THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

USINDIA BusinessCouncil

TRUSTED INFORMATION MANAGEMENT: DATA PRIVACY & SECURITY ACCOUNTABILITY IN OUTSOURCING

NASSCOM's Establishment of the Data Security Council of India

WHITE PAPER
September 2007

Maureen C. Cooney, Counsel
Senior Policy Advisor for Global Privacy Strategies

ABOUT THE CENTER FOR INFORMATION POLICY LEADERSHIP

Sponsored by companies affiliated with the United States–India Business Council (USIBC), the Center for Information Policy Leadership (CIPL or Center) produced this paper to provide guidance to the National Association of Software and Service Companies (NASSCOM) in its leadership and establishment of the Data Security Council of India (DSCI).

CIPL was founded in 2001 by leading global companies and Hunton & Williams LLP. The Center develops innovative, pragmatic approaches to information privacy and security issues from a business-process perspective, while respecting the privacy interests of individuals. Since its establishment, CIPL has addressed such issues as transparency, conflicting national legal requirements, cross-border data transfers, business practices to safeguard personal information, and government uses of private sector data.

CIPL is led by Martin Abrams, Executive Director, and Paula Bruening, Deputy Executive Director. It includes distinguished senior policy advisors, including Fred H. Cate, Commissioner Orson Swindle and Maureen C. Cooney, as well as members of Hunton & Williams' Global Technology, Outsourcing and Privacy practice. Hunton & Williams is a global firm, with more than 900 attorneys in offices spanning 19 countries. The firm's privacy practice is prominent in addressing data security breaches and information management, international privacy law and policy, and privacy management in connection with outsourcing, e-commerce, consumer protection, and health and financial services risk issues. The breadth of the privacy practice of senior advisors and attorneys provides a richness of knowledge and experience that CIPL leverages to promote practical, solutions-focused, global information policy approaches.

ABOUT THE UNITED STATES–INDIA BUSINESS COUNCIL

USIBC is the premier advocacy organization, representing 250 of the largest U.S. companies investing in India, joined by global Indian companies, promoting economic reforms with an aim to deepen trade relations and broaden commercial ties between the two countries. Celebrating its 32nd anniversary year, USIBC was formed in 1975 at the request of the governments of the United States and India to involve the private sectors of both countries in a sustained and meaningful dialogue to advance economic reforms and identify and remove impediments to investment flows to India. USIBC's primary mission is to serve as a link between key business and government decision makers to encourage progressive economic policies in India and the United States, resulting in increased trade and investment. The USIBC Committee on the Digital Economy and IT has been particularly active in promoting U.S.–India business dialogues and initiatives on information privacy and security.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper recognizes a growing global belief that, to promote competitiveness and innovation, businesses and service providers must address issues related to trust and accountability for information privacy and security in connection with outsourcing transactions. NASSCOM has been working on similar objectives in its exploration of how to develop a credible self-regulatory organization in India to promote trusted information management and data security by its member companies.

CIPL and USIBC see an opportunity for the DSCI to be a leader in raising awareness of the importance of information privacy and security in outsourcing. With this paper, CIPL and USIBC seek to assist NASSCOM in focusing the design and mission of the DSCI to advance privacy and information security accountability through guidance on:

- → Concepts of privacy accountability in outsourcing;
- → Integration of applicable portions and concepts of existing international principles, such as the APEC Privacy Framework Principles, as reference models for fulfilling the obligations that flow with personal data across borders;
- → Establishing DSCI roles, including tailoring the role as a trust agent to the particular needs of its member companies; and
- → Establishing targets and proposed timetables for achievement of the DSCI's goals — central among them, the education and development of India's own information privacy and security management sector.

Recognition of Information Privacy and Security Obligations that Flow with the Data

We recommend that the DSCI help develop a trusted information management culture across India. The DSCI should emphasize information security and the duty to honor privacy obligations that flow with the data as specified in contractual requirements. It must be recognized that information protection obligations follow the data being managed and reflect the client company's obligations and commitments to customers where a transaction originated.

Implementing a DSCI framework that recognizes cross-border responsibility for the continuing privacy obligations that travel with data is both practical and achievable.

In developing an accountability framework for businesses, the DSCI should assist member companies in improving their information privacy and security practices to promote trusted use of cross-border data flows in global sourcing. A successful framework will be consistent with applicable concepts of international privacy principles. These include the Privacy Framework developed by the Asia Pacific Economic Cooperation (APEC) forum, which builds upon longstanding concepts of data responsibility introduced in the 1980s by the Organization for Economic Cooperation (OECD). APEC and OECD privacy principles emphasize the dual goals

of promoting the free flow of information and appropriately protecting the privacy and security of personal information in data flows. The APEC Privacy Framework adds two important new principles addressing protection of individuals from harm and business accountability — bookends to data responsibility.

Key to creating a trusted information management culture in the outsourcing context is the ability of servicing operations to demonstrate commitment and competence to operate within an accountability framework that requires them to meet obligations that originate from multiple industries, companies and national systems. Service providers must build in compliance processes that enable the protections required by the obligations that flow with personal data from another jurisdiction to be honored. Data privacy and security obligations should be honored in accordance with client specifications, reflecting both the client's legal compliance duties and privacy and security promises to consumers.

A DSCI accountability framework that recognizes appropriate balancing and tailoring of protections will allow member companies to manage and architect their privacy and data security systems in a proportionate and achievable manner. Planning must take into consideration the sensitivity of data collected, its use and risks of harm to individuals or clients from misuse or unauthorized disclosure of personal information or proprietary information assets.[1] Flexible, tailored implementation of protections will permit service providers to architect privacy and data security plans that reflect best practices that are designed for the particular business sectors they service, the sophistication and/or size of their operations, and according to client needs and expectations.

Phases of DSCI Development

This paper outlines four phases of the DSCI's development of an accountability framework and strategies for success. The phases are overlapping and build upon each other in an iterative manner.

The objective for the first phase is to address operational planning and governance issues for an effective self-regulatory organization. The objective of the second phase is to develop strategies for ensuring membership preparation and readiness to meet DSCI requirements. The third phase of development would establish the organization's leadership to industry as a consultant, educator and enforcer, fostering privacy and information security compliance by sourcing service providers. Where applicable, the DSCI could provide member support by defining different types of solutions to address information privacy and security issues. Finally, the objective of the fourth phase of the DSCI is to establish and publicly promote the DSCI's likely and measurable achievements, including the benefits of transparency to gain respect and trust among all stakeholders.

1 This paper primarily addresses information privacy and security for personal information used in the context of outsourcing services. Particularly with regard to information security concepts, however, many of the concepts discussed for the DSCI can apply and are relevant to the protection of proprietary information, including research and development data.

DSCI Roles

The paper also discusses particular roles that the DSCI should take on during one or more of its developmental stages. Just as the developmental phases may overlap, so may the roles of the DSCI through many phases and over time.

We recommend that as the DSCI matures it engage in the following roles and strategies, with execution phased in as resources and capabilities allow.

- → Define mission and accountability framework.
- → Establish a credible governance structure for the DSCI that includes serving as an independent authority and trust agent for member companies, to offer oversight of business accountability efforts.
- → Work as a partner with government to promote a culture of trusted information management and compliance among Indian businesses and IT/services industries.
- → Initiate information privacy and security outreach and awareness building among DSCI's membership and relevant constituencies.
- → Help build privacy and security capacity for potential member companies so that they will be ready to meet DSCI requirements. This activity can include serving as a consultant or facilitator of consultancy services to members.
- → Encourage and facilitate the communication of information privacy and security obligations between client organizations and outsourcing service providers.
- → Monitor and enforce compliance by members; assist members as a liaison to dispute resolution services; as appropriate, refer certain matters for backup government enforcement.
- → Communicate industry initiatives and successes.

Across all the developmental phases of the DSCI, and with respect to the roles that it takes on, there is a significant need for outreach and communication with the broadest circle of stakeholders. Through input and dialogues with client, service provider, sourcing consultancy, consumer and academic and government sectors, the DSCI is most likely to achieve a balanced and pragmatic self-regulatory accountability framework that will achieve credibility and respect for its information privacy and security protection initiatives.

Brief Conclusion

The most credible accountability framework will enhance the capabilities of service providers to work with clients in honoring the privacy and data security obligations that flow with data. A one-size-fits-all approach will not fit all member companies.

Just as the development of the DSCI will likely progress through phases, the development of the DSCI's accountability framework will also be iterative. We believe and recommend that a less resource-intensive, achievable and credible accountability framework could

begin by marking membership criteria to the implementation of privacy and information security procedures and practices, rather than adherence to a specific code of conduct. The accountability framework should be premised on policies and procedures to implement an information privacy and security management plan and adherence to the obligations that flow with data, including across borders.

INTRODUCTION

In less than a decade, India has built a national environment that promotes and capitalizes on beneficial growth in the IT sector. The country has positioned itself as an outsourcing destination of choice. The ability to use information in a productive manner has been one of its main success factors.

To promote continued leadership, NASSCOM announced its intention to establish the DSCI, a self-regulatory organization whose mission is to highlight and enhance information privacy and security accountability for outsourcing and business processing operations (BPOs) in India. Through this endeavor, NASSCOM seeks to apply the highest privacy accountability practices to today's IT-enabled business processes and international data flows.

The DSCI will serve as a trust agent for data privacy and security accountability in outsourcing through education, compliance and enforcement of trusted information management practices in the handling of personal data. NASSCOM's efforts to build out a business accountability framework can serve as a global model. The effort significantly puts into action NASSCOM's Trusted Sourcing Initiative, emphasizing active engagement, education, enactment and enforcement.

As the DSCI maps out its goals, education and outreach efforts will be needed to build awareness and to prepare organizations to meet the DSCI's voluntary compliance standards. From the beginning, it will be important for the DSCI to provide consultative advice and guidance to members on information privacy and security. These steps will prepare a skilled workforce to be the privacy and security backbone of trusted sourcing service provider organizations. With the support of corporate leaders, the DSCI will assist a developing sector of information privacy and security managers to understand the importance of global data flows and promote responsible management of data in global sourcing.

Today in India, many service providers and other businesses honor the privacy and data security promises that flow with information from clients. They have well-managed, sophisticated programs on privacy and data security management. What is missing, however, is a framework against which responsible businesses can benchmark their practices and demonstrate their expertise, competence and accomplishments in this area. The absence of a framework actually impairs the credibility of highly competent companies operating in India that are leaders in implementing privacy and security controls. Therefore, the development of a business accountability framework for privacy and data security is as important to high-performing companies in India as it is for service providers that may need significant assistance with privacy and security awareness and capacity building from the DSCI.

An effective DSCI can play a significant role as an agent of trust in providing robust private-sector accountability for information privacy and security, including in cross-border outsourcing transactions. Consumers, businesses and government must all have confidence in the DSCI's voluntary framework for information privacy and security accountability by businesses. Confidence among stakeholders will be centrally important to the success of the self-

regulatory effort. The DSCI should seek to influence activity in this field, partnering with other organizations and stakeholders and encouraging the client sector to be highly participatory with the DSCI and its members.

DATA FLOWS, GLOBAL BUSINESS PROCESSES AND OUTSOURCING

Information Flows Create Value

In the past 15 years, information technology has transformed commerce. Today, the ubiquitous nature of information flows reflects the pervasive impact of the Internet and open networks of information systems around the world. Evolving information communication technologies, combined with increasingly sophisticated software to digitize information and assist business processes, allow companies to improve their business operations and meet customer expectations for “real-time” service, 24 hours a day, 7 days a week, in every time zone on the globe.

Companies increasingly optimize their customer service and business processes by looking beyond national boundaries to leverage time, resources and efficiencies. Many business functions can be sourced to service providers and may be accomplished between one or more service providers from one or more locations, including jurisdictions such as India.

The flexibility that information communication technologies provide for global servicing allows companies to shape their customer service, inventory delivery and manufacturing to maximize operational efficiencies and benefits. Business processes can be tailored based on customer demands, the availability of skilled staffing, efficiencies, costs and other strategic business considerations.

Leveraging Information Privacy and Security Protection

Just as information flows can be leveraged to create value through global sourcing, verified information security and privacy practices can enhance a company’s brand and market reputation. In an increasingly competitive market, companies will leverage trusted information management to attract and keep customers who have entrusted their personal data to them. Assuring that service providers responsibly use and safeguard personal data will increasingly be a factor influencing sourcing decisions in enterprises that outsource functions.

To promote competitiveness and innovation, businesses and sourcing service providers must address trust issues and define accountability for information privacy and security in outsourcing transactions. Steps must be taken to manage increasingly complex transactions and responsibilities related to cross-border sourcing transactions. This will require better identifying the data being shared with service providers, its sources and the obligations attendant to the data that must be honored in a sourcing transaction. It will also require privacy and information management provisions to be more explicit in sourcing contracts, specifying the data compliance responsibilities of clients and of service providers. Constructive dialogues

and relationships will be imperative between businesses, service providers and their domestic or host country regulators and self-regulatory organizations.

PRIVACY, SECURITY AND GLOBAL OBLIGATIONS

What are we talking about when we consider trusted information management and global obligations that flow with personal data?

Privacy

Every society has its own privacy culture. Data that one culture deems sensitive may be viewed as less sensitive in others. Some societies view privacy as an individual protection issue, others regard it as a human rights issue, still others look at the community value promoted by privacy protection. Particular expectations for privacy are truly local.

In commercial transactions, information privacy and security obligations are determined by local or point of origination expectations. These expectations do not change when the data moves in a globally networked environment. Rather, the businesses that originally collected data (also sometimes referred to as data controllers) are required to meet the originating privacy obligations regardless of where the data flows. They must communicate these obligations to their service providers.

Information Security

Information privacy and security are interrelated information management responsibilities and disciplines. They both need to be optimized and are most successful when privacy and security planning efforts are integrated and safeguards work in conjunction with each other in order to comprehensively protect data.

Notions of information security generally center on safeguarding the appropriate access to, use of and integrity of data. Information security also includes expectations of keeping certain personal and proprietary information confidential and safeguarding data from loss (i.e., theft, or inappropriate deletion, or alteration) or misuse that could harm an individual (i.e., identity theft or reputation risk). These notions and individual concerns for safety and confidentiality are often shared across cultures, as evidenced by worldwide concerns related to the misuse, unauthorized disclosure or loss of data in connection with publicized data breaches and cyber security attacks.

Privacy is Local, Data Flows are Global — How Can Accountability Be Reconciled With Varying Privacy Legal Regimes?

It is difficult to govern cross-border data flows under any one country's laws or legal frameworks. Cross-border data flows multiply the number of jurisdictional approaches to consider accommodating. Attempting to apply and potentially layer on different and conflicting privacy obligations from various countries can impede the use of information, interrupt business operations and communications, and not necessarily advance an individual's privacy

protection. And yet we live in an era of global information exchange, so how can companies meet privacy and information security obligations when national laws differ?

While cultural notions and laws on privacy are diverse, there is widespread agreement around international data protection and information security principles. The most significant international data protection principles and information security guidelines — the OECD Privacy Principles, the OECD Security Guidelines for the Security of Information Systems and Networks and the APEC Privacy Principles — specifically anticipate cross-border data flows as a part of modern commerce and as a goal to be promoted, along with information privacy and security protection.

While the international principles are not binding, governments and economies around the world have agreed to make best efforts to implement the principles in their own practices, through national legislation and through moral suasion to businesses and other organizations. Conceptually they have become a common threshold for general privacy and information security practices regarding collection, use, retention, access, security, enforcement and maintenance of data integrity of personal information.

There is recognition that data sharing and data processing must be global to reap the benefits of an information economy. To that end, many global businesses currently comply with data privacy requirements by beginning with an internal governance policy or binding corporate rules for data handling across their enterprise. These internal business policies or rules are consistent with the concepts underlying the OECD and APEC principles, upon which governments have developed their own specific privacy laws.

Grounded upon the APEC and OECD principles as a foundation, a corporation's enterprise-wide data-handling rules can achieve basic compliance with the majority of substantive requirements that might be found in any country. A global company will tailor its general compliance initiatives (company-wide policies or binding corporate rules) by layering on additional criteria and specific obligations that arise within a particular jurisdiction or constituency in order to achieve full legal compliance, as applicable.

The operations of an Indian service provider can be designed in the same way. Service providers can adopt a foundational security and data privacy program that embraces the guidance of internationally accepted privacy and information security principles as a general base, with layers of specialized criteria as may be required to handle specific types of information in a manner that conforms with the client's information privacy and security obligations for the type and sensitivity of the data handled and with regard to applicable laws.

Using this process, a company can assess its adherence to common data management principles, including measuring compliance with specific contractual terms for outsourcing relationships. Special obligations may include requirements for data flows from the European Union (EU) or sector-specific requirements for health, financial or other sensitive industries and data types. For example, data flows from Europe are often covered by, or subject to, contractual terms approved by data protection authorities in the EU. Likewise, financial

institutions in the U.S. may specify particular security safeguards and compliance mechanisms in provisions of sourcing contracts to ensure their own compliance with U.S. banking laws.

Broad international concurrence on general principles of information privacy and security protection provides a common platform for designing compliance programs, while allowing room for acknowledgement of some diversity in local laws. International cooperation is based upon responsibility and respect for the continuing privacy obligations that travel with data as it flows globally.

Observing International Privacy and Security Principles: The APEC Privacy Framework as a Pragmatic Model for Respecting Cross-border Data Obligations

The APEC Privacy Framework, endorsed in 2003 by its Council of Ministers representing twenty-one economies across Asia, Latin America and North and South America, charts a path for respecting cultural and legal differences in approaches to privacy, while recognizing the validity of obligations and promises attached to personal data use. APEC, building on the OECD principles, specifically framed two additional privacy principles advocating protecting individuals from harm and establishing accountability for privacy obligations. With respect to cross-border data transfers, the APEC Framework encourages mechanisms for international cooperation that stress business accountability for personal information protection, regardless of where the data travels.

Alternatively, other models for data protection and cross-border transfers rely on determinations about the “adequacy” of privacy protections, based upon one jurisdiction’s judgment concerning the level of national legal privacy protections enacted by another jurisdiction. Shortcomings of the “adequacy model” include political and trade biases, as well as national procedural requirements that impede data flows and access across borders.

In practice, because of impediments to data use, the “adequacy model” often strains, and arguably is counter to, certain international privacy and information security principles that emphasize the necessity and benefit of promoting data flows for the economic development of societies and for the betterment of individuals while protecting privacy. Today, the emphasis on permitting or limiting cross-border data use solely on the adequacy of national laws also fails to take into consideration the global nature of businesses and the possibility for organizational adherence to responsible data management on a corporate-wide basis, regardless of where the data moves or is ubiquitously accessed from one or more global locations.

Thus, an Indian service provider may access EU-originated human resources data from a U.S. database in order to provide specialized services in India, while its client’s authorized employees in the U.S. and EU access the same data from the U.S. database for other purposes. The privacy and security obligations should flow with the data, and an accountability framework that emphasizes business accountability for meeting these obligations, wherever the data is legitimately accessed, can best ensure continued lawful, efficient and beneficial use of data while protecting privacy and ensuring data security.

Currently, the APEC framework is in an international implementation phase, with companies and economies working together to pilot international cooperation mechanisms for enforcement of privacy obligations. In this phase, the important role for the private sector and self-regulatory organizations in providing information privacy and security accountability has been recognized by businesses and participating economies. Much attention has been paid to leveraging self-regulatory organization models, in the first instance. Self-regulatory organizations can monitor an organization's voluntary compliance with the APEC Privacy Principles and the company's own promises and obligations. They can verify privacy compliance by organizations, seek enforcement actions for noncompliance and refer appropriate cases to government authorities for backup enforcement.

Accountability in the Outsourcing Context

In the outsourcing context, it makes sense to honor obligations that flow directly with the data according to customer specifications to a service provider. These should reflect both the client's legal compliance duties and privacy promises to consumers. Businesses must communicate these obligations to their service providers.

The DSCI should promote a practical and effective business accountability framework that will encourage privacy and information management provisions to be explicit in sourcing contracts. Clear contractual requirements will communicate data protection responsibilities of clients that are relayed to service providers:

- → Principally, outsourcing contracts must reflect the obligations that flow with the data being outsourced.
- → These contracts may reflect legal compliance obligations from the originating country for the particular data. They might also include privacy promises made to a consumer by the organization that collected the personal data for a particular purpose and that is now being shared with a service provider.
- → Specifying the obligations that flow with the data should be appropriately detailed based on the particular information shared, rather than generic references to applicable laws.
- → This may require clients to better identify the data being shared with service providers, its sources and the obligations attendant to the data, including limitations on use.
- → This approach does not require an outsourcing site, its government or self-regulatory organizations to adopt or even blend the existing variety of privacy laws or regulatory frameworks that exist around the world that would potentially layer unexpected and unnecessarily burdensome obligations upon the original transaction obligations.
- → It requires an outsourcing site, such as India, to provide guidance on responsible data management practices and procedures that honor the privacy protections and obligations of data shared by the client, as specified in sourcing transaction contractual agreements.

Examples:

- A banking organization in the U.S. that outsources account statement processing to a sourcing service provider in Bangalore would be expected, with respect to the outsourced data, to remain responsible and maintain compliance with applicable U.S. banking laws, including the privacy and security provisions of the Gramm-Leach-Bliley Act and the institution's own privacy promises.
- This would be expected to be accomplished in managing the bank's risks through appropriate contract provisions with an outsourcing service provider and appropriate oversight of compliance with the agreement.
- It would be the originator bank's obligation to set forth the contractual specifications necessary to protect the privacy and information security obligations of the data shared with the service provider.
- The Indian sourcing supplier would be obligated to honor those specified privacy obligations and should have the appropriate policies and procedures to support those requirements.

- Similarly, while under a completely different legal regime for privacy and for financial accountability, a U.K. financial services entity in the European Union that outsources account statement processing to a service provider in Bangalore would be expected, with respect to the outsourced data, to also remain responsible and to maintain compliance with applicable UK banking and privacy laws on the client's behalf, as specified by contract.
- The UK Information Commissioner and the Financial Services Authority in the UK would look to the financial institution to manage the data obligations and risks through appropriate contract and oversight mechanisms vis-à-vis a sourcing service provider.
- The service provider would be expected to honor the continuing privacy obligations attendant to the data according to the client's expectations and responsibilities.

The obligations and promises attached to commercial transaction data that includes personally identifiable information, and the expectations of an individual or client, do not disappear because the data moves to a different jurisdiction. Service providers providing outsourcing services must build in compliance processes to assure that the protections required by the obligations that flow with personal data from another jurisdiction are honored, per the expectations and direction of the organizations engaging the service providers.

THE DSCI'S SELF-REGULATORY ROLE IN PROMOTING PRIVACY ACCOUNTABILITY IN OUTSOURCING

This paper outlines four phases of the DSCI's development of an accountability framework and strategies for success. The phases are overlapping and build upon each other in an iterative manner. Across all the developmental phases of the DSCI, however ultimately defined, is a significant need for outreach and communication with the broadest circle of stakeholders. With broad input and dialogues with client, service provider, sourcing consultancy, consumer, academic and government sectors, the DSCI is most likely to achieve a balanced and pragmatic self regulatory accountability framework that will receive support from stakeholders.

The objective for the first phase is to address operational planning and governance issues for an effective self-regulatory organization. The objective of the second phase is to develop strategies for ensuring membership preparation and readiness to meet DSCI requirements. The third phase of development would establish the organization's leadership to industry as a consultant, educator and enforcer in fostering privacy and information security compliance by sourcing service providers. Where applicable, the DSCI could provide member support by defining different types of solutions to address information privacy and security issues. Finally, the objective of the fourth phase of the DSCI is to establish and promote the DSCI's likely and measurable achievements, including the benefits of transparency to gain respect and trust among all stakeholders.

PHASE 1: Establishing An Effective DSCI

DSCI Roles:

- → Define mission and accountability framework.
- → Establish a credible governance structure for the DSCI that includes independent authority to offer oversight and accountability assurance.
- → Work as a partner with government to promote a culture of trusted information management and compliance among Indian IT/services industries.
- → Initiate information privacy and security outreach and awareness building among DSCI's potential membership and relevant constituencies.

The Mission of the DSCI

The mission of the DSCI is to improve the trusted position of Indian companies as global sourcing service providers through privacy and information security awareness and capacity building and the development of a voluntary business accountability framework.

The mission also involves monitoring compliance and enforcement of information privacy and security that will require organizations to be accountable for obligations that are attendant to personally identifiable data that they use. The obligations that flow with the data should be

responsibly honored as specified and agreed to, providing consumer confidence and customer satisfaction in the treatment of data by outsourcing service providers in India.

DSCI Mission Calls for Broader Roles

Designing and then monitoring compliance with an accountability framework is an important and central role for the DSCI. It does not, however, ensure that at the advent of the DSCI's launch its members will actually have effective information privacy and security programs.

It should be expected that some companies that currently provide business processing operations in sourcing transactions are unlikely to be uniformly sophisticated about information privacy and security best practices or to actually have an information privacy and security management program in place. Even large, well-established companies with existing safeguards programs may be required to upgrade or retool their programs, policies and procedures in order to qualify for membership in the DSCI or particular certifications.

Expecting compliance without significant education and training of membership candidates over a horizon of time may be unrealistic and could quickly draw criticism for the DSCI effort. It would be detrimental if the DSCI membership process or data management practices of members are called into question in the early, start-up phase of the Data Security Council. Therefore, the role of the DSCI from its very beginning should be service oriented beyond compliance and enforcement. The DSCI should serve as an information privacy and security awareness builder, educator, consultant and competence builder for its membership base, with outreach to potential members and relevant constituencies from its very beginning.

Capacity Building

The public success of the DSCI completely depends upon its ability to generate committed members that wish to voluntarily comply with DSCI policies. Success also depends on the DSCI membership being duly qualified and ready to ably participate under a self-regulatory framework for privacy accountability.

Capacity building by the DSCI in all areas of information privacy and security accountability for the target audience of small, medium and large sourcing companies will be necessary so that businesses will be ready to meet membership criteria premised on some existing level of capabilities, policies and practices for privacy oversight. They will need to be able to demonstrate that they can functionally comply with the DSCI's accountability framework. Sourcing clients and consultancies may also benefit from awareness and capacity-building efforts of the DSCI so that they are better able to 1) specify the obligations that service providers must honor for information privacy and security, and 2) plan for appropriate oversight mechanisms for the relevant sourcing contract provisions.

The DSCI accountability framework should recognize a foundational level of privacy and information security protection generally necessary for outsourcing service providers. Highly specialized businesses and service providers that handle more sensitive data, such as health and financial data, may require particularly thorough awareness training and assistance

in meeting more specialized and demanding certification requirements that reflect the sophistication of their businesses and the risks of harm to individuals from a potential misuse or unauthorized access to personal data handled by the service provider.

To be effective as a trust agent on information privacy and security, DSCI needs to have a robust mission. Focused and achievable phased goals should be planned that include outreach and awareness building among the business community, continuing education and assistance to potential membership, and forging partnerships with key government agencies. These goals should further include the development of an accountability framework and implementation efforts that include active coaching and consultations with member companies on the fullest range of privacy and information security compliance issues. These could include workshops and tutorials on strategic planning for physical, administrative and technical security of operations based on sector-specific standards and best practices, which vary based on the sensitivity of data and on specific data-processing activities and uses.

Operational Considerations for the DSCI

Organization

Like many other privacy and nonprivacy self-regulatory organizations, the DSCI is best served by organizing itself in a manner that will allow the DSCI flexibility to receive revenue from as many sources as possible that are compatible with its mission and strategic goals, now and in the future. Such sources could include budgetary contributions by a parent body (NASSCOM); grants from government, universities, and foundations and corporations; voluntary contributions from individuals and from the business community; potential sales of products or services; and through fees for membership and organizational events and conferences. The DSCI would benefit by guidance from local counsel, such as Amarchand Mangaldas & Suresh A. Shroff & Co., on the administrative legal requirements for its organization and in structuring activities in compliance with Indian law.

To be cost effective, the DSCI needs to plan for how its oversight processes may be scaled to small, medium and large business demands and to find revenue models that will assist such leveraging. One of the greatest challenges to the viability of self-regulatory organizations that oversee information privacy and security is to be able to nimbly retool and update means of assuring that business members are complying with applicable accountability frameworks and privacy promises and obligations, particularly as technologies and business models change. The use of technology or software solutions may aid oversight, but investment capital may be needed to take advantage of scalable solutions to privacy oversight.

Outsourcing parts of the compliance oversight function to other third-party trust agents or verification services, such as independent auditors or privacy seal programs, may be possible at the member company level. The credibility of the DSCI itself, however, will depend upon its professional competence to review, monitor and enforce compliance directly.

Certain self-regulatory organizations have been able to extend their competencies by partnering with other organizations on a functional or project-by-project basis, particularly

on privacy outreach, education, consultation programs and certain compliance aids. Notwithstanding, plans should be developed to credibly staff and carry out those functions. Strategic planning is crucial so that even a nonprofit charitable organization can chart a course for building capital reserve funds to better meet and implement core functions and long-term strategic goals.

Ancillary revenue programs are often undertaken, particularly where membership fees may not cover all of a self-regulatory organization's operating expenses. Successful organizations have used annual or biannual conferences of their membership and other interested parties as a means of generating operating funds, as well as by offering access to member-only web-based resources for a periodic fee. Legislation or regulatory initiatives of government that promote business use of information privacy and security self-regulatory organizations or other independent assurance and verification agents also can assist in strengthening the market for DSCI membership. They would elevate the importance of information management on a national level.

Planning for renewable and viable funding sources that reinforce the business case and value of the DSCI to stakeholders should be part of the DSCI's initial business plan and budget analysis, reviewed at least annually.

The Business Case for DSCI Membership and Voluntary Compliance by Industry

The DSCI has a pivotal role in shaping responsible compliance goals and trusted information management competencies among its membership. Necessarily, information security should be a primary focus for full privacy protections of data that flows to business processing operations and other service providers in India.

Given sensitivities to adverse criticism on data breaches and other conduct that can create privacy harms, businesses have an interest in separating themselves from bad actions or actors. They will benefit by becoming aligned publicly with prudent and verifiable data risk management practices that will be promoted under the auspices of a trustworthy, independent DSCI.

Participation in the DSCI by businesses should be advocated and appealing to service providers for three reasons:

- Confidence that the DSCI and its processes will provide needed guidance and information on privacy and security issues to assist in increasing the expertise and credibility of the outsourcing industry;
- Association with the DSCI will enhance trust among clients and consumers and provide financial, regulatory and market benefits through a member's public certification and compliance with the DSCI's accountability framework, as well as active participation in outreach programs; and

→ Likelihood of higher internal company compliance with information privacy and security best practices because of the DSCI's independent verification of compliance, ability to sanction members and referral authority to key government agency partners for backup enforcement following self-regulatory enforcement efforts.

The cost-benefit analysis for business will also include a fairness component regarding membership fees. Many self-regulatory organizations scale their fees to the asset size of an organization and/or to the complexity of the organization and the number of business lines for which information privacy and security reviews and oversight will be required.

DSCI Governance

The Role of the Board of Directors

Governance is perhaps the most crucial issue to any organization's success. This will certainly be true for an independent self-regulatory organization whose mission is to publicly raise the privacy accountability of its member organizations in their collection and use of personally identifiable information.

A strong board of directors and governance model is recommended, with a diversity of members from clients that outsource data to service providers, as well as including representatives of BPOs, academic, nonprofit association and legal experts, and independent directors. A board, as well as potential advisory committees to the board, made up of members with functional backgrounds in technology, privacy, data security, consumer protection, financial services, health care administration, law or other governance structures, will inform decision making on DSCI core missions and programs.

Of greatest value to the credibility of the DSCI and the effectiveness of the board itself will be balance of the board's composition and the melding of member backgrounds, such that areas of substantive and qualitative expertise can be blended and applied knowledgeably to the actual operations of global sourcing suppliers. Reviewing privacy and information safeguards in the BPO context will not be a theoretical exercise, but rather will require practical applications and reviews undertaken in consultation with industry representatives who will apply the DSCI's accountability framework to specific business operations.

Privacy protection is contextual and it is extremely important to include among members of the board representatives from the sourcing community with expertise that spans a variety of business processing operations. Including strong and independent members on the board of directors is also important in populating a responsible governing body. The credibility of their participation will be elevated by demonstrating their substantive or technical expertise to guide the DSCI mission in the context of specific oversight of privacy accountability in the global sourcing context.

Board Responsibilities

In constructing the governance structure and operational management of the DSCI, beginning with the board of directors, every effort should be taken to optimize public perceptions of the

DSCI's effectiveness and impact from the start. Pragmatic optimism at the initiation of any organization is important in visualizing its success and in forecasting realizable achievements. To that end, having confidence in the DSCI's recruitment of an energetic and knowledgeable board is important.

Following the recruitment of a balanced and knowledgeable board, realistically tailoring the responsibilities of the board will be necessary to best utilize members' special leadership capabilities within the time they are likely to allot to board duties. In planning for realizable achievements, the Center recommends caution in relying too heavily on a board of directors for authorship of the strategic planning, policy development or operational responsibilities for core DSCI functions. Even the most active board of directors is unlikely to operate as the functioning staff of the DSCI.

Key Staff

The president/chief executive has the guiding role for strategic planning, policy development and operationalizing the DSCI functions. It is the president's role to provide the board with proposals under each of these areas for endorsement, modification, adoption and further direction to DSCI staff for their implementation. But, the president will need sufficient and senior-level staff that has demonstrated experience in the privacy and data security space, as well as with compliance and risk management capabilities generally, to fully meet those objectives. The staff will need to understand business processing operations and IT technologies facilitating sourcing services. A staff member experienced in data handling or risk management attendant to financial services or health administration services could be particularly useful.

The role of staff, as in most organizations, should be focused on supporting the president of the organization and serving the membership, while being responsive to the board of directors. A deputy administrator position under the president could provide significant value in coordinating DSCI implementation efforts and issues that cross lines and areas of staff expertise.

Given the specific nature of the DSCI's mission, to raise the standards for information privacy and security among a membership of suppliers of outsourcing services involving information technologies, staff resources should reflect technical understandings of data systems, software and technical privacy and security solutions. Furthermore, since the nature of the services provided by the membership is necessarily global, the importance of having a policy specialist dedicated to legal and global privacy public policy will be key in liaising with international and domestic government representatives, organizations, international advisors and key industry sectors with regard to special data management issues around the globe.

Key DSCI staff positions will likely need to include the following roles and expertise as the DSCI matures and is able to expand its staffing:

→ President/Chief Executive Officer

- Deputy Administrator — Vice President
- Member Services and Communications
- Education and Outreach
- Data Privacy and Security Policy (perhaps separate senior advisors)
- Compliance and Enforcement
- Business Operations — Internal Audit and Finance
- Privacy Technology Specialist
- Global Privacy Policy Specialist — Domestic and International Issues

Strategic planning, policy and program development should be provided to the DSCI by competent staff and consultants/contractors approved by the Board. If staffing resources or funding for contractors for the DSCI are limited at the start-up phase, then the President would be advised to leverage private-public partnership resources. An example of this is by building alliances with private sector Centers of Excellence located in India for assistance with outreach, education and training, and policy and program development.

Similar support could be sought from universities and other educational institutions. In the area of data security, the ISC, which certifies training programs for information security professionals worldwide, provides international resource information online that highlights several high-functioning data security programs at educational institutions in India with which the DSCI could build alliances. Rotational staff contributions from the private sector or via international exchanges with existing privacy self-regulatory organizations also could be explored.

DSCI Accountability Framework — Eligibility for Membership

The DSCI seeks to have maximum influence and impact on the positive reputation of software and service providers in India for information privacy and security accountability. The hallmark of accountable action by outsourcing service providers will be responsibly honoring existing privacy obligations that travel with the data across borders in accordance with the specifications of their clients. This will need to be done in a manner that elevates and respects applicable international privacy principles as they have evolved, particularly through the APEC Privacy Framework that focuses on protecting individuals from harm and requiring organizational accountability for privacy duties and promises.

To enhance the level of awareness, interest and capabilities of all BPOs and sourcing service providers in India, an accountability framework should be developed that encourages and permits early and broad participation as DSCI members. Just as the DSCI itself will have phases of development, the DSCI should consider an accountability framework that will be iterative in its development. The framework should be flexible enough so that small, medium and large businesses will be able to credibly participate.

Marking Eligibility to Implementation of Information Privacy and Security Procedures and Practices

A less resource-intensive, achievable and credible accountability framework could begin by marking membership criteria to the implementation of privacy and information security procedures and practices, rather than adherence to a specific code of conduct. Mindful of general international privacy and information security best practices and principles already discussed in this paper, the DSCI could encourage member education and the development of company processes to specifically address data privacy, security and protection. The benefit of this model for early membership development is that it does not preclude expansion of membership criteria to a formal code of conduct in later phases of DSCI development, following awareness and capacity building among business members.

An adaptable approach for member candidates to undertake responsible privacy and security risk assessments and strategic planning will, in the short term, likely encourage greater business participation by allowing businesses to suitably design their data management and protection efforts successfully. Widespread adoption of mechanisms for ensuring information privacy and security at the company level will also most concretely advance the long-term mission of the DSCI for actualizing data security and trusted information practices.

DSCI Vets Procedures and Practices

The DSCI should consider how it can flexibly support business models that demonstrate business accountability processes for protecting personal information by any size or sector of service providers for sourcing transactions. The DSCI could vet the sufficiency of information privacy and security processes, including self-assessments, self-audits and other self-certification models developed by businesses.

This type of membership process and review is similar to effective seal program criteria used internationally by privacy and consumer protection trust agents. For larger global companies this might include the review of a business's binding corporate rules for data management and protection enterprise-wide. This approach to developing and certifying that processes and procedures are in place and results are measurable against benchmarks relevant to the particular business may be particularly attractive to small and medium-size enterprises that might otherwise find proscriptive requirements to be economically or operationally unfeasible.

At the same time, the accountability framework would not preclude larger or specialized service providers from demonstrating the rigor of their information privacy and security management practices by engaging a third party to independently verify the quality of their safeguards or by seeking formal certification under particular standards, such as the ISO 17799 security standard. Nor would it preclude DSCI investigations or spot checks, but those could be tailored to where scarce DSCI resources could be used best.

Membership Criteria

The DSCI accountability framework could set baseline membership criteria on responsible practices, such as the following:

- Appointment of a responsible person for information privacy and security management;
- A business's self-assessment or certification of data privacy and security risks;
- A privacy policy concerning the treatment of personal data;
- An information privacy and security management plan that includes physical, technical and administrative controls for information privacy and security;
- Mechanisms for contract and compliance oversight;
- Personnel management, including training, employee vetting and access controls to data systems;
- Other information privacy and security procedures and process criteria, such as compliance with any sector codes or frameworks, as appropriate for more specialized or sensitive data; and
- A complaint resolution process.

DSCI oversight for member organizations would be proportionate to the level of accreditation necessary for the organization to handle certain data, to service particular sectors, or that they voluntarily seek in order to differentiate themselves in the marketplace based upon superior privacy and data security protocols. It is not recommended that the DSCI validate the information assurance levels of companies, but the DSCI can provide verification of external security accreditation.

Using this flexible model, marking membership criteria to the steps necessary for effective information privacy and security, it is also recognized that contracts between an outsourcing client and a service provider may take on high prominence in outlining information privacy and security obligations. Thus, business demonstrations of their mechanisms for monitoring implementation of specific controls and compliance with outsourcing contracts could be a primary criteria for review by the DSCI.

Liaison Services with Clients and Third Parties

It is recommended that the DSCI consider establishing some formal mechanism to liaise with privacy officers or customer relationship managers from companies that actively outsource services to India. A process should be designed that assists the DSCI in concretely understanding privacy concerns and issues that clients' consumers and the clients themselves may have concerning data handling in sourcing transactions. This will assist the DSCI in identifying industry weaknesses and privacy risks so that they can be addressed with guidance

to members, additional compliance oversight, changes to the accountability framework or other responsive action.

DSCI outreach should include client organizations, relevant trade associations and sourcing consultancies. The DSCI might benefit from a formal or informal advisory body representing sourcing client interests. Additional benefits to clients and other third parties could be DSCI verification of the status of service providers as members and their areas of expertise.

Another valuable service to clients and member companies would be the development of a DSCI assistance program for dispute resolution. At a minimum, the DSCI could serve as a reference point between individuals and companies to service provider representatives responsible for privacy and data security issues and dispute resolution at their respective companies. The DSCI could also provide a meaningful service to member Indian companies by providing a connection to the fullest range of Indian and non-Indian companies that provide dispute resolution or independent third-party services that assist with resolving public and client complaints. These could include mediation services, alternative dispute resolution, seal programs or other independent contractors.

Furthermore, since many service providers themselves depend upon subcontractors for certain services, the DSCI could play an important role in considering issues that address the practices related to the ecosystem of sourcing service providers, including subcontractor accountability and information quality control.

Government Endorsement — Enforcement Referrals from the DSCI as Priority Government Cases

Asserting the DSCI's compliance and enforcement authority is among the most powerful and practical means of gaining respect and credibility for the role of the DSCI as a trust agent in assuring compliance with its accountability framework and members' privacy promises and obligations. The ability to demonstrate dispassionate and meaningful enforcement action at the DSCI level, as an independent self-regulatory body, is quite important. This includes making any necessary referrals — criminal or civil — to government authorities, following self-regulatory efforts.

Many self-regulatory organizations and frameworks have benefited through respected partnerships with government oversight bodies. An important way of demonstrating the "teeth" in a self-regulatory compliance and enforcement framework is for the public to see that when an organization makes a referral to a government agency, the government agency will treat a referred case as a priority. This has been the case in numerous successful self-regulatory frameworks in the United States. A few examples include the National Advertising Division's (NAD) compliance framework (under the Council of Better Business Bureaus), where the U.S. Federal Trade Commission, the Food and Drug Administration, the Transportation Department and several other agencies immediately move NAD-referred cases to the front of the line for consideration; the Children's Online Privacy Protection Act; and the U.S.–EU Safe Harbor

Framework. Examples also can be found in Canada, Singapore and Australia, among other countries.

Early agreement by the government to work closely with the DSCI on referred cases, and a public statement to that effect, will provide credibility to the DSCI's enforcement authority. It will also demonstrate the availability of workable backup enforcement by the government on select cases.

There is certainly precedent within the Indian government for promoting the protection of cross-border data flows in the e-commerce context. In 2003–2004, India signed on to a cross-border enforcement effort with the U.S. Federal Trade Commission and other countries around the world to fight cyber crime and spam by closing open and vulnerable entry points in networks. India's Consumer Affairs Ministry agreed to educate businesses and to give priority to cases emerging from the cross-border cooperative effort. The same high-level endorsement of the DSCI by appropriate regulators, particularly through a prioritization of enforcement cases referred by the DSCI, would serve to underscore the national commitment to support information privacy and security accountability in India's outsourcing services market.

PHASE 2: Getting Companies Ready for Membership

DSCI Roles:

- → Build privacy and security capacity for potential member companies so that they will be ready to meet DSCI requirements. This activity can include serving as a consultant or facilitator of consultancy services to members.
- → Encourage and facilitate the communication of information privacy and security obligations (including contractual) between client organizations and outsourcing service providers.

Understanding Information Privacy and Security — Assurance Models

As discussed at some length previously in this paper, in order to ensure a successful DSCI experience, privacy and security awareness building will be necessary. Additionally, it is anticipated that potential members will need assistance and shepherding through the membership application process. The application itself should be designed to help an organization appreciate fully what will be necessary to demonstrate compliance with the accountability framework and the membership contract agreement.

A program to assist potential members will want to address DSCI expectations, as well as possible compliance requirements that are not set forth in the accountability framework. For instance, the DSCI may wish to assist potential members with understanding their options for self-certifying compliance, undertaking a self-assessment on privacy and security safeguards, and perhaps sharing model templates or discussing other independent assurance models that might make sense for an entity depending on the size and nature of the activities of a potential member.

Given that some industry members specialize in services to particular sectors, including health administration and financial services, a basic understanding of privacy accountability linkages to law will be helpful. Providing a background in types of laws that may be pertinent, such as, by example, the Gramm-Leach-Bliley Safeguards Rule and GLBA privacy provisions, U.S. requirements on service providers under the Bank Service Provider statute and HIPAA, will illustrate frameworks that might apply to particular sectors.

A general understanding that legal obligations may exist could assist service providers and their counsel in dialogues with clients, so that contract provisions are developed in a manner reflective of legal obligations that originate with data in financial or health transactions and that carry a continuing regulatory compliance obligation. Certainly other examples under the laws of other countries would also be helpful resources.

Building in Security Standards

A central function of the DSCI will be to promote company implementation of security safeguards. During the awareness-building and membership phase of the DSCI, the DSCI can provide a valuable service by guiding companies in determining appropriate security safeguards. This can be done by sharing available security standards that are applicable to particular circumstances or lines of business, providing guidance on the range of security assessments and tools for verification of technical and other safeguards, and educating companies more generally about the need for physical, administrative/policy and technical security measures.

The importance of educating members on best practices and the basics of implementing an information security management system for their enterprise, a security risk-management planning concept with which some companies may not be familiar, is a fundamental first step to an organized framework for conducting an information security assessment and plan. A helpful international model is the Code of Practice for Information Security Management, adopted in 2005 by the IT Subcommittee of the International Organization for Standardization (ISO), ISO/IEC 17799: 2005 (ISO 177999).[2]

ISO 17799 is the best-known international standard for creating a business-wide information security management system. The standard can be a referential starting point for businesses. It represents a comprehensive global standard for assessing a business's security risks. The security standard outlines considerations for effectively managing those risks through the implementation of various deterrent, preventative, corrective and detective types of controls. The ISO 17799 standard is generally consistent with other security standards and can be flexibly used across industries and business lines to assess security vulnerabilities and plan for controls to prevent or mitigate a broad range of possible security risks.

2 As an aside, since 2004, ISO also began considering the need for privacy standards, beginning with a discussion and working group to consider a technology-specific privacy standard for biometrics. ISO has not moved forward with any particular privacy standard but has set up a broader and separate international privacy working group to consider privacy issues more broadly and to consider the standards issue.

While there is no one-size-fits-all information security management system or standard applicable to every type or size of business processing operation or other service provider business, ISO 17799 offers guidance that can be generally instructive. It also may be applied in conjunction with industry specific guidance.

ISO 17799, is a detailed security standard. Some organizations seek independent certification that they comply with the standard and use it as a market differentiator in competing with other companies within particular sectors (see ISO 27001 — requirements for establishing, implementing, maintaining and improving an information security management system, for which an organization may seek formal certification of ISO 17799 compliance). Other organizations choose to comply with some or all of the guidance as a means of benchmarking their existing and ongoing security management practices, but do not seek independent verification by a third-party auditor. Still others might review ISO 17799 as a menu from which to choose to test and address particular security risks and controls as reasonable and affordable, considering the size of a company, the sensitivity and volume of data it handles, what functions it performs, and the mediums it uses to collect, receive and possibly share personal data.

The ISO 17799 security standard, which outlines specific security measures to address and control risks, is organized into ten major sections each covering a different topic or area:

1. Business Continuity Planning

Identifying and addressing controls to counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters. These may include incident management responsibilities and procedures.

2. System Access Control

Addressing risk management through: 1) controls for access to information; 2) preventing unauthorized access to information systems; 3) ensuring the protection of networked services; 4) preventing unauthorized computer access; 5) detecting unauthorized activities; and 6) ensuring information security when using mobile computing and telenetworking facilities.

3. System Development and Maintenance

Addressing security risk management and implementing controls that will: 1) ensure security is built into operational systems; 2) prevent loss, modification or misuse of user data in application systems; 3) protect the confidentiality, authenticity and integrity of information; 4) ensure IT projects and support activities are conducted in a secure manner; and 5) maintain the security of application system software and data.

4. Physical and Environmental Security

Addressing measures to: 1) prevent unauthorized access, damage and interference to business premises and information; 2) prevent loss, damage or compromise of assets and

interruption to business activities; and 3) prevent compromise or theft of information and information-processing facilities.

5. Compliance

Identifying effective compliance mechanisms to: 1) avoid breaches of any criminal or civil law; statutory, regulatory or contractual obligations; and of any security requirements; 2) ensure compliance of systems with organizational security policies and standards; and 3) maximize the effectiveness of and minimize interference with a system audit process.

6. Personnel Security

Providing guidance and controls to: 1) reduce risks of human error, theft, fraud or misuse of facilities; 2) ensure that users are aware of information security threats and concerns; 3) ensure that users are equipped to support the corporate security policy in the course of their normal work; and 4) minimize the damage from security incidents and malfunctions and learn from such incidents.

7. Security Organization

Addressing security risk management and implementing controls that will assist in: 1) structuring the management of information security responsibilities within a company; 2) maintaining the security of organizational information-processing facilities and information assets accessed internally and by third parties; and 3) maintaining the security of information when the responsibility for information processing has been outsourced to another organization.

8. Operations Management

Addressing security risk management by outlining mechanisms and controls to: 1) ensure the correct and secure operation of information-processing facilities; 2) minimize the risk of systems failures; 3) protect the integrity of software and information; 4) maintain the integrity and availability of information processing and communication; 5) ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) prevent damage to assets and interruptions to business activities; and 7) prevent loss, modification or misuse of information exchanged between organizations.

9. Asset Classification and Control

Outlining appropriate protection of corporate assets and controls to ensure that information assets receive an appropriate level of protection.

10. Security Policy

Providing management direction and support for information security through a strategic and comprehensive written plan, outlining organizational goals.

The ISO 17799 security standard is consistent with the high-level guidance provided by the OECD in 2002 in its revision of the OECD Guidelines for the Security of Information Systems

and Networks. Those high-level guidelines emphasize awareness building, as well as the need for security measures that are tailored to the sensitivity of the information held and used and the possibility of harm to individuals through misuse, unauthorized disclosure or disruptions to the integrity of the data. The OECD Security Guidelines also emphasize that security management is an iterative process and that physical, technical and administrative safeguards should be reviewed periodically and changed as circumstances require.

A sampling of other third-party standards and guidance for security include the ISSA GAISP: Information Systems Security Association Generally Accepted Information Security Principles; NIST SP 800-14: U.S. National Institute of Standards and Technology/Generally Accepted Principles and Practices for Securing Information Technology Systems, as well as other NIST guidance for security of data on particular technologies; ISACA COBIT: Information Security Audit Control Association's Control Objectives for Information Technology; CISSP CBK: Certified Information Security Professional Common Body of Knowledge; and other ISC online resources.

A One-Size-Fits-All Security Standard Does Not Exist

Companies that provide outsourcing services should implement appropriate information security for their operations, while recognizing that a one-size solution will not fit all companies. For this reason, there is no single set of existing security standards or principles that would be appropriate for all service providers, although ISO 17799 and industry-specific guidelines provide helpful models from which businesses can consider their enterprise information security risks in order to tailor an appropriate information security management policy and safeguards.

The safeguards should implement information security as required to meet contractual obligations to a client. These may include security promised in a company's privacy policy, as promised by the client to its consumers, and in light of what is reasonable due to the sensitivity of the information held and the possibility of harm from misuse, unauthorized disclosure or compromises to the integrity of data through malfeasance, negligent handling or a breach.

Security Measures Through the Systems Development Life Cycle

As technologies used by a business for processing information change, so should security plans. For instance, information security risk assessments and controls should be factored into any new technology deployments by a company at significant junctures along a systems development life cycle — from concept planning, to procurement, through piloting technology, to deployment, and the review of an information system's programmatic effectiveness.

Security As an Iterative Process

Providing for information security safeguards must also be communicated as a repetitive, iterative process, with adjustments made after a period of time and review of the effectiveness of physical, technical and organizational policies and procedures. As business processes and risks change, so must security responses.

PHASE 3: DSCI as Consultant, Educator, and Enforcer

DSCI Roles:

- → Continue serving as a consultant or facilitator of consultancy services to members.
- → Monitor and enforce compliance by members; assist members as a liaison to dispute resolution services; as appropriate, refer certain matters for backup government enforcement.

Consultant Services and Continuing Education

As noted earlier, the DSCI may provide overlapping services through its various phases. The third phase of the DSCI will be one of continuing activity, providing direct or indirect consultant services and continuing education to members; helping them navigate compliance requirements, new privacy and data security challenges that may arise; changing privacy obligations with new business lines; and meeting the need for continuing education of employees that is tailored to their roles and responsibilities within a BPO.

For many members, the need for ongoing capacity building will continue for some time. And beyond initial awareness building of information privacy and security, the DSCI has a continuing education and training role to assist companies in keeping current on best practices and procedures.

Consultation on information and privacy management will need to be a DSCI core competency. Building out this feature will require transparent dialogues throughout the DSCI building process, creating trust and a sense of progress among stakeholders.

Enforcement

As discussed above under the DSCI's Mission and PHASE 1, clarifying the DSCI's enforcement authority and the range of sanctions it will exercise, as well as the types of referrals it will make to government enforcers, will be key to the perceived strength of the organization as a trusted agent for information privacy and security accountability.

Responses to Complaints

Given the limited resources for the DSCI and most self-regulatory organizations, enforcement actions are most likely to arise as the result of a complaint against a member company. It is also most likely that the DSCI will be addressing business-to-business complaints, in the main, between an outsourcing client and a sourcing service provider; a complaint from a competitor service provider for a breach of privacy and information security obligations, promises or representations; or even perhaps responding to a dispute arising between a sourcing service provider and a subcontractor relating to privacy and security obligations. On particular occasions the DSCI might receive a complaint directly from a consumer or other interested party, seeking investigation of a service provider's practices and actions, and possibly redress or remediation for a harm alleged.

In the first instance, with regard to all complaints, it is recommended that the DSCI direct the complaint and complaining party to the service provider company's privacy and information security complaint resolution program. As described earlier, a valuable service to member companies would be the development of a DSCI assistance program for dispute resolution. At a minimum, the DSCI could serve as a reference point between individuals and companies to service provider business representatives responsible for privacy and data security complaint resolution at their respective companies. If the complaint cannot be resolved at the company level between the parties, then the DSCI may become involved.

Below are three models to consider for resolving complaints and initiating enforcement actions.

Model 1:

The DSCI could provide a meaningful service to member Indian companies by providing a connection to the fullest range of Indian and non-Indian companies that provide dispute resolution or independent third-party services that assist with resolving public and client complaints. These could include mediation services, alternative dispute resolution, seal programs or other independent contractors. If the parties reach a mutual agreement on a resolution, there would be no more activity by the DSCI.

Model 2:

At any point following referral to a member company's dispute resolution process, if unsuccessful at that juncture, the DSCI could investigate the complaint and directly try to resolve the complaint. The DSCI could mediate between the two parties or, if warranted, request that a member company change certain practices or provide remediation or redress for a harm suffered because of a breach of a privacy or security obligation, promise, or representation. Failure of a member company to implement requested changes or remediation could result in public suspension, termination, or nonrenewal as a DSCI member, as well as possible referral for further enforcement action by a government agency for civil or criminal investigation, if warranted. Nothing in this process would preclude a complaining party from seeking court or government agency resolution of a complaint if the member company failed to agree or follow through on corrective action required by the DSCI. Referrals to government authorities for back stop enforcement efforts would not be the general course, but could be initiated after an opportunity for a member company to resolve an issue at the DSCI level.

Model 3:

The DSCI, for a fee, could allow the complaint to be filed as an administrative court-like case with the DSCI staff, providing full due process and substantive rights to both parties, as well as a route for appeal to the board of directors of the DSCI. This model fully accommodates natural law rights that may be required in India for valid, final resolutions of disputes. The DSCI may benefit from consultation with local counsel, such as Amarchand Mangaldas & Suresh A, Shroff & Co., on local requirements for nonjudicial dispute resolution processes.

Model 3 is successfully used by the National Advertising Division affiliated with the Council of Better Business Bureaus. The model provides an additional industry self-policing element to the self-regulatory organization's enforcement authority, for it is anticipated that most complaints will be between businesses rather than between a consumer and business party. Industry members could choose to police their own activities and opt for this administrative route, rather than a court action because it is less expensive and a dispute is likely to be timelier resolved.

Under Model 3, a complaint would generally be filed by a business (outsourcing client) against a member service provider. DSCI staff would be assigned the case and would act like an administrative court judge, providing for full notice to the parties on the alleged violation of a privacy or security obligation. Under this model, parties each submit written arguments and offer any proof of their claims or defenses. Each party has an opportunity to respond to the other's arguments.

After submission of all pleadings and responses to DSCI staff for additional documents or other information or testimony, the staff makes a written determination about whether a privacy obligation, promise or representation was breached. If the finding is affirmative, the DSCI staff makes a written recommendation to the member company concerning how to voluntarily resolve the complaint. The member company files a written reply and either agrees with the resolution suggested for voluntary compliance with DSCI policy (generally expected to be the case) or appeals the DSCI determination and resolution suggestion. Should the member company not win its appeal to the board of directors of the DSCI, it must choose to either voluntarily comply with the DSCI and BOD determination and resolution suggestion, or its membership can be suspended or terminated and the complaining party can proceed further to the courts for redress. The DSCI also can refer the member company for government backup enforcement action, if deemed appropriate.

In the case of the NAD, under the Council of Better Business Bureaus, approximately 130 to 150 cases are resolved annually and move through the hearing system expeditiously. Member companies agree to this procedure and the determinations of the DSCI staff hearing process and BOD appeal process as a criteria for membership in the organization. The process is completely confidential during the complaint filing and hearing phase, but the results are made public at the conclusion of the process. When referrals are made by the NAD to the U.S. Federal Trade Commission for backup enforcement action against a noncompliant member company, the Federal Trade Commission responds by prioritizing the case, adding teeth to the private-public partnership and enforcement arrangement.

Consideration could be given to any of these models. In Model 3, monetary sanctions for actual pecuniary harm suffered from a privacy or data breach could be levied against a member company for the benefit of the outsourcing client, because both parties have opted for the administrative procedure rather than other legal redress means. Otherwise, Models 1 and 2 provide only for suspension, termination, or nonrenewal of DSCI membership and the possibility of a referral for government enforcement as DSCI sanctions.

Transparency

In addition to actually taking enforcement actions, many successful self-regulatory organizations have gained added credibility by making enforcement actions public. Transparency, in conjunction with a strong partnership with backup government enforcement agencies to which both civil and criminal cases could be referred, may provide the greatest lift in the public eye for the strength and robustness of actual enforcement under the DSCI framework.

Some self-regulatory organizations have publicized their compliance and enforcement actions through press releases, through annual reports that are made public, or using a combination of methods, including voluntarily reporting of aggregate summaries of cases and outcomes with or without identifying the parties to a dispute. In the latter example, this has occurred where a model similar to Model 3 above is utilized. Case results serve as precedents for other self-regulatory actions and carry some weight with an appropriate government enforcement agency. Generally there is a charge to interested parties for access to online web resources, for instance, for access to reports on NAD cases.

Referrals for Backup Government Enforcement

Limiting enforcement referrals to potential criminal activity may be deemed weak where the potential for actionable offenses in servicing commercial transactions could more frequently arise through violations of civil contract, consumer protection or regulatory rules. A perceived reticence to make enforcement referrals to the government could adversely affect both the needed independence of the DSCI and its reputation as a reliable trust agent for information privacy and security protection.

At the same time, clearly it should be the demonstrated intention of the DSCI to actively encourage self-regulatory resolutions to complaints on information privacy and security deficiencies. Those efforts should begin through dispute resolution and redress programs at the company level and then may be escalated to the DSCI. Referrals to government authorities should not be a general means of resolving complaints, but truly a backstop measure. DSCI members should be given an opportunity to correct and remediate a problem prior to referral for government action by the DSCI.

It is recommended that the DSCI actively build positive working relationships with the Ministry of Communications and Information Technology (IT Ministry), the Telecom Regulatory Authority of India (TRAI), and the Ministry of Consumer Affairs, Food and Public Distribution (Consumer Affairs Ministry), in addition to criminal law enforcement and other relevant government divisions. The DSCI should begin engaging government officials with DSCI members to advance best practices. When deemed appropriate and necessary, as a backup enforcement measure the DSCI may make appropriate civil or criminal enforcement referrals to appropriate Indian government agencies.

PHASE 4: India IT Sourcing as a Trusted Information Management Sector

DSCI Role:

- Establishing targets and proposed timetables for achievement of the DSCI's goals — central among them, the education and development of India's own information privacy and security management sector.
- Communicating industry initiatives and successes.

Through a building-block approach, the DSCI should be in a position to report on progress made during and after each phase of its early development. The success of its outreach efforts and privacy advocacy should be measurable in terms of:

- DSCI outreach and events promoting safe and accountable practices around cross-border data flows for global sourcing transactions;
- New members joining the DSCI;
- Successful compliance by members with the DSCI accountability framework;
- Quantifiable compliance reviews, enforcement cases and enforcement referrals;
- Government support for the DSCI, including enforcement partnership progress;
- Evidence of an emerging information security and privacy management sector in India to sustain continuing high standards;
- International acknowledgement of the DSCI's leadership role on information privacy and security accountability; and
- Retained trust and market share by India in global sourcing competition.

CONCLUSION

NASSCOM and the DSCI have a unique opportunity to shape realistic and achievable benchmarks for safeguarding personal information and applying the highest privacy accountability practices to cross-border data flows that are necessary for global sourcing. Setting a framework that requires service providers to honor the data privacy and security obligations that flow with the data is a pragmatic approach, endorsed in international privacy principles and achievable through end-to-end business accountability.

There are steps along a continuum of DSCI roles and development that will assist its membership in being prepared for success and meeting client expectations for accountable data management and security. Compliance by member companies is achievable.

If well implemented, probabilities are high that the DSCI, with corporate and government endorsement, will assist a developing sector of information privacy and security managers

to promote continuing adherence to the DSCI's voluntary accountability framework for responsible management of data in global sourcing.

CIPL and USIBC and its member companies appreciate the invitation to provide guidance and support to NASSCOM and the DSCI in its implementation of a significant international information privacy and security accountability undertaking. The DSCI's work can build a lasting reputation for India as a trusted environment for outsourcing services.