Project Closeout Report

Submitted to Large Project Oversight on 06/24/2020

GENERAL INFORMATION

Project Name: Palo Alto Tool Implementation

Agency Name: North Dakota Information Technology

Project Sponsor: Duane Schell

Project Manager: Jacob Chaput

SCHEDULE AND COST METRICS

	Baseline Start Date	Baseline End Date	Baseline Budget	Actual Finish Date	Schedule Variance	Actual Cost	Cost Variance
Original Baseline	7/12/2019	6/15/2020	$11,314,150.00	6/23/2020	3% over	$11,059,191	$254,959 under

Notes:

Project was delayed by a week due to COVID-19 response activities. Despite the pandemic, teams were able to keep strong progress and meet their milestones. No risk contingency dollars were used, and project management costs came in under the estimate.

MAJOR SCOPE CHANGES

No major scope changes were made to the project over its lifecycle.

OBJECTIVES

Business Objective	Measurement Description	Met/ Not Met	Measurement Outcome
Enhance NDIT's capabilities to effectively identify, analyze, respond, and investigate cyber-attacks.	Build a Security Operations Center (SOC) including Cyber Operations Center (CyOC), Modular Incident Response (ModIR), and integrations of Palo Alto tools into the SOC	Met	SOC and CyOC were successfully built utilizing industry best practices. First operational assessment is scheduled for August.
Improve end-point detection and response (EDR) protection to successfully reduce risks to sophisticated threats.	Deployment of Palo Alto's Cortex XDR, Traps, and Demisto tools.	Met	All tools were successfully deployed to multiple systems.
Strengthen and elevate STATE's cyber operations' people and processes.	Provide workshops and trainings to build familiarity of SOCs and the Palo Alto tools they will be using. New processes and policies will be created and integrated using workshops and vendor consultants.	Met	Palo Alto successfully hosted training for SOC Team Members and SOC Champions/Tier III Analysts.

Project Closeout Report

Submitted to Large Project Oversight on 06/24/2020

Business Objective	Measurement Description	Met/ Not Met	Measurement Outcome
Improve incident response capabilities	Creation of incident scenario playbooks and workflow automation using industry best practices and Palo Alto tools.	Met	NDIT team successfully developed workflows for alerting and responses in addition to playbooks.

POST-IMPLEMENTATION REPORT

Post-Implementation Reports are to be performed after a project is completed. A "PIR" is a process that utilizes surveys and meetings to determine what happened in the project and identifies actions for improvement going forward. Typical PIR findings include, "What did we do well?" "What did we learn?" "What should we do differently next time?"

Lessons Learned
What went well?
"Thorough planning of all projects" *"Great communication throughout"* *"The weekly meetings."* *"Team did a great job in executing and working together"* *"Excellent teamwork and communication"* *"Adding project management helped a lot."* *"Coordination across multiple teams on both the Palo Alto Networks and North Dakota side was excellent given the sheer number of people involved."* *"Collaboration"* *"The partnership that developed between NDIT team and Palo Alto Networks team was a tremendous help to achieve the amount of work that went into the projects."*
What could have gone better?
"I would have liked to have visited ND more than once. But Winter and Covid hit, prevented this." *"I think there should have been more internal meetings within NDIT without PA."* *"It would have been beneficial to have introduced the planning phase in a traditional approach in lieu of how it was executed."* *"More documentation on expected work. For quite a while we were kind of running by the seat of our pants and getting actual documentation on what work needs to be done and who was responsible could have made it run better."* *"For some of the larger issues that were faced the NDIT team was very patient. The PA team strived to resolve them quickly but some took longer than expected."*