New Jersey Office of Information Technology

February 20, 2020

Overview - IT Circular

NJOIT Enterprise Public Cloud — 20-01-A-NJOIT

Security Foundations, Risks, and Responsibilities Overview

OVERVIEW

The State of New Jersey's increased reliance on cloud service providers (CSPs) can enhance agility, nimbleness, and potentially reduce costs by relying on automation and globally-shared resources; however, Agencies must fully accept the risks of operating within this unique cloud reliance.

CSPs generally operate with a "shared responsibility model." CSPs are completely responsible for the security of physical security of data center facilities through the hypervisor layer,[1] and Agencies are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud, as well as for architecting applications and systems to implement enhanced data security controls that may apply. Each CSP provides multiple tools to aid Agencies in meeting their requirements.

NJOIT provides foundational security controls built within the overall tenancy to aid in securing the enterprise environment and in compliance with baseline Statewide Information Security Manual (SISM) requirements. Utilizing NJOIT's enterprise public cloud (EPC) service offerings does not, of course, relieve Agencies of accountability of fulfilling their portion of the responsibility model.

PUBLIC CLOUD SERVICE PROVIDER SECURITY RESOURCES

Amazon Web Services (AWS)

AWS publishes several whitepapers and guides to assist users in implementing best practices in cloud deployments found here: https://aws.amazon.com/whitepapers/. Key AWS whitepapers include:

- AWS Security Best Practices;
- AWS Risk and Compliance Overview;

[1] Depending on the service, the CSP may take greater responsibility and control for security. For example, in a database as a service (DaaS) offering, e.g. Amazon RDS or Azure Cosmos DB etc., the CSP provides a fully managed "serverless" database platform where the customer does not have responsibility for the security of either the underlying operating system or servers.

- AWS Well Architected Framework – Security Pillar; and
- NIST Cybersecurity Framework (CSF) – Aligning to the NIST CSF in the AWS Cloud.

Microsoft Azure

Microsoft publishes several whitepapers to assist in implementing security best practices: https://docs.microsoft.com/en-us/azure/security/. Key Azure whitepapers include:

- Shared Responsibilities for Cloud Computing;
- Azure Security Foundations Benchmark;
- Security Best Practices for Azure Solutions; and
- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

Because NJOIT's EPC services are built entirely within the commercial cloud space, the controls and process required to meet the FBI's Criminal Justice Information Services division (CJIS) are unavailable. For a detailed baseline control matrix, please see the Cloud Security Alliance (CSA) documentation for these two providers:

- AWS CSA Self-Assessment – Consensus Assessments Initiative Questionnaire v. 3.0.1: https://cloudsecurityalliance.org/star/registry/amazon/

- Azure CSA Self-Assessment – Consensus Assessment Initiative Questionnaire v3.0.1 and STAR Certification v1: https://cloudsecurityalliance.org/star/registry/microsoft/

NJOIT ENTERPRISE PUBLIC CLOUD SECURITY FOUNDATION

NJOIT Shared Services

NJOIT hosts several shared services that support both of NJOIT's EPC services. Shared services include procurement and contract management tasks for the enterprise environment, private connectivity to the public clouds, firewalls, and internet ingress and egress access points connecting the public cloud to the internet.

- **Access to the public cloud** is facilitated through either a virtual private network (VPN) connections or a direct private circuit, e.g. DirectConnect/ExpressRoute. NJOIT is responsible for providing Agencies access to these shared resources, which will be provisioned only upon written request from Agencies, which specifies the exact source and destination IPs. Access should be as limited as reasonably possible to meet business requirements.

- **Access from public cloud to the internet** is facilitated through virtual internet gateways existing within the public cloud. Because unrestrained internet access presents a

potential risk to the entire public cloud entitlement and to on-premises resources via the direct connectivity with the public cloud, all internet access must be provisioned by NJOIT. Requests for internet access must be submitted in writing to NJOIT, and non-standard requests may involve conversations with the Office of Homeland Security (OHSP) and NJOIT's Internal Security Unit (ISU). In order to control risks presented by internet access, NJOIT and OHSP may request additional security controls or infrastructure architecture changes before internet access is approved and provisioned. Web application firewall (WAF) protection will also be required.

- **Intra-cloud communications**, meaning communications within virtual private clouds (VPCs) or subnets in a single public cloud service provider, are largely the responsibility of the Agency. However, communications between VPCs will require NJOIT provisioning, because these communications are facilitated by shared resources.

- **Security of communications** is facilitated by deployment of virtual firewall appliances with Layer 7 filtering capabilities.

NJOIT will review and approve requests to utilize shared services such as internet ingress/egress gateways and direct circuits. Where a solution represents an unacceptable risk to enterprise-shared services or on-premises resources, access may be denied. While Agencies using the *EPC Self-Hosted* service are solely responsible for the design and architecture of solutions deployed in the public cloud environments, Agencies must ensure full compliance with the SISM and all applicable laws, regulations, and adhere to cloud architecture best practices.

Additional Security Foundation Controls

In addition to controlling all traffic into and out of the public cloud space and all access to and from the internet, NJOIT has implemented baseline fundamental controls to assist in compliance with the Cloud Security (CL) requirements set forth in the SISM. Attachment A is a matrix of the controls that NJOIT has implemented, along with details of the mechanisms of enforcement. This document is subject to change and will be augmented as the EPC service matures. All changes to NJOIT's Security Foundation will comply with NJOIT Circular 01-2014, OIT Internal Configuration Management and Change Control Policy.

Attachment A:
NJOIT's Enterprise Public Cloud Security Controls Matrix: Common, AWS and Azure (Confidential Security-Related Information – Available upon request to epc-mh-prod@tech.nj.gov)