



# California Information Security Strategic Plan

October

# 2009

---

Cybersecurity and Privacy Concepts, Strategies & Goals  
Volume 4

Arnold Schwarzenegger  
Governor

Teri Takai  
Chief Information Officer, Office of the CIO

Mark Weatherford  
Chief Information Security Officer, Office of Information Security

# California Office of the State Chief Information Officer

Teri Takai  
Chief Information Officer

California is the home of innovation. As our residents and businesses are inventing a new and exciting future, California state government must be part of that transformation. Building a dynamic and value-driven statewide Information Technology (IT) program necessitates providing enterprise-wide leadership in the areas of information security, risk management, and protection of critical infrastructure. I am proud to say that the Office of Information Security (OIS) provides that leadership in this, the California Information Security Strategic Plan.

In 2009, the Governor's Reorganization Plan integrated the Office of Information Security (OIS) into the Office of the State CIO (OCIO). As part of the OCIO, the OIS has an enterprise-wide responsibility to lead the charge to protect California's technology assets and its citizens' personally identifiable information against the rising number of cybersecurity threats.

The strategies set forth in this plan are fundamental to the realization of California's ambitious vision of how information technology will be used in the future. They provide the strategic framework for the protection of state technology assets, and they will engender trust from citizens looking to interact with their government online.

California strives to become a leader in online, citizen-centric and transparent government. All of us, from California's executive leadership to every state employee, citizen, business, and state government partner, play a role in securing our state's systems and protecting the personally identifiable information entrusted to us daily.

I endorse this plan. I encourage everyone to read it and embrace California's Information Security Strategic Plan.

Sincerely,



Teri Takai

# Table of Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>SECURITY AND PRIVACY IN CALIFORNIA STATE GOVERNMENT .....</b>	<b>7</b>
<b>SECURING CALIFORNIA IN CYBERSPACE .....</b>	<b>9</b>
<b>Security Strategic Concept #1 — A Digital Infrastructure That Is Resilient, Secure, and Trustworthy .....</b>	<b>10</b>
<b>Security Strategic Concept #2 – Making Internet Use a Safer Experience for Californians .....</b>	<b>15</b>
<b>Security Strategic Concept #3 – A Secure, Trustworthy Digital Identity for Every California Citizen .....</b>	<b>19</b>
<b>Security Strategic Concept #4 – Security as an Enabler of More Efficient Technology .....</b>	<b>22</b>
<b>Security Strategic Concept #5 – Effective Security That Enhances Collaboration and Delivery of Services.....</b>	<b>26</b>
<b>ALIGNMENT OF SECURITY STRATEGIC CONCEPTS TO THE OCIO IT STRATEGIC PLAN .....</b>	<b>29</b>
<b>FROM GOALS TO ACTIONS .....</b>	<b>30</b>
<b>APPENDIX A – FOOTNOTES.....</b>	<b>31</b>

# California Office of Information Security

Mark Weatherford  
Chief Information Security Officer

We are witnessing an extraordinary time in California state government. Extraordinary because of our incredible economic challenges, extraordinary because of the rapid rate of technological innovation, and extraordinary because of the opportunities these challenges present. Facing these extraordinary circumstances requires bold action.

As outlined in the 2009 IT Strategic Plan, our State CIO is committed to driving California state government's information technology into the 21st century. Security and privacy are critical components of the IT Strategic Plan, and the move to an advanced online, citizen-centric California government requires an equally strong vision for addressing the growing cyber-threat landscape.

Gartner, a leading IT research company, calls the likely future state of information security "a Perpetual Arms Race, between hackers and criminals on one side and enterprises and governments on the other side." Every day, news articles and commentary confirm this. I believe we are at a point where state government can achieve great technical efficiencies not only by being better, faster, and cheaper, but also by being more secure.

I welcome and seek your ideas, but do not bring me small ideas; bring me big ideas to match our future.

Governor Arnold Schwarzenegger

In his 1961 speech committing the nation to putting a man on the moon before the end of the decade, President John F. Kennedy said, "If we are to go only half way, or reduce our sights in the face of difficulty, in my judgment it would be better not to go at all." I agree with President Kennedy's statement; it's all or nothing. Like going to the moon, our information security situation is complex and requires total commitment. However, our information security situation is far different in one very important respect: going to the moon was a choice. California state government must deal with cyber threats. We don't have a choice.

This Information Security Strategic Plan presents a comprehensive five-year vision to improve the security and privacy posture of California government. Many people, from state agencies and private sector partners, have contributed to the Plan, and the Office of Information Security is committed to this vision. It is my hope that others will embrace it as well and join us in working to make California a national leader in securing state and citizen information and protecting our critical infrastructure. Our state and our constituents depend on it.

Sincerely,



Mark Weatherford

# California Security Strategic Plan

## Executive Summary

We live in a technological age. In our daily lives, we access countless interconnected systems that allow us to procure services, purchase goods, and communicate with people and institutions around the world. We rely on, and even *demand*, technology to work for us smoothly, reliably, and securely to perform complex tasks that significantly enhance our standard of living.

Two years ago, analysts predicted that the number of personal computers in the world was set to break 1 billion, with that number growing exponentially to 2 billion by the year 2015.<sup>i</sup> Today, the list of proposed projects under California’s Information Technology (IT) Capital Plan, adding up to an investment of approximately \$466 million, represents California government’s technology requirements to simply *keep up* with the service expectations of Californians in an increasingly digital, citizen-oriented, and online government world.<sup>ii</sup>

In early 2009, the Office of the Chief Information Officer (OCIO) released California’s IT Strategic Plan, outlining the Six Strategic Concepts to guide the modernization of California’s aging IT infrastructure and provide better services to California citizens, businesses, and government employees in the 21st century. With a parallel vision to create new efficiencies in the organization of IT within the state, the 2009 Governor’s Reorganization Plan (GRP) began the consolidation of IT functions, including the OIS, within the OCIO. This GRP laid the organizational foundation that allows California to drive forward in achieving our IT goals within a collaborative and economically sustainable federated IT governance framework.

### OCIO 2009 Information Technology Strategic Plan

#### Six Strategic Concepts

- IT as reliable as electricity
- Fulfilling technology’s potential to transform lives
- Self-governance in the digital age
- Information as an asset
- Economic and sustainable
- Facilitating collaboration that breeds better solutions

“It’s easier to secure [information technology] when you concentrate things than when you distribute them across the government.”

Vivek Kundra  
U.S. Federal Government CIO

The OIS also began a structured discovery and strategic planning process to understand and assess the security and privacy “health” of the state and the enterprise-wide role that the OIS should play in mitigating security and privacy risks. The objective was to create the strategies and goals that fundamentally enhance California government’s ability to deliver efficient, reliable, and secure services in an economically sustainable manner. Using the above factors as inputs at the macro level, the

OIS has formulated Five Security Strategic Concepts, which align with the OCIO's Six Strategic Concepts, to guide enterprise security and privacy initiatives. These Five Security Strategic Concepts are:

- **A DIGITAL INFRASTRUCTURE THAT IS RESILIENT, SECURE, AND TRUSTWORTHY** – OIS will collaborate with state agencies, the private sector, and the federal government to implement state-of-the-art enterprise information security technologies to combat risks to the availability, integrity, and trustworthiness of California's digital infrastructure, including critical infrastructures. Strengthening the resilience of our digital infrastructure will require innovation and a holistic enterprise information security approach to address cyber risks in the state.
- **MAKING INTERNET USE A SAFER EXPERIENCE FOR CALIFORNIANS** – "Information-centric" security and privacy solutions become an even greater imperative as government grows online and services become more accessible via entry points such as the Internet, cell phones, wireless handheld devices, and other technologies yet to be invented.
- **A SECURE, TRUSTWORTHY DIGITAL IDENTITY FOR EVERY CALIFORNIA CITIZEN** – Information security and privacy are game-changers in establishing convenient, yet secure, centrally accessible, online government services. The OIS will promote robust security and privacy protecting policies, standards, and technical solutions that enable citizens to interact with government through a secure, "One California," online identity.
- **SECURITY AS AN ENABLER OF MORE EFFICIENT TECHNOLOGY** – Technology innovation should be an *enabler* to the adoption and use of new technologies in state government. The OIS will collaborate with the OCIO and agencies to engage early in the development process to support state government in aggressively pursuing, vetting, and adopting new technologies that help meet California's goals, economically and securely.
- **EFFECTIVE SECURITY THAT ENHANCES COLLABORATION AND DELIVERY OF SERVICES** – The OIS will provide the leadership to improve *secure and seamless* collaboration and enhance transparency between California's internal and external stakeholders. By creating an "end-to-end" computing ecosystem based on robust security processes and a security-aware culture, the OIS furthers the objective of a transparent and trusted environment for collaboration.

These Five Security Strategic Concepts are the drivers that will propel California's enterprise security and privacy initiatives over the next five years. These five concepts give some responsibility to everyone: every member of the Legislature, every member of every Constitutional office, every member of the Judicial branch, and every member of the Executive branch of state government. Our individual and collective compliance with these Five Security Strategic Concepts is necessary to protect the security of our IT assets and privacy of California citizens and to secure our critical infrastructures.

"The country needs and, unless I mistake its temper, the country demands bold, persistent experimentation. It is common sense to take a method and try it. If it fails, admit it frankly and try another. But above all, try something."

Franklin D. Roosevelt, 1932

This Information Security Strategic Plan is fundamentally about the future — we cannot continue to do "business as usual" with the growing threats to our critical digital infrastructure. This plan provides the road map for us to proactively address the economic, technical, and even social challenges that will establish California's leadership in cyberspace.

# Security and Privacy in California State Government

California state government is a complex organizational landscape composed of more than 130 agencies, departments, boards, and commissions with more than 220,000 employees. California owns and operates hundreds of thousands of electronic devices that support, control, or connect the critical digital infrastructure of state government. These devices, ranging from telecommunications and networking equipment; to mainframe and Web-based computer systems; to desktops, laptops, and various mobile devices, vary significantly in their built-in security mechanisms and ability to protect critical government and citizen data from intentional and unintentional misuse.

Add to this disjointed technology environment a growing variety, sophistication, and escalation of cybersecurity threats, and it becomes obvious that a more centralized enterprise approach is essential to securing our state IT environment. California, similar to other government and private sector organizations across the country, has seen an increase in the scale and frequency of security attacks and threats in recent years. In fact, a 2008 global security report made available through the Multi-State Information Sharing and Analysis Center (MS-ISAC) reported that attackers were increasingly part of well-organized and funded underground groups, generating millions of dollars in the underground economy, “where tools specifically developed to facilitate fraud and theft are freely bought and sold.”<sup>iii</sup>

“Threats to cyberspace pose one of the most serious economic and national security challenges of the 21<sup>st</sup> century for the United States and our Allies. A growing array of state and non-state actors such as terrorists and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government.”

Obama Administration’s Cyberspace Policy Review, May 2009

On a daily basis, each state organization and every state employee with access to a computer has the potential to set in motion a series of events that either contribute positively to government’s information security posture or create new vulnerabilities with devastating consequences. Because California citizens and businesses rely on state government to deliver services that help support and protect their health, safety, and economic well-being, both the OCIO and the OIS play a critical role in ensuring the state’s infrastructure is capable of delivering these vital services in a secure, reliable, and trustworthy manner. The challenges identified above provide compelling rationale for why we must not be complacent in addressing the issues that would prevent state government from serving the public.

A critical component of the process in developing this Information Security Strategic Plan was performing an inward review of our own operations and assessing how they have contributed to improving security and privacy in the state. The OIS conducted one-on-one interviews and

workshops with more than 200 security, privacy, and risk management professionals; business and IT leaders; and other stakeholders from different agencies to realize an unbiased perception of the value the OIS provides to the state.

The results from these workshops and visioning sessions clearly identified two conclusions: (1) common challenges and needs exist across the different state agencies that cannot be easily or cost-efficiently solved within any individual government agency or organization, and (2) the current decentralized approach to security and privacy places agencies in a reactive mode and hinders government's ability to understand and address significant and critical cyber threats at the enterprise level.

The OIS looked at, as additional inputs into the discovery and strategic planning process, recent industry research; the experiences of private organizations, other states, and the federal government as well as other nations; and socioeconomic factors that are shaping state government's future iterations. These macro-level inputs were factored into the process to create the strategic security and privacy guiding principles for California online government in the 21st century.

### **Security Is No Longer an Option**

- “The management focus on network performance and availability has bred an IT culture that views security as a second-class network requirement rather than a core pillar. This afterthought mentality is directly responsible for the serious lack of security advocacy within most government organizations
- This view of security can no longer exist if we are to move toward a stronger security posture for public-sector organizations. Business executives must understand that proper protection of citizens' information is a requirement and not a luxury in today's cyber-centric world
- Proper attention can prevent a large portion of security breaches, which not only prevents damaging citizens' trust in government but also removes added pressure to IT management operations. Adopting a proactive security stance can avoid a costly, time-intensive cleanup that would take management away from everyday responsibilities for days or potentially weeks. Ultimately, proper security can directly benefit IT managers and allow them to focus on the real challenge of making government more accessible.”<sup>iv</sup>

Excerpts from [www.Govtech.com](http://www.Govtech.com), *IT Security: the Least Understood Management Function in Government?* Mark Rutledge, former CIO of Kentucky

# Securing California in Cyberspace

## Security Strategic Concepts

The Information Security Strategic Plan for securing California in cyberspace focuses on enterprise initiatives that will improve security and privacy, strengthen public confidence in state systems, and provide California agencies with the resources to make sweeping improvements in information security and privacy practices, governance, and protection.

As a component of the overall planning effort, the OIS analyzed input derived from multiple sources, including its internal organizational assessment, the examination of state agency needs, recommendations of stakeholders, industry research, socio-economic factors, and inputs from the federal landscape.

The results of this analysis have been distilled into five key security strategic concepts that will guide OIS as it executes its short- and long-term goals. The Five Security Strategic Concepts are:

- A DIGITAL INFRASTRUCTURE THAT IS RESILIENT, SECURE, AND TRUSTWORTHY
- MAKING INTERNET USE A SAFER EXPERIENCE FOR CALIFORNIANS
- A SECURE, TRUSTWORTHY DIGITAL IDENTITY FOR EVERY CALIFORNIA CITIZEN
- SECURITY AS AN ENABLER OF MORE EFFICIENT TECHNOLOGY
- EFFECTIVE SECURITY THAT ENHANCES COLLABORATION AND DELIVERY OF SERVICES

The following section outlines each of the Five Security Strategic Concepts within a framework of strategies and goals. These are intended to guide California's security and privacy initiatives over the next five years, at the enterprise and agency level, and to provide a strategic, flexible framework that can adapt to each agency's unique situation.

Strategic concepts are, by nature, aspirational. In some cases, the technology, processes, and organizational structure to achieve the strategic concepts do not exist today — but almost certainly will exist in the near future. Hence, these Five Security Strategic Concepts are intentionally designed to plan for future technological advances and to incorporate strategic and forward-looking vision into California state government's daily decision-making. By acting today, we will be better prepared to reap the benefits of future societal, economic, and technological changes.

### **Achieving the Vision: Leadership's Role**

California's leaders play a significant role in the achievement of the strategies and goals within this Information Security Strategic Plan. This includes business and IT leaders, the Legislature, Cabinet secretaries, Department Heads, Agency Information Officers (AIOs), Chief Information Officers (CIOs), and ISOs. Leadership's actions set the security tone and example for every state employee.

# SECURITY STRATEGIC CONCEPT #1 — A DIGITAL INFRASTRUCTURE THAT IS RESILIENT, SECURE, AND TRUSTWORTHY

The purpose of Security Strategic Concept #1 is to develop and implement state-of-the-art enterprise information security technologies to manage, combat, and deter current and future cybersecurity risks to California state government's enterprise IT infrastructure, including critical infrastructures, and the information used, processed, and stored within.

The 2008 Center for Strategic and International Studies (CSIS) report, *Securing Cyberspace for the 44th Presidency*, noted that the "Cyber attack is a new kind of threat to the safety and well-being of the United States."<sup>iv</sup> The report highlighted that cyber attacks were taking ever-changing shapes and forms and had the potential to cause increasing amounts of damage to the nation's security and economy.

Examples of recent cyber attacks include the following:<sup>v</sup>

- Law enforcement computers were struck by a mystery computer virus in May 2009, forcing the FBI and the U.S. Marshals to shut down part of their networks as a precaution.
- Spies have hacked into the electric grid of the United States and left behind malicious computer programs, allowing them to disrupt service at will, according to a former government official in April 2009 and as reported in *The Wall Street Journal*.
- America's air traffic control systems are vulnerable to cyber attacks, and support systems have been breached, allowing hackers access to personnel records and network servers according to an audit released in May 2009 by the U.S. Department of Transportation Inspector General.
- The 2008 military conflict between Russia and Georgia was preceded by a coordinated cyber attack that defaced numerous Georgian government Web sites and disrupted government communications. The attack, called the "birth of modern cyber warfare," demonstrated the potential weaknesses in Internet Infrastructure.

## Securing California's Electric Grid

California's electrical grid is an intricate network of high-voltage power lines that stretch more than 25,000-circuit miles. The California Independent System Operator (ISO) control room, one of the largest in the world, directs the delivery of more than 200 billion kilowatt-hours of power annually to 30 million Californians. The California ISO acts as a clearinghouse for nearly 30,000 market transactions every day and is the gatekeeper to power lines connecting California to neighboring states as well as to Canada and Mexico.

Even closer to home are cyber attacks that have recently occurred in California. Examples include the following:

- A six-month hacking effort at the University of California, Berkeley, resulted in 97,000 stolen Social Security Numbers. Hackers infiltrated restricted computer databases from October 2008 to April 2009, putting the health records and other personal information of 160,000 students, alumni, and others at risk.<sup>vi</sup>

- In May 2008, during routine monitoring of a campus computer network, the University of California, San Francisco (UCSF), discovered unusual data traffic on one of its computers. UCSF determined that an unauthorized movie-sharing program had been installed on the computer by an unknown individual. The computer contained files with lists of patients from the UCSF Pathology Department's database. While it is unclear whether patient files were compromised, installation of this program required high levels of system access, which led UCSF to consider the incident a dangerous security breach.<sup>vii</sup>
- In April 2009, vandals intentionally cut underground fiber optic cables causing Internet and telephone outages to thousands of San Francisco Bay area residents and businesses, including 9-1-1 and mobile phone service. The outage affected customers of most major telecom service providers.<sup>viii</sup>

On May 29, 2009, the White House published the results of a 60-day cybersecurity review of the federal government. The Preface declared, "Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests."<sup>ix</sup>

"It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation... We're not as prepared as we should be, as a government or as a country."

President Obama, May 29, 2009, on introducing the *Cyberspace Policy Review*

At all levels of government, there is a common recognition that cyberspace is woven inextricably into the fabric of our economy and society and must be protected. Cyber attacks pose very real threats, for which government must be prepared to protect "those physical and cyber-based systems essential to the minimum operations of the economy and government."<sup>x</sup>

The OIS will take a leadership role in developing strategies and guiding the implementation of enterprise solutions that mitigate not only against cyber threats, but also against the natural and man-made risks to our IT environment and critical infrastructures. The success of California state government depends on the ability of both citizens and government to leverage cyberspace as a reliable and secure platform to conduct business.

A state-of-the-art California Information Security Operations Center (CA-ISOC) will provide real-time analysis of cyber attacks and other security intrusions across all state agencies. The CA-ISOC will provide an early warning system that would significantly increase the probability of detecting a coordinated cyber attack against California's digital infrastructure, use tools to isolate the attack, and prevent multiple agencies from suffering potential system failures.

**STRATEGY 1** – Build advanced security processes and technologies into California's critical networks for better cyber and information security attack identification, analysis, and response in a coordinated and efficient manner across agencies.

**GOAL 1A** – Establish and operationalize the California Information Security Operations Center (CA-ISOC). The CA-ISOC will provide leading class security operations to detect,

prevent, and respond to agency and enterprise-level cyber attacks that could disrupt state government's critical digital infrastructure.

**GOAL 1B** – Evolve the CA-ISOC into a world-class security operations facility that includes monitoring of state government Supervisory Control and Data Acquisition (SCADA) networks and control systems as well as other critical infrastructures across the state. The CA-ISOC will provide support for local government networks that require assistance as well as promote data sharing and collaboration between public (i.e., federal, state, local) and private asset owners and regulators.

**GOAL 1C** – Develop and operationalize an enterprise California Computer Incident Response Team (CA-CIRT) capability that encompasses the state's digital infrastructure and integrates with the CA-ISOC, California Emergency Management Agency (CalEMA), State Fusion Center, U.S. Department of Homeland Security, and U.S. Computer Emergency Readiness Team (US-CERT).

**GOAL 1D** – Validate that the CA-ISOC is world-class by adopting the National Institute of Standards and Technology (NIST) 800-37<sup>xi</sup> guidelines for certification and accreditation of information systems. Applying NIST guidelines to state government systems will demonstrate California's leadership in building a resilient, secure, and trustworthy digital infrastructure.

**STRATEGY 2** – Strengthen collaboration and information sharing across local, state, and federal government to improve interagency coordination.

**GOAL 2A** – Establish formal relationships with the California Office of Emergency Management (CalEMA) Critical Infrastructure Directorate, State Fusion Center, U.S. Department of Homeland Security National Cybersecurity Division (DHS/NCSD), and the White House's cybersecurity policy official to facilitate information and resource sharing between California and the federal government related to cyber attacks, cyber activity trends, and cyber research and development (R&D).

**GOAL 2B** – Establish the California Information Sharing and Analysis Center (CA-ISAC) as a Web portal to provide a central resource for gathering information on cyber threats to the state's IT environment and critical infrastructures. The CA-ISAC will also serve as a means for sharing of information between state government and local governments and institutions of higher education through the guiding principles of coordination, collaboration, and cooperation.

The CA-ISAC will provide the following benefits to state and local governments and higher educational organizations:

- Direct access to cybersecurity threat information from the California Office of Information Security (OIS) and the State Fusion Center
- Access to security awareness materials, including computer-based training modules

- Access to information security policy templates
- Access to information security products and services at enterprise price points
- Periodic meetings, teleconferences, and webcasts to promote peer networking and information sharing
- Secure communications via secure messaging

**GOAL 2C** – Establish enterprise security and privacy policies, standards, and guidelines that support an agile, adaptable, and resilient digital infrastructure.

**GOAL 2D** – Expand participation in U.S. Department of Homeland Security National Cybersecurity Division (DHS/NCSD) cybersecurity planning and exercises.

**GOAL 2E** – Increase statewide planning, testing, and coordination activities for cybersecurity, continuity of government (COG), and disaster recovery (DR) readiness.

**STRATEGY 3** – Establish an enterprise governance structure for privacy within California state government agencies.

**GOAL 3A** – Create an enterprise Chief Privacy Officer (CPO) role within California state government to develop appropriate government policies and risk management strategies that will:

- Ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information
- Ensure that personal information is collected and handled in full compliance with fair information practices as set out in California Civil Code (civ: 1798-1798.78) Information Practices Act of 1977
- Evaluate state legislative and regulatory proposals involving collection, use, and disclosure of personal information by state government

**STRATEGY 4** – Provide state agencies with access to security and privacy solutions that strengthen and fortify the state’s digital infrastructure.

**GOAL 4A** – Establish standards and qualification criteria for state agency Information Security Officers (ISOs). Develop training programs to enable prospective and designated ISOs to achieve the necessary skills to consistently support agency and enterprise information security goals.

**GOAL 4B** – Develop and deploy specialized security and privacy training and certification courses for IT program managers, systems architects, developers, and other stakeholders involved in significant IT capital new acquisitions or upgrades.

**GOAL 4c** – Develop and deploy a Managed Security Services (MSS) program within the CA-ISOC to provide specialized information security services to state agencies. On a prioritized basis, services may include the following:

- State policy, standards, and procedures consultation
- Security event correlation and monitoring services
- Web application, internal network, external network, and wireless network vulnerability assessments
- Perimeter security services, such as firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) administration and monitoring

**BOTTOM LINE** – Achieving these goals will significantly increase California’s ability to protect its digital infrastructure, including critical infrastructures, against cybersecurity attacks. Ultimately, achieving these goals allows state government to provide its citizens, business partners, and federal, state, and local government partners with the confidence to conduct business online in a secure, trustworthy, and resilient manner.

## SECURITY STRATEGIC CONCEPT #2 – MAKING INTERNET USE A SAFER EXPERIENCE FOR CALIFORNIANS

The purpose of Security Strategic Concept #2 is to implement enterprise information-centric security solutions for the state whereby the security is always with the asset (i.e., information) regardless of where the information resides within the state's IT infrastructure.

Information is the lifeblood of any organization and even more so for government. Achieving California's enterprise vision of open and transparent government requires a transformative strategy to deal with the state's information. The OIS will play an enterprise role in shaping the future strategies that protect and validate the state's information while also allowing for its open and transparent use.

In the physical world, important assets are protected by means, such as safes, locks, and vaults. The more valuable the asset, the more protection is required. In the digital world, information is also an asset of increasingly significant value that must be protected. Information is important to the ability of our economy to function, as well as to the functioning of our society and to the building of assurance and partnerships between government, private enterprise, and citizens through the secure, trusted exchange of sensitive information.

The National Association of State Chief Information Officers (NASCIO) recently published a study identifying numerous risks to states' data, some of which include the following:

- Information is at the heart of how government conducts business and serves citizens. As information increasingly becomes available in electronic form or is "born digital," state government, as an enterprise, must find ways to ensure that the information's confidentiality, availability, and integrity is not compromised.
- Data is frequently understood to be "owned" by individual business units rather than the agency and the larger enterprise. As a result, information and application systems are "stove piped," with varying degrees of collaborative information sharing or protection of the information assets.

### The Digital Universe Is Still Growing

"In a time when so many things seem to be shrinking in response to the global economic crisis, the digital universe continues its skyrocketing growth. People continue to take pictures, send e-mail, blog, and post videos. Companies are still adding to their data warehouses. Governments are still requiring more information be kept. In fact, the creation of new digital information in 2008 actually exceeded IDC predictions by three percent. The digital universe is expected to continue to grow by a factor of almost five in the next four years."

IDC Multimedia whitepaper sponsored by EMC<sup>2</sup>, *As the Economy Contracts, the Digital Universe Expands*, May 2009

- It is well documented that lost or stolen mobile devices account for a significant number of data breaches. Laptops, personal digital assistants (PDAs), thumb drives, etc., are not being properly protected.
- The sheer expansion, volume, and proliferation of data have almost made it impossible to maintain a meaningful inventory of information, its criticality, where it resides, and how to protect it.<sup>xii</sup>

Balancing the public’s expectations for accountability and transparency with the state’s need to protect sensitive information and adhere to privacy regulations is a difficult task that must be directed from the top levels of state government. The OIS will play a leadership role in developing enterprise information security programs that focus on information-centric security, securing the information itself, and having the security follow the information anywhere, anytime, and in any form. Instituting strong privacy practices and privacy-enhancing technologies is essential to meeting the state’s and the public’s goals.

### Protecting Health Information – Medical Identity Theft

“Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity — such as insurance information — without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses.”

World Privacy Forum, *The Medical Identity Theft Page*

Information is everywhere within California’s digital infrastructure and is growing at an exponential pace. The information moves within, and between, state agencies and morphs into various forms so quickly that it is almost impossible to manage. As it moves across processes and systems, and is exchanged between people, the information is exposed to varying degrees of risk and is subject to differing standards for its protection.

By its nature, government manages significant quantities of sensitive information. This includes Personally Identifiable Information (PII) and other sensitive information, subject to regulation and other special handling requirements. California citizens, legislators, privacy professionals, and privacy advocacy organizations have voiced concerns at various times regarding government’s ability to protect this information in accordance with applicable laws while also protecting against identity theft. At the same time, the financial consequences of not adequately protecting PII continue to grow year over year. A 2008 study from Ponemon Institute found the average total cost of a data breach rose to \$6.6 million per breach, an increase from \$6.3 million in 2007 and \$4.7 million in 2006. This *per breach* cost translates to a cost of \$202 *per record* breached, according to the study.<sup>xiii</sup> These are clear cost implications for failing to adequately protect against sensitive information breaches.

The Federal Trade Commission (FTC) estimates that as many as 9 million Americans have their identities stolen each year<sup>xiv</sup> and government systems have increasingly become a target for identity theft by criminal organizations due to the inherently sensitive nature of the information contained in these systems. It is well recognized that government's aging IT infrastructure struggles to maintain the high levels of security required for the millions of sensitive transactions that occur on a daily basis. Yet, security must be an essential part of providing government services.

California has already taken a leading role in protecting citizens' personal information and must continue to do so. The state created the nation's first Office of Privacy Protection, dedicated to promoting and protecting the privacy rights of consumers. California also played a leadership role in promoting legislation, such as SB1386<sup>xv</sup>, which requires residents to be notified if their personal information has potentially been breached.

The OIS has also made significant strides in improving California's incident management processes, yielding better information about how and why breaches are occurring. This, however, does not address the root cause of the problem, which is building IT systems with "baked-in" security and data protection controls. Strategic Concept #2 seeks to build those inherent controls.

The OIS will continue to drive California's leadership in privacy and data protection. As the state executes its vision to modernize government by replacing legacy IT applications and revamping its infrastructure, the OIS will work to develop appropriate enterprise policies, standards, and guidance that builds security and privacy into the IT infrastructure. New software applications, systems, and IT infrastructure must also include strong privacy-enhancing technologies as part of their foundation to improve the state's ability to protect sensitive information and to help lower the rising costs associated with data breaches and loss of important information assets.

**STRATEGY 1** – Establish an information-centric, enterprise Data Loss Prevention (DLP) strategy and solution(s) that address the security and privacy of *data at rest*, *data in use*, and *data in transit*.

**GOAL 1A** – Develop an enterprise data protection strategy that identifies data protection requirements for high-risk, regulated (e.g., PII and Protected Health Information, or PHI) and other sensitive data within the state's digital infrastructure.

**GOAL 1B** – In collaboration with technology partners and based on the data protection strategy, the OIS will help identify, select, and deploy DLP solutions that address the state's data protection requirements. The OIS will facilitate access to DLP knowledge, solutions, and resources for state agencies.

**GOAL 1C** – Establish an enterprise information security metrics program that will be used to determine the effectiveness of data protection standards and security program efficiency within state agencies.

**STRATEGY 2** – Protect California citizen and employee privacy by implementing relevant privacy enhancing technologies, standards, and processes.

**GOAL 2A** – Collaborate with the OCIO Enterprise Architecture program to develop and publish privacy and data protection standards aligned with California’s Enterprise Architecture for implementation within new statewide IT capital systems and infrastructure. Areas for standard development include:

- Encryption
- Enterprise Rights Management
- Data De-identification
- Privacy Impact Assessment

**GOAL 2B** – Collaborate via private and public partnerships to identify, explore, select, and implement robust privacy-enhancing technology solutions for state government. For example, data de-identification solutions, encryption solutions, enterprise rights management solutions, and other tools to enhance online privacy and prevent unauthorized access to data.

**GOAL 2C** – Work with the California Office of Health Information Integrity (CalOHII) to develop data protection standards that enhance the protection of health information of California citizens transmitted through proposed statewide Health Information Exchanges (HIE).

**STRATEGY 3** – Ensure transparency is a key principle of government’s use, collection, and disclosure of PII.

**GOAL 3A** – Establish an annual online scorecard that reports on the effectiveness of state agencies’ privacy and data protection practices.

**BOTTOM LINE** – Achieving these goals will significantly increase California’s ability to protect its citizens’ and businesses’ sensitive and personal information against cyber attacks, intentional or unintentional alteration, misuse, and destruction. Ultimately, achieving these goals means that state government will be able to provide California citizens and businesses, the federal government, and other state and local governments the ability to conduct business online with the confidence that transacted information is appropriately secured.

## SECURITY STRATEGIC CONCEPT #3 – A SECURE, TRUSTWORTHY DIGITAL IDENTITY FOR EVERY CALIFORNIA CITIZEN

The purpose of Security Strategic Concept #3 is to define, develop, and deploy a secure, trusted digital identity scheme in which every California citizen, business, and government employee has a single digital identity with which to interact online through a secure “One California” point of access to state government services.

As with any large organization using information technology to support their operations, the state of California has experienced an overwhelming growth of data and applications. This growth is resulting in the steadily increasing cost of IT services. One significant factor of this increasing cost is the administrative and support burden necessary to manage the many user accounts that provide access to the state’s software applications and network services. Essentially, this problem is one of Identity and Access Management (IAM).

### What is Identity & Access Management (IAM)?

IAM is a broad administrative area that deals with identifying individuals in a system, and controlling their access to resources within that system, by associating user rights and restrictions with the individual’s established identity.

The projected population growth in California over the next 15+ years is significant. By 2025, California will gain between 7 and 11 million new residents.<sup>xvi</sup> California, however, like most other states, the federal government, and many private sector organizations, is struggling through one of the worst economic recessions in recent memory. This challenges leadership to look for new efficiencies and ways of doing work with fewer financial resources.

### Cybersecurity and Identity Management

“Identity management has the potential to help individuals and organizations form trusted communities based on varying degrees of identity exposure and mutually agreed accountability, while helping exclude unwanted intruders or inappropriate membership. Identity management also has the potential to enhance privacy through additional protection against the inappropriate release of personal identifiable information.”

*Cybersecurity Policy Review*, presented to the White House, May 29, 2009

Several key issues are driving adoption of IAM technologies by both public and private organizations:

- **REGULATORY COMPLIANCE** – Enterprise-wide IAM technologies are increasingly being used based on the value they provide in automating and centrally consolidating security and regulatory compliance programs. Many of the various state, federal, and industry regulations require some degree of user authentication, user authorization, and auditing and reporting against system access. In many cases, this has been shown to be cost-effective using enterprise-wide identity management technologies.

- **CROSS-ORGANIZATIONAL EFFICIENCY** – Partners, vendors, and constituents are increasingly accessing data and applications directly and electronically, “inside the walls” of an organization, circumventing traditional physical security mechanisms. An IAM infrastructure provides the necessary foundation to facilitate this access securely for each authorized user population.
- **COST REDUCTION/AVOIDANCE** – The proliferation of identity systems and data has added significantly to the cost of IT for many organizations. These studied costs include lost productivity while new employees are on-boarded; administrative costs to provision new users, decommission old users, and reset passwords; and the costs to deploy and maintain disparate ID and password management systems, processes, and infrastructure. A 2008 Gartner study placed the cost of a call to IT help desk for a password reset at \$12 per transaction. The study also found that password resets alone accounted for 20 to 30 percent of the overall IT Help Desk call volume.<sup>xvii</sup> Proper use of identity management and, in particular, a consolidated identity management infrastructure, presents both long-term and short-term cost-saving opportunities for agencies while improving quality of service to the end users.
- **SECURITY AND PRIVACY** – The complexities created by managing multiple user IDs and passwords across numerous systems translates into more complex security requirements. The tendency for users is to write down their user IDs and passwords, thereby circumventing security controls. IAM solutions, and particularly a single, trusted digital identity *used and controlled by each individual*, creates the opportunity for citizens to be more aware of the data they share with the state and makes information flows more transparent. It also empowers citizens to understand the information they share with the state and elevates the requirement for state government to protect that information.

Identity management has evolved over the past decade into a viable solution to deliver secure, online government services that also protect citizen privacy. As California agencies begin evaluating and implementing identity management technologies, the time is right to increase cross-agency collaboration and look for opportunities to improve processes, establish consistent standards, and consolidate identity management-related investments. The OIS will work in collaboration with the OCIO, State Enterprise Architect, and state agencies to help define flexible, federated, and interoperable identity management standards that will drive a “One California” vision of accessing state services through a centralized, secure, online portal.

**STRATEGY 1** – Make a single, secure digital identity possible across state agencies.

**GOAL 1A** – Working with key stakeholders, including the OCIO, Enterprise Architecture Standards Committee, the Identity Management Council and state agencies; establish an enterprise standard for a secure, trusted digital identity.

**GOAL 1B** – Assist in developing an enterprise standard and a road map for integrating multiple agencies within a statewide federated enterprise identity management environment, providing citizens with a single set of *citizen-owned* credentials to access all state government services.

**STRATEGY 2** – Make government services accessible through a single, secure digital identity that provides end-to-end security and enhances collaboration.

**GOAL 2A** – Assist in the development and implementation of a secure, enterprise federated identity model.

**GOAL 2B** – Implement a secure, enterprise federated identity solution that enables single sign-on for employees, citizens, and approved business partners.

**BOTTOM LINE** – Achieving these goals will allow California to adhere to state, federal, and industry requirements, realize cost savings in IT, and strengthen cybersecurity controls while raising the bar on protecting citizen privacy. This strategic concept will help to establish a collaborative “One California” platform for government to offer new, innovative services to citizens, businesses, and internal users.

## SECURITY STRATEGIC CONCEPT #4 – SECURITY AS AN ENABLER OF MORE EFFICIENT TECHNOLOGY

The purpose of Security Strategic Concept #4 is to embrace more efficient and secure technologies that result in elimination of waste within the IT infrastructure and ultimately lead to a more economically and environmentally green environment. The OIS will collaborate with OCIO and state agencies to engage early in the development and procurement processes to aggressively adopt new technologies that help meet California’s goals, economically and securely.

Information and communication technology (ICT) accounts for 2 percent of global carbon dioxide (CO2) emissions and is projected to double by the year 2020, according to a report published by the Climate Group.<sup>xviii</sup> However, innovative use of ICT also has the unique ability to monitor and maximize energy efficiency both within and outside of its own sector. According to the report, harnessing technology for uses such as teleworking, video-conferencing, e-paper, virtualization, and the design of smart telecommunications and infrastructure grids, would help cut 7.8 gigatons of CO2 equivalent from the atmosphere by the year 2020 — a cut greater than the current annual emissions of either the United States or China.

By rethinking the use of technology, we can have both a transformational impact on the environment and also provide California with significant economic opportunities. Security *is an enabler* to realizing substantial environmental and economic benefits. Consider the following:

- **SECURITY PLAYS A ROLE IN LEVERAGING NEW, GREENER TECHNOLOGIES** – New technologies such as virtualization and cloud computing benefit the environment by consolidating servers and running fewer, highly utilized virtual systems. Economic savings include reduced hardware and energy costs as well as the sheer ability to streamline the provisioning and deprovisioning of virtual machines. While there are serious challenges from a security, privacy, and regulatory perspective to implementing virtualized environments, the OIS will collaborate and work with our private sector partners to find solutions that enable government to leverage these technologies.
- **SECURITY CAN MOVE DATA CLOSER TO THE PEOPLE, ELECTRONICALLY AND WITHOUT PAPER** – Perhaps nothing defines a bureaucracy as much as its “paper pushing” processes. Forms are ever prevalent: Citizens submit forms containing the same information to multiple agencies, causing data entry inefficiencies and work duplication. These processes waste paper, increase the likelihood of data entry error, and add both cost and risk stemming from *one more piece of paper* that must be secured and stored. Security must be an enabler to achieving cost and process efficiency by pushing electronic data securely to the people that need it. Technologies, including IAM, digital signatures, automated workflow, encryption, and information-centric security are enablers to “greening” government’s paper-intensive processes.

- **ENTERPRISE-LEVEL SECURITY PLAYS A DIRECT ROLE IN STREAMLINING COSTLY AND INEFFICIENT PROCESSES –** Centralizing security resources, processes, and technology *when it makes sense* creates more consistent security practices and provides cost leverage. As an example, securing one network is less expensive and creates better resiliency than securing 20 disparate networks. Cost-efficient security also means building in security from the beginning to avoid after-the-fact retrofits or fallout from a compromised asset. California must aggressively pursue security strategies that focus on eliminating waste while providing better security and visibility into California’s IT environment.
- **SECURITY ENABLES CITIZENS, BUSINESS, AND STATE EMPLOYEES TO LIVE AND WORK THE WAY THEY WANT TO IN THE 21ST CENTURY -** Security must keep pace with people’s preferences to work in much more flexible and innovative ways than have previously existed in government. California must adopt solutions, such as remote access for teleworking, virtual conferencing, and the use of Web 2.0<sup>xx</sup> technologies to not only create a flexible, innovative workplace, but also to attract a “digitally aware,” diverse workforce to state government. The OIS will play a leadership role in speeding the secure enterprise adoption of these technologies.

**California Performance Review Recommendation  
GG11:  
Reduce Costs and Improve Customer Service  
through Use of Internet Forms**

The CPR Report recommends that all state agencies should publish fillable forms online and transition to secure, online filing as soon as practical. CPR staff looked at 20 agencies and found examples of successful use of online forms that improved both customer service and state efficiency. Examples include the following:

- Department of Toxic Substances Control (DTSC): Since 2001, businesses can access federally required environmental information online and register compliance. This has dramatically increased compliance with state/federal laws, improved convenience, and reduced inefficiencies (businesses previously contacted DTSC by telephone). About 100,000 transactions per year are now done electronically. The online service has increased compliance and revenues from regulated entities from \$4 million per year pre-2001 to \$11 million today.
- Department of Motor Vehicle (DMV): An Electronic Lien and Title (ELT) program allows financial institutions to perform certain title and lien-related transactions electronically. 375 financial institutions participate in the ELT program and more than 1.6 million electronic titles were issued over a period of 12 months. ELT has helped DMV reduce the volume of transactions processed by an estimated 1.2 million transactions per year, realizing a savings of \$4.9 million. Lastly, DMV’s website was updated in April 2004 to allow motor carrier permit applicants to submit forms electronically. By June 2004, phone calls relating to this program had been reduced by 37%, translating to staffing and operational savings.
- Since 2001, the Secretary of State has moved nearly 1 million paper documents per year to online filing (e.g., reports and licenses for lobbyists and corporations). This allowed the Secretary of State to eliminate duplicate data entry and paper filings. The Secretary of State also developed an online California Business Search database to reduce business name inquiries telephone calls. Both measures have created workload savings and helped clear data entry backlogs.<sup>xix</sup>

- **SECURITY PRACTICES MUST BE ALIGNED WITH DEMANDS FOR MORE ACCOUNTABILITY AND TRANSPARENCY OF STATE GOVERNMENT** – The near-daily reports of sensitive citizen information exposed through poor government practices can no longer be accepted as the status quo. California citizens, the Governor and the OCIO have called for greater security oversight to benefit the state and its partners. Citizens expect to know government’s progress and action plans to safeguard their personal information.

**STRATEGY 1** – Streamline, simplify, and consolidate security and risk management practices to create a single, enterprise-wide view of California’s cyber and privacy risks.

**GOAL 1A** – Consolidate and harmonize the disparate sets of information security and privacy-related policies, standards, and guidelines within the OCIO organizations realigned as a result of the 2009 Governor’s Reorganization Plan.

**GOAL 1B** – Implement an enterprise IT risk management platform and supporting risk management framework to consolidate disparate, redundant, or siloed risk management operation across state agencies.

**GOAL 1C** – Establish a California modified version of the NIST 800-30<sup>xxi</sup> risk management standard as the risk management standard for all state agencies.

**STRATEGY 2** – Develop policies and standards that enable the secure use of new technologies that support economic and environmental sustainability.

**Goal 2A** – Develop policies and standards to enable secure Telework.

**GOAL 2B** – Develop policies and standards to enable cost-efficient Web 2.0 technologies in a secure manner for all state agencies.

**GOAL 2C** – Develop policies and standards to enable cost-efficient technologies that reduce California’s carbon emissions and shrink the overall IT footprint (e.g., virtualization, cloud computing).

**STRATEGY 3** – Make government accountable to “*bake-in*” security and privacy requirements and controls during the design and requirements definition phase of new IT projects.

**GOAL 3A** – Establish a common set of security metrics for state agencies to use in measuring their security and privacy health. Publish state agency summary results via the Governor’s Reporting Transparency in Government Web site.

**GOAL 3B** – Include information security and privacy requirements in all state IT procurements from the Feasibility Study Report (FSR) process onward.

**GOAL 3C** – Establish a process for the review and approval of all IT capital projects by the OIS as part of the OCIO IT project approval process.

**STRATEGY 4** – Consolidate and/or eliminate duplicative business processes and associated online forms.

**GOAL 4A** – Leverage a secure, trusted digital identity to identify and eliminate online duplicative data collection processes and forms across state agencies.

**GOAL 4B** – Develop and deploy an enterprise Security Incident Reporting System for California government.

**BOTTOM LINE** – Executing these goals is fundamental to providing Californians with better customer service in a cost-effective fashion. At the same time, executing these goals also contributes to California's green initiatives in a substantial manner.

## SECURITY STRATEGIC CONCEPT #5 – EFFECTIVE SECURITY THAT ENHANCES COLLABORATION AND DELIVERY OF SERVICES

The purpose of Security Strategic Concept #5 is to establish secure and seamless communication standards to support online collaboration between California government, its business partners, and other state governments. By developing an end-to-end computing ecosystem based on robust security processes, standards, and techniques, the OIS will help further the state's objective in achieving a transparent and trusted environment for collaboration.

In the current environment, state government does not always have a clear view of who is on its digital network. Each state agency follows its own processes to allow users, including vendors and external business partners, to access internal systems. As state systems become increasingly interconnected, California's digital infrastructure is only as strong as its weakest link.

Trust must exist in the virtual environment of people, processes, and technologies that come together in order to achieve successful collaboration. Trust is developed and sustained in a digital environment when all parties have confidence in the security, reliability, and integrity of the online transaction.

Establishing trust must be an essential principle in the implementation of any new technology that opens or connects government systems to its partners. A baseline requisite is that the connected parties have established common standards to protect the security and privacy of sensitive information that is exchanged. The OIS can help in this process so that agencies do not have to reinvent the wheel. In fact, the OIS recently published guidelines for information sharing designed to establish a consistent and reusable framework upon

### Benefits of Online Trust

- Interactions between governments and people often involve sensitive information such as tax data or intellectual property included in patent filings. In some parts of the world, people trust their governments with this information — but not mobile devices or even the Internet itself. In other places, the governments themselves are held suspect, and cybersecurity can enable a degree of transparency that will increase the public's confidence in its leaders.
- Consider what a reliably secure Internet, safe to use from both wired and mobile touch points, can do in both situations: bolster trust and speed the process of government itself. Cybersecurity thus becomes an investment with payoff.
- Lack of trust in the Internet is a barrier to greater, faster, more widespread commerce. Cybersecurity has the potential to unlock those transactions and speed the economy of any jurisdiction that makes the investment.<sup>xxii</sup>

which entities at all levels of California government, including state, county, and city, can facilitate trusted system interconnection and data exchange.<sup>xxiii</sup>

Information security and privacy are not solely an IT problem. When security is relegated to being “just a technology issue,” there is less opportunity to create the best practices that can support the organization in achieving its goals. Effective security requires people to collaborate across all levels of the organization, and that management is part of the security decision-making process. Agency leadership must play a strong role, and is ultimately responsible, for the “security conscious” culture that must exist in every state agency to properly execute government’s goals.

One of the key outputs from the OIS strategic planning process was the need for increased top leadership awareness and better information sharing to promote, compare, and disseminate leading-class IT risk management practices across state government.

Management does not currently have access to information that would allow them to better assess risks to their organization or benchmark their practices against other agencies. Providing better information targeted to executive leadership would enable state agencies to better understand, evaluate, and remedy the exposures emanating from their respective organizations.

**STRATEGY 1** – Implement a common security framework for use by all state agencies to ensure consistent, trustworthy information sharing between agencies.

**GOAL 1A** – Establish a California-modified version of the NIST 800-53<sup>xxiv</sup> recommended security controls within all state agencies.

**GOAL 1B** – Establish the Consensus Audit Guidelines (CAG)<sup>xxv</sup> as an alternative, risk-based security risk management framework for those agencies formally exempted from NIST 800-53 requirements.

**GOAL 1C** – Implement risk-based policies, standards, and guidelines for data exchange and systems interconnectivity between state agencies and its public and private business partners.

### **It’s about Risk Management: Action Items for State Leaders**

The rapidly evolving digital infrastructure carries with it a correspondingly dynamic range of security threats that state security professionals must constantly contend with to maintain the integrity and availability of government services. ...While informing themselves, making sometimes difficult choices between standards, and executing the follow-on policies, standards, and controls are significant challenges to CIOs and their CISOs, there are no short-cuts to securing state IT systems and the services they provide.

Excerpt from NASCIO’s *Desperately Seeking Security Frameworks-a Roadmap for State CIOs*, March 2009

**STRATEGY 2** – Raise the state’s Security and Privacy Risk Management “IQ” by increasing training and awareness activities at all levels within state agencies.

**GOAL 2A** – Develop and deploy role-based security and privacy training for all state employees and contractors using cost-efficient training delivery technologies and platforms.

**GOAL 2B** – Provide regular security and privacy briefings for executive, legislative, and program leaders to create a common level of understanding and awareness of security threats and risks at the state enterprise level.

**GOAL 2C** – Enhance existing seminars for state IT risk management professionals, including ISOs, Privacy Officers and Coordinators, Disaster Recovery (DR) Officers and Coordinators, and auditors. Formally expand the seminars to the state’s public and private business partners, including regional government and contractors.

**BOTTOM LINE** – Collaboration must occur to create a secure environment; equally important, strong collaboration cannot occur without good security. The OIS will work with the OCIO and state agencies to create a more collaborative environment that *influences the mindset* of leadership, employees, and state government partners to view security as an enabler to their objectives. The benefits of collaboration through increased, online government are tangible — including better use of the state’s assets; improved service; and secure, cost-effective data sharing between the public and state entities.

### Maxims for Strong Security <sup>xxvi</sup>

- There are effective, simple, and low-cost countermeasures (at least partial countermeasures) to most security vulnerabilities. Training and awareness can be considered one such measure.
- Voltaire stated that, “Common sense is not that common.” Adopting a standards-based security framework based on studied risk principles reduces the potential for errors in judgment that could compromise state systems.
- Security weaknesses often go unaddressed until they have resulted in potentially catastrophic damage. Strong security means addressing security vulnerabilities before they are exploited.
- Organizations are often unprepared for the security implications of new technology, and the first impulse will be to ban it. Security functions must work toward being an enabler of new, more efficient technologies.
- Awareness of the issue is the first step toward strong security: In 1633, as Galileo was brought before the Roman Inquisition, Church officials refused to look into Galileo’s telescope out of fear of what they might see.

# Alignment of Security Strategic Concepts to the OCIO IT Strategic Plan

The five key principles set forth in the Information Security Strategic Plan to secure Californians in cyberspace are fundamentally aligned to the vision for the future of California’s IT environment, as outlined in the OCIO’s IT Strategic Plan. Each of the security, privacy, and data protection concepts outlined in this plan map to one or more of the IT Strategic Plan’s Six Strategic Concepts. The overarching enterprise vision guiding the security and privacy principles is to enable government to be a transformational leader in providing services that meet the needs of California citizens in the 21st century.

OCIO IT Strategic Plan: Strategic Concepts					
IT as reliable as electricity	Fulfilling technologies potential to transform lives	Information as an asset	Self-governance in the Digital Age	Economic and sustainable	Facilitating collaboration that breeds better solutions
Securing California in Cyberspace – Information Security Strategic Plan: Strategic Concepts					
A Digital Infrastructure that is Resilient, Secure, and Trustworthy	Make Internet Use a Safer Experience for Californians	A Secure, Trustworthy Digital Identity for Every California Citizen	Security as an Enabler of More Efficient Technology	Effective Security That Enhances Collaboration and Delivery of Services	
Implement state-of-the-art enterprise information security to combat and manage current and future cyber risks to California’s enterprise IT infrastructure and the information housed within it.	Implement enterprise “information-centric” security solutions for the state, whereby the security is always with the asset (information) regardless of where the information resides within the state’s IT infrastructure.	Every California citizen, business, and government employee owns and controls a digital identity and interacts online through a secure “One California” access point to government.	Embrace new technologies that help to eliminate waste within the IT infrastructure and ultimately lead to a more economically and environmentally green environment.	Establish secure communication standards to support online collaboration between California state government, its business partners, and other state governments.	

# From Goals to Actions

The concepts set forth in this Information Security Strategic Plan are built on a platform of strategies and concrete goals for action. The next critical step is development of the tactical actions required to implement these strategies and realize tangible progress toward the goals. This requires strong partnerships and collaboration with state agency business and IT leaders.

Despite current resource limitations, California must continue to make strategic investments to enable the safe, secure, and trustworthy use of government services. This becomes of paramount concern as California executes its vision to move more and more government services online.

The timing of the state's actions is crucial. Leadership at both the state and federal levels *are serious* about cybersecurity. The White House has detailed the federal agenda for specific goals, including strengthening cybersecurity leadership, investing in research and development, developing national strategies, mandating increased standards to protect personal data, and requiring organizations to disclose potential data breaches. We must not lose momentum.

As previously stated, this Information Security Strategic Plan presents a vision that will guide our information security and data privacy initiatives over the next five years. The strategic concepts in this plan build on one another and are designed to support the goals outlined in the OCIO IT Strategic Plan. Therefore, California must achieve its security goals in order to achieve the modernization, transparency, and accountability goals of the overall IT Strategic Plan.

The time is now to move from study of the problem to concerted action. We must address known security and data protection issues to fulfill our obligations to protect California citizens, businesses, and state employees, now and in the future.

“We must act today in order to preserve tomorrow. And let there be no misunderstanding — we’re going to begin to act beginning today.”

President Ronald Reagan, First Inaugural Address, January 20, 1981

# Appendix A – Footnotes

<sup>i</sup> Quote from Forrester Research, *Worldwide PC Adoption Forecast, 2007 To 2015*, June 11, 2007, <http://www.forrester.com/Research/Document/Excerpt/0,7211,42496,00.html>

<sup>ii</sup> In October 2008, 85 state agencies and departments submitted five-year IT Capital Plans (ITCPs) to the OCIO and the Department of Finance. These were published in the OCIO's Statewide Information Technology Capital Plan, Volume Two of California's IT Strategic Plan. Per that Plan, these selected ITCPs "establish the foundation for ensuring that IT investments support state priorities, business direction, and align with statewide technology standards." \$466M is the summation of those ITCPs.  
[http://www.itsp.ca.gov/pdf/2009\\_Statewide\\_IT\\_Capital\\_Plan.pdf](http://www.itsp.ca.gov/pdf/2009_Statewide_IT_Capital_Plan.pdf)

<sup>iii</sup> Symantec 2008 Global Security report, Volume XIV, April 2009, [http://www.msisac.org/awareness/documents/20016963\\_GA\\_RPT\\_ISTR14\\_Global\\_04.09.pdf](http://www.msisac.org/awareness/documents/20016963_GA_RPT_ISTR14_Global_04.09.pdf)

<sup>iv</sup> *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, [http://www.csis.org/files/media/csis/pubs/081208\\_securingcyberspace\\_44.pdf](http://www.csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf)

<sup>v</sup> References for this paragraph:

- FBI Shutdown: <http://www.msnbc.msn.com/id/30882735/>
- Spies Hacked into the Grid: <http://online.wsj.com/article/SB123914805204099085.html>
- Air Traffic Control is Vulnerable: <http://www.msnbc.msn.com/id/30602242/>
- The Russian Georgian Military Conflict: <http://blogs.zdnet.com/security/?p=1670>

<sup>vi</sup> University of California Berkeley Statement, May 8, 2009 <http://datatheft.berkeley.edu/>

<sup>vii</sup> *Movie Sharing Program Causes A Security Breach In University Of California San Francisco*, May 31, 2008, <http://cyberinsecure.com/movie-sharing-program-causes-a-security-breach-in-university-of-california-san-francisco/>

<sup>viii</sup> San Francisco Chronicle, *Sabotage Attacks Knock out Phone Service*, <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/04/09/BAP816VTE6.DTL&tsp=1>, April 10, 2009

<sup>ix</sup> *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure*, [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf), Melissa Hathaway, Cybersecurity Chief at the National Security Council, May 29, 2009

<sup>x</sup> Presidential Decision Directive NSC/63 on the subject: Critical Infrastructure Protection, May 22, 1998 <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

<sup>xi</sup> The National Institute of Standards and Technology (NIST) 800-37 provides guidelines for the certification and accreditation of Federal IT systems. State, local, and tribal governments, as well as private sector organizations comprising the critical infrastructure of the United States, are encouraged to consider the use of these guidelines, as appropriate. <http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf>

<sup>xii</sup> NASCIO, *Protecting the Realm, Confronting the Realities of State Data at Risk*, 2008, <http://www.nascio.org/publications/documents/NASCIO-ProtectingRealm.pdf>, (NASCIO represents CIOs, IT executives and managers from state government across the U.S.)

---

<sup>xiii</sup> The Ponemon Institute, *Fourth Annual US Cost of Data Breach Study, Benchmark Study of Companies*, <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf>, January 2009

<sup>xiv</sup> About Identity Theft, Federal Trade Commission, <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>

<sup>xv</sup> SB1386, operative as of July 1, 2003, is a California Law regulating the privacy of personal information. SB1386 mandates the notification of any California resident whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person. [http://info.sen.ca.gov/pub/01-02/bill/sen/sb\\_1351-1400/sb\\_1386\\_bill\\_20020926\\_chaptered.html](http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html)

<sup>xvi</sup> California Information Technology Strategic Plan 2009, Strategic Concepts, Strategies & Goals, Volume 1, [http://www.itsp.ca.gov/pdf/Strategic\\_Plan.pdf](http://www.itsp.ca.gov/pdf/Strategic_Plan.pdf)

<sup>xvii</sup> Gartner, *Key Metrics for IT Service and Support*, April 29, 2008, ID Number: G00154802, David M. Coyle, Kris Brittain

<sup>xviii</sup> *SMART 2020: Enabling the Low Carbon Economy in the Information Age*, The Climate Group and The Global e-Sustainability Initiative (GeSI), 2008  
<http://www.theclimategroup.org/assets/resources/publications/Smart2020Report.pdf>

<sup>xix</sup> *California Performance Review Recommendation GG11, 2007*, [http://cpr.ca.gov/CPR\\_Report/Issues\\_and\\_Recommendations/Chapter\\_1\\_General\\_Government/Creating\\_Custom\\_er\\_Friendly\\_Government/GG11.html](http://cpr.ca.gov/CPR_Report/Issues_and_Recommendations/Chapter_1_General_Government/Creating_Custom_er_Friendly_Government/GG11.html)

<sup>xx</sup> "Web 2.0 is commonly associated with web development and web design that facilitates interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. Examples of Web 2.0 include web-based communities, hosted services, web applications, social networking sites, video-sharing sites, wikis, blogs, "mashups," and folksonomies. A Web 2.0 site allows its users to interact with other users or to change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is provided to them." [http://en.wikipedia.org/wiki/Web\\_2.0](http://en.wikipedia.org/wiki/Web_2.0)

<sup>xxi</sup> The National Institute of Standards and Technology (NIST) 800-30 *Risk Management Guide for IT Systems* provides information on the selection of cost-effective security controls that can be used to mitigate risk for the better protection of mission-critical information and IT systems that process, store, and carry this information. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

<sup>xxii</sup> *Cybersecurity: Everybody's Imperative Protecting our Economies, Governments, and Citizens*. Deloitte Publication, May 6, 2009, [http://www.deloitte.com/dtt/cda/doc/content/CybersecurityDeloittePointofViewlowres\(1\).pdf](http://www.deloitte.com/dtt/cda/doc/content/CybersecurityDeloittePointofViewlowres(1).pdf)

<sup>xxiii</sup> [http://www.oispp.ca.gov/government/documents/docs/Guideline%20for%20Establishing%20Data%20Exchange%20and%20System%20Interconnection%20Agreements%20Between%20Government%20Agencies\\_05252009.doc](http://www.oispp.ca.gov/government/documents/docs/Guideline%20for%20Establishing%20Data%20Exchange%20and%20System%20Interconnection%20Agreements%20Between%20Government%20Agencies_05252009.doc)

<sup>xxiv</sup> The National Institute of Standards and Technology (NIST) 800-53, *Recommended Security Controls for Federal Systems* provides guidelines for security controls within an effective information security program. Used in conjunction with other NIST publications, NIST 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>

<sup>xxv</sup> The Consensus Audit Guidelines (CAG) was released February 23, 2009 by a consortium of Federal and private organizations and defines the most critical security controls to protect federal and contractor information and information systems. Each of the 20 defined controls is designed to mitigate against actual attacks known to be

---

used against government, financial institutions, the defense industrial base, and retailers. Experts have noted the twenty key actions defined in the CAG, i.e. the 20 security controls, as “reality and risk based security.”  
<http://www.sans.org/critical-security-controls/guidelines.php>

<sup>xxvi</sup> Adapted from Security Maxims by Roger G. Johnston, Ph.D. CPP,  
<http://www.ne.anl.gov/capabilities/vat/seals/maxims.html>