Moving the Token Forward

A Layered Approach to Securing State Government Networks

Version 1.1
Updated: 5/7/2016

Contents

The Problem:

There are numerous reasons why States across the country are in the cybersecurity state they are in. This can generally be attributed to factors such as cybersecurity is hard in that there are so many avenues to defend. You have perimeters, shared or multi-tenancy network segments, internally developed software, vendor provided software, firmware, supply chain issues, misconfigurations, people who can be socially engineered, and incompatible legacy system requirements. Some of these conditions predate the 1970's, while others are far more recent. Typically, agencies are in widely varying states of cyber readiness. Those whom have large budgets, adequate manpower, and external compliance requirements tend to fair far better than those who do not. Fixing the blame is not only non-productive, but is far less germane to this discussion at this point than fixing the problem. While it is true that many states have provided governance directives for their subordinate agencies to follow, it is only one leg of the stool. Missing from this process is technical assistance, education, and a strong validation processes. While there are numerous variations for attribution of this sentiment, its best summarized as "You must Inspect what you Expect" [1]. This document attempts to forecast a series of initiatives that when layered together will deliver significant cybersecurity protections for the citizen data stored, processed, and shared across state enterprises. As with any well-conceived plan it cannot be a cookie cutter approach but rather one that provides for maximum flexibility. As Helmuth von Moltke said in his 1800's Moltke's Theory of War "No plan survives enemy contact" [2]. We would be remiss to not take heed of this time honored Axim when formulating strategies in cyberspace.

Understanding Potential Impediments to Success:

In order to establish a lasting foundation for cybersecurity within state government, we must take an honest look at today's culture across all facets of this issue. For the sake of discussion, the core constituencies will be addressed (Figure 1). We must recognize that change is organizationally challenging, requires executive support, and must be embraced by the majority of its operational stakeholders. No change as fundamental as the one proposed in this paper can be successful without executive support within agencies and the top levels of government. It must not only establish the Way Forward, but it must back up the plan with resources, access, and meaningful support. We must ensure the solutions approach we embark upon be from continuously evaluated to ensure it maintains an enterprise perspective.

The Enterprise Perspective:

Today, many state IT enterprises are run in a fashion similar to several hundred impendent companies who are individually managed, follow a similar set of general guidelines (industry best practices), and determine risk and mitigation strategies using varying standards of acceptance. We need to adjust our thinking to one of an Enterprise-centric focus. In this metaphor, agencies are subsidiaries of the corporation, take direction for their operations and security from the C-Level Staff, and answer to the Chief Executive Officer (CEO), whom is the Governor in this case. The Chief Information Officer (CIO) assesses and facilitates capabilities development and synergies that enable business execution and efficiencies across business operations. The Chief Security Officer (CSO) is responsible for the analysis, architecture, and management the protective measures for the whole of Enterprise IT Operations. The CSO also is responsible for enforcing, measuring, and reporting the compliance success and risk factors of the enterprise to the C-Level team. Finally, the Audit Team is a separate but critical component of enterprise risk. The audit team is entrusted to validate the IT metrics, processes, and procedures implemented throughout the enterprise ensure compliance

standards, including the consideration of the compensating controls described in POA&M's, to provide validation of risk assertions provided by the CSO office. Typically, the audit activity is not under the oversight of the CSO and reports directly to the CIO to preclude any potential for undue influence.

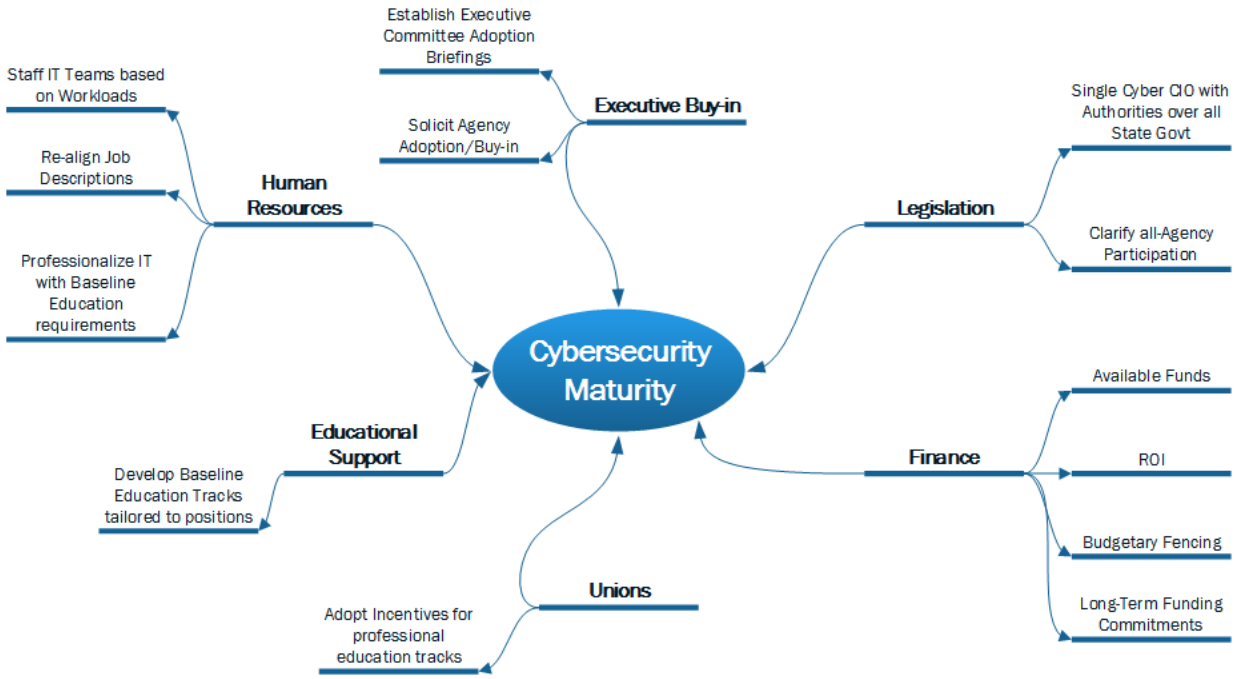

Figure 1. High-level Constituency Stakeholders

Resourcing: We must make a dispassionate review of our current budgetary allocations at agencies. This analysis should determine what appropriate funding levels are for the current operational services that each agency must provide to its constituencies. It should seek to:

- Identify outdated programs or services siphoning operational funds that could be better allocated elsewhere?
- Generate a list of recommended legislative changes to relieve government from any unnecessary mandated programs or streamline requirements to take into account maximum IT efficiencies
- Ensure every operational IT requirement is correlated to a Line Item in the agencies budget
    - Determine by program appropriate funding levels
    - Streamline the reallocation of funds upon program transfer or termination
- Ensure IT Line Item allocations are right-sized to the actual operational costs
- Shift operational costs for new procurements to the most cost effective methods (leasing or Data Center workloads .vs purchase) when said methods can meet the required FEDRAMP and State mandated cybersecurity requirements

- Recognize that the consolidation of data centers and state-run / monitored cloud service offerings could provide tremendous cybersecurity benefits if their operational costs were subsidized as part of the overall operations cost of protecting their state stakeholders
    - Consolidation allows for uniform enforcement of standardized configuration
    - Uniform deployment of security controls
    - Providing an immediate operational and measurable benefit to enterprise IT security
    - Provide cost avoidance opportunity to the enterprise when operated at scale

Manpower: In 1984, the Rand Corporation was commissioned to perform a study of the impact of technology on the workforce. That legacy study concluded that the shift to IT related services had grown by 18-30 percent over the past 20 years and was expected to accelerate [3]. Government, has embraced technology through the various efficiency initiates such as e-government. This shift in workload was gradual and in many cases not supported by an increase in the appropriate IT operational support personnel necessary to install, operate, secure, and maintain this transitional technology. However as obvious as this seems, far too often new requirements drive the addition of applications, services, and hardware without any change in staffing. Doing more with less leads to improperly configured systems, significant 3rd party vendor costs related to maintenance and installation, and inadequately secured and maintained systems. These conditions leave state organizations vulnerable to exploit and uncontrolled future costs. To be successful, State government must:

- Identify appropriate staff levels for IT organizations, directly correlated to program management workloads
- Establish standards that ensure that we recruit the appropriate candidates rather than select from inadequately trained or unprepared applications, solely based on prior government service
- Work with Human Resources to establish an incentives program based on the difficulty to attract and retain high-demand classifications to be more competitive with new graduates and early-term career professionals
- Leverage our top-tier educational system to develop training and education programs that upgrade our employees' current skills and prepare them for tomorrows challenges
- Approach the training of our employees as an investment, which trades employee efforts for no-cost training
- Ensure the training is of sufficient quality that our employees see this as favorable weighted factor when contemplating private industry offers
- Establish reasonable educational standards for the continued growth and career progression of our technical workforce
- In collaboration with our Union partners, develop a reasonable phased implementation that supports this self-improvement culture
- Tie future promotions within upper tier positions to these new educational standards

Support: One of the most significant cybersecurity initiatives undertaken by state government was the wide-spread adoption of NIST 800-53, revision 4 as the standard for cybersecurity. These standards are based on established best practices designed to facilitate a cross between operational requirements and security. Unfortunately, for non-regulated agencies these standards can seem daunting and highly ambiguous.

> For example, with regards to password complexity NIST 800-53, revision 4 control IA5(1) states: "Enforces minimum password complexity of *[Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type]*" [4].

In direct contrast, Microsoft recommends a minimum password length of 8 and complexity requiring no less than one upper and lowercase letter, a number, and a special character [5]. To add some context to this recommendation, the Foundstone Brute Force calculator estimates a random password of this complexity would take approximately 9 Years and 337 days to loop through all 1,127,875,251,287,708 password combinations [6]. Unfortunately, our users are more likely to choose something more like "B@seball1", followed by "B@seball2", etc…. Cracking these passwords are trivial using a dictionary attack, notwithstanding a full days efforts [7].

We owe our agencies clear guidelines that disambiguate wherever possible the foundational standards for state cybersecurity. Fundamental minimal security control values must be set by the CSO's Office. This empowers our agency Information Security Officers (ISOs) to affect change when reviewing security control settings. However, it's unreasonable to assume every legacy platform and appliance in every environment can meet every standard. Agencies who are unable to meet those requirements due to a technical shortfall in any system must submit a Plans of Action and Milestones (POA&M). POA&M's are addressed separately within this plan. At a minimum the CSO must apply an enterprise-centric approach to cybersecurity and publish / provide at a minimum:

- Clear directives and guidelines for minimum cybersecurity standards that all agencies are required to meet
- Produce assistive tools, technical guides, white papers, and training designed to facilitate agencies success in implementing and sustaining the required standards
- Act as a trusted resource multiplier and facilitator of solutions when our agencies request support or report issues
    - Agencies must view the CSO office as a trusted partner that adds value if we are to encourage an open and honest dialog related to risks and vulnerabilities
- A simplified compliance reporting channel that provides the needed information without unnecessarily burdening the agency staff with repetitive questions, questionable data calls, and provides plain spoke inquires and help tools. Consider it like the TurboTax for State Compliance Reporting
- Support resources for agencies to address cybersecurity related configurations and function questions. This one-team one-mission concept could potentially be supported through available manpower from already funded data centers professionals where capacity exists
- Develop and offer a program that leverages existing state IT support professionals that provides best pricing for technical services, reducing the time, cost, and complexity to obtain agency needed support
- Develop and maintain a repository of baseline templates for EVERY mandatory governance policy that address embeds the minimum acceptable standards, sections, and provides variable placeholders for organizational unique data.

- Provide clear, detailed legal guidelines concerning the minimal acceptable use of all state information technology resources including but not limited to computers, phones, tablets, internet usage, PII handling and transmission, breach reporting, and Incident reporting
- Develop or facilitate the procurement of meaningful user training that addresses both the core requirements and attempts to integrate emerging threats.
    - Develop unique offerings for IT Privileged Users; Executives; and International Travelers constituencies
    - Develop a system to track and dashboard successful completion of user security training across the enterprise
    - Establish metrics to hold both users and agencies accountable for compliance

Establishing Foundational Programs for Success:

In order to lay an appropriate foundation for success, we must develop, deploy, resource, monitor, and report the status of these initiatives. Reporting is a management control designed to measure standards compliance, risk, and readiness against the agencies current state. It is also a lagging indicator of potentially required enterprise-wide initiatives designed to move systemic shortfalls closer to compliance, thereby reducing potential risks. This plan calls for a series of initiatives in an effort to deploy, resource, monitor, and report metrics for agencies. These initiatives include:

State-wide Threat Collection and Analysis:

In addition, starting with the State Data Centers, and expanding to all agencies over an extended period, all agencies would be required to share all perimeter collected threat indicators with CSO or other state established Security Operations Center (SOC) or Threat Intelligence Center (TIC). This would provide a whole of state government threat assessment capability. Though sharing across many potential points of ingress / egress, threat indicators, actors, and techniques can be identified. This would drive threat reporting and indicator sharing with all agencies. While sharing of traffic would not obviewscate affected agencies at the SOC / TIC level, any derived indicators shared would require impacted agency obviewscation prior to release within the community. By leveraging this rich dataset and pairing it with classified threat indicators provided by DHS, it has the potential to shorten the time from intrusion detection to beginning of mitigation. To further enhance these efforts, a direct liaison between the state agency with statutory authorities for state cybercrimes and the SOC / TIC would facilitate a more rapid response to detected threat actors. This liaison could be further enhanced by an open and sharing dialog with federal law enforcement officials such as FBI and Secret Service (when appropriate). Due to the nature of cyber threat data, this may require all state privacy notices be modified to reflect a caveat for sharing of threat data for the purposes of threat assessment. This language should be drafted at the State Department of Justice level and mandated by the CSO prior to implementation. State agencies should be integrated into this Line of Effort based on capacity, license cost, and manpower for analysis. Highest risk agencies should be prioritized. As we add potentially millions of events for analysis, internally the SOC/TIC will need to identify what is a sustainable rate of entries to analyst per hour ratio and seek staffing accordingly. We must be sensitive acquiring data that is not properly analyzed, otherwise we're doomed to repeat the mistakes of Home Depot, who had indicators that were never reviewed.

Centralized Threat Information Sharing and Reporting: Today, most states have multiple groups officially and privately distributing cybersecurity related information. This is because of two factors. First, there is no authoritative one-stop resource in state government for this information. Additionally, due to constitutional separation, not all agencies in state government report to a single authoritative individual. As a result of these conditions, cybersecurity information sharing often results in one of two states:

- Multiple / Duplicate notifications resulting in overwhelming noise
- Missed notifications due to a lack of mandatory list participation and acknowledgement

Threat Sharing: The state SOC / TIC (or if one does not exist, the CSO office) should be the one-stop cyber threat information sharing center for state government. In order to facilitate this line of effort, the SOC / TIC must develop, deploy, and maintain a curated knowledge transfer and acknowledgement system designed to share cyber threat intelligence, risks, outage notifications, and indicators of compromise with all of State Government. This system should support notice:

- Curated Communities of Interest: These communities should consist information filtering caveats such as Law Enforcement Sensitive (LES), Technical, Informational, and DHS TLP Authorizations (e.g. TLP White .vs Green, etc…). The CSO and SOC/TIC should develop a series of caveats and determine the criteria for membership. For State Government, the CSO should maintain the listing management affecting those users. For LES caveats the State Cybersecurity Law Enforcement Liaison should manage those memberships. All other categories addressing other communities of interest should be SOC / TIC managed. When stakeholders have message traffic for the communities, they should provide the information to the SOC/TIC for review, caveat assignment, and distribution. The provided content should include the urgency for transmission (e.g. Normal, important, critical, etc…), intended audience(s), and Distribution caveats. It is possible this could be integrated into the CSO reporting system or a stand-alone web-based tool as appropriate based on stakeholder input.
- Standardized Cyber Threat Ranking: The state must develop a policy to classify risks into threat categories for the purpose of impact assessment. This policy must specify when a risk rating of a specific threat (e.g. Security Patch, Hardware Vulnerability, or Software Vulnerability) equals or exceeds a designed risk value, that the receiving agency representative must identify if the risk applies to their agency. This provides both the intelligence and Defensive teams with valuable data regarding the

Threat Sharing Acknowledgement and Reflexive Impact Assessment: Sharing information is critical, but performing a rapid assessment of a particular impact is just as critical. Responsible parties must review the threats, acknowledge receipt, and when appropriate based on policy, identify impacts of critical risks. In order for the tracking and larger overview of the risk impacts to such a diverse enterprise, those oversight teams must understand the dynamic changes to the threat surface. To that end, the system should implement in an initial phase a required acknowledgement of each issue transmitted. When threats rated beyond a certain agency threshold are transmitted, the acknowledgement must include a rapid assessment of agency impact.

> For example: Message 2234 – Acme Firewall running IOS version 14.3.5a; reported VPN bypass vulnerability…

Each agency would receive the message and be required to:

- Acknowledge receipt within (x) days; outliers would be contacted by the CSO office until the agency reports acknowledgement and impact
- Agencies affected by these high risk issues would include in the reply confirmation of impact via an affirmative checkbox titled "Impacted" and fill in a brief summary of impact unique to the agency (e.g. Agency has 2 firewalls running this version. Security update scheduled for emergency application on mmm dd yyyy).

These responses should appear in a dashboard-like view for the appropriate CSO and SOC/TIC team members (Figure 2). This allows the team to track the risk and ensure lagging responders receive support and coordinate assistance.

Message ID: 2234 **Title:** Acme Firewall running IOS 14.3.5a VPN Bypass vulnerability **Ack by:** 4/15/2016

Agency:	Rpt Code:	Ack	Impacted	Description
Air Resources Board	3900	Y	N	
Alcoholic Beverage Control	2100	Y	Y	2 Firewalls impacts, patch scheduled for application on 1 May 2016
Alt Retirement Prog	9955	N		*** Past Due **

Figure 2. Conceptual Threat Message Acknowledgement and Reporting Summary

This capability should be integrated into the states Incident Reporting tool should one exist to reduce complexity of acknowledgement and reporting. If a tool does not exist, a custom developed tool may be an appropriate choice. Consider this as a team graduate project opportunity that ties cybersecurity students, developers, and IT management students together into a single system collaboration. This solution would provide the state cost avoidance, development of custom code designed to implement the desired workflows and outcomes desired, and the retention of the code-base for later modification and development as changes are needed.

Vulnerability Assessment, Remediation, and Continuous Monitoring: A core component in evaluating the risk to a given system architecture or network is understanding known vulnerabilities. This is addressed in NIST 800-52, revision 4 control RA-5 [4]. Simply put, "you can can't fix what you don't know is broken" (Author unknown). Cybersecurity has taught us that simply applying a vendor patch does not guarantee success. Examples of this situation include:

- One-off systems that fail to properly replace libraries in use
- 3rd party vendor software that deploy modules / code that places the at risk code in a different location than patched by the OS vendor
- Unintended post-patch reintroduction of the at-risk code (e.g. add-ins, modifications to configurations, etc…)

A mature vulnerability remediation process includes the assessment of the success of the applied security patch deployment and confirmation of whole of system remediation. This capability should exist in every agency. The monitoring of timely patch deployment is a metric the state should measure as part of its dynamic risk assessment (Figure 3). Agencies should be held accountable for timely secure patch deployment and reporting. To that end, metrics should be developed that assess and rates:

- Date security patch was released
- # systems remaining vulnerable
- If the established due date for compliance has been exceeded
- If a POA&M has been approved for each un-remediated system (beyond compliance date)
- These factors should relate to a percentage of compliance score
- A minimum acceptable score and non-compliance widow should be delineated in policy
- Agencies who fail to achieve acceptable metrics should be penalized in a meaningful manner

Vulnerability Status Reporting
Agency XXXXX

Vendor	***Security Patch***	***Date Issued***	***Due Date***	***# Systems Vul***	***POA&M Issued***	***Compliant***
Microsoft	2016-0345	May 13, 2016	Jul 13, 2016	23	n/a	No
Adobe	2016-2	Jan 4, 2016	Mar 4, 2016	3	Yes	No
Oracle	2015-222-1	Nov 11, 2015	Feb 11, 2016	0	n/a	Yes

Figure 3. By Agency Security Patching Status Report

These metrics should be developed and rolled up for every Agency, Department, Board. Underperforming subordinate activities should be actively monitored and supported to reach acceptable compliance by their parent agencies. All agencies should roll up to the CSO office as part of their dynamic threat monitoring and mitigation process. The implementation of a web-based solution, hosted in a secure space in the states data center should be considered to address this requirement. This is another opportunity for a graduate-level project to provide this capability with maximum cost avoidance.

Once each organization has established a vulnerability assessment process, then historical metrics can be developed that show the owning activities the overall risk to given systems over time. This requirement is referred to in NIST 800-53, revision 4, control CA-7, Continuous Monitoring [4]. This helps to identify outlier system that are not successfully patching. This is often an indicator of either required touch-labor or potentially more permanent remediation requirements (e.g. reimage, reinstall, upgrade, etc…).

Newly Deployed Systems & Vendor Deployed Solutions: Vulnerability analysis and successful security patch application should also be a documented requirement for the movement to production of any new system, service, or other network modification. In cases were 3rd party vendors have designed and deploy the solution, a successful “Clean” scan certification or POA&M list should be

generated. No 3rd party vendor should be paid for deploying a system that inadequately addresses its detectable cybersecurity flaws through either government accepted (CSO) and documented compensating controls or through the application of the appropriate security patches and revalidation of required operational capacity.

Development of Standardized Dashboards and Reporting Metrics:

Cybersecurity and Risk Mitigation are conjoined requirements. Developing metrics that provide meaningful measurement of the current state of the state IT enterprise provide both informed management governance and well as provide elected officials and Senior Executives with the necessary oversight to be both informed and drive mission priorities. Tips for developing meaningful metrics include:

- Avoid qualitative metrics where possible; they are difficult to consistently measure therefore likely to make results analysis suspect and difficult to justify
- Identify quantifiable core baseline standards that are measurable
    - Secure Patch Application
    - User Training Completion
    - Legacy OS instances in Production
    - Number of Virus Infections (Monthly)
    - etc…
    - Measure only what important and meaningful, otherwise its noise that distracts management from the important indicators
- Establish acceptable limits for a given metrics that are both reasonable and achievable across the enterprise
    - This may require initial higher limits that are decreased over time
- Establish a simplified rating system to standardize current progress (e.g. Red – Amber – Green) or a Numeric System (1 – 5)
    - Define rated values for standardized understanding
- Develop Outlier and Roll Up reporting for Senior Executives
    - Ensure this topic receives attention at reoccurring staff meetings
- Tie unsuccessful metrics to POA&M reporting requirements and track progress to resolution or until management oversight actions are undertaken to resolve the problem

Plans of Action and Milestones (POA&M) Process:

This is the process for the identification, impact analysis of baseline non-compliance, and includes the formalized risk acknowledgement, acceptance, and documentation mechanisms. Today, in many states there are no clear guidelines established for whom, and more importantly at what level(s) the acceptance of information security risk is authorized and appropriate. This impacts agencies because without an enterprise-centric risk acceptance program:

- Any agency is able to accept any risk level, regardless of overall enterprise impact
- Visibility to acceptance of risks occurs absent of enterprise visibility or concurrence
- The potential for acceptance of unacceptable risk levels could occur

- Prevents the identification of enterprise-wide systemic issues that if addressed may have dramatic impact to overall security

Without a workflow that ensures the visibility and graduated approval process, it is virtually impossible for an enterprise-level risk assessment of any meaning to occur. To resolve this issue, a policy to formalize the Risk Acceptance process by developing a tiered rating system, assign acceptance levels based on tier, streamline the reporting and documentation process. These artifacts should be tied to the overall System Certification and Accreditation (C&A), Vulnerability Assessment, and Lifecycle Management processes.

Requests and Documentation: The PAO&M process should be an electronic workflow that is initiated by the owning activity. It should document:

- Impacts asset(s)
- Risk(s) that cannot be remediated by the established due date
- A summary of the steps the activity will undertake to bring the assets into compliance
- Date the remediation's are projected to be completed
- Impact(s) including statutory and regulatory, if the asset(s) are permanently removed from production for non-compliance
- Requesting ISO / AIO / CIO
- Requesting Individuals contact information (voice and email)

This workflow should allow the initiator to track through the management control hierarchy to include whom has the request, its approval status, and any comments or notes made through the require process.

Approval Process: Requests initiated by the owning activity will flow through the agency management control hierarchy. In each step within the management control hierarchy, the request must meet with either concurrence or disapproval. In either case comments are required. Each level within the management hierarchy will include the digital attribution of the approval for documentation auditing purposes. Activities within the agency hierarchy process whom disapprove a PAO&M should expect to provide guidance and assistance (as appropriate) to the requesting activity to achieve compliance or remove the resource from production.

Cost Mitigation Measures: In some cases, legacy systems or changes in technology render a production system at a level of unacceptable risk. In those cases, were the risk cannot be reasonably mitigated and the services provided by the system are mandated for continuous delivery, the POA&M should be used to document the CSO's recommendation for earliest possible replacement using the states supplemental budgetary support or other fiduciary justification processes.

Enterprise-wide Standardization and Procurement Vehicles: State government IT is in a constant state of change. Legacy systems are being updated, retired, cloud hosted, and mobile enabled at an accelerated rate. We must ensure that the CSO partners with the state procurement agency to standardize the minimum acceptable standards for new, updated, and retirement of IT systems and services. This will require two core initiatives occur on two different fronts:

- CSO:

    - Partner with procurement to develop common, plain English language that will be mandated in all future IT services contracts to ensure baseline security standards are implemented in all SDLC phases.
    - Develop IT policy that requires all IT software, hardware, and services be procured using these contracting vehicles unless a formal waiver of unsuitability is approved by CSO office
    - Identify one-off, critical, high cost services and facilitate development of streamlined contracting language for their procurement
    - POA&M's requesting remediation procurements should include CSO review and concurrence to ensure solutions address findings and follow enterprise approved strategies
- State Procurement Activity:
    - Identify IT services under significant demand across Agencies and supported activities
    - Partner with the CSO office to develop and streamline standard language for solicitations that allow DGS to procure Indefinite Delivery, Indefinite Quantity (IDIQ) services at scale, providing best possible pricing and streaming agency procurement ease at lowest cost
    - Work with agencies to streamline the procurement process using workflows, automation, and other standardization tools designed to shorten the time from requirements identification to product delivery and ultimately vendor payment
    - Develop emergency contracting vehicles to address pre-negotiated best cost rates for Incident Response, PCI-DSS Auditing, and Disaster Recovery related construction services

We must also recognize the secondary benefits of standardized procurement. Buy streamlining the selection process, it also standardizes the tools, thus enables for the universal development of tactics, and techniques for operations and defense across the enterprise. Consider from a support perspective having a library of white papers maintained by enterprise operations. Within the library, IT operators from the various agencies could locate best practice deployment and configuration guidelines for many of the states' infrastructure and services. This would speed deployment of more secure installations. It could also assist auditors in evaluating general configuration compliance.

3rd Party Assessments and Audits: As stated earlier, we must evaluate our mandates to ensure they are appropriately implemented. For agencies this should occur using two vehicles. From a Security and Operations Technical standpoint, each agency should undergo a Biennially Independent Security Assessment (ISA). These assessments are important for a variety of reasons which include:

- Independent review of vulnerability mitigation effectiveness
- Evaluation of the effective implementation of a subset sampling of selected NIST controls
- Potential for identification of improperly implemented IT security measures or practices
- Validation of risk factors reported to the CSO
- Potential to identify previously undetected threat actor presence within agency networks
- Provide actionable recommendations for further network hardening
- Provides technical analysis of secure controls

These assessments are core to the overall security of State Government IT. As such, they are an operational cost and should be funded as such. Funding both the Assessment and Audit functions within state government should occur external to agency budgets. This ensures that 100% of the agencies budget is expended on the daily operations and security of the provided services, rather than siphoning funds for compliance activities owned at the enterprise level. If you must siphon funds, then consider a model that provides for budget for the programs total operations (personnel, equipment, transportation, training, and maintenance) by decrementing an equal share from each agencies budget at time of allotment (e.g. 2%), thus making the cost and the burden both equal and proportionate on the budget. By creating a distributed funding model, the budgetary impact:

- Will cost less per activity to fund
- Eliminates contracting fees currently assessed procurement
- Ensures the capacity and availability of the resources
- Establishes an operational capacity for an incident response force should a network be attacked, breached, or other cyber offensive operations befall the activity

For this course of action to be successful, a working group would need to be commissioned, staffed with State Human Resources, State Emergency Services, CIO representation, State Finance Department, and current state agency provider Subject Matter Experts (SMEs) to determine an appropriate staffing level, identify operational costs, and proposed timeline for execution. I believe with Executive Staff emphasis, a proposal including costing models, proposed Activity decrement, and go-live forecasting could be delivered for review within 45 days of assignment.

Establishing a Professional Cyber Workforce: A critical consideration in the securing state Government sensitive systems and information is its workforce. Our workforce in many ways is the engine of success. If we overburden the engine or fail to maintain it, more expensive repairs will be required. We avoid these issues through intelligent employee investment. In order to maximum employee return, we must ensure we provide them high quality, role appropriate training that is designed to maximum their individual contributions. We must also demonstrate a plan that rewards continued growth and skills through professional development. Finally, we must develop methods to implement the professional development program in partnership with our unions by partnering with them in the development process so that issues related to salary realignment, educational benefits, and increased opportunity are equitably addressed.

In the case of California, there is a significant line of effort underway within the states' Cybersecurity Taskforce with this regard. This effort should serve as a model for other states whom should consider the integration of the following minimum components:

a) Establishing a counsel, staffed from various sized IT group representation from across the state to identify opportunities for IT Classification consolidation and standardization
b) Adopt the National Initiative for Cybersecurity Education (NICE) position titles and descriptions within our standardization process [8]
c) Establish an Apprentice, Journeyman, Expert leveling for all classifications that requires successful completion of standards-based education and training to occur as a requirement for greater roles and responsibilities
    I. Include a grandfather clause for current employees in their current positions

d) Leverage states higher educational institutions to develop training content to meet the state employee educational requirements. A fusion of IT and Educators, working in collaboration to provide high quality content, deliverable via a distributed Learning Management System (LMS). This system should be accessible to our employees and work and at home allowing them maximum opportunity to prepare and excel
e) Review industry and current classification compensation options to identify way to better compete for these scarce resources. Additional compensations may include reduced cost for Post-secondary education for themselves or family; access to unique assignment opportunities; or Internships with civilian industry. We must temper some of these benefits with employee retention commitments to ensure maximum equality for all involved.

Data Destruction and Certification:

Data at Rest represents one of the most common breach sources that state government encounters. For purposes of clarification, I am referring only to digitally stored media. The massive inflow of media storage is staggering. Consider these risk drivers:

- Desktop / Laptop Lifecycle
- Printer Lifecycle (MFPs) Replacement / Maintenance
- Flash Drives usage / loss / lack of accountability
- CD / DVD / Back-up Tapes use and lifecycle
- SAN Drive lifecycle
- Mobile Device loss and lifecycle

Today it is not uncommon for individual agencies to be responsible for the tracking and remediation of magnetic media repositories. Often states do not provide clear guidance, resulting is varying levels of administrative controls regarding the process. This leads to the loss of positive control over citizen data sources. This is an area where policy and resources at the State Level can play a positive role in managing the risk. Consider these recommendations:

- Establish a state-wide inventory tracking system for all Servers, SANs, Workstations, Laptops, Mobile Devices, Removable Drives, and Flash Drives
- Require Devices to be tracked by Agencies within the system by Asset tag and Serial Number
- Require devices transitioned to End of Life status undergo a media wipe, degauss, or the removal and certified storage device physically destruction
- Require a Certificate of Compliance be uploaded for each device into the tracking system
- Devices stolen or lost should have a copy of the Incident Report uploaded in place of the Destruction Certificate
- Negotiate best price contracting vehicles that allow agencies to increase the ease and quality of destruction services at reduced rates

Incident Response Capabilities:

This is a capability far too often proven to be a necessity in state government. Rather than wait for an incident to occur, states must develop proactive processes, tools, and procedures to streamline their response to these occurrences. At a bare minimum every state should:

Reporting Processes and Procedures:

- Develop and maintain clear and concise policies that addresses the criteria for an incident, a categorization of the impact, and specific reporting requirements for agencies to follow
- Reporting requirements should consider incidents are not always discovered during normal operating hours / days; maximum use of technology, reporting portals, and workflows should be utilized
- Develop and deploy formal, ongoing awareness campaign for reporting that includes the elements of How to Report, Where to Report, and What to Report. The reporting process must create a climate where the risk of not reporting incidents are too detrimental to be tolerated
- Develop feedback loops that add value and assist reporting agencies in meeting their requirements
    - In cases where significant manpower or costly post-breach remediation issues manifest, ensure the state procures best value, lowest cost services for affected agencies to engage
- Develop fusion and information sharing avenues that publish timely avoidance processes and recovery procedures designed to aid other agencies from similar issues manifesting
    - Ensure these products prevent the accidental exposure of the affected agency
- Develop and maintain cybersecurity threat data on incidents as a rich repository for future / ongoing threat forecasting
- When the decision to deploy a response team is made, ensure that the action is actively tracked and reported through the management hierarchies through the initial notification, initial deployment, remediation, and post-remediation phases.

Incident Response Play-book:

- Establish working groups of incident response professionals from government and industry to chart scenarios for consideration
- Develop working concepts for scenarios
- Seek lessons learned from prior incidents
- Ensure processes include requirements for actions documentation and retention
- Develop the tools, tactics, and procedures to ensure a through and consistent response
- Ensure the focus is not limited to a specific vendor, accounts for all operating systems, and is repeatable
- Procure the tools and software identified, establish and standardize ‘Go-Boxes’ and SOPs
    - Stage Go-Boxes where they are accessible 24/7/365 by team leaders
- Develop an escalation and de-escalation plan for incidents
- Identify 3rd party Incident Response providers and pre-negotiate emergency contracting procedures and pricing for use when needed
- Mandate training events that walk the team through the Crawl, Walk, Run methodology of execution

- Ensure all training events receive senior management visibility, support, and participation
- Ensure the State and agency Public Information Officers (PIOs) and agency legal teams are active participants in training
- Ensure a process for transition of Incident Response teams accounts for both the return to agency full control as well as a path for escalation to 3rd party or Law Enforcement hand-off

Develop both a Ready and Surge Capacity Incident Response Force

- Tools and software are worthless if you do not establish and maintain trained personnel able to effectively leverage their capabilities
- Identify no less than two core incident response teams which will alternate as the Primary response team
- Establish In-band and Out-of-Band alert procedures and add those methods to the training plans of the SOC / TIC and teams
- Ensure team members are training to the standards established in your Incident Response guidelines
- Develop rosters of surge capability responders for specialty areas such as SCADA, Database, Malware Disassembly, Main Frames, etc…
- Develop training events that increase responder's capabilities and ensure both primary, alternate, and surge capability members are trained

Establish a Cyber Annex to the State All-Hazards Plan:

Cybersecurity is unique in that when issues manifest they are not as readily observable as are the impacts of an Earthquake or Flood. They can however be far more devastating and far more wide reaching in impact. Cyber incidents can manifest as the result of natural or man-made events with both intentional and non-intention destructive outcomes. To provide the best options for readiness, every state should develop a Cyber Annex to their All-Hazards plan. The plan should address:

- What constitutes an Emergency .vs localized Operational Impact
- Who is responsible for recommended the declaration of an emergency
- Who will be responsible for the deployment, management, resourcing, and redeployment of response forces
- Who is the incident commander and how will they report status / requirements
- Consider reviewing the NASCO Cyber Disruption Model for guidelines and recommendations [9]
- Consider crafting public information messaging in advance for issues that could result in a cyber-related emergency
- Ensure the plan addresses out-of-band communications and data access (as required)

Works Cited

[1] Unk, "Inspecting What You Expect," nd. [Online]. Available: http://thepositivedarkside.com/articles/Inspecting_What_You_Expect.pdf. [Accessed 13 March 2016].

[2] D. J. Hughes, Moltke on the Art of War: selected writings, New York, USA: Presidio Press, 1993, pp. 33-40.

[3] Rand Corporation, "THe Future at Work - Trends and Implications," 2004. [Online]. Available: http://www.rand.org/pubs/research_briefs/RB5070/index1.html. [Accessed 13 March 2016].

[4] NIST, "NIST Special Publication 800-53," April 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed 22 September 2013].

[5] Microsoft Incorporated, "Minimum Password Length," May 2012. [Online]. Available: https://technet.microsoft.com/pt-pt/library/hh994560(v=ws.10).aspx. [Accessed 13 March 2016].

[6] Foundstone Research, "Open Security Research," nd. [Online]. Available: http://calc.opensecurityresearch.com/. [Accessed 7 May 2016].

[7] PassFault, "Welcome," nd. [Online]. Available: http://passfault.com/. [Accessed 7 May 2016].

[8] US Department of Homeland Security, "National Cybersecurity Workforce Framework," 18 December 2015. [Online]. Available: https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework. [Accessed 18 March 2016].

[9] NASCIO, "Cyber Disruption Response Planning Guide," April 2016. [Online]. Available: http://www.nascio.org/Publications/ArtMID/485/ArticleID/358/Cyber-Disruption-Response-Planning-Guide. [Accessed 16 April 2016].