MEMORANDUM

TO: VERMONT LEGISLATIVE JOINT FISCAL COMMITTEE
FROM: DANIEL SMITH / JOINT FISCAL OFFICE INFORMATION TECHNOLOGY CONSULTANT
SUBJECT: ACT 11 - H.16 – SEC. E.105 – ADS SECURITY OPERATIONS CENTER REPORT
DATE: JULY 18, 2018

Requirement. The FY 2019 Budget Bill[1] includes a requirement that the Joint Fiscal Office (JFO) Information Technology consultant report on the Agency of Digital Services' (ADS) planned Security Operations Center. The specific text is:

Sec. E.105 Agency of digital services

(a) Of the internal service funds appropriated in Sec. B.105 of this act, up to $600,000 is appropriated for a 24/7 cybersecurity operations center. These funds may only be spent upon approval of a budget and a spending plan by the Joint Fiscal Committee at its July 2018 meeting.

(1) The Agency shall consult with the information technology consultant to the Joint Fiscal Office in developing the budget and plan.

(2) The Joint Fiscal Office Information Technology Consultant shall present a report to the Joint Fiscal Committee to accompany the Agency's submission to provide an independent recommendation and review of the proposed budget and plan.

Background. The initial request for funding for a Security Operations Center (SOC) was included in the ADS FY2019 Budget Request[2] presented to the House Appropriations Committee on January 25, 2018. The stated purpose of the SOC is to protect intellectual property and sensitive customer data; this is intended to be achieved by the following items (paraphrased from the budget request):

- Protecting confidentiality – Keeping citizen data, employee data, and state records confidential, and assisting to prevent unauthorized access;

[1] FY 2019 Budget Bill - https://legislature.vermont.gov/assets/Documents/2018.1/Docs/Acts/ACT011/ACT011%20As%20Enacted.pdf

[2] ADS FY2019 Budget Request - https://legislature.vermont.gov/assets/Documents/2018/WorkGroups/House%20Appropriations/FY2019%20State%20Budget/1.%20General%20Government/DR18-0457~John%20Quinn,%20III,%20Secretary,%20Agency%20of%20Digital%20Services~FY2019%20Budget%20Request%20-%20Presentation~1-25-2018.pdf

- Protecting integrity – Working to ensure data is not tampered with and maintaining records according to the Law;

- Protecting access – Ensuring that citizens and state staff and can access the right data at the right time without fear that the data is missing or incorrect.

The funding request was for $600K, and this was subsequently approved in the Big Bill (Act 11 / H.16) that was passed during the 2018 Special Session. This approval was subject to the constraints (Sec. E.105 ADS plan / JFO report) described previously.

SOC Plan Overview. The first draft of the required SOC Plan was provided on June 14, 2018. The draft plan included a brief description of the SOC purpose, a phased concept of implementation, a breakdown of budgets and expenditures, and general metrics to evaluate success. Essentially, ADS is proposing a one year collaboration with Norwich University to expand security monitoring and response capabilities beyond what is currently available through ADS alone. If implemented satisfactorily, the SOC will result in a more proactive monitoring of security threats, and a faster, more effective response to actual incidents. For example, greater access to national intelligence via external Norwich partnerships may result in identification and mitigation of weaknesses (communications security, data protection, election integrity, etc.) prior to the detection of an actual intrusion or other security incident.

After reviewing the initial draft, I provided ADS with questions and comments that included the following. Summaries of their revisions in the subsequent draft are shown in bold/brackets:

1. *Why is ADS proposing the SOC? I believe that you have this justification somewhere, but would be helpful to recap it in the plan.* ***[ADS expanded the Purpose section of the plan to more fully explain why the security operations center is needed]***

2. *Why Norwich? The idea of a partnership seems reasonable, but the draft does not indicate why it is with Norwich. What is their background with this type of effort, why does it makes sense for SOV [State of Vermont], who else they are supporting, what national partnerships and programs do they have, etc.* ***[ADS added Attachments A, B, and C to the plan which explains the rationale for selecting Norwich as a partner in the SOC]***

3. *From the "Budget and Expenditures" chart it appears that SoV will be paying Norwich approximately $400K over the next year. What is the contractual vehicle for this?* ***[ADS added information to the Expenditures section that indicates that they intend to execute a sole source contract with Norwich]***

4. *What are the estimated costs for the security information and event manager (SIEM), and where do they appear in the budget?* ***[ADS added information to the Expenditures section that explains that the initial SIEM costs are included in the first year budget, but may increase over the life of the project]***

5. *What are the estimated ongoing operational costs of the SOC once Phase 4 completes?* ***[ADS does not have estimates for operational costs, but instead added a statement to the Expenditures section that indicates that these costs will be determined at the end of FY2019]***

The revised plan was provided on June 26th. This draft included additional attachments and content as described above.

Security Operations Center (SOC) Plan Comments. The plan provided by ADS appears to be generally satisfactory, both in the approach used and the initial estimated cost of implementation. However, the plan does include some items that require more explanation or action from ADS. These include the following (when quotes are used, these are from the SOC Plan unless stated otherwise):

- Contract vehicle: The proposed contract vehicle may be problematic ("Using Norwich as a sole-source vendor…"). The Department of Buildings and General Services (BGS) provides IT procurement guidelines in Bulletin 3.5[3] of 3/29/2018. The proposed approach of a sole source contract, while it may allow for a more rapid implementation of the SOC plan, does not appear to meet either the spirit or the letter of these procurement guidelines. For a more detailed explanation of the appropriate use of sole source contracts, see the State Auditor's report of 2015[4]. In that report the Auditor states that 1) sole source contracts are intended only for extraordinary circumstances, but are being used in ordinary situations, and 2) sole source contracts over $100K should only approved by the Secretary of Administration after full justification is received.

- Implementation cost estimates: The stated implementation cost estimate of $592K may be lower than actual ("The SIEM [Security Information and Event Manager] cost is rolled into the implementation for the first year. This expense will likely increase as we move into year two"). Given the phased approach in the plan (which is considered appropriate), the determination of actual hardware, software, and personnel costs will likely not be completed before the end of the final phase in late 2019. As a result, actual costs will likely exceed the initial estimate.

[3] Bulletin 3.5 - http://bgs.vermont.gov/sites/bgs/files/files/purchasing-contracting/Technology%20Handbook%20-%20Net%20Neutraility%20Revision%20-%203-29-18.pdf

[4] State Auditor's report of 2015 - http://auditor.vermont.gov/sites/auditor/files/files/reports/reports-reviews/Sole-Source.pdf

- Total project costs: Operational / long term costs are unknown ("As year one progresses, ADS will work with Norwich to understand the expenses involved in an ongoing relationship and plan accordingly based on a balance of cost, benefit, and information systems risk"). Again, actual costs of setting up and operating the SOC will not be known until late due to the phased nature of the plan. This is not a necessarily a weakness, since a phased approach normally reduces project risk, however it must be acknowledged that the actual costs may be significantly greater than they appear up front. The following table from the SOC lists the planned costs through FY19, and it is noteworthy that operational costs are not included or estimated.

Item	Description	Phase 1 9/1/18	Phase 2 1/2/19	Phase 3 4/1/19	Phase 4 6/30/19	Total
Norwich Contracting	Labor and materials	$15,777	$81,487	$126,181	$176,219	$399,664
Training	ADS staff training for proficiency	-	$25,830	$6,210	-	$32,040
Equipment	Incident response (IR) kit	-	$6,500	-	-	$6,500
Equipment	Network security sensors	-	$153,600	-	-	$153,600
Total by Phase		$15,777	$267,417	$132,391	$176,219	$591,804

- Lack of external review: Although responsibilities are unclear due to the reorganization (see Recommendations below), 3 V.S.A. § 2222(g)(1) requires that "The Secretary of Administration shall obtain independent expert review of any recommendation for any information technology activity initiated after July 1, 1996, as information technology activity is defined by subdivision (a)(10) of this section, when its total cost is $1,000,000.00 or greater or when required by the State Chief Information Officer". Given that the initial implementation cost is $600K and could rise, and operational costs are currently unknown, it is likely that the overall cost of the SOC will exceed $1M and thus would be a candidate for an independent review.

Recommendations. Before listing recommendations it is important to note that the authority and responsibilities of ADS are not clear at this time. Although ADS was created by Executive Order 06-17[5], the House bill that would update the statutes to reflect the reorganization (H.920[6]) was not passed in either the regular or special legislative sessions. While the Executive Order states that "All duties, obligations, responsibilities and authority, including all contracts, grant agreements, service level agreements and MOUs of the Department of Information and Innovation are hereby transferred to the Agency of Digital Services and shall continue in force", the organizational change makes the existing statutes difficult to interpret. As a result, previous requirements for legislative reports, plans, independent reviews, etc. may no longer be fully effective. This means that any oversight of ADS, including oversight related to the SOC, should be performed by specific direction from the legislature until such time as the statutes are updated. That said, the following recommendations are provided:

- The SOC should be implemented as described in the plan, but with restrictions as described below;
    - If ADS elects to continue with a Sole Source procurement, it should be required to report to the Joint Fiscal Committee how this approach is consistent with the letter and intent of existing procurement regulations (Bulletin 3.5), and why it is in the best interest of the State;
    - ADS should be required to present to the interested committees (defined in the Budget Bill, Sec. E.105.1 as the Senate Committees on Appropriations and on Government Operations and the House Committees on Appropriations and on Energy and Technology) a report on the status of SOC Phases 1 (Design) and 2 (Procurement). This report should be presented in mid-January 2019, approximately 2 weeks after the planned conclusion of Phase 2;
    - ADS should be required to present to the interested committees (listed above) a report on the status of SOC Phase 3 (SOC standup), as well as the estimate of the actual cost of plan implementation, including long term costs. The report should also include a summary of how Vermont security readiness will compare to other states at the conclusion of SOC Phase 4 (Operations). This report should be presented no later than March 31, 2019;

[5] Executive Order 06-17 - http://governor.vermont.gov/content/creation-agency-digital-services-executive-order-06-17
[6] H.920 - https://legislature.vermont.gov/bill/status/2018/H.920

- ADS should be required to present the SOC metrics defined in the plan as part of a publicly available dashboard that reflects the overall state of ADS performance, including security, infrastructure, cost effectiveness, customer satisfaction, etc. This dashboard, if complete and effective, might also be used to address the interested committees' requirements under section E.105.1 the Budget Bill.