We have prepared a quote for you

SOA OIT - Statewide - OIT Security Phase 1

Quote # 027627 Version 1

Prepared for:

State of Alaska - SSO

Mark Breunig
mark.breunig@alaska.gov

Prepared by:

Alaska Communications Services, Inc.

Roger Garcia
Roger.Garcia@acsalaska.com

INTRODUCTION

The State of Alaska Office of Information Technology (or "Client," herein) understands the criticality of securing their identities, data, devices, and applications. To that end, the State of Alaska seeks assistance to review and improve their security posture using Identity & Access Management and Threat Protection tools that are provided by Microsoft in the Microsoft 365 G5 Suite.

The State of Alaska has a decentralized IT model and supports multiple State Agency IT departments such as HSS and DOR. The State of Alaska is currently using Cybereason and McAfee products for EDR/EPP and have expressed a desire to transition to Microsoft Defender ATP. Proofpoint is in place for email security, and there is an interest in Office 365 ATP. There are multiple "Shadow IT" applications running in the environment and the State of Alaska has expressed a desire to identify and regulate their usage by implementing Microsoft Cloud App Security (MCAS)

Alaska Communications / Enabling Technologies will provide a Subject Matter Expert (SME) with expertise in Office 365, Windows 10, and Enterprise, Mobility + Security suites to assist the State of Alaska in reviewing and validating their currently deployed security solutions. This technical expert will also help the State of Alaska implement and/or configure Azure Sentinel, Defender ATP, Microsoft Cloud App Security (MCAS) in the existing tenant. During this time, the State of Alaska can develop operational processes with their new security capabilities. Alaska Communications / Enabling Technologies Project Manager will coordinate prerequisites, scheduling, and deliverables.

This engagement is to be conducted in two phases:

Phase I - Education, planning, design, review and validation.

This phase begins with an assessment of the current security environment and culminates with a design and implementation road map. Once the assessment and recommendations of the existing and proposed security recommendations have been delivered, it is recommended that the State of Alaska review the deliverables with all project stakeholders. Once the review is complete, Alaska Communications / Enabling Technologies recommends a review call with the SME and Project Manager to answer any questions and make any modifications.

Phase II - Implementation, roll out, and training for up to 350 users

ALASKA COMMUNICATIONS / ENABLING TECHNOLOGIES WILL PROVIDE:

STRATEGIC ADVISORY SERVICE

The State of Alaska recognizes the strategic importance of this initiative, and how essential it is at this juncture to set a way forward with an understanding of content the State of Alaska needs to retain and secure, as well as new responsibilities the IT organization will likely be assuming as part of this information protection initiative. To that end, Alaska Communications / Enabling Technologies will provide a series of consultations with its Advisory Services

Practice to review and discuss the following:

- Existing information security policy, incident response plan, and security operations center operations. Evaluate against recommended practices for cloud readiness and recommend changes to account for new threats and capabilities.
- Goals/objectives/challenges of the stakeholders as it pertains to the trade-off between productivity, security, and compliance
- Current document retention requirements, practices, and policies
- Current regulatory requirements with respect to content retention, privacy, and security
- Current data privacy requirements, practices, and policies
- Changes to IT/SOC roles and responsibilities
- Revisions to IT/SOC operations
- Organization change management implications of new Microsoft information protection/data loss features
- Data Classification and Retention Policy to align with O365 requirements

Alaska Communications / Enabling Technologies Adviser will provide recommendations for refinement of retention, privacy, and security policies, provide a framework for revised IT operations with roles and responsibilities, and areas for attention with respect to organizational change management and training. The resulting deliverable will be a Microsoft Word document from 5 to 10 pages in length.

PHASE I - PLANNING AND DESIGN SESSION

The Modern IT Enterprise Security Planning and Design Session (PDS) is to educate the State of Alaska on the path to becoming a secure modern enterprise through strategic investments in both digital transformation and security enhancements.

Primary Focus Topics:

1. Meet with technical personnel/sponsors/stakeholders to discuss the art of the possible with Microsoft security solutions
2. Review of existing Office 365, Enterprise Mobility and Security, and Windows security. Enabling will assess the current security configuration and make recommendations on changes and recommended practices.
   a. Identity and Access Management
      i. Identity-based security measures such as multi-factor authentication (MFA) and conditional access policies
      ii. Discuss password strength and multi-factor authentication (MFA) of important user accounts, and the potential impact to end users
      iii. Global banned password list
      iv. Self-service password reset (SSPR), password change, and account lockout
      v. Self-service group management (SSGM)
      vi. Single sign-on
      vii. Conditional access
      viii. Credential Guard, Device Guard or VPN
      ix. Azure AD Identity Protection (EMS G5)

x. Privileged Identity Management (EMS G5)

b. Threat Protection

i. Exchange Security

1. SPF, DKIM, DMARC
2. Review of existing Exchange Transport Rules (ETR)
3. Review of spam and malware filters

ii. Office 365 Advanced Threat Protection (ATP)

1. Plan and design policies for ATP
2. Advise on testing ATP policies for Safe Links, Safe Attachments, and anti-phishing
3. Allow/Block lists
4. Zero-hour Auto-Purge (ZAP)
5. Detonation
6. ATP reports and alerts

iii. Defender Advanced Threat Protection (ATP)

1. Exploit Guard
2. EPP/EDR
3. Threat Hunting
4. Integration with Cloud App Security

iv. Microsoft Cloud App Security (MCAS)

1. Discovery and analysis of shadow SaaS
2. Sanctioned and unsanctioned applications
3. Activity auditing and logging
4. Policies, Templates and Governance
5. Custom alerting
6. Integration with Defender ATP
7. Integration with Azure Information Protection

v. Office 365 Threat Intelligence

1. Attack simulator
2. Defender ATP integration
3. SIEM integration
4. Threat explorer
5. Threat trackers

vi. Azure Advanced Threat Protection

1. Discuss identity behavior, analysis, detection, and alerting, including:
   1. Honeypots
   2. Pass the Ticket
   3. Lateral Movement
   4. Remote execution
   5. Reconnaissance
   6. Abnormal modification of sensitive groups
   7. Malicious replication of directory services
   8. Suspicious authentications

        9. Azure Advanced Threat Protection integration with Defender ATP

vii. Azure Sentinel

1. Tech Overview
2. Discussion of applicability within State of Alaska environment
3. Gather requirements for data sources:
    1. M365 & Azure
    2. AWS
    3. On-premises (firewalls, proxies, appliances) and protocols (CEF, logstash, Syslog, Sentinel REST API)
        - a. Educate/outline integrations for F5, Zscaler, Palo, ASA, and Meraki
4. Outline requirements for on-premises collector, and ideal positioning within OCS (and possibly agency) infrastructures
5. Discuss cost elements
    1. Explain tradeoffs between cost and analytic tradeoffs of ingesting some inputs to MCAS vs Sentinel
6. Discuss runbooks and automations/integration with Azure Logic Apps to optimize SOC resources
7. Educate on Kusto Query Language and its application within Sentinel

viii. Insider Risk Management:

1. Explain, demonstrate, and evaluate the applicability of Information Barriers

ix. Microsoft Endpoint Manager (Formerly Intune)

1. Lead envisioning sessions outlining capabilities, caveats, and options for:
    1. Microsoft Intune for mobile device management (MDM) and mobile application management (MAM):
        - a. MAM policies to help prevent data leakage
        - b. Device policies like PIN or device encryption
        - c. Conditional access and compliance policies:
        - d. Ensure design is in alignment with security goals while maximizing productivity
        - e. Review client's information security policies and map requirements to EM+S functionality
2. Windows 10 features:
    1. Azure Active Directory Join
    2. Windows Hello for Business
    3. MDM auto-enrollment
    4. Self-service Bitlocker recovery
    5. Additional local administrators
    6. Enterprise State Roaming
    7. Attack Surface Reduction

x. Current environment discovery and analysis:

1. Perform discovery of the existing Active Directory and Office 365 environment
2. Review 3rd-party MDM solution currently in use (If applicable)

xi. Design Planning:
   1. Work closely with State of Alaska to create and/or modify security plan
   2. Consult to learn needs regarding design and integration
   3. Research required components and system integration notes
   4. Whiteboard sessions with State of Alaska to complete designs and migration plan
   5. Answer questions regarding compliance, risk management, mitigation and auditing

xii. Advanced security reporting and alerting

c. Azure Information Protection (AIP) and Data Loss Prevention (DLP)

i. Review applications and features associated with Security in Office 365:
   1. Discuss goals, objectives, and challenges with information protection
   2. Discuss scope of sensitive organization data to be protected
   3. Identify sensitive organization data requiring persistent protection
   4. Discuss classification and labelling
   5. Discuss discovery of in-scope data to be protected

ii. Enterprise Mobility + Security (EM+S):
   1. Azure Information Protection (AIP):
      1. Retain control of sensitive documents
      2. Automatically protect mail containing privileged information
      3. Ensure files stored in SharePoint are rights protected
      4. Message encryption
      5. File classification and labelling
      6. Define services, applications, and workloads to be considered for AIP discovery
      7. Define protection policies

iii. Additional DLP Policies:
   1. Determine the scope for whom to apply to DLP policy to
   2. Determine the sensitive information types to protect (Credit Card, SSN, custom, etc.)
   3. Determine the amount of sensitive data instances a document or email can contain before being blocked
   4. What other sensitive data should be included in besides the default types?
   5. Determine whom to send Incident reports to. (i.e. Compliance Officer)
   6. Determine plan to inform and train end users on policies

iv. Planning:
   1. Review State of Alaska data policies in advance to understand driving business requirements:
      1. What rights / restrictions will employees have to store / share files online
      2. If / what data should be stored / sent from the cloud as confidential
      3. Which Data Loss Prevention (DLP) capabilities should be employed (Office 365 capabilities, EMS options, or something else)
   2. Discover sensitive organization data to be protected
   3. Perform Gap Analysis

v. Design:
   1. Work closely with State of Alaska to create and/or modify the data management plan

        2. Consult to learn needs regarding design and integration
        3. Research required components and system integration notes (as needed)
        4. Whiteboard sessions with State of Alaska to complete designs and plan
        5. Answer questions regarding compliance, risk management, mitigation and auditing
3. Ensure design is in alignment with security goals while maximizing productivity

ADOPTION & CHANGE MANAGEMENT ENVISIONING SESSION

The Modern IT Enterprise Security Planning and Design Session (PDS) is to educate the State of Alaska on the path to becoming a secure modern enterprise through strategic investments in both digital transformation and security enhancements.

Primary Focus Topics:

1. Meet with technical personnel/sponsors/stakeholders to discuss the art of the possible with Microsoft security solutions
2. Review of existing Office 365, Enterprise Mobility and Security, and Windows security. Enabling will assess the current security configuration and make recommendations on changes and recommended practices.
    a. Identity and Access Management
        i. Identity-based security measures such as multi-factor authentication (MFA) and conditional access policies
        ii. Discuss password strength and multi-factor authentication (MFA) of important user accounts, and the potential impact to end users
        iii. Global banned password list
        iv. Self-service password reset (SSPR), password change, and account lockout
        v. Self-service group management (SSGM)
        vi. Single sign-on
        vii. Conditional access
        viii. Credential Guard, Device Guard or VPN
        ix. Azure AD Identity Protection (EMS G5)
        x. Privileged Identity Management (EMS G5)
    b. Threat Protection
        i. Exchange Security
            1. SPF, DKIM, DMARC
            2. Review of existing Exchange Transport Rules (ETR)
            3. Review of spam and malware filters
        ii. Office 365 Advanced Threat Protection (ATP)
            1. Plan and design policies for ATP
            2. Advise on testing ATP policies for Safe Links, Safe Attachments, and anti-phishing
            3. Allow/Block lists
            4. Zero-hour Auto-Purge (ZAP)
            5. Detonation
            6. ATP reports and alerts
        iii. Defender Advanced Threat Protection (ATP)

1. Exploit Guard
2. EPP/EDR
3. Threat Hunting
4. Integration with Cloud App Security

iv. Microsoft Cloud App Security (MCAS)

1. Discovery and analysis of shadow SaaS
2. Sanctioned and unsanctioned applications
3. Activity auditing and logging
4. Policies, Templates and Governance
5. Custom alerting
6. Integration with Defender ATP
7. Integration with Azure Information Protection

v. Office 365 Threat Intelligence

1. Attack simulator
2. Defender ATP integration
3. SIEM integration
4. Threat explorer
5. Threat trackers

vi. Azure Advanced Threat Protection

1. Discuss identity behavior, analysis, detection, and alerting, including:
   1. Honeypots
   2. Pass the Ticket
   3. Lateral Movement
   4. Remote execution
   5. Reconnaissance
   6. Abnormal modification of sensitive groups
   7. Malicious replication of directory services
   8. Suspicious authentications
   9. Azure Advanced Threat Protection integration with Defender ATP

vii. Azure Sentinel

1. Tech Overview
2. Discussion of applicability within State of Alaska environment
3. Gather requirements for data sources:
   1. M365 & Azure
   2. AWS
   3. On-premises (firewalls, proxies, appliances) and protocols (CEF, logstash, Syslog, Sentinel REST API)
      a. Educate/outline integrations for F5, Zscaler, Palo, ASA, and Meraki
4. Outline requirements for on-premises collector, and ideal positioning within OCS (and possibly agency) infrastructures
5. Discuss cost elements
   1. Explain tradeoffs between cost and analytic tradeoffs of ingesting some inputs

to MCAS vs Sentinel

6. Discuss runbooks and automations/integration with Azure Logic Apps to optimize SOC resources
7. Educate on Kusto Query Language and its application within Sentinel

viii. Insider Risk Management:

1. Explain, demonstrate, and evaluate the applicability of Information Barriers

ix. Microsoft Endpoint Manager (Formerly Intune)

1. Lead envisioning sessions outlining capabilities, caveats, and options for:
    1. Microsoft Intune for mobile device management (MDM) and mobile application management (MAM):

        a. MAM policies to help prevent data leakage
        b. Device policies like PIN or device encryption
        c. Conditional access and compliance policies:
        d. Ensure design is in alignment with security goals while maximizing productivity
        e. Review client's information security policies and map requirements to EM+S functionality
2. Windows 10 features:
    1. Azure Active Directory Join
    2. Windows Hello for Business
    3. MDM auto-enrollment
    4. Self-service Bitlocker recovery
    5. Additional local administrators
    6. Enterprise State Roaming
    7. Attack Surface Reduction

x. Current environment discovery and analysis:

1. Perform discovery of the existing Active Directory and Office 365 environment
2. Review 3rd-party MDM solution currently in use (If applicable)

xi. Design Planning:

1. Work closely with State of Alaska to create and/or modify security plan
2. Consult to learn needs regarding design and integration
3. Research required components and system integration notes
4. Whiteboard sessions with State of Alaska to complete designs and migration plan
5. Answer questions regarding compliance, risk management, mitigation and auditing

xii. Advanced security reporting and alerting

c. Azure Information Protection (AIP) and Data Loss Prevention (DLP)

i. Review applications and features associated with Security in Office 365:

1. Discuss goals, objectives, and challenges with information protection
2. Discuss scope of sensitive organization data to be protected
3. Identify sensitive organization data requiring persistent protection
4. Discuss classification and labelling
5. Discuss discovery of in-scope data to be protected

ii. Enterprise Mobility + Security (EM+S):

1. Azure Information Protection (AIP):
   1. Retain control of sensitive documents
   2. Automatically protect mail containing privileged information
   3. Ensure files stored in SharePoint are rights protected
   4. Message encryption
   5. File classification and labelling
   6. Define services, applications, and workloads to be considered for AIP discovery
   7. Define protection policies

iii. Additional DLP Policies:

1. Determine the scope for whom to apply to DLP policy to
2. Determine the sensitive information types to protect (Credit Card, SSN, custom, etc.)
3. Determine the amount of sensitive data instances a document or email can contain before being blocked
4. What other sensitive data should be included in besides the default types?
5. Determine whom to send Incident reports to. (i.e. Compliance Officer)
6. Determine plan to inform and train end users on policies

iv. Planning:

1. Review State of Alaska data policies in advance to understand driving business requirements:
   1. What rights / restrictions will employees have to store / share files online
   2. If / what data should be stored / sent from the cloud as confidential
   3. Which Data Loss Prevention (DLP) capabilities should be employed (Office 365 capabilities, EMS options, or something else)
2. Discover sensitive organization data to be protected
3. Perform Gap Analysis

v. Design:

1. Work closely with State of Alaska to create and/or modify the data management plan
2. Consult to learn needs regarding design and integration
3. Research required components and system integration notes (as needed)
4. Whiteboard sessions with State of Alaska to complete designs and plan
5. Answer questions regarding compliance, risk management, mitigation and auditing

3. Ensure design is in alignment with security goals while maximizing productivity

ADOPTION & CHANGE MANAGEMENT ENVISIONING SESSION

Custom User Communications Plan

Alaska Communications / Enabling Technologies will host a communications planning session with stakeholders responsible for communicating the change. During this exercise, Alaska Communications / Enabling Technologies and Client will further define key persona types and differentiators. Grouping workers in this way is a critical initial step in a successful communications plan. This method allows for development of “What’s in it for me?”, or WIIFM content.

Key organizational goals associated with the change initiative will be incorporated to drive the desired cultural shift to a Modern Workplace. Such goals may support financial, cultural, or interpersonal concerns for Client; supporting these objectives as part of the WIIFM-based communication plan is paramount to an inclusive and cohesive strategy.

Alaska Communications / Enabling Technologies will create a Communications Plan for the State of Alaska to address the following key areas:

- Change initiative: who, what, when, where, why and how
- Target personas or usage profiles
- Key messaging for M365 security feature impacts
- Communications Calendar
- Communication overview
    - Target audience
    - Delivery time and channel
    - Accountability for execution of each suggested communication

Custom Training Plan

Alaska Communications / Enabling Technologies will host a training planning session for the State of Alaska resource(s) responsible for preparing resources to train staff. Alaska Communications / Enabling Technologies will document a holistic training plan supporting those impacted by the change. This plan will detail:

ADOPTION PROGRAM DEPLOYMENT SERVICES

Custom End User Communications

Alaska Communications / Enabling Technologies will leverage the communication plan to design a custom branded communication template for use when communicating to staff. Each communication will showcase similar branding to drive brand recognition. The communication plan will dictate the messaging and communication template needs for this change. WIIFM, ‘What’s in it for me?’ content will be prevalent among the template along with necessary calls to action.

Alaska Communications / Enabling Technologies will create up to ten communications templates to reach up to eight key usage personas. Each communication will be designed to drive awareness and engagement leading the use of Teams Voice and the associated devices.

Up to two rounds of edits will be made to support changes to the communications, additional edit requests billed as time and materials.

The State of Alaska to provide the Alaska Communications / Enabling Technologies Adoption Consultant with email credentials for the State of Alaska to allow for deployment of communications to end users from an internal source.

Training Services

Alaska Communications / Enabling Technologies will leverage the training plan to dictate content development and training needs. Content development and training hours are included within this plan.

Up to fifty hours of content development and training support will be provided by Alaska Communications / Enabling Technologies Trainers. Content development will be based on that outlined in the training plan, but may include:

- PowerPoint training deck(s) for the device
- Quick reference guides
- Video shorts (1-3 min videos, topical content)
- Recorded webinar training session

Optional training services:

- Train-the-trainer webinar or in-person session(s)
  - This is not an end-user training session, content is designed and delivered to prepare others for delivering end-user training
- Remote webinar or in-person session(s)
  - Focused content to successfully adopt by persona

REMEDIATION

Up to twelve hours of remediation activities based on the outcome of the Microsoft security review. If less than twelve hours of remediation is needed, the remaining hours could be applied towards technical training and proof of concept. If more than twelve hours of remediation are required, Alaska Communications / Enabling Technologies will consult with the State of Alaska and decide if training and proof of concept hours would be applied towards remediation. Alaska Communications / Enabling Technologies will be able to provide an estimate of remediation hours needed following completion of the Microsoft security review

PHASE II – PRODUCTION PILOT

The Modern IT Enterprise Security Implementation will provide a better opportunity to evaluate the functionality, user experience, and deployment of these features to prevent, detect, and respond to cyber-attacks, protect intellectual property, and maintain a competitive advantage in the marketplace. All work will be completed on the State of Alaska's OIT Azure and O365 tenant.

Primary Focus Topics:

1. Configuration within Existing Tenant
   a. For each of the security services listed and of interest, Enabling will:
      i. Review/explain the purpose and strategy of each service
      ii. Activate the licenses (if needed)
      iii. Assign licenses to up to 350 users
      iv. Review the configuration / policy options of each service
      v. Configure Role Based Access Controls for up to five (5) personas
      vi. Make initial configurations of up to two policies for each security service of interest

    vii. Test to ensure experience is as expected

b. Services covered include:

    i. Identity and Access Management

        1. Configuration of MFA and conditional access policies
        2. Configuration of Global banned password list
        3. Self-service password reset (SSPR), password change, and account lockout
        4. Self-service group management (SSGM)
        5. Azure AD Identity Protection
        6. Privileged Identity Management (EMS G5)

    ii. Threat Protection

        1. Configuration of Exchange Online SPF, DKIM and DMARC Records
        2. Configuration of Office 365 ATP Safe Links and Safe Attachment policies
        3. Configure up to five anti-spoofing rules and other configurations available on protection.office.com

    iii. Defender Advanced Threat Protection (ATP)

        1. Enrollment of up to 350 Windows or Mac devices
        2. Demonstrate inventory, threat intelligence
        3. Configure cloud-enablement and block at first sight
        4. Integrate with MCAS and Azure ATP
        5. Demonstrate Advanced Hunting
        6. Configure and demonstrate auto-remediation
        7. Demonstrate remote removal of malware using Live Response feature

    iv. Microsoft Cloud App Security (MCAS)

        1. Activate MCAS (Requires Global Administrator or Security Administrator permissions)
        2. Enable Cloud Discovery
        3. Enable ingestion from up to two supported firewalls or proxies
        4. Configuration of up to three custom alert policies
        5. Configure OneDrive for Business restore controls
        6. Enable integration into other Microsoft Services (i.e. Defender ATP, Sentinel, etc)
        7. Demonstrate reporting and controls of shadow and 3rd party IT

            a. G Suite and in as much as possible, AWS (where client has S3 buckets and some databases)

    v. Office 365 Threat Intelligence

        1. Execute simulated Spear Phishing Attack, demonstrate report
        2. Execute simulated Brute Force Password (Dictionary Attack), demonstrate report
        3. Execute Password Spray Attack, demonstrate report

    vi. Azure Advanced Threat Protection

1. Set up monitoring of up to ten domain controllers, including:
    a. Identity behavior analysis and detection
    b. Honeypots
    c. Pass the Ticket
    d. Lateral Movement

vii. Azure Sentinel

1. Set up initial configurations
    a. Create Log Analytics work space
    b. Define retention period
    c. Assign RBAC group permissions
8. Connect up to three service to service data sources
    a. Microsoft Threat Protection solutions configured
    b. Office 365
    c. Azure Activity
9. Configure Azure Sentinel Workbooks
    a. Add up to three Built-In Workbooks
    b. Add up to one custom workbook
10. Configure Azure Sentinel Analytics
    a. Create up to three new detections queries
    b. Enable up to three built in rules
    c. Create up to three custom analytic rules with schedules
    d. Activate Advanced Multistage Attack Detection
        i. Microsoft Cloud App Security
        ii. Azure Active Directory Identity Protection
        iii. Microsoft Defender ATP
11. Configure Azure Sentinel Playbooks
    a. Create up to two security playbooks:
        i. Create automated threat responses for each of the two security playbooks created.
12. Provide Training and Demonstration on Azure Sentinel operations
    a. Hunting
        i. Built-in and customized hunting queries
        ii. Live stream Hunting
        iii. Bookmarks
        iv. Up to two hours of Kusto Query Language training
    b. Incident Management
    c. Workbooks

iii. Microsoft Endpoint Manager (Formerly Intune)

1. Configure Intune to secure, control and manage OIT-owned and BYOD devices and apply up to nine policies using a combination of Windows, Mac OS X, iOS and Android Operating Systems to:
    a. Enforce OS updates
    b. Enforce Anti-Virus software usage
    c. Mobile Application Management (MAM)
2. Configure Intune to secure, control and manage BYOD mobile devices via mobile application management (MAM) capabilities:
    a. Password Policies
    b. Manage / Configure Applications
    c. Corporate Data Usage and Sharing
    d. Remove Company Data
    e. Single Sign On
    f. Multi-Factor Authentication
    g. Conditional Access
3. Configure Intune to secure, control and manage company owned mobile devices via mobile device management (MDM) and mobile application management (MAM) capabilities:
    a. Full control of device
4. Create device profiles for managed devices, and demonstrate the process to State of Alaska’s IT staff
5. Apply application protection policies to protect corporate data usage
6. Define Intune Device compliance policies
7. Apply Intune configurations to up to ten Production Pilot users and Enabling to standby to assist up to an additional 350 OIT users:
    a. Select pilot users from a range of suitable device “owners”
    b. Test Intune configurations
    c. Remediate as needed
    d. Demonstrate the process to State of Alaska’s IT staff

iv. Azure Information Protection and DLP

1. Prepare tenant for AIP:
    a. Enable information rights management
    b. Configure Office 365 Message Encryption
2. Validate AIP templates
3. Create security groups to scope AIP policies
4. Configure super users for data recovery as required
5. Deploy AIP Scanner Server:
    a. Prerequisites:

            i. Server 2012 R2 or 2016:
                1. 4CPU, 8GB RAM (More RAM the better performance)
                2. Internet Connectivity
            ii. SQL 2012 or greater:
                1. Local or remote
                2. Express or above
            iii. Service account on-prem and synced to Azure AD:
                1. Log on locally and log on as a service right
                2. Read to each repository for discovery, Read/Write for classification/protection
            iv. AzInfoProtection.exe available on the Microsoft Download Center (The scanner bits are included with the AIP Client)
            v. Labels configured for AIP set to Automatic Classification/Protection
        b. Run AIP Scanner tool to discover sensitive organization data on one file server

6. Configure up to two (2) AIP Policies:
    a. For each policy, configure up to five labels
7. Configure Office applications and services for AIP
8. Deploy Azure Information Protection client to up to six Windows clients
9. Demonstrate the process of configuring policies to the State of Alaska IT Team
10. Configure DLP:
    a. Create up to three DLP policies:
        i. Simple, single use policies to validate their function and effectiveness
        ii. Review and evaluate in monitoring mode for tuning purposes
    b. Demonstrate the process of configuring policies to the State of Alaska IT Team

TRAINING AND KNOWLEDGE TRANSFER

Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as informal activities provided when the State of Alaska associates, or contractors, are working side-by-side with Alaska Communications / Enabling Technologies that include: whiteboard discussions, email threads, conference calls, and facilitated meetings on technical topics. Knowledge transfer activities are secondary to completing work products and maintaining the project schedules.

Technical Training and Proof of Concept for Microsoft G5 Components

Up to forty hours of technical training will be provided to educate and assist the State of Alaska in configuring the following Microsoft features:

1. Azure Active Directory

2. Office 365 ATP
3. Azure Advanced Threat Protection
4. Microsoft Defender Advanced Threat Protection
5. Microsoft Cloud App Security
6. Microsoft Azure Sentinel
7. Microsoft Endpoint Manager
8. Any additional Microsoft Office 365 Features of interest in the allotted forty hours including advising, consulting, and educating other State of Alaska agencies on the above features at the discretion of the State of Alaska OIT.

Education and configuration will be conducted on the State of Alaska's actual systems. No training documentation, deliverables, work products or meeting summaries will be provided for the above session or activities.

Project Deliverables

Alaska Communications / Enabling Technologies will provide the following deliverables:

- A (15-30) page report in PDF or MS Word format including:
  - An assessment and gap analysis of the current Microsoft security environment and recommendations on suggested practices
  - Suggested prerequisite projects required prior to completing migration to the appropriate Enterprise Mobility + Security Suite model
  - A high-level plan (road map) outlining the migration to, or services to enable the in-scope services, with a suggested order of operations
- Production Tenant configuration as described above
- Up to forty hours of Microsoft G5 Training as described above
- As-built document details all applied configurations
- Final Q&A discussion with the Enabling Architect and the Project Manager about the report
- Adoption Deliverables:

- Documented End User Communication Plan & Training Plan
- End User Communication Templates
- End User Training Content

THE STATE OF ALASKA RESPONSIBILITIES

1. The State of Alaska must have production or trial licenses for each security service of interest
2. The State of Alaska must have an existing Office 365 / Azure tenant in which the proof of concept can be executed
3. Provide existing policy and governance information
4. Share knowledge of existing systems and collaborate with Alaska Communications / Enabling Technologies
5. Provide Alaska Communications / Enabling Technologies adequate access to stakeholders in compliance, governance, management

OUT OF SCOPE

The following items are out of scope unless otherwise agreed to in additional statements of work:

1. Business case development
2. A full roll-out of all security services for *all users* in the State of Alaska's tenant
3. Security discussions beyond the in-scope services above
4. Certificate or AD work, except as listed above.
5. Detailed training documentation.
6. Decommissioning of old systems.
7. Other deliverables, installation of hardware or software, or configuration of applications that are *not* specifically listed as an Enabling Technologies Corp responsibility.

CHANGE CONTROL AND CANCELLATIONS

Change Control

Both the State of Alaska and Alaska Communications / Enabling Technologies must approve any changes to the schedule, tasks, deliverables, terms, or pricing presented in this document. To request a change, the requesting party the State of Alaska or Alaska Communications / Enabling Technologies must provide a change order to the other party in writing. The Alaska Communications / Enabling Technologies Client Account Manager will review the change order and its impact on the project If both parties agree to the Change Order, the Alaska Communications / Enabling Technologies Client Account Manager will incorporate the change into the project plan and manage the change accordingly.

Initiation of Work and Scheduling

Once Alaska Communications / Enabling Technologies has received a signed Statement of Work, Alaska Communications / Enabling Technologies will identify the staffing for this project. Project staffing and activities will be scheduled based upon the date the signed Statement of Work is received by Alaska Communications / Enabling Technologies. Alaska Communications / Enabling Technologies staff will work with the State of Alaska to determine start date.

Staff

Alaska Communications / Enabling Technologies staff consists of consultants with a broad range of practical backgrounds and expertise. Alaska Communications / Enabling Technologies will draw upon this extensive pool of talent to meet the requirements of the project. Alaska Communications / Enabling Technologies will determine the appropriate staff to assign to the project based upon the requirements of the engagement and the experience, skills and availability staff.

Travel & Expenses

The consulting costs are exclusive of any required Travel and Expense charges. The State of Alaska will be billed for the actual expenses incurred for agreed upon events. If the State of Alaska, wants Alaska Communications / Enabling Technologies to follow certain travel expense guidelines, these guidelines must be provided prior to the time travel arrangements are made. Alaska Communications / Enabling Technologies will review these proposed guidelines and make reasonable effort to adhere to them as long as they are not in conflict with Alaska Communications / Enabling Technologies travel policies.

Project Billing

Alaska Communications will bill this project in four equal monthly installments of $104,597.35 beginning September 2020 through December 2020.

Project Management / Security Engineer

In support of the above mentioned scope of work, Alaska Communications will provide a Project Manager and Security Engineer

Project Manager / Security Engineer

- Assigned project manager / security engineer will support the State of Alaska security project during its standard 40-hour work week
- Alaska Communications project manager / security engineer will work with project owners directly on project tasks.
- Alaska Communications project manager / security engineer will report to OIT for overall monitoring of project and activities.
- The Project Manager / Security Engineer shall commence on September 1, 2020 and complete work December 31, 2020

The State of Alaska Deliverables

The State of Alaska will provide the following to the project manager / security engineer so that they can be successful in their endeavors and provide adequate support to the State of Alaska. Delay in providing these requirements will impact Alaska Communications / Enabling Technologies ability to complete work in a timely manner.

- Dedicated point of contact for the duration of the engagement.
- The Alaska Communications project manager / security engineer will have adequate access and connectivity to perform the tasks required for the project.
- Existing relevant documentation, will be provided by the State of Alaska to ensure timely delivery of services.
- Adequate staffing is included in this response. If the State of Alaska unexpectedly accelerates the stated time line in their request, a Change Order may be generated to cover additional staffing or overtime to meet the new deadlines.
- No formal end user training is included in this Statement of Work.
- Alaska Communications project manager / security engineer will be afforded the opportunity to complete Alaska Communications internal training and employee HR, Legal, Security, Safety, PM compliance training requirements during the standard 40- hour work week. The Alaska Communications project manager / security engineer will prioritize the State of Alaska times and needs to the maximum extent possible, and not charge the Sate of Alaska if he/she is not available to meet the State of Alaska needs during these events.
- Alaska Communications project manager / security engineer should visit client for face-to-face meetings as needed by the State of Alaska.
- The State of Alaska will provide all systems, applications, hardware, and IT devices to perform work along with applicable access credentials to buildings to perform work.

Professional Services Alaska Communications/Enabling Technologies

Description	Price	Qty	Ext. Price
Subcontractor Fixed Fee Alaska Communications / Enabling Technologies Professional Services to deliver the Microsoft 365 Security Planning/Design/Discovery and Production Pilot services for up to 350 users as defined in the provided Statement of Work	$243,029.41	1	$243,029.41
	Subtotal:		$243,029.41

Project Management / Security Engineer Fees

Description	Price	Qty	Ext. Price
Project Management	$67,200.00	1	$67,200.00
Security Engineer	$108,160.00	1	$108,160.00
	Subtotal:		$175,360.00

alaska COMMUNICATIONS.

SOA OIT - Statewide - OIT Security Phase 1

Prepared by:

Alaska Communications Services, Inc.

Roger Garcia
(907) 375-1150
Fax (907) 375-1188
Roger.Garcia@acsalaska.com

Prepared for:

State of Alaska - SSO

5th Fl. State Office Building
PO Box 110206
Juneau, AK 99811
Mark Breunig
(907) 269-6719
mark.breunig@alaska.gov

Quote Information:

Quote #: 027627

Version: 1
Delivery Date: 08/19/2020
Expiration Date: 09/11/2020

Quote Summary

Description	Amount
Professional Services Alaska Communications/Enabling Technologies	$243,029.41
Project Management / Security Engineer Fees	$175,360.00
Total:	$418,389.41

Alaska Communications generates billing and/or recognizes revenue for work performed on a monthly basis. This may consist of material delivered and accepted by the customer for storage at the customers location or if agreed upon at an Alaska Communications facility, non-tangible software licenses or subscriptions, and professional services performed to date.

Alaska Communications Services, Inc.

Signature: Bill Bishop
Bill Bishop (Sep 15, 2020 17:34 AKDT)
Name: Bill Bishop
Title: President
Date: Sep 15, 2020

Alaska Communications
R.Wardrop
2020.08.20
CONTRACTS

State of Alaska - SSO

Signature: DocuSigned by:
DFC79A53C0734CD...
Name: Bill Smith CIO
Date: 9/15/2020

Signature: Bill Bishop
Bill Bishop (Sep 15, 2020 17:34 AKDT)

Email: william.bishop@acsalaska.com

Title: President

Company: Alaska Communications