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

Initial Release

July 10, 2019

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Initial Release – July 10, 2019				
N/A	ISE	New guide created.	N/A	N/A
1	Jeremy Gillikin	Updates and comments	Updates before initial publication	

Approval

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

7/10/2019

X Bo Berlas

Bo Berlas
GSA Chief Information Security Officer
Signed by: General Services Administration

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

Table of Contents

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 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 GSA 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 the commencement of the system build (architecture, infrastructure, and code). 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 prior to implementation or redesign.
- Ongoing Security Consulting/Engineering Support- ISE will serve as a subject matter expert providing on-demand security consulting/engineering support to system and security staffs.

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 IT Security Procedural Guide: *Security Engineering Architecture Reviews* describes security engineering services provided by the GSA Security Engineering Division, in the Office of the Chief Information Security Officer. It is designed to assist agency personnel with engaging the Security Engineering Division with both formal and ad hoc security consulting services.

1.2 Scope

The Security Engineering Architecture considerations 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

CIO 2100.1 Chapter 1, The GSA Information Technology Security Program, Section 13, Cloud services states:

> *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 or a FedRAMP provisional ATO.*
>
> *b. GSA users or S/SO/Rs may leverage GSA authorized Cloud Service Provider offerings reviewed by the GSA Security Engineering Division (ISE) and approved by the GSA CISO. Allowed CSP offerings are identified in CSP approval memos on the IT Security Procedural Guides page.*
>
> *c. The use of PII can only be involved in such products/services when the ATO grants such authorization specifically. PII shall never be introduced into any pilot program at any time*

CIO 2100.1 Chapter 4, Policy for Protect Function, Section 3, Data Security states:

> *f. ISE must approve all Security Architecture designs prior to implementation.*

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 the GSA 06-30.

Role	Responsibility
Information System Security Manager (ISSM)	Oversees and coordinates ISSO activities to ensure the architecture submission sufficiently addresses required artifacts and elements identified in this guide.
Information Systems Security Officer (ISSO)	Coordinates Security Engineering and Architecture reviews with relevant stakeholders and completes and submits requests for security engineering architecture review. . The ISSO provides attestation through the security engineering checklist that all items are addressed. The ISSO submits the request for a security architecture review. The ISSO works with the ISSM to conduct a

	review prior to submission.
Security Engineer	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. Security Engineering will review feedback with ISSOs and DevOps teams to ensure sufficient understanding of requested changes; ISSOs are responsible for coordinating implementation of needed changes.

2 Security Architecture Review

GSA Security Engineering must review all proposed Security Architectures prior to the commencement of the system build (architecture, infrastructure, and code). 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 prior to implementation or redesign. In general, Security Engineering must perform a security architecture review as part of the A&A process for ALL new systems and systems undergoing a major change. See below for details.

- New Systems - During the system design phase of a new system before Assessment and Authorization; and,
- 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 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, datacenters, or the adoption of SaaS PaaS or IaaS.
    - Integration with third party services via API or making available an API 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 *GSA CIO-IT Security 06-30*, *"Managing Enterprise Risk"* and in section 2.3.2 of the *GSA CIO-IT Security 14-68*, *“Lightweight Security Authorization Process.”*

ISE will work with GSA platform teams that have ATO'd cloud platform solutions and deploy applications into standard architectures to certify the standard application deployment architecture thereby significantly streamlining the review process. In such cases, ISE will leverage DevSecOps team self-assessments against the ISE Security Architecture Checklist. Application architectures will be presumed approved unless it has clear architecture related gaps.

2.1 Security Architecture Work Flow

A summary of the Architect Review Process is as follows:

1. The ISSO reviews the security architecture checklist items to ensure their supporting diagrams and System Security Plan (SSP) have the required items
2. The ISSO submits their request through the Security Engineering Form
3. A security engineer in the Security Engineering Division (ISE) will triage the request for the following items:
    a. 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 estimate time to provide initial comments.
5. The ISE Security Engineer will review submitted architecture and provide feedback within the estimated time line. The ISE Security Engineer (upon request) is available to meet with the ISSO and DevOps teams to ensure sufficient understanding of requested changes.
6. ISSOs are responsible for coordinating implementation of needed changes to documentation and submit updates.
7. ISE will review updated documentation that is responsive to ISE comments. Once all findings are closed, notification will be emailed to ISSO, ISSM, and any relevant system POCs that the review is complete.

2.2 Step 1 - Review Security Architecture Checklist

The ensuing tables identify a series of checks, informed by existing requirements in NIST SP 800-53, Revision 4, and/or GSA or Federal IT Security policy to be 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 System Security Plan, GSA Security Engineering will use this checklist as guidance to ensure alignment of the proposed architecture to NIST Federal/GSA security requirements (i.e., NIST SP 800-53 controls) and/or GSA's security fabric (if internally hosted).

Nothing in the tables should 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: Architecture Diagram - Information System Components and Boundary Considerations

#	Checklist Item	Control Reference
1	The Authorization to Operate (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 system security plan.	CM-8 Information System Component Inventory
2	The system boundary contains all components, devices, services, communication paths (VPNs, 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). Please be sure the tables identifying ports reflect whether they are encrypted or not. Tables should easily track to the architecture diagram.	CM-8 Information System Component Inventory AC-20 – Use of External Information 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 Information System Component Inventory AC-20 – Use of External Information Systems
4	If on-prem or cloud services are used to support operation, maintenance, management, security of the services in scope of the ATO, be sure they are reflected in the network architecture with related flows. Depending on the nature and type of integration and sensitivity of the data, these dependent systems may also need to be ATO'd; usage considered for risk acceptance; or, if not risk accepted, potentially removed from the architecture. All SaaS, IaaS or PaaS leveraged that support delivery of the system must have an ATO, approved by GSA or FedRAMP.	FedRAMP Policy Memo CA-6 Security Authorization AC-20 Use of External Information Systems SA-9 External Information System Services

Table 2-2: Architecture Diagram - Information System Components and Boundary Considerations

#	Checklist Item	Control Reference
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 System Connections AC-20 Use of External Information Systems SA-9 External Information 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 2.0 Reference Architecture requires all Cloud traffic to be routed through TIC. See https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf
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) CIDR block allocations will be provided for each team or tenant of Cloud Services Providers (CSP's) 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 Provisioning for Name / Address Resolution Service
8	For public facing systems, integration with external systems including but not limited to other cloud assets via Application Programming Interfaces (APIs) or third party enablers shall be appropriately secured. Please 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	CA-3 Information System Connections AC-20 Use of External Information Systems SA-9 External Information System Services

#	Checklist Item	Control Reference
	implementing SSL/TLS connections.	
9	All access control mechanisms, such as firewalls, router 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 Information System Documentation SC-7 Boundary Protection
10	Ensure all authentication points (this includes but is not limited to AWS console, jump, machine resources, application, API, enablers, etc. [as applicable]), in the architecture diagram and described in the supporting discussion. 2FA should be for privileged, non-privileged and/or Internet accessible logins within this system. At FIPS 199 Moderate and up, all authentications shall be 2FA; privileged authentication is required to be MFA for all FIPS impact levels. Per NIST 800-63b, Digital Identity Guidelines, Authentication and Lifecycle Management, 2FA 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. 2FA methods shall favor approaches that do not expose pins to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn. **Note:** System architectures must adhere to the considerations identified in the System Boundary AD and Remote Administration Guidance document.	IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

Table 2-3: Use of Approved Software and Security Standards

#	Checklist Item	Control Reference
11	Ensure that the proposed software stack aligns with EARC approved standards. Any proposed software which is not on EARC list of approved software must reviewed by the EARC prior to inclusion in the defined architecture. The process can be found here. Proposed software will undergo a Security Review, 508 Accessibility Review, and TSC/CTO review by the EARC team.	CM-2 Baseline Configuration CM-6 Configuration Settings SA-22 Unsupported System Components

#	Checklist Item	Control Reference
12	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). If a GSA benchmark exists; it must be used for GSA IT systems; vendor owned and operated system's benchmarks may be used as approved by the AO. Hardening Guides are available on the IT Security Technical Guides and Standards page, Benchmarks are available on GitHub.	CM-6 Configuration Settings GSA IT Security Policy

Table 2-4: Data Flow and Routing Paths

#	Checklist Item	Control Reference
13	Sections 9 and or 10 of the SSP shall document all data flows in both narrative and diagram versions. Diagram(s) in this section should be sufficiently detailed and identify flows to all components and support services with source/destination, ports/protocols, or 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 track to the architecture diagram. The ports, protocols, and services table should list if the communication is encrypted or not. If not encrypted, there needs to be a description of the data contents, sensitivity, if the data is Government 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.	SA-5 Information System Documentation AC-4 Information Flow Enforcement
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 SSP.	SA-5 Information System Documentation AC-4 Information Flow Enforcement

Table 2-5: 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, SIEM, Log Management, Security Scanning, etc. Integration must be documented in prose and system diagrams.	RA-5 Vulnerability Scanning IR-5 Incident Monitoring AU-6 Audit Review, Analysis, and Reporting AU-6(1) Audit Review, Analysis, and Reporting | Process Integration AU-6(3) Audit Review, Analysis, and Reporting | Correlated Audit Repositories

Table 2-6: Key Technical Security Considerations

#	Checklist Item	Control Reference
16	FIPS 199 Low, Moderate and High systems shall utilize a GSA-approved multi-factor authentication mechanism for privileged authentication. FIPS 199 Moderate and High shall utilize a GSA-approved multi-factor authentication mechanism for non-privileged authentication as well. As a best practice, ALL Internet accessible systems regardless of FIPS 199-impact level shall implement multi-factor authentication for user-level authentication. Further, systems leveraging certificate-based authentication shall not be downgraded to only user name and password authentication. Per NIST 800-63b, Digital Identity Guidelines, Authentication and Lifecycle Management, 2FA 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. 2FA methods shall favor approaches that do not expose pins to intercept risk including but not limited to HOTP, TOTP, SAML/OIDC, PIV, FIDO/WebAuthn.	IA-2 (1) Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts IA-2 (2) Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

#	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 assures Business Continuity, (BCP), Disaster Recovery (DR) and Continuity of Operations (COOP) consistent with NIST requirement per impact FIPS 199 impact level. For further details, see the GSA CIO-IT Security-09-43, *"Key Management Guide*."	SC-12 Encryption Key Establishment and Management
18	Systems that process PII or other sensitive information shall employ encryption of data while at rest and while in transit. Authenticators (i.e., passwords), PII and 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 Data at Rest SC2-28(1) Protection of Data at Rest | Cryptographic Protection
19	Ensure encryption in particular for web services utilizes FIPS approved ciphers, FIPS validated encryption modules, at a minimum TLS 1.1 and up, HSTS, and HTTPS only. Complete details can be found in *GSA CIO-IT Security-14-69*, *"SSL/TLS Implementation Guide"*. ● Digital signature encryption algorithms - Reference: https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/Digital-Signatures ● Block cypher encryption algorithms - Reference: https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/Block-Ciphers ● Secure hashing algorithms – Reference: https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/Secure-Hashing ● Binding Operational Directive 18-01 - Reference: https://cyber.dhs.gov/	SC-8 Transmission Confidentiality and Integrity SC-8 (1) Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection SC-13 Use of Cryptography

#	Checklist Item	Control Reference
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 in order to assure high availability. * A High Availability architecture is required for FedRAMP; but not LATO.	CP-6 Alternate Storage Site CP-6 Alternate Storage Site | Separate from Primary Site CP-7 Alternate Processing Site CP-7(1) Alternate Processing Site | Separate 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 2-7: Other Considerations

#	Checklist Item	Control Reference
22	Ensure that the proposed architecture includes all applicable essential security controls as identified in the GSA 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

Table 2-8: AWS Specific Considerations

#	Checklist Item	Control Reference
24	Host backend database and services on private VPCs that are not visible on any public network.	SC-7 Boundary Protection PL-8: Information Security Architecture

#	Checklist Item	Control Reference
25	Enable encryption at rest for ALL 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 Data at Rest
26	Ensure all flows are documented in the architecture diagram. Further, encrypt all flows, including: ● 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) ● 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).	PL-8: Information Security Architecture SC-8 (1): Transmission Confidentiality and Integrity BOD 18-01 https://cyber.dhs.gov/bod/18-01/
27	VPC peering transmits data in the clear through AWS's backbone; it may be acceptable in certain use cases (e.g., when data is non-sensitive (e.g., NTP, DNS when not publicly resolving, etc.); or, when the protocols traversing the peering connection is itself encrypted (e.g., SSL, SSH, SRDP, etc.). 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 CSR, the latter has proved most effective.	SC-8 (1): Transmission Confidentiality and Integrity
28	Egress flows require the ability to regulate traffic via URL; not just port, protocol, and IP. AWS 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
29	SSL termination should extend through to the web server. If terminating at ELB, extend through to the VPC with ALB (SSL offloading).	SC-8 (1): Transmission Confidentiality and Integrity

#	Checklist Item	Control Reference
30	If leveraging AWS services for boundary protection, need to be implement AWS 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 enhance DOS protection.	SC-7 Boundary Protection PL-8: Information Security Architecture
31	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: Information Security Architecture
32	Egress/ingress perimeter security devices that include AWS WAF, Shield Advanced, AWS SGs/NACLs, and proxy/fw for outbound url filtering and ssl packet decryption (when necessary) is suitable.	SC-7 Boundary Protection PL-8: Information Security Architecture
33	Ensure AWS services used are either FedRAMP authorized or approved for usage by GSA. Reference the ISE Master AWS Services Tracking List Current Version If desired service is not reviewed or FedRAMP approved, you may submit a request to seceng@gsa.gov.	CM-7 (5): Least Functionality | Authorized Software/Whitelisting
34	Required Key AWS Security Services: ● 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 SecurityHub, GuardDuty, Macie, CloudFront and AWS WAF are other services that could be enabled to address a capability gap.	PL-8: Information Security Architecture
35	Required IAM configurations for GSA Incident Response Support ● 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

2.3 Step 2 – Provide Security Architecture for Review

Security architecture reviews can be submitted to the Security Engineering Division via the SecEng Security Architecture Checklist Form in Google. The Checklist form is intended to assist ISSOs 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 System Security Plan (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 SDLC approach to system development may result in an iterative, rapidly change security architecture. We recommend 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 LATO processes, ISE must approve the final security architecture prior to go-live. We encourage system owners to account for this review when determining project scheduling.

2.4 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 Lightweight Authorization or Operate 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, 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. 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.

3 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.

3.1 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, please see appendix B below. In order 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, please 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 or not 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 in order to assist with the review.

GSA Security Engineering reviews new technology in coordination with the Enterprise Architecture Review Committee approval process. New technology reviews and approvals will be performed by ISE as a matter of routine. The GSA CISO will be consulted for exceptional technologies. For new software consideration, please contact the Enterprise Architecture Review Committee. The EARC will contact Security Engineering to coordinate the review of the software.

Appendix A: AWS Architecture Best Practices

This section 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, system's designed in AWS are balanced by trade-offs between pillars tailored to individual system needs. Trade-offs mainly occurs 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 well architected system.

1. 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	● 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	● Develop all systems in multiple availability zones (AZs). ● Moderate and High system classifications should leverage multi-regional deployments.

Best Practice	Recommendations
Network Topology	● Plan for connectivity requirements to legacy data centers. ● Have highly 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. ● Ensure no overlapping of private IP addresses.
Failure Management	● Test Recovery Procedures and responses to unexpected events and component failures. ● Learn from operational events and failures by capturing and review all operational events and using them for improvements. ● Ensure adequate backups are performed. ● Automatically recover from failure. ● Test production systems at full scale load.

2. 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, review your choices on a continual basis to ensure you're taking advantage of an evolving platform. Continually benchmark, load test, and monitor your environment to have the data needed to inform change.

Table A-2: Performance Efficiency Best Practices

Best Practice	Recommendations
Democratize Advanced Technologies	● Consume new technology and rely on services rather than hosting and building your own.

Best Practice	Recommendations
Keep the Data Close to Customers to Minimize Latency	● 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	● Leverage services such as storage that can host a web server removing the operational burden.
Experiment More Often	● Quickly carry out comparative testing on different types of storage, services, and components.
Mechanical Sympathy	● Use of technology that aligns best with what you're trying to achieve
Component Selection	● Component Selection (Compute, storage, database, network) - Select components specific to your needs, and often there is a need to combine multiple approaches. o Compute: Instances (virtual servers), Containers (run an app and dependencies in resource isolated processes), and Functions (area provided to execute your code). o 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. o Database: Select a DB solution based on your requirements for availability, consistency, partition tolerance, latency, durability, scalability, and query capability. Critical to consider access patterns and workload. o 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.

Best Practice	Recommendations
Review	● 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	● 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	● Think about available trade-offs in conjunction with business needs in order to select optimal approach. ● Can trade consistency, durability, and space, vs time or latency to deliver higher performance. ● Consider read-replicas of data or caching solutions.

3. 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	● Monitor and report on only items critical to business objectives.
Operate with Code	● 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
Automate Processes	● 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	● Responses to unexpected operational events should be automated. Not just alerting, but for mitigation, remediation, rollback and recovery activities.

Best Practice	Recommendations
Make Regular, Small, Incremental Changes	● 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	● Use queuing systems, streaming systems, workflows, load balancers, etc. to minimize dependencies.
Graceful Degradation	● 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	● 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	● Operations should be standardized and manageable on a routine basis. ● Focus on small frequent changes, regular quality assurance testing, tracking and auditing changes.

4. 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	● 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 EC2 key-pairs; leverage IAM roles for EC2 ● Institute least privilege principle.
Detective Controls	● 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 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.

Best Practice	Recommendations
Data Protection	● 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.
Incident Response	● Implement detailed logging of events and changes for analysis. ● Configure automatic log processing and alerting. ● Conduct forensics in an isolated environment.
Shared Service Model	● Ensure all parties are aware of their responsibilities.
Automate	● 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	● Leverage AWS Security services, WAF, Shield, Inspector, Trusted Advisor, CT, CW, IAM,
Egress Flow	● 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	● Using approved services (FedRAMP / CISO conditional) (Link to master AWS services approval sheet)

5. 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 in order to optimize over time.

Table A-5: Cost Optimization Best Practices

Best Practice	Recommendations
Adopt a Consumption Model	● Pay for what you use. ● Use scaling in production. ● Shut down test / dev resources when not in use.
Use Managed Services	● Use managed services to reduce costs instead of building out your own infrastructure.
Licensing	● Review and consider license costs of various options.
Pick Cost-Effective Resources	● 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	● 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	● 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. ● Manage limits to avoid over-provisioning.
Optimize Over Time	● Be aware of new services and features as they become available. ● Regularly review your deployments.

References:

AWS Security Best Practices (August 2016) - Authoritative guidance for security when using AWS services.
AWS Well-Architected Framework (November 2017) - Overview of the Well-Architected Framework to validate your architecture.
Architecting for the Cloud: AWS Best Practices (February 2016) - Prescriptive guidance for architects designing solutions with AWS services.
AWS White Papers - Compilation of AWS Whitepapers covering topics such as architecture, security, and economics.
AWS Documentation – Detailed AWS service documentation.

Appendix B: AWS Service Approvals

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. In order 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 a tracking document of approved services and usage conditions. This tracking document, linked here, 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 memo, signed by the GSA CISO, formally approves the above linked AWS services tracking 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 my 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 w/out 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 2 weeks.

Appendix C: PostgresSQL Database Encryption

If utilizing a Postgres database and storing, PCI, PII and authenticator data in the database, ensure you can encrypt the data in the database. 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 PostgresSQL as a database solution presents a challenge to meeting this requirement because native Postgres encryption solutions are not available. There are several options to meeting this requirement if using PostgresSQL.

- **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 PostgresSQL 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.