pGc Paul Garstki Consulting

INDEPENDENT REVIEW

OF A PROPOSED

SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) PROJECT

For the
State of Vermont
Agency of Digital Services (ADS)

Submitted to the
State of Vermont, Office of the CIO
by:

Paul E. Garstki, JD, Consultant
d/b/a/ Paul Garstki Consulting
344 Laird Pond Rd.
Plainfield, VT 05667
paulg.consulting@gmail.com

August 30, 2022

version 1.3a

TABLE OF CONTENTS

TABLES

1 EXECUTIVE SUMMARY

This project proposes to implement and operate a Security Information and Event Management (SIEM) system, along with supporting technology and an outsourced Security Operations Center (SOC) to make use of the system most efficiently.

Although SIEM systems are a relatively recent development, they have quickly become a core necessity for enterprise networks. In brief, a SIEM makes use of logging data already generated by most network infrastructure items (servers, firewalls, routers, switches, etc.) to allow administrators to search, analyze, and visualize the gathered data by indexing and organizing it, and to perform structured analyses, in order to identify and respond to potential and actual cyber security threats ("attacks"). Some responses are automated and can take place orders of magnitude faster than human administrators could respond. Some potential threats require the attention of analysts in a SOC, who may respond to the threat, or, if needed, escalate the analysis and response. The SOC is in constant communication with State personnel and accountable to them.

The selected vendor is NuHarbor Security, Inc., of Colchester, Vermont. With a long history of excellent performance on a wide variety of State security projects, NuHarbor has a national reputation for security expertise and accomplishment.

1.1 COST SUMMARY

Table 1 - Cost Summary

IT Activity Lifecycle:	**3**
Total Lifecycle Costs:	**$3,722,272.96**
Total Implementation Costs:	**$194,833.00**
New Annual Operating Costs:	**$1,175,813.32**
Current Annual Operating Costs:	**$0.00**
Difference Between Current and New Operating Costs:	**$1,175,813.32**
Funding Source(s) and Percentage Breakdown if Multiple Sources:	**Implementation: 100% State Operating: 100% State**

1.2 DISPOSITION OF INDEPENDENT REVIEW DELIVERABLES

Table 2 - Disposition of Independent Review Deliverables

Deliverable	Highlights from the Review *Include explanations of any significant concerns*
Acquisition Cost Assessment	Total acquisition cost is **$194,833.00.** This cost only refers to implementation services provided by NuHarbor. Annual subscription costs are significantly more. We assess the project costs as valid and appropriate. The State benefits from the fact that the project team has broad experience and knowledge in the security field, whereas a different organization might have to pay for that expertise.
Technology Architecture Review	The functional architecture as proposed is, in our view, an ideal arrangement for the State at this time. The platform is state of the art, but not "bleeding edge" technology, supporting reliability and high likelihood of a quick and successful deployment. The decision to employ SOC as a service is smart and effectively ties the whole project together by bridging State internal security resources and with the capabilities of the technology platform.
Implementation Plan Assessment	An examination of the detailed plan as listed in the proposal shows that the vendor has a clear sense of the activities required and the time expected for each. The description of the participation required of the State is clear and appropriate. We see no problems with the plan, and we think it is very likely to succeed in the defined timeframe.
Cost Analysis and Model for Benefit Analysis	The costs for this project are primarily monetary, and are well-defined, mostly by the costs as represented in the contract. The benefits for this project are overwhelmingly intangible – although significant and important – and were gleaned by interviews, project documentation, and analysis. The benefits of this project are crucial to the continued protection of the State's information assets and IT infrastructure. The costs are reasonable and proportional to the technology employed. The benefits, even though intangible, are so important to the State that we can state without qualification that they outweigh the costs.
Analysis of Alternatives	The proposed solution can be seen as a modernization project and at the same time as an automation project, because it uses computing power to accomplish analysis and response tasks that humans could not do in the same amount of time, even given an arbitrarily large staff. It is reasonable to conclude that there is no

	practical way to accomplish the same ends as a SIEM system without by other means.
Impact Analysis on Net Operating Costs	There are no current costs offset by the proposed project, and consequently there is no breakeven point for this activity.
Security Assessment	Splunk Cloud FedRAMP is authorized by the General Services Administration FedRAMP PMO at the Moderate Impact Level. Splunk Cloud is hosted in the AWS Government Cloud Plus and inherits the Security Controls of that cloud. The State has significant experience with and knowledge of AWS Government hosting, as well as a long relationship with the vendor and an understanding of the vendor's security stance. NuHarbor's proposed Splunk system is consistent in every way with the State's security requirements.

1.3 IDENTIFIED HIGH IMPACT &/OR HIGH LIKELIHOOD OF OCCURRENCE RISKS

NOTE: Throughout the narrative text of this document, **Risks and Issues are identified by bold red text**, and an accompanying tag (**_RISK_ID# _0_**) provides the Risk or Issue ID to reference the risk, response, and reference in the Risk Register.

The following table lists the risks identified as having high impact and/or high likelihood (probability) of occurrence.

Please see the **Risk & Issues Register, in Section 10**, for details.

Table 3 - Identified High Impact &/or High Likelihood of Occurrence Risks

Risk Description	RATING IMPACT/ PROB	State's Planned Risk Response	Reviewer's Assessment of Planned Response
[no risks have been identified as having high likelihood or impact]			

1.4 OTHER KEY ISSUES

none

1.5 RECOMMENDATION

We recommend that this project proceed as planned, without qualification.

1.6 INDEPENDENT REVIEWER CERTIFICATION

I certify that this Independent Review Report is an independent and unbiased assessment of the proposed solution's acquisition costs, technical architecture, implementation plan, cost-benefit analysis, and impact on net operating costs, based on the information made available to me by the State.

DocuSigned by:
Paul Garstki
493B2479DEA04AE...

8/31/2022

Independent Reviewer Signature **Date**

1.7 REPORT ACCEPTANCE

The electronic signature below represent the acceptance of this document as the final completed Independent Review Report.

DocuSigned by:
Alex Ibey
289191A4D6AB4C0...

8/31/2022

ADS Oversight Project Manager **Date**

DocuSigned by:
John Quinn
4333BDE6B4F74AB...

8/31/2022

State of Vermont Chief Information Officer **Date**

2 SCOPE OF THIS INDEPENDENT REVIEW

2.1 IN-SCOPE

The scope of this document is fulfilling the requirements of Vermont Statute, Title 3, Chapter 056, §3303(d):

2.1.1 THE AGENCY SHALL OBTAIN INDEPENDENT EXPERT REVIEW OF ANY NEW INFORMATION TECHNOLOGY PROJECTS WITH A TOTAL COST OF $1,000,000.00 OR GREATER OR WHEN REQUIRED BY THE CHIEF INFORMATION OFFICER

2.1.2 THE INDEPENDENT REVIEW REPORT INCLUDES:

A. An acquisition cost assessment;
B. A technology architecture and standards review;
C. An implementation plan assessment;
D. A cost analysis and model for benefit analysis;
E. An analysis of alternatives;
F. An impact analysis on net operating costs for the Agency carrying out the activity; and
G. A security assessment.

2.2 OUT-OF-SCOPE

- A separate deliverable contracted as part of this Independent Review may be procurement negotiation advisory services, but documentation related to those services are not part of this report.

3 SOURCES OF INFORMATION

3.1 INDEPENDENT REVIEW PARTICIPANTS

Table 4 - Independent Review Participants

Name	Date	Employer and Title	Participation Topic(s)
Tylor Lahue	July 26, 2022	ADS EPMO	Project Management
Alex Ibey	July 20, 2022	ADS EPMO	Portfolio Management
Scott Carbee	July 27, 2022	ADS Security Office	Executive/Technical/Security
David Kaiser	July 27, 2022	ADS Security Office	Executive/Technical/Security
Michael Steves	July 27, 2022	ADS Security Office	Executive/Technical/Security
William Hoffman	July 27, 2022	ADS Security Office	Executive/Technical/Security

3.2 INDEPENDENT REVIEW DOCUMENTATION

The following documents were used in the process and preparation of this Independent Review

Table 5 - Independent Review Documents

Document	Source
SIEM IT ABC Form	State
SIEM RFP Final Draft	State
SIEM State Risk Register	State
Registry of SIEM Project Participants	State
Contract for services between the State of Vermont, Agency of Digital Services (hereinafter called “State”), and NuHarbor Security, Inc. Ver 3 – 7-15-2022	State
BID SUBMISSION SECURITY INFORMATION & EVENT MANAGEMENT SOLUTION	NuHarbor, Inc.
v2Vermont SIEM Solution BAFO - NuHarbor Security - Managed SOC Services Proposal and Breakdown	NuHarbor, Inc.

MGT State of Vermont BAFO Response Final	MGT CyberSecurity Solutions, Inc.
Presidio Response to State of Vermont - SIEM RFP BAFO	Presidio
SIEM Score Averages Spreadsheet	State
Worldwide Security and Information Event Management Market Shares, 202: SaaS-Focused Rise	IDC
SPLUNK CLOUD PLATFORM SECURITY ADDENDUM	Splunk
https://www.splunk.com/en_us/about-splunk/splunk-data-security-and-privacy/accessibility.html	Splunk

4 PROJECT INFORMATION

4.1 HISTORICAL BACKGROUND

A Security Information and Event Management (SIEM) system, although a fairly recent development, is now considered a core functionality of any cybersecurity program. Currently, the State employs a multi-instance "Federation" of disparate SIEMs, which in some ways has been a hindrance when responding to a security incident. There is no "current system" to be replaced; There are some manual processes, but those processes are in correlation between other automated sources. An interviewee for the present Review put it this way, "Let's say our intrusion detection system at the State's edge of the Internet might pick something. Then that alert has to be flagged and correlated with other systems, tracked down, and correlated with a number of other systems."

For several years, the ADS has wanted to deploy an enterprise-wide SIEM, but other ADS priorities (such as platform consolidation) had taken priority. In 2021 it became clear that the Agency was ready to move on this matter. The legislature was approached for funding and granted it.

In February of 2022 the State issued a Request for Proposals (RFP) for a SIEM solution. 10 proposals were received, evaluated by a procurement team, and scored. The State requested a Best and Final Offer (BAFO) from 3 vendors, and after consideration selected NuHarbor Security, Inc., of Colchester, Vermont.

Along with the implementation of and subscription to the SIEM, the State has elected to engage NuHarbor to provide Security Operations Center services (SOC as a Service), providing the first tiers of threat detection.

4.2 PROJECT GOAL

Implement a SIEM system to provide active monitoring of security threats related to SoV technology platforms

4.3 PROJECT SCOPE

4.3.1 IN-SCOPE

- Implementation of Splunk Cloud Platform, Splunk Enterprise Security, and Splunk Security Orchestration, Automation and Response (SOAR)
- 3 years of subscription to the above systems
- NuHarbor SOC as a Service implementation and service for the same period

4.3.2 OUT-OF-SCOPE

- Upper tiers of threat response

4.3.3 MAJOR DELIVERABLES

Table 6 - Major Deliverables

Kick-off meeting, Planning and preparation of project management planning documentation.
Additional background checks, fingerprinting, populate daily status report template
• Identify access into client environment • Meet with client to review account access requirements • Provision accounts for all apps/add-ons • Provision PS engineer access to on-premise Splunk infrastructure • Validate individual account access to CLIENT on-prem Splunk infrastructure • Provision PS engineer access to Splunk Cloud • Validate individual account access to Client Splunk cloud Infrastructure • Troubleshoot and remediate access
Send daily status reports to all stakeholders
Architecture, deployment service configurations, license utilization, system overview, THP and uLimits, Splunk User Best Practices, indexing and data overview, search overview, security overview, data quality/source typing, App/Add-on installations
Install, upgrade, configure, and/or tune Splunk Instances
Create State data source configurations with: • Up to 34 data source inputs from the standard Splunk input source types • Up to 20 search-time data source types • Using a total of up to 2 CSV table lookups • Up to 30 total field extractions Client data sources are:
• Verify data model health and volumization • Configure Assets and Identities • Disable views and searches that do not apply to client data • Download, install and configure CMMC App
• Review monitoring results with STATE • Identify outstanding STATE documentation requests • Review STATE use cases and alignment to installed configuration • Schedule Administration and Development calls for Q1
Lessons learned meeting held

4.4 PROJECT PHASES, MILESTONES, AND SCHEDULE

Table 7 - Project Phases

Project Milestone
Initiation/Planning
Personnel Logistics
Access Provisioning/Remote Connectivity
Execution
Health Check
Upgrade/Configure Splunk Instance
Data Source Onboarding
ES Installation and Configuration
Professional Services Closeout call and State Acceptance
Lessons Learned

FOR IMPLEMENTATION SCHEDULE, SEE SECTION 7, ASSESSMENT OF IMPLEMENTATION PLAN

5 ACQUISITION COST ASSESSMENT

Table 8 - Acquisition Costs

Acquisition Costs	Cost	Comments
Hardware Costs	**$0.00**	*No hardware costs to State*
Licensing Costs	**$0.00**	
Implementation Services	**$153,304.00**	
State Personnel	**$23,760.00**	*Project Manager*
Professional Services	**$17,769.00**	*provided by IR consultant*
Total Acquisition Costs	**$194,833.00**	

5.1 COST VALIDATION:

Describe how you validated the Acquisition Costs.

Implementation Services costs are exactly as represented in the draft contract we reviewed[1] and consistent with the vendor's Best and Final Offer (BAFO). Project manager cost was estimated by the State at 27 weeks, 10/hrs. Weekly, for a total of $23,760.00. The Independent Review cost is per the reviewer's signed Statement of Work.

Assumptions:

- That costs paid to the vendor will be exactly as represented in the contract draft we received
- That the estimate of State personnel time and costs devoted to this project are accurate and will remain so
- That no so-far unidentified current costs will be offset by this project

5.2 COST COMPARISON:

[1] State of VT (SIEM Services) v3 (LJM Edits 7.15.22).docx

How do the above Acquisition Costs compare with others who have purchased similar solutions (i.e., is the State paying more, less or about the same)?

The SIEM platform for the proposed project, Splunk, has the largest worldwide SIEM vendor market share for 2020, at 22.4%.[2] Splunk sells their products directly to customers with the capacity and capability to install and configure the system, or through "Partners" who plan, install, configure, and sometimes operate the system. The proposed vendor, NuHarbor, is an "Elite Splunk Partner." NuHarbor has offered a 60% discount on the base Splunk subscription costs. The implementation costs above represent the fees NuHarbor charges for the implementation of the Splunk platform and the initiation ("onboarding") of the SOC as a Service offering. The NuHarbor fees are a small fraction of the annual subscription costs, so taking the annual costs into account (as we should), we assess that Vermont would be paying **less than most Splunk customers**, especially those who have the capacity to self-implement (such as large states or universities).

5.3 COST ASSESSMENT:

Are the Acquisition Costs valid and appropriate in your professional opinion? List any concerns or issues with the costs.

Yes, they are valid and appropriate. The State benefits from the fact that the project team has broad experience and knowledge in the security field, whereas a different organization might have to pay for that expertise.

Additional Comments on Acquisition Costs:

We note that the draft contract we reviewed lists the implementation and subscription costs and fees in 3 separate tables, in both the Payment Provisions and the Statement of Work. We think there may be a possibility of ambiguity should the contract be amended at some point and recommend that the State consider listing the agreed costs in only the Payment Provisions.

[2] IDC, *Worldwide Security and Information Event Management Market Shares, 2020: SaaS-Focused Rise,* pg. 5, October 2021.

6 TECHNOLOGY ARCHITECTURE REVIEW

After performing an independent technology architecture review of the proposed solution, please respond to the questions that follow.

The proposed Security Incident & Event Management (SIEM) solution comprises 2 Software as a Service (SaaS) licensed cloud-based services and 1 managed service performed by the vendor:

- **Splunk Cloud Platform** with **Splunk Enterprise Security**
- **Splunk Security Orchestration, Automation and Response (SOAR)**
- **Security Operations Center** first-tier(s) threat detection and reporting ("**SOC as a Service**")

OPERATIONAL ARCHITECTURE

Splunk Cloud Platform with Splunk Enterprise Security

Splunk is a platform designed specifically to manage the large volume of system log or "syslog" data produced continuously by IT infrastructure – servers, routers, firewalls, switches, etc. Syslog data records routine events (e.g., a successful login) as well as unusual events (e.g., a failed login attempt) and "suspicious" events (e.g., repeated failed login attempts). This data is ostensibly human-readable, but as a practical matter is so voluminous and continuous that in past decades it was mostly used forensically, to manually determine the source and extent of a breach or attack more or less after the fact. (The examples above are security-related; but syslog data is also produced for other system events, like hard-drive access, CPU temperatures, network traffic, etc.)

Splunk was developed (initially in 2004) to allow administrators to search, analyze, and visualize the gathered data by indexing and organizing it, and performing structured analyses which may be defined by the user or by third-party "apps" designed to identify particular conditions. Splunk is not exclusively a security analysis tool, as it is also used to analyze the operational health of IT infrastructure, networks, and enterprises. The present project, however, is security-oriented.

- **Splunk Cloud Platform** is a cloud-based version of Splunk Enterprise, the enterprise-class version of Splunk. The State's data is subject to a regulated environment. Consequently, the State would elect the **FedRAMP Moderate** subscription option. Splunk Cloud FedRAMP is authorized by the General Services Administration FedRAMP PMO at the Moderate Impact Level.
- **Splunk Enterprise Security** is a Splunk-sourced app which optimizes security-oriented functionality. It uses security-oriented add-ons providing dashboards, searches, and tools that summarize the security posture of the enterprise, allowing users to monitor and act on security incidents and intelligence.

Splunk SOAR

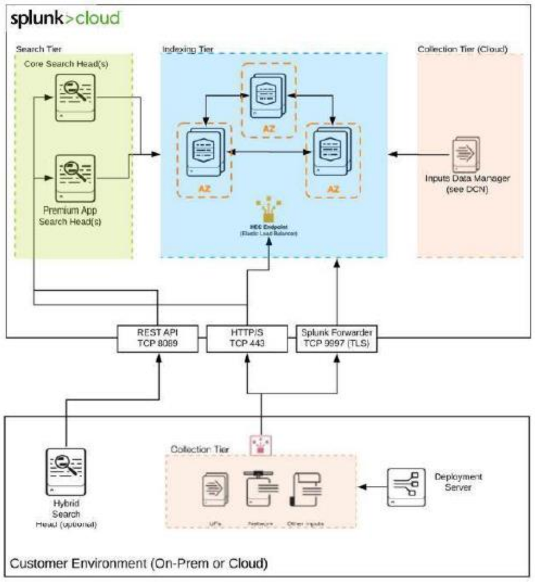
SOAR automates customizable responses to pre-defined threats as they are detected in Splunk Enterprise Security. For example, a particular detected or suspected threat might trigger a pre-defined "playbook," which can take protective actions (for example, isolating a part of the network or restricting access to a server) much faster than a human administrator perform the same actions. Of course, this tool is most useful for known threats, or at least threats with familiar patterns. As one interviewee put it, "That's the *best-case* scenario, when you think about it." Cyber-attacks are ever evolving.

SOC as a Service

The Security Operations Center (SOC) is the human core of any modern cybersecurity operation. An (ideally) experienced and knowledgeable staff monitors the network and its infrastructure using the above tools to investigate alerts and proactively identify potential threats. A sort of triage takes place: an alert or potential threat may be dismissed if it is determined to be harmless; dealt with if an effective response is at hand; or escalated to a higher level of experienced analysis and decision. SOC as a Service puts these first tiers of identification, analysis, and response in the hands of a highly experienced organization focused solely on security.

LOGICAL ARCHITECTURE

As indicated by the name, Splunk Cloud Platform is a cloud-based solution. The application is hosted in an AWS Government Plus cloud, certified as FedRAMP Moderate (both the application and the cloud hosting facility). However, the purpose of Splunk is to process data generated by the State network infrastructure, and so this data must be continuously gathered and securely sent on to the Splunk cloud for further processing. The high-level diagram below, supplied by the vendor, illustrates this arrangement:


splunk>cloud
Search Tier
Core Search Head(s)
Premium App Search Head(s)
Indexing Tier
AZ
AZ
AZ
HEC Endpoint (Elastic Load Balancer)
Collection Tier (Cloud)
Inputs Data Manager (see DCN)
REST API TCP 8089
HTTP/S TCP 443
Splunk Forwarder TCP 9997 (TLS)
Hybrid Search Head (optional)
Collection Tier
Deployment Server
Customer Environment (On-Prem or Cloud)

In distributed deployments, processes are distributed across multiple Splunk Enterprise instances running on multiple machines. Each instance performs a specialized role, such as data input, indexing, search management, or various housekeeping functions.

The State will host 5 virtual servers on-prem(ises):

- 5 Servers –
  - 2 syslog servers,
  - a Splunk heavy forwarder,
    - A Splunk Enterprise instance that sends data to another Splunk Enterprise instance. Unlike other forwarder types, a heavy forwarder parses data before forwarding it and can route data based on criteria such as source or type of event. It can also index data locally while forwarding the data to another indexer.
  - a deployment server
    - A Splunk Enterprise instance that acts as a centralized configuration manager. It deploys configuration updates to other instances.
- 3 servers will be hosted in the State's Tech Vault datacenter.
- 2 servers will be hosted in the State's datacenter at National Life.

When the SIEM is deployed enterprise-wide, the "federation" of locally focused Splunk and Elastic instances will be retired.

ASSESSMENT OF ARCHITECTURE

The functional architecture as proposed is, in our view, an ideal arrangement for the State at this time. SIEM is a young technology which continues to evolve, and it is entirely possible that the State might rely on a different platform with different capabilities at some future time. At this time, however, the choice of Splunk Enterprise Security with Splunk SOAR is wise and appropriate, because:

- Splunk is arguably the most widely used SIEM in this country, ensuring a very broad base of development expertise
- The platform is state of the art, but not "bleeding edge" technology, supporting reliability and high likelihood of a quick and successful deployment
- The vendor is a Splunk partner, experienced in Splunk deployment and use, with security as its sole line of business
- The vendor's reputation appears to be extremely good, and national in reach.

The decision to employ SOC as a service is smart and effectively ties the whole project together by bridging State internal security resources and with the capabilities of the technology platform. Vermont is a very small State with a small executive branch. The State's security analysts, like the people in many other Agencies, wear many hats and have many demands on their time. It is not within the scope of the present Review to assess the current operations of the Security Division, but it is a pretty safe bet to assume that the existing staff cannot effectively match the scope of a SOC team devoted full-time to threat detection and response. Outsourcing the first tiers of SOC operations more efficiently uses the State's resources to focus on issues already "triaged" and identified as needing attention at an appropriately high level. Most importantly of all, SOC as a Service and the Splunk platform, in conjunction with the expertise already extant in the ADS Security Division, would greatly improve the State's cyber defense posture.

The logical architecture of the proposed solution is clear and consistent with State preferences and requirements both functional and non-functional. As a cloud solution it does not require capital investment and puts the State in a flexible position to take advantage of developments in the field.

6.1 STATE'S ENTERPRISE ARCHITECTURE GUIDING PRINCIPLES

6.1.1 A. ASSESS HOW WELL THE TECHNOLOGY SOLUTION ALIGNS WITH THE BUSINESS DIRECTION

ADS has for some time anticipated the implementation of this core functionality for its cybersecurity operations. As explained above, this project would very likely increase the agility and efficiency of the Security Division.

6.1.2 B. ASSESS HOW WELL THE TECHNOLOGY SOLUTION MAXIMIZES BENEFITS FOR THE STATE

The proposed solution would go a long way toward securing and protecting the information and productivity assets of State government as well as significantly enhancing the protection of citizens' private information at the State government level.

6.1.3 C. ASSESS HOW WELL THE INFORMATION ARCHITECTURE OF THE TECHNOLOGY SOLUTION ADHERES TO THE PRINCIPLE OF INFORMATION IS AN ASSET

Splunk addresses this principle specifically and directly, by making productive use of an existing continuous data stream to an extent not previously available to the State.

6.1.4 D. ASSESS IF THE TECHNOLOGY SOLUTION WILL OPTIMIZE PROCESS

It will very directly optimize process as it leverages outsourced expertise and data analysis technology to allow State workers to engage in cyber defense in a more coherent and high-level manner.

6.1.5 E. ASSESS HOW WELL THE TECHNOLOGY SOLUTION SUPPORTS RESILIENCE-DRIVEN SECURITY.

The proposed solution would implement a cohesive and proactive line of defense in place of a "putting out fires" approach.

6.2 SUSTAINABILITY

Splunk and its associated tools are evolving platforms, and Splunk Cloud Platform, a Software as a Service (SaaS) solution, rolls out improvements and updates to customers on a regular basis. This will ensure that the SIEM evolves as the state of the art evolves. Additionally, the State has limited the initial term of the contract to 3 years (with possibility of extending for 2 more years) which allows the State to change platforms at some point in the future, should it be advisable.

Since the solution is SaaS, no hardware is acquired. In a capital sense, the solution is future-proofed.

6.3 HOW DOES THE SOLUTION COMPLY WITH THE ADS STRATEGIC GOALS ENUMERATED IN THE ADS STRATEGIC PLAN OF JANUARY 2020?

6.3.1 A. Leverage successes of others, learning best practices from outside Vermont

The Chief Information Security Officer (CISO), his staff and many associates at ADS are schooled, experienced, and knowledgeable concerning the state of the art in cybersecurity nationally and industry-wide. From this knowledge came the understanding that implementation of an SIEM for Vermont government was a need and priority.

The IT ABC form notes that "Oklahoma uses Splunk in a manner similar to our proposal. Other states (Alaska, Maryland, and more) use Splunk in varying levels of daily operations."

6.3.2 B. Leverage shared services and cloud-based it, taking advantage of it economies of scale

The proposed solution is cloud-based with the exception of the small amount of necessary on-prem deployment as described above.

6.3.3 C. Adapt the Vermont workforce to the evolving needs of state government

The proposed solution would more efficiently employ the talents of the Security Division analysts with a more coherent defense posture.

6.3.4 D. Apply enterprise architecture principles to drive digital transformation based on business needs

Please see **section 6.1**, *above*.

6.3.5 E. Couple IT with business process optimization, to improve overall productivity and customer service

Please see **section 6.1.1**, *above*.

6.3.6 F. Optimize IT investments via sound project management

The State has assigned a Project Manager for the implementation phase of this project. The vendor's project management planning description in the proposal is appropriate and responsive to the requirements of the RFP.

6.3.7 G. Manage data commensurate with risk

The project as a whole is explicitly designed to manage data that is currently under-utilized in order to diminish the risk of damage due to cyber-attack.

6.3.8 H. Incorporate metrics to measure outcomes

The IT ABC Form Business Value Table lists the following metrics:

- Number of threats identified and gaps in general security practices.
- Number of threats mitigated/stopped as well as reporting trends to allow for better security planning and strategy

The Security Division does not generate appropriate baselines for these metrics. The new system may not be easily comparable to current practices in these terms. The Chief Information Security Officer (CISO) believes that, over time, useable baseline metrics for project success can be developed.

6.4 COMPLIANCE WITH THE SECTION 508 AMENDMENT TO THE REHABILITATION ACT OF 1973, AS AMENDED IN 1998

Splunk is tested for WCAG 2.1 Level A and AA Success Criteria and Section 508 guidelines. Voluntary Product Accessibility Templates (VPAT) and detailed conformance reports for each product are available at https://www.splunk.com/en_us/about-splunk/splunk-data-security-and-privacy/accessibility.html

6.5 DISASTER RECOVERY

The vendor states: *Disaster Recovery within Splunk Cloud is architected to be transparent to the customer. Splunk Cloud backs up customer configurations and most recent data into Amazon S3. These backups are scheduled on an hourly basis. Splunk Cloud also operates across multiple AWS Availability*

Zones, which provides redundancy in the event an instance of Splunk Cloud fails and provides a 100% uptime SLA.[3]

This is appropriate to the high level of recoverability required by the State. Additionally, as the application is hosted in FedRAMP Moderate AWS Government Cloud Plus, all the recovery features of that hosting are inherited.

6.6 DATA RETENTION

As part of the implementation plant, NuHarbor will discuss and accommodate by configuration the State's requirements for data retention. At the time of this writing those requirements have not been determined. Contract provisions indicate separate "hot" and "archive" data storage, with "hot" searchable storage of 90 days and "archive" storage of 275 days. Technologically, data storage is no longer limited by hard drive capacities, and "infinite" or "indefinite" storage is available. However, we note that:

- Syslog data is voluminous, and it's value is primarily forensic. The older it gets, generally the less useful it is.
- Extra storage will incur additional cost. (Billed in 500GB increments)
- There may be a limit to how much data Splunk can search as a practical matter.

1 V.S.A. § 317a governs the retention of public records. It is not clear to this reviewer that syslog data constitutes public records. This is probably a matter for the Secretary of State. As far as this reviewer can discern, there is no record schedule for ADS. (See https://sos.vermont.gov/vsara/manage/retention-disposition/agency-record-schedules/).

6.7 SERVICE LEVEL AGREEMENT

6.7.1 WHAT ARE THE POST IMPLEMENTATION SERVICES AND SERVICE LEVELS REQUIRED BY THE STATE?

The RFP requires the proposing vendor to attach a sample Service Level Agreement (SLA) rather than defining those requirements in advance. The selected vendor attached an SLA; see below.

6.7.2 IS THE VENDOR PROPOSED SERVICE LEVEL AGREEMENT ADEQUATE TO MEET THOSE NEEDS IN YOUR JUDGMENT?

The vendor's proposed SLA (Attachment #9 in the original proposal) is the Splunk Cloud Service Level Schedule, summarized as follows:

[3] Vendor's Proposal, pg. 47

Service Level Commitment

The Splunk Cloud Services will be available 100% of the time, as measured by Splunk over each calendar quarter of the Subscription Term, and subject to the exclusions set forth below (the “Service Level Commitment”). A Splunk Cloud Service is considered available if the Customer is able to login to its Splunk Cloud Service account and initiate a search using Splunk Software.

Service Level Credit:

If Splunk fails to achieve the above Service Level Commitment for a Splunk Cloud Service, Customer may claim a credit for such Splunk Cloud Service as provided below, up to a maximum credit per calendar quarter equal to one month's Splunk Cloud Service subscription fees.

Percentage Availability per Calendar Quarter Credit	
100	No Credit
99.99-99.999	2 Hours
99.9-99.99	4 Hours
99.0-99.9	8 Hours
95.0-99.0	1 Day
0-95.0	1 Month

This SLA is fine and generally appropriate (there are additional terms and conditions beyond the summary above). We usually do not like to see a limit on service level credits, as that may disincentivize the vendor. However, in this case, the maximum credit is one month, which is one-third of the quarterly period, a significant loss for the vendor. So, this seems adequate.

We note that the SLA above concerns Splunk Cloud Services availability only and does not address availability of NuHarbor SOC services. We recommend that the State consider negotiating an SLA for those services.

6.8 SYSTEM INTEGRATION

6.8.1 IS THE DATA EXPORT REPORTING CAPABILITY OF THE PROPOSED SOLUTION CONSUMABLE BY THE STATE?

Yes, Splunk natively interfaces with Business Intelligence and Office applications currently in use by the State.

6.8.2 WHAT DATA IS EXCHANGED AND WHAT SYSTEMS (STATE AND NON-STATE) WILL THE SOLUTION INTEGRATE/INTERFACE WITH?

The system as envisioned does not interface with existing State databases *per-se*, although it has the capability to accept data from any source providing human-readable text. However, in the proposed project it primarily serves to organize and index existing machine-generated syslog data which may not be currently organized in that way (aside from existing “local” SIEM instances).

Additional Comments on Architecture:

Although the State currently operates some standalone SIEM instances, an enterprise-wide system represents new technology, bringing with it some unknowns. In particular, the impact of SIEM traffic on the State network is unknown. We identify this as a risk (**_RISK_ID# _R3_**) to unimpeded network operations. We rate this risk as “Unlikely” with a “Moderate” impact. The State is mitigating this risk in the following way:

- The rate of data being transferred out will not be known until the volume of the logs is tested.
- If at that assessment the SIEM implementation threatens to saturate the pipeline, the State already has in place the capability to expand the circuit bandwidth.
- The State is considering expanding circuit bandwidth proactively to accommodate any likely increase in traffic

We found this response to be appropriate and sufficiently comprehensive.

As this Review was drawing to a close, additional information in the form of estimates of expected data rates was obtained from engineers at NuHarbor, who wrote:

> *After the sizing exercise that we conducted on the ADS sources, the State is expected to ingest somewhere in the range of 1 TB/day. With 1 TB/day of data ingestion, we would expect to see 11 – 12 Megabytes per second [MBps] for outbound traffic over the network. However, we have the ability to configure Splunk to limit output rate on universal forwarders and heavy forwarders if there is a network concern.*

The State’s Chief Information Security Officer (CISO) wrote:

> *I think the estimate per second should be doubled to accommodate a 12-hour window. Logs can get backed-up during the day during peak usage but the forwarder can help manage that…I just think that the majority of the logs will move between 8 am and 8 pm.*

NuHarbor agreed with that approach. Consequently, **an estimate of the average data rate required for outgoing traffic during the busiest parts of the day would be 24-24 MBps (@ 1 TB per day).**

The State's existing connection to the Internet is 3 Gigabytes per second (GBps).

With this information in hand, and with their knowledge of existing data rate patterns for the State's Enterprise Network, we assess that ADS will be able to make a sound decision regarding any need to proactively expand circuit bandwidth to the Internet to accommodate Splunk Cloud traffic. Final adjustments will of course be made after the solution is implemented.

7 ASSESSMENT OF IMPLEMENTATION PLAN

The implementation process has two major components:

- Configuration, implementation, and deployment of the Splunk SIEM and Splunk SOAR
- Planning and initiation of SOC as a Service (NuHarbor calls this “onboarding.”)

SPLUNK SIEM AND SOAR IMPLEMENTATION

The following table shows a high-level view of the phases and major tasks of the Splunk Enterprise Security platform and Splunk SOAR platform implementation, as listed in the draft contract we have examined. The table in the contract also includes dates for each phase, but those dates have passed and we have omitted them from the table for clarity. The process would take approximately 4-5 weeks total.

A more detailed sample implementation plan is included in the vendor’s proposal as Attachment #4.

Table 9 - Splunk SIEM Implementation Phases

Phase	Phase Description
Initiation/Planning	Kick-off meeting, Planning and preparation of project management planning documentation.
Personnel Logistics	Additional background checks, fingerprinting, populate daily status report template
Access Provisioning/Remote Connectivity	Identify access into client environment Meet with client to review account access requirements Provision accounts for all apps/add-ons Provision PS engineer access to on-premise Splunk infrastructure Validate individual account access to CLIENT on-prem Splunk infrastructure Provision PS engineer access to Splunk Cloud Validate individual account access to Client Splunk cloud Infrastructure Troubleshoot and remediate access
Execution	Send daily status reports to all stakeholders
Health Check	Architecture, deployment service configurations, license utilization, system overview, THP and uLimits, Splunk User Best Practices, indexing and data overview, search overview, security overview, data quality/source typing, App/Add-on installations
Upgrade/Configure Splunk Instance	Install, upgrade, configure, and/or tune Splunk Instances Implement defined indexes and retention settings

Data Source Onboarding	Create State data source configurations with: • Up to **34** data source inputs from the standard Splunk input source types • Up to **20** search-time data source types • Using a total of up to **2** CSV table lookups • Up to **30** total field extractions Client data sources are:
ES Installation and Configuration	Verify data model health and volumization Configure Assets and Identities Disable views and searches that do not apply to client data Download, install and configure CMMC App
Professional Services Closeout call and State Acceptance	Review monitoring results with CLIENT Identify outstanding CLIENT documentation requests Review CLIENT use cases and alignment to installed configuration Schedule Administration and Development calls for Q1
Lessons Learned	Lessons learned meeting held

MANAGED SERVICES (SOC AS A SERVICE) ONBOARDING TIMELINE

The table below is a sample of the timeline for initiating SOC managed services. The draft contract lists these activities but does not assign dates for them. The process takes approximately 5 weeks.

Table 10 - SOC as a Service Onboarding Timeline

NuHarbor Managed Services Example Onboarding Timeline					
Activities:	Wk1	Wk2	Wk3	Wk4	Wk5
Handoff from Professional Services to MSP Onboarding	■	■			
MSP Onboarding					
Planning & Documentation	■	■	■	■	
Service Provisioning		■			
Initial Engineering Tuning			■		
Monitoring Soft-Launch				■	
Monitoring Production Launch					■

ASSESSMENT

As an Elite Splunk Partner, NuHarbor closely follows Splunk implementation procedures as developed by Splunk. An examination of the detailed plan as listed in the proposal shows that the vendor has a clear sense of the activities required and the time expected for each. The description of the participation required of the State is clear and appropriate. We see no problems with the plan, and we think it is very likely to succeed in the defined timeframe.

The onboarding process for SOC as a Service similarly demonstrates the vendor's experience with the process and, given the vendor's experience working with the State on other projects, we see no reason why it would not succeed .

After assessing the Implementation Plan, please comment on each of the following.

7.1 THE REALITY OF THE IMPLEMENTATION TIMETABLE

There are two-time constraints, both operating in approximately the same timeframe:

- "political" constraints – As we were told in interview, "Funding was given; results are expected." The legislative session begins in January, 2023, and the ADS expects to report positive results by that time.
- The vendor who currently provides SOC as a Service holds contract expiring 12/25/22

We identify this as a risk (**_RISK_ID# _R1_**) of reputational damage and/or increased cost (of extending SOC contract). We rate the Likelihood of the risk as "Rare" and the Impact as "Moderate." The State is mitigating this risk by ensuring that the timeline includes some "slack" to minimize pressure; the timeline ends mid-December, but a realistic estimate is to finish by end of November or beginning of December. We agree with this approach.

We also noted that the selected vendor has requested several changes to contract language in Attachment D, IT System Implementation Terms and Standards. Some are minor (such as typographical corrections or clarifications); some are moderate; and some are more significant (such as a change to breach notification requirements set forth in 9 V.S.A. §2435(b)(3)) We identify this as a risk (**_RISK_ID# _R4_**) to the timeline, rated "Unlikely" but "Moderate" in impact. The State avoids this risk and notes: The selected vendor has, by the terms of the RFP, already accepted the language of Attachments D and C by submitting their proposal. Having noted that, the State has in the past sometimes accommodated certain changes requested by the vendor if they do not disadvantage the State. The State's negotiating team is confident of reaching an agreement with the vendor.

We assess this response as appropriate to the risk.

7.2 READINESS OF IMPACTED DIVISIONS/ DEPARTMENTS TO PARTICIPATE IN THIS SOLUTION/PROJECT

(Consider current culture, staff buy-in, organizational changes needed, and leadership readiness).

The ADS has for some time desired and expected implementation of an enterprise-wide SIEM. It would have significant benefits. We witnessed only enthusiasm for the project, and indications are that this enthusiasm prevails at all levels of the organization.

We do note that the unavailability of certain key project member(s) for any reason could:

- impact other Security Division projects, because this project is the number one priority of the Security Division (we are told).
- potentially negatively impact the timeline.

NOTE: This does not rise to the level of a "key person dependency," because successful completion of the project is not dependent on one individual

We identify this as a risk (**_RISK_ID# _R2_**) to the timeline with a “Rare” likelihood and a “Moderate” impact. The State responds with these mitigations:

- Requisite knowledge (including institutional knowledge) is broadly available in team
- Splunk is a very widely-used platform; if necessary, additional support is very likely available in the hiring market
- The vendor has adequate resources to take on some State tasks
- Timeline has built-in slack (see above)

Given that the likelihood of realizing this risk is very low, we think these mitigations cover all the needed bases.

7.3 DO THE MILESTONES AND DELIVERABLES PROPOSED BY THE VENDOR PROVIDE ENOUGH DETAIL TO HOLD THEM ACCOUNTABLE FOR MEETING THE BUSINESS NEEDS IN THESE AREAS:

7.3.1 A. PROJECT MANAGEMENT

The vendor agrees to supply all the project management deliverables required by the State and indicates familiarity with each one. The only exception, as indicated in the contract draft, is that the vendor does not believe that a project management plan is necessary, given that This is a 7-week professional services engagement using standard onboarding processes and procedures and managed using PMBOK standards, employing MS Project, Risk, Action, Issue and Decision logs, Weekly status updates.

7.3.2 B. TRAINING

Splunk Premium Support & Success Plan, elected by the State, includes:

- 30 credits per quarter of Technical OnDemand Services
- 2,500 EDU credits per year

We think this availability is adequate, given that the State already has some internal experience with Splunk, and that first-tier use of the system will largely take place within the vendor-provided SOC team.

7.3.3 C. TESTING

Acceptance testing criteria and documentation of acceptance signoff for each deliverable is managed by the vendor's project manager. Well-defined project management documentation will be submitted for acceptance and approval at each phase of the implementation.

7.3.4 D. DESIGN

As an Elite Splunk Partner NuHarbor will follow current Splunk best practices for enterprise system design. We have no concerns.

7.3.5 E. CONVERSION (IF APPLICABLE)

N/A

7.3.6 F. IMPLEMENTATION PLANNING

Implementation planning (including requirements discovery) is covered by the vendor's sample implementation plan and looks to be appropriate to the project.

7.3.7 G. IMPLEMENTATION

Implementation deliverables and documentation are appropriately defined and reasonably extensive. The implementation plan itself is assessed above.

7.4 DOES THE STATE HAVE A RESOURCE LINED UP TO BE THE PROJECT MANAGER ON THE PROJECT? IF SO, DOES THIS PERSON POSSESS THE SKILLS AND EXPERIENCE TO BE SUCCESSFUL IN THIS ROLE IN YOUR JUDGMENT?

Yes, the State's project manager is qualified, experienced, efficient and demonstrated his responsiveness and effectiveness numerous times in the course of the present Review. He is good-natured, and the project team responds well to his actions.

Additional Comments on Implementation Plan:

none

8 COST ANALYSIS AND MODEL FOR BENEFIT ANALYSIS

8.1 ANALYSIS DESCRIPTION:

Provide a narrative summary of the cost benefit analysis conducted.

The costs for this project are primarily monetary, and are well-defined, mostly by the costs as represented in the contract. The benefits for this project are overwhelmingly intangible – although significant and important – and were gleaned by interviews, project documentation, and analysis.

8.2 ASSUMPTIONS:

List any assumptions made in your analysis.

- That costs paid to the vendor will be exactly as represented in the contract draft we received
- That the estimate of State personnel time and costs devoted to this project are accurate and will remain so
- That no so-far unidentified current costs will be offset by this project

8.3 FUNDING:

Provide the funding source(s). If multiple sources, indicate the percentage of each source for both Acquisition Costs and on-going Operational costs over the duration of the system/service lifecycle.

Funding for this project was procured from the Legislature and is 100% State (i.e., no federal funding).

8.4 TANGIBLE COSTS & BENEFITS:

Provide a list and description of the tangible costs and benefits of this project. It's "tangible" if it has a direct impact on implementation or operating costs (an increase = a tangible cost and a decrease = a tangible benefit). The cost of software licenses is an example of a tangible cost. Projected annual operating cost savings is an example of a tangible benefit.

TANGIBLE COSTS:

Project implementation and operating costs, totaling $3,722,272.96

TANGIBLE BENEFITS:

None identified

8.5 INTANGIBLE COSTS & BENEFITS:

Provide a list and descriptions of the intangible costs and benefits. Its "intangible" if it has a positive or negative impact but is not cost related. Examples: Customer Service is expected to improve (intangible benefit) or Employee Morale is expected to decline (intangible cost.

- **Greatly improved cyber defense posture for the State's data and IT systems.**
- **Greatly improved privacy protection for citizens' information as held in State systems**
- **Better use of ADS Security Division analyst resources**
- **Retirement of multiple standalone SIEMs and resultant consolidation of cyber-defense activities**
- **Increased ability to identify security threats**
- **Increased ability to mitigate security threats**

8.6 COSTS VS. BENEFITS:

Do the benefits of this project (consider both tangible and intangible) outweigh the costs in your opinion? Please elaborate on your response.

The benefits of this project are crucial to the continued protection of the State's information assets and IT infrastructure. The costs are reasonable and proportional to the technology employed. The benefits, even though intangible, are so important to the State that we can state without qualification that they outweigh the costs.

8.7 IT ABC FORM REVIEW:

Review the IT ABC form (Business Case/Cost Analysis) created by the Business for this project. Is the information consistent with your independent review and analysis? If not, please describe. Is the lifecycle that was used appropriate for the technology being proposed? If not, please explain.

The IT ABC Form is very recent and reflects the costs as they became known following the BAFO and vendor selection. Therefore, the form is exactly consistent with the project in its current form. (The exact cost of the Independent Review was unknown at the time the form was approved, so the nominal cost was used.)

Additional Comments on the Cost Benefit Analysis:

none

9 ANALYSIS OF ALTERNATIVES

The proposed solution can be seen as a modernization project and at the same time as an automation project, because it uses computing power to accomplish analysis and response tasks that humans could not do in the same amount of time, even given an arbitrarily large staff. It is reasonable to conclude that there is no practical way to accomplish the same ends as a SIEM system by other means.

9.1 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS THAT WERE DEEMED FINANCIALLY UNFEASIBLE.

During the review of offers submitted in response to the BAFO requests, one of the vendors offered a cost model that was so low compared to the others – “an order of magnitude less,” as one team member put it – that the evaluation team concluded there was no conceivable way the vendor could deliver, even using open-source software. We have examined that BAFO response and agree with the State’s conclusion.

9.2 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS THAT WERE DEEMED UNSUSTAINABLE.

There are some vendors with new or alternate technologies that were of interest to team members. SIEM technology is evolving quickly, and it is entirely possible that the State may at some point in the future opt for an alternate vendor and/or technological approach. This is one of the reasons for the short (3 years) initial term of the contract; i.e., the State will not be “locked in” to one vendor’s approach. However, *at the present time,* these alternate approaches are too new and untested to be an appropriate choice for the State’s forward line of cyber defense. We strongly agree with this conclusion.

9.3 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS WHERE THE COSTS FOR OPERATIONS AND MAINTENANCE WERE UNFEASIBLE.

N/A

10 IMPACT ANALYSIS ON NET OPERATING COSTS

10.1 INSERT A TABLE TO ILLUSTRATE THE NET OPERATING COST IMPACT.

Table 11 - Project Cost by Year

	Procurement	FY1	FY2	FY3	Total
Total Project Cost	$194,833.00	$1,175,813.32	$1,175,813.32	$1,175,813.32	$3,722,272.96

Table 12 - Cumulative Cost Savings

	Procurement	FY1	FY2	FY3
Project Cost Cumulative	$194,833.00	$1,370,646.32	$2,546,459.64	$3,722,272.96
Current Costs Cumulative	$0.00	$0.00	$0.00	$0.00
Cumulative Cost Savings	-$194,833.00	-$1,370,646.32	-$2,546,459.64	-$3,722,272.96

10.2 PROVIDE A NARRATIVE SUMMARY OF THE ANALYSIS CONDUCTED AND INCLUDE A LIST OF ANY ASSUMPTIONS.

Assumptions:

- That costs paid to the vendor will be exactly as represented in the contract draft we received
- That the estimate of State personnel time and costs devoted to this project are accurate and will remain so
- That no so-far unidentified current costs will be offset by this project

10.3 EXPLAIN ANY NET OPERATING INCREASES THAT WILL BE COVERED BY FEDERAL FUNDING. WILL THIS FUNDING COVER THE ENTIRE LIFECYCLE? IF NOT, PLEASE PROVIDE THE BREAKOUTS BY YEAR.

N/A

10.4 WHAT IS THE BREAK-EVEN POINT FOR THIS IT ACTIVITY (CONSIDERING IMPLEMENTATION AND ON-GOING OPERATING COSTS)?

There are no current costs offset by the proposed project, and consequently there is no breakeven point for this activity.

11 SECURITY ASSESSMENT

Assess Information Security alignment with State expectations. ADS-Security Division will support reviewer and provide guidance on assessment.

Splunk Cloud Federal Risk and Authorization Management Program (FedRAMP) is authorized by the General Services Administration FedRAMP Program Management Office (PMO) at the Moderate Impact Level. Splunk Cloud is hosted in the Amazon Web Services (AWS) Government Cloud Plus and inherits the Security Controls of that cloud. The State has significant experience with and knowledge of AWS Government hosting, as well as a long relationship with the vendor and an understanding of the vendor's security stance.

In our opinion NuHarbor's proposed system is consistent in every way with the State's security requirements.

11.1 WILL THE NEW SYSTEM HAVE ITS OWN INFORMATION SECURITY CONTROLS, RELY ON THE STATE'S CONTROLS, OR INCORPORATE BOTH?

The system incorporates controls of both the State and the vendors (both AWS and Splunk/NuHarbor) as part of the system is necessarily resident on the State's network. (See **6. Architecture Assessment**, *above*.)

11.2 WHAT METHOD DOES THE SYSTEM USE FOR DATA CLASSIFICATION?

The Splunk SIEM solution is an approved Federal Information Security Management Act (FISMA) compliant reporting and alerting solution. Splunk is also compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 standards for "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

11.3 WHAT IS THE VENDOR'S BREACH NOTIFICATION AND INCIDENT RESPONSE PROCESS?

Section 5, Incident Response and Breach Notification, of the of the Splunk Cloud Platform Security Addendum, states in part:

Splunk has an incident response plan (the Splunk Incident Response Framework or SIRF) and team to assess, respond, contain and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Splunk reviews and updates the SIRF annually to reflect emerging risks and "lessons learned."

Additionally, it states

In the event of a Data Breach involving Personal Data, if a customer reasonably determines notification is required by law, Splunk will provide reasonable assistance to the extent required for the Customer to *comply with applicable data breach notification laws, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.*

This seems reasonable and reasonably compliant with the Vermont data breach requirements. (Attachment D of the standard contract terms for IT projects also requires compliance with that law.)

11.4 DOES THE VENDOR HAVE A RISK MANAGEMENT PROGRAM THAT SPECIFICALLY ADDRESSES INFORMATION SECURITY RISKS?

Yes. **Section 3, Risk Management, of the Splunk Cloud Platform Security Addendum** specifically addresses Risk Management (see https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html)

3.1 Splunk manages cybersecurity risks in accordance with its Risk Assessment Method, which defines how Splunk identifies, prioritizes and manages risks to its information assets and the likelihood and impact of them occurring.

3.2 Splunk management reviews documented risks to understand their potential impact to the business, determine appropriate risk levels and treatment options. Mitigation plans are implemented to address material risks to business operations, including data protection.

11.5 WHAT ENCRYPTION CONTROLS/TECHNOLOGIES DOES THE SYSTEM USE TO PROTECT DATA AT REST AND IN TRANSIT?

Cryptographic modules used in the Splunk Cloud FedRAMP offering are FIPS 140-2 validated encryption modules. The State’s contract with the vendor specifically requires encryption at rest. Encryption at rest is enabled by default in the Splunk FedRAMP Moderate subscription. Splunk manages the encryption keys on behalf of the State and they are regularly rotated.

11.6 WHAT FORMAT DOES THE VENDOR USE FOR CONTINUOUS VULNERABILITY MANAGEMENT, WHAT PROCESS IS USED FOR REMEDIATION, AND HOW DO THEY REPORT VULNERABILITIES TO CUSTOMERS?

Section 10, Threat and Vulnerability Management of the Splunk Cloud Platform Security Addendum (see https://www.splunk.com/en_us/legal/splunk-cloud-security-addendum.html) states:

10.1 Splunk has a Threat and Vulnerability Management (TVM) program to continuously monitor for vulnerabilities that are discovered internally through vulnerability scans, offensive exercises (red team), and employees; or externally reported by vendors, researchers or others.

10.2 Splunk documents vulnerabilities and ranks them based on severity level as determined by the likelihood and impact ratings assigned by TVM. Splunk assigns appropriate team(s) to conduct remediation and track progress to resolution as needed.

10.3 An external vendor conducts security penetration tests on the corporate and Splunk Cloud Platform environments annually to detect network and application security vulnerabilities. Findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation based on severity level. In addition, Splunk conducts internal penetration tests quarterly on its Splunk Cloud Platform infrastructure and remediates findings as appropriate.

11.7 HOW DOES THE VENDOR DETERMINE THEIR COMPLIANCE MODEL AND HOW IS THEIR COMPLIANCE ASSESSED?

The compliance model is determined by the Subscription Type, in this case FedRAMP moderate. Splunk Cloud FedRAMP is authorized by the General Services Administration FedRAMP PMO at the Moderate Impact Level.

According to **the Splunk Cloud Platform Security Addendum**:

At least once a year, Splunk Cloud Platform (Standard Environment) undergoes a security audit by an independent third party that attests to the effectiveness of the controls Splunk has in place to safeguard the systems and operations where Customer Content is processed, stored or transmitted (e.g., System and Organizational Control (SOC 2), Type 2) audit in accordance with the Attestation Standards under Section 101 of the codification standards (AT 101). At a minimum, the audit covers the Security, Confidentiality, and Availability control criteria developed by the American Institute of Certified Public Accountants (AICPA). Currently, Splunk Cloud Platform is audited against ISO 27001 and SOC 2, Type 2. Upon request, Splunk will supply Customer with a summary copy of Splunk's annual audit reports, which will be deemed Confidential Information under the Agreement.

12 RISK ASSESSMENT & RISK REGISTER

The risks identified throughout this review are collected below, along with an assessment of their significance, a description of the State response and timing, and our evaluation of the State response.

In our assessment, this is a project with little risk, largely because of the security-related experience of the proposed vendor and the ADS Security Division.

12.1.1 ADDITIONAL COMMENTS ON RISK

none

12.1.2 RISK REGISTER

The following table explains the Risk Register components:

Risk ID:	Identification number assigned to risk or issue.
Risk Rating:	An assessment of risk significance, based on multiplication of **(probability X impact ratings)** (*see below*). **1-9 = low** **10-48 = moderate** **49-90 high** See table below
Probability:	Assessment of likelihood of risk occurring, scale of **1,3,5,7, or 9**, from least to most likely
Impact:	Assessment of severity of negative effect, scale of **1,3,5,7, or 10**, from least to most severe
Finding:	Review finding which led to identifying a risk
Risk Of:	Nature of the risk
Source:	Project, Proposed Solution, Vendor or Other
Risk domains:	What may be impacted, should the risk occur
State's Planned Risk Strategy	Decision to *avoid*, *mitigate*, or *accept* risk
State's Planned Risk response	Detailed description of response to risk, in order to accomplish decision
Reviewer's Assessment:	Reviewer's evaluation of the State's planned response

Risk Rating Matrix			IMPACT				
			Trivial	Minor	Moderate	Major	Extreme
			1	3	5	7	10
LIKELIHOOD	Rare	1	1	3	5	7	10
	Unlikely	3	3	9	15	21	30
	Moderate	5	5	15	25	35	50
	Likely	7	7	21	35	49	70
	Very Likely	9	9	27	45	63	90

Risk ID: R1	Rating:	**5**	
	Likelihood:	**1**	
	Impact:	**5**	
Finding:	There are two-time constraints, both operating in approximately the same timeframe: - "political" -- "funding was given; results are expected" - legislative session begins in **January, 2023**. - The vendor who currently provides SOC as a Service holds contract expiring **12/25/22**		
Risk Of:	reputational damage and/or increased cost (of extending SOC contract)		
Risk domains:	timeline		
SOV Response:	Mitigate: The timeline includes some "slack" to minimize pressure; the timeline ends mid-December, but a realistic estimate is to finish by end of November or beginning of December.		
Reviewer's Assessment of State's Planned Response	Concur		

Risk ID: R2	Rating:	**5**	
	Likelihood:	**1**	
	Impact:	**5**	
Finding:	The unavailability of certain key project member(s) for any reason - could impact other Security Division projects, because this project is the number one priority of the Security Division - could negatively impact timeline *NOTE: This does not rise to the level of a "key person dependency," because successful completion of the project is not dependent on one person*		
Risk Of:	timeline delay		
Risk domains:	timeline		
SOV Response:	Mitigate: - Requisite knowledge (including institutional knowledge) is broadly available in team - Splunk is a very widely-used platform; if necessary, additional support is very likely available in the hiring market - The vendor has adequate resources to take on some State tasks - Timeline has built-in slack (see above)		
Reviewer's Assessment of State's Planned Response	Concur		

Risk ID: R3	Rating:	**15**	
	Likelihood:	**3**	
	Impact:	**5**	
Finding:	impact on State network is unknown at this point		
Risk Of:	Interruption or interference with State network operations		
Risk domains:	Enterprise Architecture		
SOV Response:	Mitigate: - The volume of data being transferred out will not be known until the volume of the logs is tested. - If at that assessment the SIEM implementation threatens to saturate the pipeline, the State already has in place the capability to expand the circuit bandwidth. - The State is considering expanding circuit bandwidth proactively to accommodate any likely increase in traffic		
Reviewer’s Assessment of State’s Planned Response	Concur		

Risk ID: R4	Rating:	**7**	
	Likelihood:	**1**	
	Impact:	**7**	
Finding:	The selected vendor has requested several changes to contract language in Attachment D, IT System Implementation Terms and Standards. Some are minor (such as typographical corrections or clarifications); some are moderate; and some are more significant (such as a change to breach notification requirements set forth in 9 V.S.A. §2435(b)(3))		
Risk Of:	failure of contract agreement		
Risk domains:	project basis		
SOV Response:	Avoid: The selected vendor has, by the terms of the RFP, already accepted the language of Attach. D and Attach. C. by submitting their proposal. Having noted that, the State has in the past sometimes accommodated certain changes requested by the vendor if they do not disadvantage the State. The State's negotiating team is confident of reaching an agreement with the vendor.		
Reviewer's Assessment of State's Planned Response	Concur		

13 ATTACHMENTS

Attachment 1 – Cost Spreadsheet

Attachment 2 – Risk Register

Attachment 1: ADS SIEM Cost Spreadsheet ver. 1.0a - Paul Garstki Consulting - 2022/August/04

Project Name:	ODG Case Management System							Lifecycle Total @ Current Annual Cost	Benefit
Description	Qty	Unit Price		Maintenance	Maintenance	Maintenance	Total		
Fiscal Year			Procurement	FY1	FY2	FY3			
Vendor Implementation Services									
NuHarbor Splunk professional services	**7**	**$ 11,000.00**	$ 77,000.00				$ 77,000.00		
Splunk SOAR Implementation Services Package – Base Remote	**4**	**$13,700.00**	$ 54,800.00				$ 54,800.00		
24/7 Managed SOC Service Onboarding Fee			$21,504.00				$ 21,504.00		
Vendor Implementation Services Total			**$ 153,304.00**	**$ -**	**$ -**	**$ -**	**$ 153,304.00**	$ -	**$ (153,304.00)**
Vendor Licensing									
Splunk Cloud Platform Licensing				$449,029.23	$449,029.23	$449,029.23	$ -	$ -	
Splunk Enterprise Security Licensing (SIEM Module)				$70,610.53	$70,610.53	$70,610.53			
Splunk SOAR Cloud Subscription with Premium Success Plan	**10**			$154,385.96	$154,385.96	$154,385.96			
Splunk Cloud Subscription with attested FedRAMP Moderate (Hot Data Storage)				$34,281.60	$34,281.60	$34,281.60	$ -		
Splunk Cloud Subscription with attested FedRAMP Moderate (Archived Data Storage)				$37,938.00	$37,938.00	$37,938.00	$ 75,876.00		
Complete Bundle 24/7 Managed SOC Service (80 SVC/800 GB)				$429,568.00	$429,568.00	$429,568.00			
Vendor Licensing Total			**$ -**	**$1,175,813.32**	**$1,175,813.32**	**$1,175,813.32**	**$ 3,527,439.96**		**$ (3,527,439.96)**
State-Provided Licensing									
Virtual Servers for Splunk Forwarder			$ -				$ -		
State-Provided Licensing Total			**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	$ -	**$ -**
Consulting									
Independent Review			$ 17,769.00	$ -	$ -	$ -	$ 17,769.00		
Consulting Total			**$ 17,769.00**	**$ -**	**$ -**	**$ -**	**$ 17,769.00**	$ -	**$ (17,769.00)**
Training									
[included in Vendor Services Implementation]	**0**	**$ -**	$ -	$ -	$ -	$ -	$ -		
Training Total			**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	$ -	**$ -**
Implementation Services Additional									
[none]			$ -	$ -	$ -	$ -	$ -		
Implementation Services Total			**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	$ -	**$ -**
State Personnel									
State Personnel - ADS[2]									
ADS EPMO Project Manager for implementation			$ 23,760.00	$ -	$ -	$ -	$ 23,760.00		
State Personnel Total			**$ 23,760.00**	**$ -**	**$ -**	**$ -**	**$ 23,760.00**	$ -	**$ (23,760.00)**
Grand Total			**$ 194,833.00**	**$ 1,175,813.32**	**$ 1,175,813.32**	**$ 1,175,813.32**	**$ 3,722,272.96**	$ -	$ (3,722,272.96)

ATTACHMENT 2 - ADS SIEM INDEPENDENT REVIEW -- Risk and Issues Register -- version 1.0.a **2022/August/02 -- Paul E. Garstki, JD -- Paul Garstki Consulting**

RISKS	**What is the finding that leads to identifying a risk? (This is a highly condensed version that is explained more fully in the report narrative)**	**What are the risks implied by the finding?**	**What aspects of the project are at risk if the risk(s) are realized?**	**What is the State's response to the risk?**	**Is the State's response to this risk adequate?**	**Reviewer's assessment of likelihood risk is realized 1,3,5,7, or 10**	**Reviewer's assessment of impact if risk is realized 1,3,5,7, or10**	**1-9 low** **10-48 medium** **49-100 high**
Note: Risk ID # list may have gaps, in order to maintain consistency with earlier drafts								
Risk #	**Finding**	**risk of**	**risk domains**	**SOV response**	**Reviewer Assessment of SOV Response**	**likelihood 1-10**	**impact 1-10**	**total rating**
R1	There are two time constraints, both operating in approximately the same timeframe: - "political" -- "funding was given; results are expected" - legislative session begins in **January, 2023**. - The vendor who currently provides SOC as a Service holds contract expiring **12/25/22**	reputational damage and/or increased cost (of extending SOC contract)	timeline	Mitigate: The timeline includes some "slack" to minimize pressure; the timeline ends mid-december, but a realistic estimate is to finish by end of November or beginning of December.	Concur	**1**	**5**	**5**
R2	The unavailability of certain key project member(s) for any reason - could impact other Security Division projects, because this project is the number one priority of the Security Division - could negatively impact timeline *NOTE: This does not rise to the level of a "key person dependency," because successful completion of the project is not dependent on one person*	timeline delay	timeline	Mitigate: - Requisite knowledge (including institutional knowledge) is broadly available in team - Splunk is a very widely-used platform; if necessary, additional support is very likely available in the hiring market - The vendor has adequate resources to take on some State tasks - Timeline has built-in slack (see above)	Concur	**1**	**5**	**5**
R3	impact on State network is unknown at this point	Interruption or interference with State network operations	Enterprise Architecture	Mitigate: - The volume of data being transferred out will not be known until the volume of the logs is tested. - If at that assessment the SIEM implementation threatens to saturate the pipeline, the State already has in place the capability to expand the circuit bandwidth. - The State is considering expanding circuit bandwidth proactively to accomodate any likely increase in traffic	Concur	**3**	**5**	**15**
R4	The selected vendor has requested several changes to contract language in Attachment D, IT System Implementation Terms and Standards. Some are minor (such as typographical corrections or clarifications); some are moderate; and some are more significant (such as a change to breach notification requirements set forth in 9 V.S.A. §2435(b)(3))	failure of contract agreement	project basis	Avoid: The selected vendor has, by the terms of the RFP, already accepted the language of Attach. D and Attach. C. by submitting their proposal. Having noted that, the State has in the past sometimes accomodated certain changes requested by the vendor if they do not disadvantage the State. The State's negotiating team is confident of reaching an agreement with the vendor.	Concur	**1**	**7**	**7**
R5						**0**	**0**	**0**
ISSUES	**Issue Description**			**State Response**				