NASCIO State IT Recognition Awards
Nomination Form

NASCIO Nomination Form:

Nomination Requirements Formatting

- Length of nomination not to exceed seven (7) pages total
- Margins no smaller than one (1) inch
- Font should be easily readable and no smaller than 12pt
- Nomination must be submitted in PDF

Required Sections and Page Allotment

- **Page 1: Cover Page (title, category, state, contact, project initiation and end dates)**
    - Title: Turning Machine Data into Security Intelligence
    - Category: Cybersecurity
    - State: Alaska
    - Contact: Chris Letterman, CISO, State of Alaska
    - Project Initiation: March 2014
    - Project Completion: In production January 2015
- **Page 2: Executive Summary**

The State of Alaska is the largest and most sparsely populated U.S. state. Established in 2003, the mission of Alaska's security office is to prevent cybersecurity malicious events and identify vulnerabilities in the Alaska.gov space. With seven full-time employees spread across two offices in Anchorage and Juneau, the office helps various departments with their security planning, provides forensic and investigative support and manages the state's security operations center. This responsibility is critical to protecting both government data and citizens' information.

With a lean staff, the State Security Office had a need for operational-level visibility and a way to more effectively investigate cyber events. Alaska found it extremely difficult to efficiently analyze security events, as it took hours of analysts' time to go through the rudimentary process system by system to aggregate information. Alaska also saw problems with its legacy solutions and its ability to assess massive amounts of data. After trying a traditional security incident event management (SIEM), security leaders understood they needed a more robust solution to truly improve the security operations practices.

The state of Alaska is now using a data analytics platform to proactively monitor and report on network activity for multiple state agencies. This platform works as one easy solution that can be customized to fit unique needs of the state. Alaska now has the ability bring in all data streams across its IT infrastructure, taking place of the traditional SIEM.

- **Pages 3-7: Project Narrative: Concept, Significance and Impact**

Project Narrative

Protecting assets, information and data is becoming an increasingly bigger focus for state IT leaders nationwide. As security threats emerge, it's more important than ever for states to not just meet standards, but become proactive in their approach to identifying threats and evaluating risk management overall. The difficulty is finding a solution that has the capabilities and flexibility to support security needs today and in the future.

The increasing sophistication and velocity of cyber threats has made cyber defense a top priority for Alaska. Nowhere is this pressure more acute than within local and state governments. However, until recently, budget constraints and a lack of cybersecurity resources have created problems for the state. For instance, last year when oil prices began to fall, it became apparent the state's budget would be impacted. Alaska was put under a hiring restriction, which prevented the state from filling crucial positons. The team within the security office knew they needed tools to enable them to fulfill an increasingly heavy workload in a more efficient manner.

With seven full-time employees spread across two offices in Anchorage and Juneau, Alaska's security office is charged with security planning, providing forensic and investigative support and managing the state's security operations center. This responsibility is critical to protecting both government data and citizens' information. A long standing and stalled project for Enterprise Auditing and Logging languished for years without much impact. After employing a traditional security incident event management (SIEM), security leaders understood they needed a more robust solution to truly improve security operations practices.

A major challenge Alaska is now empowered to address is the enterprise security factor of its infrastructure. The new platform enabled the state to jump forward by "at least a couple of years in its consumption of logging information and establishing Splunk as an enterprise service," said Chris Letterman, CISO, state of Alaska. Chris went on to say that, "otherwise we would have had to find the staff and manpower to write queries and handle all of the data matching." According to Letterman, the new technology deployment was akin to the 'fast pass at Disneyland' for the state in terms of having our enterprise security analysis capabilities right there in front of them.

Alaska is now using Splunk Enterprise, a data analytics platform that can both meet the need for providing an Enterprise Logging service as well as proactively monitor and report on security event activity for multiple state agencies. The security office was able to quickly streamline

their efforts with platform analytics capabilities that ensure cyber events are investigated effectively and efficiently. State agencies are also now able to address security challenges much faster and with improved solutions and tactics.

Concept

State CISOs are finding ways to make sure they can not only meet, but thrive in the face of adversity. Now, Alaska is able to solve real problems without breaking their constraints. Overall, the mission of this new process for logging, monitoring, correlating and analyzing data is to achieve a robust cybersecurity posture and successfully fulfill the commitment to safeguard the informational assets of the state of Alaska. Due to the state's significant deficit, Alaska had no choice but to explore solutions and utilize a tool that enables them to work effectively within a minimal budget.

The project was born out of a long-standing and lagging project in support of Enterprise Logging. After many years of stops and starts, the Alaska team, under Chris's leadership, looked for alternative ways that could not only act as a logging aggregator, but also provide functionality for analyzing and correlating data across sources and timeframes.

With a novel approach to data tagging and sorting, the State Security Office has shown the ability to protect and segregate logged data based upon agency. This in turn addresses concerns over potentially sensitive logged data from being viewed or accessed by non-authorized IT staff. Coupled with a self-service approach, agencies are now able to access logged data whenever needed.

Significance and impact

Alaska is facing a 4 billion shortfall due to declining oil prices, which is a fundamental driver of the state's revenue. Not only are increasing cyber threats a problem, Chris Letterman, the state CISO, and his team also have to ensure that the executive agencies meet several mandates. Certain that he would not be able to hire additional personnel, or invest in traditional and costly SIEM solutions, he focused on finding ways to reuse the tools he already had and extract more value out of them.

The state of Alaska's security office now has the flexibility to do things its lean team was not capable of doing before. For instance, it can now ingest data across various security devices and network appliances, and then catalog them in such a way that enables them to pull intelligence information, monitor threats state-wide and respond appropriately. After implementing the security platform, the team reaped big dividends without increasing costs.

With the new platform, the security office can now perform in depth analysis on indicators of compromise and quickly get pertinent information to state agencies. The platform has also provided a capability for easier audits. Questions from the auditors around system logging can now be answered within a few minutes, by quickly pulling appropriate information from data that is indexed and tagged, making it readily available via Splunk Enterprise portal.

Now, even though the team is lean, they can help other agencies bolster cybersecurity posture across the state. In one instance, the state's fusion center requested their help with some 'interesting traffic'. Chris and team were able to assess it and provide useful intelligence within minutes. "This platform has enabled me and my team to respond effectively and efficiently to cyber threats in a manner we were never able to do prior to deploying the new platform," said Letterman.

Though the team had always been able to perform data logging, they weren't always able to provide meaningful outcomes with that data. "It was like knowing there was a cave full of treasure, without having the map to actually find it," Letterman said when describing the state's capabilities prior to deployment. With the new platform, Alaska is able to unlock the significant information that lies within all of its data and gain meaningful insights.

The impacts of the Splunk project to the state of Alaska directly contributes to the integrity and safety of citizen data. Which is crucial, because in Alaska citizens receive an annual Permanent Fund Dividend (PFD). The PFDis the citizen's share of natural resources revenue which derives from resource industries operating in the state. Every citizen who wishes to take part in the dividend must apply annually and supply their personal information online. Such a comprehensive online database of the state's citizenry must be monitored and protected. With the Splunk platform, Alaska can ensure the safety of its' citizens data, as well as the monitor for any potential fraud.

Supplemental Materials

Nominations may include URLs of public-facing project-specific sites. Judges may visit a site for clarification, but the project narrative will be the main basis of scoring. When writing the narrative, please assume judges will not visit the site. The inclusion of URLs is beneficial to other states when the nomination is included in the NASCIO Awards Library.

Scoring

- Exemplar (20%) – The project represents visionary and transformation use of information technology in state government.
- Concept (20%) – The project successfully addresses an important dilemma in public service and/or encourages civic engagement
- Significant (20%) – The project is consequential, relevant and transformational for state government and/or constituents
- Impact (40%) – The project leads to substantial and measurable changes; it makes state government better