Private Cloud (VPC) peering transmits data in the clear through AWS's backbone; it may be acceptable in certain use cases, for example when data is non-sensitive (e.g., Network Time Protocol (NTP), Domain Name Service (DNS) when not publicly resolving); or, when the protocols traversing the peering connection is itself encrypted (e.g., Secure Sockets Layer [SSL], Secure Shell [SSH], Self-Referral Disclosure Protocol [SRDP]). The latter tends to be problematic over time as not all flows can be limited to just secure protocols; hence the need for a VPN solution for inter-VPC connections. GSA has experimented with OpenSwan, StrongSwan, and Cisco Cloud Services Router (CSR); the latter has proven most effective.	SC-8(1): Transmission Confidentiality and Integrity Cryptographic Protection
29	Egress flows require the ability to regulate traffic via Uniform Resource Locator (URL), not just port, protocol, and Internet Protocol (IP). AWS Security Groups (SGs) provide, allow, and deny rules for inbound and outbound traffic for VPCs at layer 4; an outbound proxy solution with rules and policies that allows controlled outbound layer 7 traffic inspection is ideal. Traffic inspection may be opportunistically enabled when necessary to support incident investigations.	SC-7 Boundary Protection IR-4: Incident Handling
30	SSL termination should extend through to the web server. If terminating at Elastic Load Balancer (ELB), extend through to the VPC with Application Load Balancer (ALB) - SSL offloading.	SC-8(1): Transmission Confidentiality and Integrity Cryptographic Protection
31	If leveraging AWS services for boundary protection, need to implement AWS Web Application Firewall (WAF) with inbound allow/deny rules (and manage deny rules over time based on threat information from GSA and external entities). Further, need to implement Shield Advanced for enhanced Denial of Service (DOS) protection.	SC-7 Boundary Protection PL-8: Security and Privacy Architectures
32	Inter-VPC flows including cross-tenant flows and flows to shared VPCs (e.g., transit, security, etc.) need to be limited based on port/protocol to what is minimally required.	SC-7 Boundary Protection PL-8: Security and Privacy Architectures
33	Egress/ingress perimeter security devices that include AWS WAF, Shield Advanced, AWS SGs/Network ACLs (NACLs), and proxy/firewall for outbound URL filtering and SSL packet decryption (when necessary) is suitable.	SC-7 Boundary Protection PL-8: Security and Privacy Architectures
34	Ensure AWS services used are either FedRAMP authorized or approved for usage by GSA. Reference the ISE Master MFA List .	CM-7 (5): Least Functionality

#	Checklist Item	Control Reference
	If desired service is not reviewed or FedRAMP approved, you may submit a request to seceng@gsa.gov.	Authorized Software Allow-By-Exception
35	<p>Required Key AWS Security Services:</p> <ul style="list-style-type: none"> • Enable CloudTrail in ALL regions • Enable VPC Flow Logs per ENI, subnet or VPC; create CloudWatch metrics from log data; log to CloudWatch logs; and alarm on metrics • CloudWatch • Shield and Shield Advanced • Inspector • Config • Trusted Advisor <p>SecurityHub, GuardDuty, Macie, CloudFront and AWS WAF are other services that could be enabled to address a capability gap.</p>	PL-8: Security and Privacy Architectures
36	<p>Required IAM configurations for GSA Incident Response Support</p> <ul style="list-style-type: none"> • GSA Incident Response team • GSA Security Operations team • ISSO/DevSecOps Engineer to support ongoing security monitoring/A&A/security assessment 	IR-4: Incident Handling IR-3: Incident Response Testing

Step 2 – Provide Security Architecture for Review

Security architecture reviews can be submitted to the Security Engineering Division via the Security Architecture Checklist Form. The Checklist form is intended to assist ISSOs/ISSMs with engaging the Security Engineering Division for security architecture reviews. This checklist contains the high-level considerations as defined in this guide that Security Engineering looks at when reviewing system architecture. The process is intended to clearly set review expectations and facilitate a pre-submission self-evaluation to identify and resolve key issues that often contribute to delays. Adherence to the checklist review items and the practices in this guide will ensure timely review and approval of system security architectures.

Review documentation, such as the SSPP (at a minimum Sections 9, System Description, and 10, System Environment), can be directly uploaded via the Google Form. Sufficient documentation must be provided to GSA Security Engineering supporting a determination as to whether the system will meet essential security requirements and align with architectural requirements.

Security Engineering further recognizes that an Agile Software Development Lifecycle (SDLC) approach to system development may result in an iterative, rapidly changing security architecture and recommends that system owners and architects involve GSA Security Engineering early in the design process. The GSA ISE may assign, upon request, an engineer to participate in meetings periodically to facilitate security adoption. Any changes made to the system's security architecture after ISE approval will require a re-evaluation of those changes to ensure ongoing compliance with security requirements. As part of the full A&A and Lightweight

Security Authorization processes, ISE must approve the final security architecture prior to go-live. Security Engineering encourages system owners to account for this review when determining project scheduling.

Step 3 – ISE Security Architecture Approval

The Security Architecture review process is focused specifically on systems that will follow the A&A process, either the Limited or full ATO, and systems undergoing significant change or redesign as described in NIST SP 800-37 Revision 2, Appendix F, Section for Event-Driven Triggers and Significant Changes.

Once the required documents are received from ISSOs/ISSMs, Security Engineering will perform a review, generally within 3-5 business days (complex architectures may take more time) and provide feedback. If necessary, ISE will schedule a meeting with the relevant stakeholders to present the results of the review and to address any concerns. ISSOs are responsible for coordinating implementation of needed changes to documentation and submit updates. Security will review updates and work with stakeholders to address residual issues. Formal approval will be conveyed via email and report. Upon Security Engineering approval, implementation of the system and/or A&A assessment can proceed. Major changes (if any) made to the system's security architecture after ISE approval, will require follow-on review and approval.

2. Ongoing Security Consulting / Security Engineering Support

In addition to the services enumerated in the preceding sections of this guide, ISE will provide Security Engineering and Consulting support for key IT initiatives seeking to utilize new and emergent technologies or undergoing major architectural changes to ensure such systems are designed and built securely from the start. ISE engineers will provide design and architecture guidance following the best practices in this guide.

2.3 New Technology Review / Approval

GSA Security Engineering will provide feedback, and in some cases, approval of new technologies and services. Services or technologies not currently FedRAMP or Agency approved may be submitted for a Security Engineering review. Upon request, Security Engineering will review new technologies including services in AWS, GCP, and Microsoft Azure and present findings to the GSA CISO for approval consideration. Approval of cloud services not FedRAMP authorized is a function of risk and may be with or without usage conditions; approval is not assured.

For the AWS Service Review Process, see [Appendix B](#). To request reviews of non-AWS cloud services (or other technologies), send an email to SecEng@gsa.gov describing the request, along with a list of relevant stakeholders and technology implementers. Consider including vendor representatives among the stakeholders. Security Engineering will review the request (generally within 14 business days) and render an approval determination. If necessary, a

meeting with the stakeholders will be scheduled. Please provide relevant documentation, analysis, or justification to Security Engineering one week prior to the meeting.

If a meeting is needed, be prepared to discuss the technology and the specific way the technology will be utilized in the GSA system and any mitigation controls. The decision on whether to approve a new technology or service will depend in part on technologies' intended use and mitigating controls in place. Security Engineering may request a detailed explanation or analysis of the technology to assist with the review.

GSA Security Engineering reviews new technology in coordination with the CTO following the IT Standards approval process. New technology reviews and security recommendations will be performed by ISE as a matter of routine. The GSA CISO will be consulted for exceptional technologies. For new software consideration, please submit a Software Review Request (SRR) in ServiceNow.

Appendix A AWS Architecture Best Practices

This appendix aligns with AWS recommendations for a well architected framework. The framework is based on five pillars: reliability, performance efficiency, operational excellence, security, and cost optimization. In general, systems designed in AWS are balanced by trade-offs between pillars tailored to individual system needs. Trade-offs mainly occur between the reliability, performance, and cost pillars. The security and operational excellence pillars are generally not part of trade-off decisions.

The remainder of this document will provide specific best practice recommendations for each pillar to help facilitate a well architected system.

Reliability

Design the system in anticipation of failure. Incorporate the ability to automatically recover from infrastructure or service failures. Utilize scaling to dynamically acquire computing resources to meet demand and mitigate disruptions such as misconfigurations or transient network issues. Scaling will allow you to stop guessing capacity needs and respond to change in demand.

Table A-1. Reliability Best Practices

Best Practice	Recommendations
Scaling	<ul style="list-style-type: none"> Scale horizontally (additional nodes) and vertically (additional resources within nodes) to increase aggregate system availability. Design an elastic architecture that can grow and shrink on demand. Utilize parallel processing to split workloads into parts that execute simultaneously.
Multiple Locations	<ul style="list-style-type: none"> Develop all systems in multiple availability zones (AZs). Moderate and High system classifications should leverage multi-regional deployments.
Network Topology	<ul style="list-style-type: none"> Plan for connectivity requirements to legacy data centers. Have high availability / multiple connections. Implement VPN between data centers and for user connectivity. Proper VPC/Account allocation - Use separate accounts for each VPC and avoid integrating all VPCs into a singular account. Typically, you should have Production, Staging, and Development/Test, each in their respective accounts and consider production as an immutable environment that is strictly controlled with full-on automation (i.e., changes are ALL pushed via API and not manually via direct machine access or through the AWS Console). Proper VPC allocation - 1-2 VPCs per account (see above). Proper subnet allocation. Limit the number of subnets to what is minimally required ensuring appropriate segmentation of public/web tiers and internal database tiers.

Best Practice	Recommendations
Failure Management	<ul style="list-style-type: none"> • Ensure no overlapping of private IP addresses. • Test Recovery Procedures and responses to unexpected events and component failures. • Learn from operational events and failures by capturing and reviewing all operational events and using them for improvements. • Ensure adequate backups are performed. • Automatically recover from failure. • Test production systems at full scale load.

Performance Efficiency

Utilize available computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve. Rely on data-driven decisions and continually review choices made to ensure taking advantage of an evolving platform.

Continually benchmark, load test, and monitor the environment to have the data needed to inform change.

Table A-2. Performance Efficiency Best Practices

Best Practice	Recommendations
Democratize Advanced Technologies	<ul style="list-style-type: none"> • Consume new technology and rely on services rather than hosting and building your own.
Keep the Data Close to Customers to Minimize Latency	<ul style="list-style-type: none"> • Use multi-AZ/multi-region architectures. • Leverage AWS CloudFront to distribute data to edge locations. • Use managed services that automatically scale, if using RDS, redeploy across AZs and read replicas; if using RedShift, deploy clusters cross AZs
Use Serverless Architectures	<ul style="list-style-type: none"> • Leverage services such as storage that can host a web server, removing the operational burden.
Experiment More Often	<ul style="list-style-type: none"> • Quickly carry out comparative testing on different types of storage, services, and components.
Mechanical Sympathy	<ul style="list-style-type: none"> • Use technology that aligns best with desired goals.
Component Selection	<ul style="list-style-type: none"> • Component Selection (Compute, storage, database, network) - Select components specific to your needs, and often there is a need to combine multiple approaches. <ul style="list-style-type: none"> ○ Compute: Instances (virtual servers), Containers (run an app and dependencies in resource isolated processes), and Functions (area provided to execute your code). ○ Storage: Select storage based on desired access methods/patterns and performance needs. Considerations include block, file, or object access needs, patterns of access, throughput, frequency of access (online, offline, archival), availability, and durability. Well architected solutions typically leverage many options. ○ Database: Select a database (DB) solution based on your requirements for availability, consistency, partition tolerance,

Best Practice	Recommendations
	<p>latency, durability, scalability, and query capability. Critical to consider access patterns and workload.</p> <ul style="list-style-type: none"> ○ Network: Dependent on latency, throughput requirements, data location. Remember to plan for connectivity to legacy on-prem resources. Consider placing data closest to resources to reduce distance. Take advantage of regions, placement groups, and edge locations. • Take advantage of managed services. A data driven approach will help with the most optimal solution. • Collect data from benchmarking or load testing to further optimize the architecture. • Take advantage of elasticity mechanisms to ensure sufficient capacity.
Review	<ul style="list-style-type: none"> • Understand where your architecture is performance constrained. • Be on the lookout for new releases or products that could alleviate constraints. • Take advantage of continual innovation.
Monitor	<ul style="list-style-type: none"> • Set thresholds and monitor performance. • Tune monitoring to minimize false positives. • Automate triggers to reduce human error. • Have routine gameday tests to simulate events in production.
Analyze Trade-Offs	<ul style="list-style-type: none"> • Think about available trade-offs in conjunction with business needs to select the optimal approach. • Can trade consistency, durability, and space, vs time or latency to deliver higher performance. • Consider read replicas of data or caching solutions.

Operational Excellence

Run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

Table A-3. Operational Excellence Best Practices

Best Practice	Recommendations
Align Operations Processes to Business Objectives	<ul style="list-style-type: none"> • Monitor and report on only items critical to business objectives.
Operate with Code	<ul style="list-style-type: none"> • Perform operations with code to avoid error with manual interaction. • Create all infrastructures following Infrastructure as Code (IaC) model using cloud automation tools like AWS CloudFormation, Terraform etc. not via the cloud console. Infrastructure should be defined as “code” and be able to be recreated readily in an automated way. • Create immutable hosts instead of long-lived servers that you patch and upgrade.

Best Practice	Recommendations
Automate Processes	<ul style="list-style-type: none"> • Use automation for common repetitive processes or procedures. • Ensure you can do upgrades without downtime. Ensure you can quickly update software in a fully automated manner.
Automate Responses	<ul style="list-style-type: none"> • Responses to unexpected operational events should be automated. Not just alerting, but for mitigation, remediation, rollback, and recovery activities.
Make Regular, Small, Incremental Changes	<ul style="list-style-type: none"> • Workloads should be designed to allow components to be updated regularly. • Make changes in small increments and be able to roll back without affecting operations (no downtime).
Loosely Coupled Dependencies	<ul style="list-style-type: none"> • Use queuing systems, streaming systems, workflows, load balancers, etc. to minimize dependencies.
Graceful Degradation	<ul style="list-style-type: none"> • Ensure when a component's dependencies are unhealthy, the component itself continues to serve requests in a degraded manner. • Implement Auto-Healing to detect failures, remediate, and continuously monitor system health.
Create Documentation	<ul style="list-style-type: none"> • Create documentation such as operational checklists, operations guidance, runbooks, playbooks, and keep them current. These documents are used to support day-to-day operations and respond to events.
Standardize	<ul style="list-style-type: none"> • Operations should be standardized and manageable on a routine basis. • Focus on small frequent changes, regular quality assurance testing, tracking, and auditing changes.

Security

Run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

Table A-4. Security Best Practices

Best Practice	Recommendations
Identity and Access Management	<ul style="list-style-type: none"> • Define what users, groups, services, and roles can access within the environment. • Protect the root account. • Require strong passwords and enforce password and key rotation. • Require multi-factor authentication. • Create administration IAM roles with minimum privileges • Evaluate AWS Security Token Service (STS) and Roles • Secure federated connections. • Restrict or remove human access to root credentials, management consoles, and remote access. • Restrict automated access such as applications, scripts, and 3rd party tools. • Securely store static credentials used for automation. • Protect Elastic Compute Cloud (EC2) key-pairs; leverage Identity and Access Management (IAM) roles for EC2 • Institute least privilege principle.
Detective Controls	<ul style="list-style-type: none"> • Implement inventory tools to establish operational baselines. This allows you to set appropriate alerting thresholds and understand the scope of routine vs anomalous activity. • Log all actions and changes within your environment. • Log everything for your stack and from AWS services; integrate into either a SIEM or to CloudWatch (CW) with alerting/monitoring. • Process logs, events and monitoring that allow for auditing, automated analysis, and alarming. • Have a log repository to lock and retain logs. Logging (all actions and changes) • Ensure that no resources are enumerable in your public APIs. • Use canary checks in APIs to detect illegal or abnormal requests that indicate attacks.
Data Protection	<ul style="list-style-type: none"> • Review data classification and retention policies. • Properly store and manage encryption keys. • Implement logging to create records of changes. • Implement storage resiliency. • Implement versioning control and protection against accidental overwrite / deletes. • Store data in multiple locations. • Encrypt data at rest and in transit everywhere you can, especially when crossing VPCs and external to your environment. • Securely decommission data.

Best Practice	Recommendations
Incident Response	<ul style="list-style-type: none"> Implement detailed logging of events and changes for analysis. Configure automatic log processing and alerting. Conduct forensics in an isolated environment.
Shared Service Model	<ul style="list-style-type: none"> Ensure all parties are aware of their responsibilities.
Automate	<ul style="list-style-type: none"> Use software-based security to scale, patch, harden, deploy. Create templates and deploy with version control. Automate response for routine and anomalous events. Use configuration management tools.
Leverage AWS Security Services	<ul style="list-style-type: none"> Leverage AWS Security services, WAF, Shield, Inspector, Trusted Advisor, CloudTrail (CT), CW, IAM, etc.
Egress Flow	<ul style="list-style-type: none"> Egress flow for Moderate/High systems with sensitive data should be routed through Proxy/FW for visibility into traffic and additional control (i.e., filtering by URL in addition to IP/Port).
Use of Approved Services	<ul style="list-style-type: none"> Using approved services (FedRAMP / CISO conditional) See ISE Master MFA List.

Cost Optimization

Monitor utilization and investigate efficiencies to avoid or eliminate unneeded cost or suboptimal resources. Consider all areas of cost outside direct infrastructure costs such as licensing and data transfer costs. Leverage available data to optimize over time.

Table A-5. Cost Optimization Best Practices

Best Practice	Recommendations
Adopt a Consumption Model	<ul style="list-style-type: none"> Pay for what you use. Use scaling in production. Shut down test / dev resources when not in use.
Use Managed Services	<ul style="list-style-type: none"> Use managed services to reduce costs instead of building out your own infrastructure.
Licensing	<ul style="list-style-type: none"> Review and consider license costs of various options.
Pick Cost-Effective Resources	<ul style="list-style-type: none"> Look into available options such as dedicated instances, on-demand instances, reserved instances, or spot instances. Consider deferring processes such as backups and reporting to off hours when resources could be less expensive.
Matching Supply and Demand	<ul style="list-style-type: none"> Leverage auto scaling and demand, buffer, and time-based approaches to automatically provision resources as needed. Monitor to ensure capacity matches but does not exceed demand.
Monitor Usage and Spending	<ul style="list-style-type: none"> Consider all areas of cost including data-transfer costs. Decommission resources that are longer used. Stop resources that are temporarily not needed. Set access controls and procedures to govern usage. Tag assets to track projects.

Best Practice	Recommendations
	<ul style="list-style-type: none">• Manage limits to avoid over-provisioning.
Optimize Over Time	<ul style="list-style-type: none">• Be aware of new services and features as they become available.• Regularly review your deployments.

References:

[AWS Best Practices for Security, Identity, & Compliance](#) – Authoritative guidance for security when using AWS services.

[AWS Well-Architected Framework \(December 2021\)](#) – Overview of the Well-Architected Framework to validate architecture.

[AWS Whitepapers & Guides](#) – Covers topics such as architecture, security, and economics.

[AWS Documentation](#) – Detailed AWS service documentation.

Appendix B AWS Service Approvals Ready for Delivery to ISP

Amazon Web Services (AWS) offers over 100 unique services providing compute, storage, database storage, content delivery and other functionality that allow customers to build their own infrastructures and applications. Of these available services, over 20 are presently FedRAMP authorized, mostly in GovCloud. For GSA to take full advantage of available services, the Office of the Chief Information Security Officer (OCISO) reviews non-FedRAMP authorized services for possible usage at GSA; requested services are subjected to security review by the GSA Security Engineering Division (ISE) and approved by the GSA Chief Information Security Officer (CISO) with or without usage conditions.

The OCISO maintains the [ISE Master MFA List](#), a tracking document of approved services and usage conditions. This document details FedRAMP authorized services and services which have been reviewed and approved by the GSA CISO with and without usage conditions, as applicable. The tracking document is maintained by ISE and reflects the current usage posture for individual AWS services within. The list will be updated as new services and changes to existing services are evaluated by ISE and approved by the CISO. This [AWS Services Approval Memo](#) signed by the GSA CISO, formally approves the above linked MFA document as the official source for maintaining the approval of individual AWS services.

GSA programs seeking to use an AWS service that is presently not FedRAMP or GSA OCISO approved for usage may request approval consideration by completing the [AWS Service Review Template](#) detailing key service particulars and submitting it to SecEng@gsa.gov. Approval of non-FedRAMP approved AWS services is a risk function and possible where the service is ancillary in nature; does not directly store or process information (may do so transiently in encrypted form); is a security service; or is core service that processes, stores, and transmits data in mostly encrypted form. Not all services can be approved for usage without a FedRAMP authorization. Upon submission of the completed AWS Service Review Template, ISE will validate the information, perform sandbox testing, and present the AWS service to the GSA CISO for approval consideration. Typical requests will take two weeks.

Appendix C PostgreSQL Database Encryption

If utilizing a Postgres database and storing PCI, PII, and authenticator data in the database, ensure the data in the database can be encrypted. Per checklist item #18, any database with PCI, PII, and or authenticator data must encrypt the data. This can typically be achieved by encrypting in-scope data via field, column, or table level encryption using FIPS-approved ciphers. Using PostgreSQL as a database solution presents a challenge to meeting this requirement because native Postgres encryption solutions are not available. There are several options to meet this requirement if using PostgreSQL.

- **Pgcrypto:** Pgcrypto is a built-in module that can encrypt data at a column level. However, there are several risks included with using Pgcrypto.
 - Encryption happens in the database. This can lead to exposure of encryption keys in queries and logs.
 - The issue can be mitigated if:
 - The team has a key management solution
 - Configurations are made to avoid exposing keys in logs and queries.
- **Application Encryption:** The goal of requirement #18 is to make the data useless to an attacker in the event of a breach and the data is exfiltrated. Therefore, if the data going into the database is already encrypted from the application, that is another acceptable solution for using PostgreSQL or any other GSA approved database solution.
- **Third Party Tools:** There are several commercial products that can be procured and implemented to enable the necessary encryption. These tools would need to be evaluated and approved for GSA use before implementation.