Office of the Inspector General

Patrick J. Maley

State Government Information Security Initiative

Current Situation & A Way Forward

Interim Report

November 30, 2012

I. Executive Summary

The newspaper headline, “Millions of Taxpayer Records Exposed,” captures the triggering event to initiate a review of state government’s information security (INFOSEC) posture. This report does not examine the recent Department of Revenue (DOR) breach of taxpayer information; law enforcement is addressing that issue. The DOR breach raised the immediate due diligence concern about the level of information security at other state agencies. This review examines the current condition of the statewide INFOSEC posture, and provides a way forward to ensure the state does everything possible to reduce the risk of a future data loss and protect our citizens’ information.

Currently, South Carolina does not have statewide INFOSEC standard policies. There is no state entity with the authority, or responsibility, to provide leadership, standards, policies, and oversight. The Division of State Information Technology (DSIT), which is led by the state’s Chief Information Officer (CIO), has no authority to mandate INFOSEC standard policies to agencies. The DSIT only provides “suggested” policy and ad hoc support to help interested agencies, and it does not provide any oversight to agencies’ individual INFOSEC plans. By default, authority has been delegated to each agency to decide its own risk tolerance for data loss and its own INFOSEC plan.

This decentralized INFOSEC environment inherently produces less than an adequate statewide INFOSEC posture. The lack of standard policies produces uneven quality in individual agency security postures. This decentralized approach also prevents the state from understanding, let alone managing, statewide INFOSEC risk which has the capacity to impact the entire state government.

INFOSEC activities are carried out every day in every agency. Many agencies are required to meet federal INFOSEC standards due to maintaining categories of personally identifiable information (PII), such as health, tax, or credit card information. Further, every agency CIO fully understands the duty to protect information and implement INFOSEC protective measures. The question is—do these independent INFOSEC judgments carried out in an uncoordinated manner without any common standard policies in more than 100 state agencies, universities, and commissions, all add up to meet the post-DOR risk threshold of protecting our citizens’ information? No.

The review interviewed 18 agency CIOs, primarily members of the Information Technology Solutions Committee (ITSC), which is a DSIT advisory board of CIOs representing the various sectors of state agencies. There was near universal agreement for the need for statewide standard policies, and a candid assessment that statewide INFOSEC is less than adequate. Resources were an issue, but not to the extent anticipated. There was a sense agencies were conducting mission critical INFOSEC, but had little capacity to be proactive in an increasing threat and vulnerability environment. The uneven INFOSEC staffing, skill, and experience among agencies raised concern, particularly small agencies with limited IT staff. According to CIOs, the aggregate issues pertaining to resources, staffing, expertise, and statewide standards creates a less than adequate statewide

INFOSEC posture, particularly in an environment of increasingly complex threats and vulnerabilities.

The DSIT agreed with the CIOs' less than adequate assessment of statewide INFOSEC. All data sources, CIOs, DSIT and experts, recommended transitioning from a decentralized environment to a statewide program with a standard policy framework to reduce agency and statewide INFOSEC risk.

South Carolina is not alone. A 2012 national survey of State Chief Information Security Officers determined only 24% were very confident in protecting information assets against external threats. The top two survey issues were: INFOSEC funding; and working in highly decentralized environments with little central authority over individual agency security. The motivation to address these same two issues now in South Carolina looks completely different through the prism of the post-DOR breach. We recognize security breaches can be far more costly than robust INFOSEC programs, especially when coupled with the incalculable cost of regaining lost citizen trust.

Given the state's low risk tolerance for another significant data loss, the current level of statewide INFOSEC risk is not acceptable. Further, regardless of the assessment of statewide risk, the current decentralized INFOSEC environment provides no visibility of risks within agencies, which is incompatible with state government's due diligence responsibility to do everything possible to protect citizens' information. The first step towards a statewide INFOSEC program is establishing a governance model. According to an expert, "the governance structure is the defining activity that serves as the foundation and sustains all others (activities)." All sources highlighted the need for a consultant, with prior statewide INFOSEC implementation experience, to assist in governance development, statewide strategy, and individual agency risk assessments and mitigation strategies.

Governance starts with leadership. Establishing a statewide Chief Information Security Officer (CISO) is required to take ownership of a statewide INFOSEC program. The governance framework has many components, such as strategies, structure, resource and technical support, risk management, authorities, policies, and audit. A key governance component decision is the level of centralized authority. The vast majority of data sources, to include agency CIOs, recommended a traditional federated model with responsibility for the statewide INFOSEC program and comprehensive strategies. A federated model has authority to establish a standard policy framework for all agencies. This standard policy framework can then be delegated, in most areas, to agencies to tailor statewide policies to their operational environment, yet still be subject to oversight and audit.

If approved, a CISO, a federated model, and the use of a consultant with expertise in implementing INFOSEC statewide programs should construct a governance framework in a collaborative manner with agency representation, as well as develop implementation plans. The next interim report will focus on implementation options and recommendations, in terms of cost and schedule, to develop a long term sustainable statewide INFOSEC program to reduce agencies and statewide risk.

Table of Contents

II. Background

A. Objective

On October 26, 2012, Governor Nikki R. Haley issued Executive Order 2012-10 and requested the State Inspector General make recommendations, on a comprehensive and holistic basis, to improve information security policies and procedures in state agencies. The Governor noted that throughout state government, information technology policy for security procedures and protocols have been largely uncoordinated and outdated exposing our state to greater risks of internal and external cyber-attacks.

Governor Haley's request was in response to the announcement the same day of a network breach at the DOR resulting in millions of stolen records containing taxpayer personal information. This breach, one of the largest of its kind, directly diminished the trust and confidence of the public in state government, and elevated concerns about the security of data at other state agencies.

B. Description of INFOSEC

INFOSEC, also called Cyber security, can seem overwhelming to many. The technical definition is, "safe-guarding an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity." In non-technical terms, it is a business decision using a variety of control procedures to protect an organization's information needed to conduct business, as well as its obligation to protect information entrusted from others. No single control procedure provides adequate INFOSEC, nor can deploying every possible control completely eliminate the risk of a data loss. The general approach is to build controls in a layering process, which when aggregated, provide a "depth of defense" to reduce the risk of a data loss. Controls include, but not limited to, passwords, data compartmentalization, encryption, mobile device access, Internet firewalls, operating system patches, systems monitoring, data loss protection technology tools, and employee training. Ideally, all these controls act in an additive, overlapping, and dynamic manner to provide an effective INFOSEC program. INFOSEC is a continuous process, rather than a single solution.

The starting point in developing an INFOSEC program is understanding an organization's unique vulnerabilities to threats, which when combined add up to an organization's risk. Only after this analysis can the appropriate controls be designed and implemented in the most cost effective manner. INFOSEC has a fundamental operating framework, but it takes substantial technical skill and professional judgment to find that appropriate balance of addressing vulnerabilities with the appropriate cost/effective controls.

Organizations' vulnerabilities to cyber threats have been dramatically escalating over the past several years, and this trend will continue, if not accelerate. The cyber threats from individual "hobbyist" hackers have evolved to organized Cybercriminals and a new breed of hacker known as hacktivism, which has political or social agendas. Both use increasingly sophisticated methods to target computer systems for monetary gain and to make political statements. Nation states continue their advanced persistent efforts in economic espionage and stealing national security secrets. INFOSEC security measures will protect us from most threats. However, the level of hacker sophistication is clearly increasing at a faster rate than our ability to comfortably defend.

At the same time, organizations are becoming more vulnerable as the amount of data within and flowing between companies is increasing exponentially. Access to these systems is increasing in numbers and complexity as more employees access agency networks and files from remote locations on a 24/7 basis with non-traditional devices, such as smart-phones and tablets. This volume, complexity, and velocity of information increases the risks associated with maintaining citizens' data, held in trust. These increased vulnerabilities translate into a startling statistic from a recent 2012 cyber security study where government agencies have lost more than 94 million records of citizens since 2009 (Rapid7 report on the "Data Breaches in the Government Sector").

As evidence of the significance of this threat level, FBI Director Robert Mueller anticipates cyber threats could unseat terrorism as the Bureau's top priority in the near future. Director Mueller said, "there are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be hacked again."

INFOSEC has a tendency to be viewed as only an expense to avoid the pain of a data loss, which certainly is a prime objective. However, the benefits of an effective INFOSEC program are now being recognized as a key productivity "driver" to leverage technology in e-business, which is an important avenue to add efficiency and effectiveness in state government delivering services. Leveraging technology to interface with customers streamlines government operations, best characterized as citizens doing business from their kitchen tables rather than standing in line.

C. Short Term Statewide Efforts

After the DOR breach, each agency was tasked with completing a list of short term statewide protective measures. These tasks were:

- Conduct short term remediation steps: Each Agency "double checked" specific INFOSEC procedures having the highest impact on lowering INFOSEC risk. Emphasis was on reviewing these fundamentals in each agency through the new optic of the post-DOR breach world in which we now operate.
- Agency self-assessment: Each Agency CIO completed an electronic INFOSEC self-assessment survey, as did each Agency Head from their perspective. Then, the Agency Head and CIO met to discuss the results to ensure Agency Heads were fully engaged in this statewide issue.
- Data Classification: Each agency located all high risk data, primarily personal identifying information (PII) and protected health information (PHI). Additionally, agencies were tasked to request help on any PII or PHI not sufficiently secured.

Agencies addressed these tasks, as well as self-generated initiatives based on their own internal identified vulnerabilities.

III. Current Assessment of Statewide INFOSEC Risk

From basic passwords to high technology network monitoring, every agency performs INFOSEC activities daily. The problem is that each agency decides its own risk tolerance for a data loss and determines what it thinks is an appropriate INFOSEC plan. Each agency sets up its own INFOSEC plan because there is no statewide INFOSEC program providing leadership, support, and establishing statewide INFOSEC expectations in the form of standards, policies, and procedures.

In today's environment, a critical component of every organization's governance is INFOSEC, particularly protecting personal identity information (PII) due to the potential of catastrophic organizational damage if compromised. South Carolina has no governance mechanism for statewide INFOSEC; it has been, by default, delegated to each agency to decide its own INFOSEC plan. This decentralized approach prevents the state from understanding, let alone managing, statewide INFOSEC risk, which creates potentially negative consequences for all of state government.

The DSIT, which is led by the state CIO, lacks the authority to lead statewide INFOSEC. The DSIT's role has been to provide "suggested" policy and ad hoc support to help interested agencies. For example, the Information Technology Solutions Committee (ITSC), an advisory board to DSIT, recently set forth a recommended security policy template in October 2012 requesting all state government entities to develop and publish an individual agency IT Security Policy no later than February 1, 2013. This proactive step is good, but it is still just "requesting" without the authority to monitor compliance.

To obtain a time sensitive assessment of statewide INFOSEC risk, information was obtained from the following groups: state agency CIOs, DSIT, universities, experts from the private sector, and professional research and literature.

A. State Agency Chief Information Officers

To give decision makers the best evidence in a time sensitive manner of the current INFOSEC conditions "on the ground," 18 agency CIOs, primarily members of the ITSC, were systematically interviewed. The ITSC is composed of CIOs representing the various sectors of state government agencies. Given their unique positions on the front line, their aggregated input was considered a good barometer of the INFOSEC risk in statewide government.

An aspect of these interviews was asking the 18 agency CIOs the same questions on a "1" (low/decreasing) to "5" (high/increasing) scale, which provided an overview of their collective perspectives:

QUESTION:	Responses From 1 (Low) to 5 (High)					Average
	1	2	3	4	5	
What is the current threat level of breaches?			5	5	8	4.2
How has the threat level changed in last 5 years?			1	10	7	4.3
What is the threat forecast for next 5 years?		1	2	6	9	4.3
Rate your agency's INFOSEC capabilities?	1	7	6	1	3	2.9
Rate the statewide INFOSEC capabilities? *	7	8	2			1.7

*one CIO did not answer this question

The CIOs rated their own agencies' INFOSEC capabilities, which averaged just marginally below adequate (2.9). Their assessment of statewide INFOSEC capabilities was clearly less than adequate (1.7). This statewide assessment is inherently subjective and limited to each CIO's unique vision on the issue from their personal experience and agency's perspective. However, when a cross section of INFOSEC leadership on the front line rates statewide capabilities at 1.7, to include 15 (88%) of the 18 CIOs' ratings were less than adequate, it has meaning. Comments illustrating this issue were:

- An agency's Information Security Officer (ISO) with unique access into other state agencies INFOSEC postures reported that agencies are clearly less than adequate in their INFOSEC. There are many instances where agencies have a false sense of security by having a policy covering a vulnerability, yet their procedures to implement the policy don't work.

- A CIO with large amounts of personal identifying information (PII) in a complex operation with employees and contractors with remote accesses described his concern, echoed by many others, 'what scares me is what I don't know.' The factors described raise the risk of increasing vulnerabilities not being fully understood, let alone mitigated.

- A CIO with unique access to related state agencies, described statewide INFOSEC "as a 2 on a good day." Small agencies have challenges in terms of expertise and resources.

The CIOs' assessments were underpinned from a variety of perspectives, and certainly no one issue drove their less than adequate statewide assessment. Areas causing concern included deficiencies in standard policies, resources, staffing, and INFOSEC expertise, as well as the recent significant breach. It was clearly the aggregate of these factors that created a less than adequate statewide INFOSEC posture.

CIOs recognized the benefits of statewide standards. Almost without exception, the state needs to move away from its current decentralized approach to INFOSEC. A few leaned towards full centralization of this statewide function, but the vast majority favored a federated model with central governance with authority to set standard policies, yet allow agencies to tailor policies to their operational environment while subject to oversight and audit. Ideally, a federated model would provide support in many ways, including resources, expertise, threat intelligence, and lessons learned from other state agencies, all in a timely manner. Further, as agencies become mutually interconnected, use third party processors, and move toward providing citizens with convenient web based services, there is a critical need for statewide policy decisions addressing these new challenges.

Illustrating the need for statewide standard policies, the Executive Branch Inspector General initiated an April 2012 policy compliance review of 10 state agencies, which noted four (40%) did not have an employee INFOSEC awareness training program. DSIT offers a computer based employee training program for a nominal cost. During CIO interviews, one CIO was completely unaware of this DSIT program, while another learned about it from a third party, not DSIT. Employee training is a well known component of INFOSEC programs, yet without clear mandatory standards, translating “knowing” into “doing” is problematic. Mandatory annual computer based employee security awareness training was a pattern in other states contacted.

Most state agencies have in place the basic technical hardware and software needed to control access to their agency-level networks and data, as well as provide some protection from malware and viruses. More comprehensive security requires complete network monitoring, which many agencies have through DSIT or through an outside third-party vendor. However, many agencies have technical obstacles to overcome, such as aging, legacy applications and hardware that do not support necessary information security measures. These types of obstacles require multi-year planning initiatives and capital infusion that current funding levels inhibit.

Resource funding was a concern to CIOs, but to a lesser extent than anticipated by this review. CIOs were asked how resource funding correlates with adequate INFOSEC using a five point scale [1 (weakly correlated), 3 (correlated), and 5 (strongly correlated)]. The CIOs average response was 2.96, which seemed reasonable and certainly not extreme. This data seems consistent with practices cited by many interviewees of enhancing INFOSEC through low-cost or no-cost procedural and employee attitudinal changes. There was not a sense of dire resource constraints, but rather of barely adequate resources to match their perception of adequate INFOSEC capabilities.

CIOs cited the lack of employee awareness training and developing a culture of security with unusual frequency and intensity. This was the second highest rated strategy to improve and was deemed to be a low cost and high return INFOSEC investment. The lack of executive support was noted to a much lesser extent, with only one CIO identifying it as a top tier issue.

The CIOs repeatedly affirmed the need for INFOSEC training and expertise for their IT staff. The consensus is that a higher level of proficiency is required to move from a reactionary stance to a proactive posture in regards to INFOSEC. A casual conversation with a front-line IT person highlighted this issue. After the DOR breach, this agency, like all agencies, re-examined their INFOSEC with focused effort, which led to several potential improvements at minimal cost. The difference between pre and post DOR breach was the agency's priority to create a proactive posture, which then enhanced their INFOSEC posture. This reinforces the reality with the press of business and tight staffing, short term operational needs will always tend to draw IT attention at the expense of proactive INFOSEC. The remedy for this condition is for an enterprise to develop policies, processes, and staffing levels to create a proactive work space to develop and mature its INFOSEC expertise.

The IT departments of many state agencies have lost positions in recent years due to statewide budget cuts. By adding INFOSEC to the tasks assigned to an already busy application developer or database administrator, or by splitting INFOSEC duties among multiple staff, a comprehensive view of the agency's data security vulnerability and mitigation strategy can be blurred.

Even among agencies with the funding capacity for a dedicated Information Security Officers (ISO), hiring has been difficult. Two of the larger agencies have been attempting unsuccessfully to hire a full-time ISO for over a year due to the inability to provide a competitive salary. A state CIO from the east coast echoed the challenge of hiring qualified ISOs due to short supply and competitive salaries. That state had to create a separate pay structure for INFOSEC and IT personnel to attract qualified candidates. Creative solutions also emerged, such as two smaller agencies sharing a full-time ISO.

Part of the resource and technical skills discussion was the role of consultants in a new statewide INFOSEC program. Almost universally, the use of consultants was recommended for several reasons. First, they have unique subject matter expertise and experience in implementing enterprise wide INFOSEC programs, which the state lacks. Second, consultants add a level of needed objectivity, which is critical at a time when trust has been eroded. Consultants will be costly, but the state can't develop this government-wide initiative without their assistance. Many experts encouraged the use of technical advisory boards to assist the state in managing the consultant's plans and deliverables.

CIOs were in near full agreement that the risk of breaches can be controlled and reduced, but the risk can never be zero. At the same time, they were nearly unanimous that the statewide risk tolerance for another significant breach is near zero. This tends to reinforce the common theme, 'we have to do everything possible to protect out citizens' information.' The 18 CIOs were asked to rank their top three strategies to reduce INFOSEC risks, which were (frequency cited) as follows: statewide standards/governance (14); employee awareness training (7); agency risk assessments (4); INFOSEC expertise (4); audits (4); PII classification (3); resources (3); computer hardware (2); network monitoring (2); network architecture (1); hardening procedures (1); determine role of DSIT (1); penetration testing (1); physical protection (1); personal security (1); DOR debrief (1); and communications (1). Even though "resources" were itemized by only three CIOs, many of the other categories tend to require some level of additional resources to execute the strategy. The priority of strategies may vary based on each CIO's unique agency culture and experience, which further illustrates the need for the proposed federated governance model to allow flexibility to agencies to meet their operational needs and risk, yet still be accountable to a common statewide strategy, oversight, and review.

CIOs viewed their challenge to secure their data with INFOSEC pragmatically. There was a sense each was accomplishing basic INFOSEC, but there was uneasiness about risks they might be missing. Ideally, INFOSEC is a function of applying standards to operations, which then identifies risks to be addressed. In the real world of state government, resource limitations and demand for IT resources for operations may be subtly, or possibly not so subtly, driving INFOSEC decisions more than risk. But we know for sure, there are no standards against which to measure an agency, nor recurring processes for agencies to conduct systematic risks assessments. Under these conditions, it is difficult to see how all 100 agencies, universities, and commissions can accurately understand their respective risks, or how the state has any capability to meet its due diligence responsibility to understand and manage statewide risk.

B. <u>The Division of State Information Technology</u>

The DSIT viewed their role as an information technology service provider and not as a traditional state CIO with authority and oversight for state agencies' IT or INFOSEC. DSIT offers a federally funded INFOSEC network monitoring system to agencies, which, when fully developed, could play an integral role in a statewide INFOSEC program. The DSIT maintains an Internet site offering policy templates, as well as threat and vulnerability information which agencies can elect to access. DSIT also offers INFOSEC services, such as risk and vulnerability assessments, for a fee. Through all these activities, the DSIT staff develops many professional relationships with agency personnel providing lines of communication for informal advice. Even with this level of engagement, DSIT's statewide INFOSEC role is only ad hoc support to agencies who seek assistance, since agencies are responsible for their own individual INFOSEC programs and not subject to oversight.

Interview responses at DSIT were similar to CIO's perspectives. With DSIT's daily interaction with a wide variety of state agencies, it possesses a unique insight into assessing statewide INFOSEC. DSIT, as did CIOs, assesses statewide INFOSEC as less than adequate for similar reasons. DSIT also supports the need for a federated statewide INFOSEC model with statewide standard policies, tailored at the agency level, and subject to oversight and audit.

DSIT was fully conscious of agencies' skepticism and distrust toward DSIT owing to a history of friction, primarily related to the cost of services provided. Throughout this review, many see DSIT transitioning to a stronger customer orientation, but DSIT still suffers from a substantial trust deficit among state agency CIOs. Therefore, having DSIT "drive" any change initiative comes with some historical trust baggage.

C. Experts from Private Sector, Universities, and INFOSEC Research and Literature

The review interviewed experts from the National Association of State CIOs, Multi-State Information Sharing and Analysis Center, Gartner, Deloitte, CISCO, University of South Carolina, and Clemson; CIOs and officials from six other states, including three states with experience in significant data losses; and INFOSEC literature from a variety of sources to include, but not limited to, CERT-Carnegie Mellon, Sans Institute, and Information Security Audit and Control Association. The data was consistent with interview responses of state agency CIOs and DSIT. The direction for long-term success is to establish a statewide INFOSEC program with statewide standard policies.

Most states implementing statewide programs relied on assistance from expert consultants. The one exception identified did not use a consultant due to lack of funds, but would have if funds were available. Consultants with the experience implementing INFOSEC statewide have much to offer in terms of unique knowledge, skill, speed, and avoiding pitfalls, as well as the independence and objectivity needed following a significant breach where questions of confidence and trust linger. It was fully recognized such a change initiative will have consulting costs, but these can be mitigated through a hybrid approach by adding state employees to the project. This will build the state's capabilities, leverage existing personnel to reduce the consultant's footprint, and ultimately allow the state to mature internal IT staff to fully operate the resulting statewide program.

INFOSEC threats and vulnerabilities are increasing. Some measure worldwide hack attempts in the billions per year. The sheer volume of exploits creates risk, but the major concern is the increasing sophistication of hacking attacks as nation states conduct espionage; criminals realize how to exploit information; and groups leverage the Internet to promote political ends.

Comments illustrating these issues and other important advice were:

- According to a CIO who led a change from a decentralized environment to a statewide INFOSEC program: In today's environment of dramatically escalating risks from hackers, proportionally escalating vulnerabilities of agencies connected to one another, large amounts of data, web-based commerce, and an increase use of mobile devices, not having a central INFOSEC framework amounts to "abdicating responsibility."

- A state CIO reinforced his advice for the need for common statewide standards because most agencies are linked through networks, "it only takes one; once in, we are all exposed." Mobile device applications are not going away and create new levels of risk and vulnerability. We need statewide consistency to address this threat to our networks.

- All agencies are connected in some degree with each other through information sharing networks, so an agency with inadequate INFOSEC exposes all agencies in these networks. 'A state government is like a house with many windows, and each window represents an agency. It only takes one agency leaving the window open to expose all agencies to a threat.' A second expert provided an example of an Eastern European hacker who entered a city's network through its Transportation Department, and then, once "inside", escalated his privileges in the network in order to enter the Finance Department and steal $400,000 via an on-line bank account.

- An expert who led his state's efforts to move from a decentralized environment to a statewide INFOSEC program described the decentralized environment as "some good and not so good; there was no common security posture. The days of going it alone are over." The consequences for the entire enterprise are too great, the threats are too great, and the risks are too high.

- One expert reported, "as leaders in your organization, you are responsible for protecting the information in your care." This concept was reiterated by another expert who stated that leadership's due diligence is inhibited in a decentralized environment because they have no visibility on what is going on in the enterprise.

- A nationally recognized INFOSEC expert was asked to assess the INFOSEC risk in an entity, such as the state of South Carolina, with over a hundred agencies, universities, and commissions developing their own INFOSEC programs without any central governance policy, standards, or expectations? The response was pessimistic.

- An expert commented, "you must assume someone is in your system" when developing your INFOSEC plan. Continuous monitoring of networks was deemed critical by repeated experts to address the reality that hackers will penetrate our systems. At a state level, seeing across the enterprise with a common set of eyes reduces INFOSEC risks by seeing threat patterns, something that is nearly impossible for individual agencies operating in their own monitoring silos. This risk was highlighted by DSIT, which frequently identifies computers on agencies' networks under a hacker's control after the initial installation of its network monitoring equipment.

- An experienced CIO who has built several enterprise-wide INFOSEC programs advised that such efforts should focus on building relationships, communities, and education among agency directors, IT components, and users to promote a “culture” of information security. INFOSEC education should be a centralized function due to its critical role in program success. A state CIO who suffered a major data loss emphasized the relationship approach in building an INFOSEC community to raise capabilities and reduce risk, rather than an authoritarian approach, to gain state agency compliance. Having the authority is important, but CISO leadership skills to connect to state agencies to gain their interest, commitment, and build a community among agencies are vital to success.

- A state, with a highly decentralized INFOSEC, initiated its statewide efforts by empowering a Cabinet level CIO to exercise authority over statewide INFOSEC. The initial cost was not technology, but primarily hiring staff with INFOSEC expertise, which required new authority to hire above state pay scales to compete with the private sector for this needed skill set. Another expert weighed in on this topic stating that an enterprise-wide implementation is “90% management (staffing, roles & responsibilities, policy, procedures, audit, and training) and 10% technical.” A third expert agreed that resources will be required more for establishing policy and procedures through staff enhancements and training, rather than procurement of hardware and technology.

Several national Cyber security firms provided overviews of a typical process to implement a statewide INFOSEC plan. The process begins with establishing a governance model with standards, as well as gaining a high level situational awareness of statewide agencies to develop a priority order for action plans. One firm slightly emphasized performing a risk based assessment cutting across all state agencies to develop short-term tactical plans to impact all agencies, while developing a longer term strategy. The other slightly emphasized prioritizing agencies, then conducting full risk assessments by agency while helping lower priority agencies self-develop through education, training, and tools. Their processes may vary a bit, but the philosophy was the same—conduct risk assessments to identify gaps and weakness; develop mitigation plans with resource requirements and time frames; and execute plans to mature agencies’ INFOSEC postures and capabilities to be self-sustaining over the long-term. This allows the state to monitor individual agencies to understand its INFOSEC risk posture, and manage it to continually lower levels of statewide risk assuring everything possible is done to protect citizens’ information.

The experts were consistent in their advice to avoid the temptation of a single solution or short term reactionary fix. INFOSEC must be an enterprise-wide process led by executive management because its success or failure affects the entire organization. A significant loss of data can disrupt the effectiveness of an entire organization or government, both monetarily and, more importantly, the intangible loss of citizens' trust and confidence. Executive management can no longer delegate INFOSEC responsibility or allow it to be fragmented in various operations throughout an enterprise.

IV. A Way Forward

A. Leadership Through Governance

Given the state's risk tolerance for absorbing another significant data loss, the current INFOSEC risk level, assessed at less than adequate, is not acceptable. Further, regardless of the assessment of statewide risk, the current decentralized INFOSEC environment provides no visibility of risks in agencies, which is incompatible with state government's due diligence responsibility to do everything possible to protect citizens' information. The first step in a statewide INFOSEC program is to establish a governance model. This model provides a sustainable statewide platform for leadership, structure, processes, and assurance that INFOSEC risk, policy, and resource needs are addressed at the state level. According to one expert, "the governance structure is the defining activity that serves as the foundation and sustains all others (activities)."

Governance starts with leadership. A Chief Information Security Officer (CISO) position should be established to take ownership to lead a statewide INFOSEC program. There is no one model of how to locate the CISO within a state. Currently, the vast majority of CISOs in other states report to their CIO. The rationale behind placing the CISO outside of the CIO office is a basic organizational segregation of duties practice; the individual implementing security (CIO) can't be the same as the person responsible for testing security, conducting audit, and reporting on security weaknesses. Two factors in South Carolina impact this decision. First, the South Carolina state CIO leads DSIT. The agency CIO community has a long history of friction and trust issues with DSIT. Second, given the post-DOR world where state government is fully committed to doing everything possible to protect citizens' information, making the CISO independent of the CIO provides a higher level of objectivity and independence which may be beneficial at this time. Regardless of the CISO's location in the organizational chart, the CISO will need relationships with statewide governance executives to fully incorporate INFOSEC governance into the fabric of statewide governance.

The INFOSEC governance framework is simply the structure, strategies, policies, and practices put in place at the state level to provide support and ensure INFOSEC expectations and controls are adequately communicated to all agencies in state government, implemented, and enforced. It allows the executives responsible for state government to have visibility into agencies INFOSEC, and assurance the state, collectively, is doing everything possible to protect our citizens' information. The benefits of this approach include:

- A foundation for effective organization-wide risk management;
- Business needs are balanced against information security requirements to find that cost/effective tipping point to maximize the value of information security resources;
- Assurance of effective information security policy and execution;
- Protection from the increasing potential for civil or legal liability as a result of data loss, particularly if there is an absence of due care;
- A framework to optimize the allocation of limited security resources;
- Increased predictability and reduced uncertainty of business operations; and
- Improving trust in citizen relationships and protecting the state's reputation.

A legal review determined legislation would be required to establish a CISO with the authority to require agencies to comply with statewide INFOSEC standards and policies, as well as defining its role in the various branches of state government. In the near term, regardless of title, the state needs to designate a leader on an interim basis to take the lead on statewide INFOSEC issues while legislative alternatives are weighed. This leader's responsibility will include facilitating legislative proposals, preparation and planning for retaining a consultant with necessary expertise, engaging agency CIOs and ISOs, and additional short-term tactical INFOSEC initiatives as deemed appropriate.

Essential to the process and the success of this interim leader is the simultaneous creation of a steering committee of executives, such as human resources, finance, agency CIOs, and experts from the university community and private sector. The state has tremendous talent wanting to contribute; a steering committee mechanism at the highest level of government facilitates opening the communication pipes for input and relationship building. This steering committee may be modified as the governance model develops, but the right people need to be at the table at the same time to expedite decisions, in a timely manner, to address this crisis.

During the course of the review, the broader issue of overall statewide Information Technology governance was raised. This issue is one of the top issues under discussion by State CIOs across the country. However, statewide Information Technology governance was not within the scope of this review.

B. Federated Model

A key governance component issue among state CIOs is the desirable level of centralized INFOSEC authority. Without question, the current highly decentralized model needs to be eliminated. South Carolina needs a traditional federated model with central responsibility for the statewide INFOSEC program and authority to establish a statewide umbrella framework and policies, and then delegate authority, in most areas, to agencies to tailor statewide policy to fit their operational environment subject to oversight and audit. This general approach was near overwhelmingly endorsed by CIOs, DSIT personnel, and experts. Moving even farther along the centralization spectrum was recommended by a few CIOs. Successful implementation of any statewide INFOSEC program requires the full commitment of CIOs, so consideration of moving along the authority spectrum beyond the federated model to a more drastic change environment of centralization is not considered wise. Such a development remains an option as the INFOSEC program matures and evolves.

C. Programmatic Approach

Despite the complexity of INFOSEC, the statewide solution is fundamental program management. There has been some expectation this review would develop a laundry list of policies, procedures, and technology to improve INFOSEC. Before a solution can be designed, the problem needs to be understood. The first step in understanding the problem is developing statewide standards so we know what success looks like. Then, standards can be applied to individual agency operations through the risk assessment process, which will expose gaps or weaknesses. Only after looking at an agency's weaknesses in a holistic manner, can the optimum cost/effective mitigation plan be developed, along with resource requirements and timelines. Even with a mitigation plan, the plan is only unique to each individual agency because agencies have different types of operations leading to different risk issues and corresponding mitigation plans.

After all this front end planning effort through risk assessments and mitigation plans are completed, statewide governance provides technical and resource support to agencies on an ongoing basis, as well as coordinates periodic audits. These audit results provide feedback for both individual agency actions and statewide reassessment of policies and practices. The cycle repeats continually, resulting in improved INFOSEC maturity and capabilities over the long-term. Statewide INFOSEC is a process, and not a single solution.

Initially, it will not be easy to coordinate this new programmatic approach. It will take more resources in terms of staffing, expertise, technology, and hardware. However, there are two worthy goals to keep in mind during this urgent effort. First, a world class INFOSEC program creates the enabling platform to leverage technology to dramatically increase the state's service delivery at much lower cost. Second, and most important by far, regain some of the lost trust from our citizens by doing everything possible to protect their information entrusted to the state.

V. Findings & Recommendations

Finding # 1: The state does not have a statewide INFOSEC program, which undermines an effective statewide security posture, as well as creating unmanaged and uncontrolled statewide INFOSEC risks having potential impact on the entire state government.

Recommendation #1a: Establish a statewide INFOSEC program.

Recommendation #1b: Establish a federated governance model.

Finding #2: The state has not fixed responsibility, accountability, and authority for statewide INFOSEC.

Recommendation #2a: Establish a Chief Information Security Officer (CISO) position outside of DSIT to lead the development and implementation of a statewide INFOSEC program.

Recommendation #2b: Immediately, on an interim basis, designate a leader to take responsibility for proactively driving statewide INFOSEC issues while legislative alternatives pertaining to the statewide CISO position are weighed.

Recommendation #2c: Establish a Steering Committee to expedite and provide oversight of the development of a statewide INFOSEC program.

Finding #3: A consultant, with expertise in developing and implementing a statewide INFOSEC programs, will be required to assist in establishing a statewide INFOSEC governance framework and develop statewide INFOSEC implementation options.

Recommendation #3: Identify and procure the use of a consultant to assist building the governance framework and developing statewide INFOSEC implementation options.

VI. Next Phase of Review

If approved, a CISO, a federated model, and the use of a consultant with expertise in implementing INFOSEC statewide programs should construct a governance framework in a highly collaborative manner with state executive leadership and agency representation. The next interim report will focus on implementation options and recommendations, in terms of cost and schedule, to develop a long term sustainable statewide INFOSEC program to reduce agency and statewide risk.