DSCI-BSA STUDY

SECURITY CONSIDERATIONS IN SOFTWARE PROCUREMENT BY GOVERNMENT AGENCIES IN INDIA

BSA The Software Alliance

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

FOREWORD

R. Chandrashekhar, President

NASSCOM

Government spending on software is rising steadily in India, predominantly due to extensive implementation of e-governance projects and other government initiatives undertaken by government at center and state level. These projects are contributing in the adoption of the technology in government departments across different domains. Government, as a sector, is expected to become an important contributor in the growth of domestic IT market.

Using secure software, applications and portals becomes important, given the expanding threat landscape and targeted cyber attacks on the government infrastructure. Privacy protection of citizens is also important given that government processes vast amounts of personal data of citizens through its infrastructure. Mature software procurement practices, with required focus on security considerations, would play a vital role in protection of government IT infrastructure and information and enhancing trust among the stakeholders including the citizens.

It is very opportune that DSCI and BSA undertook a detailed study to come out with this report which outlines prevalent legal and regulatory ecosystem, highlights software procurement practices of government departments and agencies, and analyze these practices from a security point of view. The report also provides key policy recommendations that government can consider to strengthen the existing policy and legal framework to bring the required focus on security within the overall software procurement ecosystem.

I sincerely hope this study will add value to the ongoing deliberations on the subject and contribute in enhancing the maturity of software procurement processes resulting in safer and securer government operations.

CEO MESSAGE

Dr. Kamlesh Bajaj, CEO

DSCI

Government procures software and services across various platforms, particularly in e-Governance projects, as a medium to drive change. With government service delivery swiftly moving onto electronic platforms, software procurement by government agencies has picked up rapidly. Applications, tools, software, etc. are used in processing information and in delivery of essential services that may be G2G, G2B or G2C, at both central and state levels. The aim of delivering efficient and timely services can be achieved by using quality software that satisfies organizational and user requirements while simultaneously addressing security risks and challenges that can potentially hamper its functionality and usability.

As a concept, security has gained prominence in the last few years in India. Sensitization towards security and practices for addressing security risks has risen in government departments and agencies. The idea of this study germinated from one of the over-the-coffee discussions with government officials and BSA in one of our events. We are happy to collaborate with BSA to undertake this study that aims to describe the current state, highlight key issues and challenges, and recommend some steps that can help better the software procurement processes on security front.

It is well known that the government procurement process has not kept pace with the rapidly changing threat. Our interaction with various stakeholders, backed by background research, shows that there is not enough focus on security aspects in the procurement process of software by the government agencies and practices are not standardized. Absence of a comprehensive legal framework and mandatory policy guidelines driving software procurement results in each department, at centre and state level, setting its own norms and conditions for procurement. Further, there is little involvement of security experts in software identification and design phase, less participation in the decision-making process, low weightage to security parameters during solution evaluation – these need attention.

I am particularly pleased that a broad range of government officials came forward to share software procurement practices in their agencies. This helped DSCI identify the practices and crystallised the process to present a 'software procurement lifecycle' from security viewpoint. The recommendations that thus emerged are compelling.

I trust that the government will find this report informative and useful, and the recommendations worthy of being considered to formulate procurement policies and practices. DSCI team members will be happy to discuss ways on implementation.

CEO MESSAGE

Victoria A. Espinel, President & CEO

BSA | The Software Alliance

The rapidly evolving cyber threat landscape means that technology infrastructure and information assets are increasingly vulnerable. This is occurring even as governments move more and more services online, making cyber security a real challenge for governments around the world. With that in mind, BSA | The Software Alliance presents this study for the Government of India and its various agencies. The study outlines global benchmarks and best practices for software procurement, and it aims to minimize the security threat caused by the use of unlicensed – and insecure – software.

Such best practices are particularly important for India, where the government has made such significant strides in embracing e-Governance and rolling out a range of citizen services. The government also continues to make investments in strengthening cyber security as critical national capabilities such as power grids, emergency communications systems, financial systems and air traffic-control networks become increasingly dependent on Information Technology (IT) and therefore, vulnerable to cyber threats.

BSA works with governments across the globe to promote a safe and legal digital world. We impart global best practices, offer in-depth research and analysis, and bring together the collective knowledge of our members, the world's leading technology companies, to advance an open, transparent environment for software innovation. Such policies will allow businesses and governments alike to harness the power of innovative software solutions to enhance efficiencies, reduce costs, improve responsiveness to customers and constituents and, importantly, to ensure that IT systems are secure.

The use of genuine, properly licensed software is a key element for ensuring cyber security in both companies and governments. Unlicensed software can expose businesses and governments to security threats because it may not be properly updated with the latest security patches and may not interact properly with other elements of the IT infrastructure. By clearly outlining security considerations in software and IT procurement policies, including steps to eliminate counterfeit software and ensure the proper licensing of legitimate software, the Government of India and its component agencies can reduce vulnerabilities to cyber threats and enhance overall cyber security.

BSA looks forward to joining forces with other industry stakeholders and working with the Indian Government both at the central and the state level to assist in further streamlining software procurement and development guidelines to promote security and efficiency through the use of legal software.

ACKNOWLEDGEMENT

DSCI and BSA are glad to have received the support of all the stakeholders in undertaking this study and would specially thank the following stakeholders for their expert inputs and suggestions that have helped draft important sections of this report: Ministry of Communication & Information Technology (Department of Electronics & Information Technology – India Computer Emergency Response Team, National e-Governance Division, Standardization Testing and Quality Certification, National Informatics Centre, National Informatics Centre Services Inc.), Ministry of Home Affairs, Ministry of External Affairs (Passport Seva), National Institute of Smart Governance, Centre for Railway Information Systems, Unique Identification Authority of India, Microsoft, IBM, KPMG, PwC, TCS and Wipro and other members of BSA. Some inputs were also gathered from experts in their personal capacity, who chose not to be identified.

Their inputs, suggestions and recommendations have helped shape the overall procurement process section that explains government software procurement processes and the security considerations usually put in such projects.

CONTENTS

INTRODUCTION

Scope: The study is focused on learning about security considerations in software procurement by government agencies in India. This study is limited to software procurement by government ministries, departments and agencies at the central and state level, but does not include regulators, Public Sector Enterprises (PSEs) and Public Sector Undertakings (PSUs), Critical Information Infrastructure (CII) operators. The term software, as used in this document, includes proprietary software, Commercial Off-The-Shelf (COTS) software, customized software and applications, Operating Systems (OS), Open Source Software (OSS), SaaS and website but does not include firmware, middleware, kernels that are bundled with the hardware. The scope also does not include software procurement which is sensitive from a national security point of view. Also, the study does not touch upon ICT supply chain practices.

Methodology: Background research, mainly from primary information sources wherever feasible, coupled with expert inputs from senior government officials, consultants, vendors and system integrators have helped gain insight into the prevailing software procurement ecosystem of government agencies, identify the lacunae and crystallize a set of recommendations that are pragmatic and would help government mature the procurement processes with focus on risk reduction. The recommendations are derived from global best practices, keeping in mind the Indian context and the views and opinions expressed by the security experts interviewed.

Limitations: Small sample size for gathering inputs, unavailability of information in public domain, limited information sharing by government agencies & other stakeholders, primary source of information not available for all aspects, etc. are some of the limitations that we faced during this study.

EXECUTIVE SUMMARY

Software procurement by government agencies in India is not centrally governed or driven by laws and regulation that mandate the inclusion of security requirements during procurement. Security considerations during software procurement, and throughout the lifecycle of software deployment, are imperatives to ensure that software-related security risks are addressed against the backdrop of worsening threat landscape. The importance of the subject is becoming increasingly vital. Software supply chain risks in the software procurement lifecycle need to be addressed with solutions that are practical. Furthermore, it is realized that the initiatives that are recommended can be achieved if the steps are fully aligned with the government's overall goal of reducing security risks in government's software supply chain. The study is undertaken with an aim to learn security challenges at all stages of government software procurement and suggest forward leaning and pragmatic solutions which are relevant from Indian perspective. The outcome of the study in the form of key issues and recommendations has been summarized below:

KEY OBSERVATIONS AND ISSUES

Policy and Legal Framework

- A comprehensive legal framework driving software procurement by government agencies does not exist. Section 43A of the IT (Amendment) Act 2008 mandates 'reasonable security practices' to be maintained by body corporate for protection of 'Sensitive Personal Data or Information' (SPDI) throughout information lifecycle – though the section limits its applicability to only 'body corporate[1]' and scope to SPDI. Most government departments or agencies may not be body corporates. Further, it is implied that reasonable security practices would cover management of software security risks, but there is no specific focus in the Act and rules issued under it
- A patchwork of laws and multiple guidelines issued by different agencies exist that drive procurement in India. Central and state governments have evolved their own

[1] As defined in Section 43A of the IT (Amendment) Act 2008 – means any company and includes a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities

laws and regulations. However, these laws and regulations do not provide for specific treatment to software procurement and neither do they address incorporation of security requirements in the procurement of IT or software

- The national and state IT and/or cyber security policies including the National Cyber Security Policy mention IT supply chain security in varying degrees. However, these are high level statements, and no concrete implementation guidelines, which are mandatory, have been directly issued under them till date
- There is lack of well-established and operating institutional mechanisms that can monitor, enforce and drive security related aspects in software procurement by government agencies, in accordance with changing landscape of threat ecosystem
- Enablers have been developed by the government to enhance security in government agencies including for software procurement such as e-Security Assurance Framework (e-SAFE), model RFP and model Master Service Agreement (MSA) are not being used by the majority of government agencies. This can possibly be attributed to lack of awareness around these enablers
- There is inadequate IT testing infrastructure in the country to test and certify IT products including software based on international standards such as common criteria. Testing and certification ecosystem is being envisaged by the government, with contribution from private sector; more so after India got the 'authorizing nation' status under the Common Criterial Recognition Arrangement (CCRA) last year

A comprehensive legal framework driving software procurement by government agencies does not exist

Policy, Procedural, Administrative and Technical (Organizational)

- In absence of well-accepted or mandatory standards and guidelines issued by the government, software procurement policy and software development lifecycle adopted and enforced by organizations are ad-hoc and lack extensive security coverage; the security requirements of government agencies related to software procurement are not standardized
- Security requirements and specifications are majorly driven by project team's vision and understanding of security
- Insertion of malware in software and leakage of personal data of citizens are biggest concerns of the government agencies from security point of view
- Security requirements are not extensively discussed and covered in the identification and requirement phase and it results in security being addressed at a high level in RFPs, contracts, etc. There are high expectations from service providers to provide highly safe and secure products without laying down specific security requirements
- There is non-standardization in RFPs – even for similar requirements but issued by different government agencies. Also, RFPs issued by the same agency, but for different projects that are similar in nature, many a times do not have comparable security requirements
- When evaluating proposals for software procurement, due importance to security is not given. The weightage assigned to security parameters is low despite the risk factor associated with it
- The clauses in contracts, SLAs and SoWs, specific to security requirements, do not extensively cover the security aspects and are non-standardized

- Security policies of organizations do not 'mandate' use of organization approved, validated and certified software products – this gives rise to increased use of counterfeit and non-genuine products
- Government agencies invest inadequately in training, skill building and awareness. There is a dearth of skilled security experts, especially within government agencies, in domain of information security – across various stages of software lifecycle from design to development to testing to maintenance to disposal
- Well-defined processes for Threat and Vulnerability Management and updating organizational knowledge management with up-to-date security issues are not very mature
- Software update, patch installations and change management practices are not well-defined and rigorously followed
- Use of advanced software testing techniques for security testing are not extensive and carried only for a few mission-critical systems
- There are issues related to ownership of software source code and documentation for customized software solutions
- There are limitations when it comes to comprehensively testing COTS products from security point of view. Only configuration testing is done after procurement

There is lack of well-established and operating institutional mechanisms that can monitor, enforce and drive security related aspects in software procurement by government agencies

- Poor after-sales technical support by vendors to government agencies, given that experts are based outside India

KEY RECOMMENDATIONS

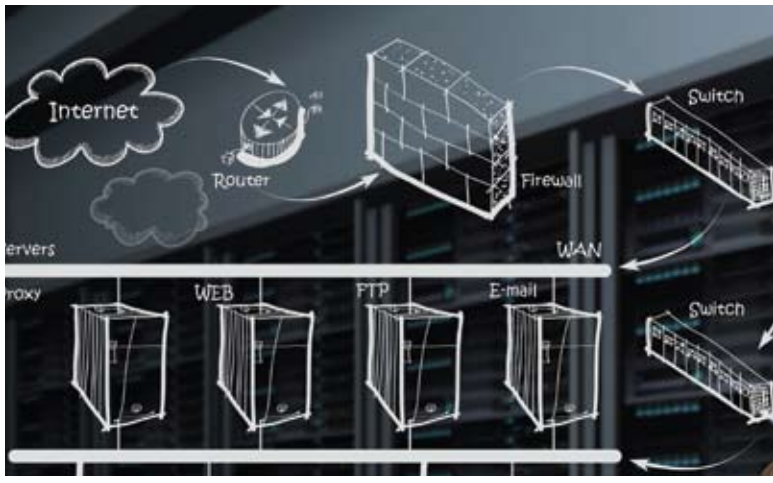
For Government (Policymakers)

- The government should mandate incorporation of information security requirements in the procurement of software by government agencies including central and state agencies through an appropriate policy and legal framework. The policy and legal framework should recommend incorporation of security requirements that are based on international standards and best practices
- Through the policy and legal framework, the government should work towards elimination of counterfeit and unlicensed software from government software supply chains with an objective to reduce security vulnerabilities and strengthen security
- To provide procedural and technical guidance to the government agencies vis-à-vis addressing software security risks and meeting the legal or regulatory requirements, the government, through the policy and legal framework, should assign responsibility to a dedicated agency to act as a Centre of Excellence (CoE). Such a CoE may be created leveraging public-private partnership model
- In cases where the software is required to be tested from a security point of view before procurement, the testing should be done using international standards (such as Common Criteria). Testing labs within the country should be established for this purpose but the government should also accept testing done in foreign labs based on international standards
- To enable procurement of SaaS services by the government agencies from the private sector, there should be an empanelment mechanism for authorizing SaaS service providers

- The government, in partnership with the industry, should create a national awareness campaign to educate government agencies across India on software supply chain issues, risks, solutions, standards, guidelines and best practices

For Government Agencies (Buyers)

- Include security considerations in the software/IT procurement policy of the organization. The policy should mandate integration of security requirements across the software procurement lifecycle including those related to eliminating counterfeit and unlicensed software
- Define security requirements for the software to be procured after consulting all the relevant stakeholders. To the extent possible, security requirements should be based on or aligned to international standards and industry best practices
- Include detailed security requirements in the RFI/RFP and very importantly, enquire about the secure software development capabilities of the software provider. Include security as one of the evaluation criteria for assessing software and/or software provider. After selection of a software provider include agreed detailed security provisions in the contract or Statement of Work (SoW). Identify criteria for software acceptance and verify whether these criteria are met when software is delivered



- Keep track of latest threats and vulnerabilities and if applicable to own environment, devise ways to address them
- Establish infrastructure, processes and roles necessary for the effective management, control and protection of software assets based on international standards and best practices
- Implement and enforce policies on software updates and patch management in consultation with the software provider. Regularly upgrade software versions and apply patches post impact analysis and testing
- Focus on capacity building of resources in domain of information security to strengthen security components in procurement lifecycle and reduce software supply chain risks

BACKGROUND

GOVERNMENT PROCUREMENT IN INDIA

Procurement of goods, services and technologies form an important part of government operations across all domains and services. Many government services are now performed online. Government, at both the central and state level, provides various G2G, G2B and G2C services. Almost all entities within a government department are connected to each other, transacting large amounts of data and processing information for delivery of services. With India steadily moving towards an e-Economy, the quantum of projects run by the central and state governments provide a huge opportunity for vendors and service providers.

Government procurement in India is a system-wide activity across the central and state governments, their autonomous and statutory bodies, public-sector enterprises and undertakings, the defence sector among others, with a wide variety of sector and institution-specific requirements. Local governments, at the Municipal and Panchayat levels also follow their individual procurement practices, usually approved and vetted by the respective state governments. [2]The entire Indian Government procurement market is estimated to be more than USD 300 billion, which is

Government spending on software alone is pegged at nearly INR 43 billion, with major spending on e-Governance projects

nearly 25 to 30 % of the country's Gross Domestic Product (GDP). Government spending on software alone is pegged at nearly INR 43 billion[3], with major spending on e-Governance projects. India's advancement towards becoming an e-Economy enforces the importance of the subject. Use of software tools and products across myriad of sections and divisions in government departments, providing multitudes of services is becoming increasingly vital. The quality of the software used by the project entities, for work within and among agencies, also plays an important part in the sustainability of the project.

Diversity in procurement practices is an integral feature of the vast governmental system in the country. Principles of transparency and competition form the backbone of the procurement lifecycle. Central and state governments have undertaken a lot of e-Governance initiatives. A massive countrywide infrastructure reaching down to the

[2] 'Government Procurement in India' – Domestic Regulations & Trade Prospects: CUTS International, 2012
[3] Frost & Sullivan, NASSCOM Survey – NASSCOM Strategic Review

remotest villages is evolving, and large-scale digitization of records is taking place to enable easy, reliable access over the Internet. Given the magnitude and criticality, government departments are also tasked with protecting critical data thus generated and transacted over e-Governance applications and portals. 31 Mission Mode Projects (MMPs), at the central and state level, are being used to provide numerous e-Governance services. Government also procures software for G2B and G2G transactions. Given the complexity and scale of software being deployed by government agencies today, one of the major challenges is to build secure software and applications. Secure software development involves many aspects from security requirement definition; formal modeling; security architecture and software model development; testing verification and validation; and finally, evaluation, certification, and accreditation. It does not end here – the process continues throughout the lifecycle of the software system. Incorporating security into the software development process and across the lifecycle of software procurement is an important aspect. Governments are putting across provisions and practices to manage security in extended software supply chains and lifecycles.

ISSUES AND CHALLENGES

An increasing number of government departments and agencies procure software and applications, including mission-critical systems, leveraging globally sourced products and components. Due to the global nature of supply chain threats, there is a need for recognition and assessment of global interdependencies among suppliers and consumers with the aim of making supply chains safer and more secure. The threat landscape expands with each passing day. Sophisticated attack vectors

[4]In the last five years, the number of reported incidents of website compromise has grown 5.5 times

31 Mission Mode Projects (MMPs) at the central and state level are being used to provide numerous e-Governance services

and Advanced Persistent Threats (APTs) are being operationalized on a daily basis with the intent of exploiting applications, portals, databases, operating systems, etc. Over the years, the quantum of attacks and vulnerability exploitation over Layer 7 of the OSI model, i.e. layer, has proliferated. The increasing complexity of software and its architecture, arising out of complex demands, requires ever-more rigorous development and testing processes in order to minimize the potential of exploits or misuse.

Developers make these processes highly stringent and deploy tools and solutions to minimize risk exposure. Organizations employ various techniques such as secure development practices, rigorous testing, and regular maintenance and update. Given the complexity and variation of software, it is vital to set the right risk expectations and create a robust process when acquiring software.

"Security" is not a commodity that can be bought, purchased or exchanged. Even so, it is increasingly gaining importance on the must-have requirements list for technology consumers, including governments

[4]http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf

Given the complexity and scale of software being deployed by government agencies today, one of the major challenges is to build secure software and applications

and critical infrastructure operators. "Secure-by-Design" is not an entirely new concept, but all developers and designers might not practice it. Not all security features are built-in by default. In many cases, features – such as particular security features – are the result of requirements expressed by the government agencies in their procurement plan, and for which they are paying. This can be true for extensive security features as well, including those a government agency might require for a particular department's mission.

Recent studies indicate that three out of four websites are vulnerable to attacks[5] – attacks that go beyond traditional security incidents. Unfortunately, attackers can make use of security flaws in these web applications to steal information, expose sensitive records and eventually ruin government reputation. There are also growing concerns about the scarcity of practitioners with requisite skills and knowledge to build secure software. This concern is directly linked with vendors' capability to build and deliver secure software with requisite levels of security. For developers with malicious intent, the software development process also provides a window to insert malicious code. The use of an unvetted software supply chain increases risk exposure by giving rise to the use of counterfeit products that expose the risk exposure of government organizations that procure them.

Another challenge is to secure the entirety of the software architecture and ecosystem, which can be compromised by just one of its interconnected components. These components may come from different organizations or teams working on different platforms or in different languages in the supply chain. It is important to also ensure security of the overall system. Government departments increasingly understand the importance of using genuine software products that are thoroughly tested and validated. This helps strengthen the overall software supply chain ecosystem and reduces risks.

Top Application Security Threats

- SQL injection
- Security mis-configuration
- Reverse engineering – Code regeneration
- Cross Frame Scripting (XFS)
- Cross-Site Request Forgery (CSRF)
- Broken authentication & session management
- Insecure direct object references
- LDAP injection
- PHP code injection
- Malicious code insertion – Back doors/Trap doors
- OS command injection
- Remote XSL inclusion
- Script/Source code disclosure
- Directory traversal
- Man in the Middle (MITM) attacks
- Cross-site scripting

[5]http://www.quotium.com/Resources/whitepapers/Application_Security_in_the_SDLC.php

Many government agencies generally have limited resources to examine and assess the security of software that they induct and likely do not have sufficient expert knowledge to adequately perform the task, with deployment of software using a myriad of components with varied features and functions. Leaving this task to the individual government agency also results in considerable duplication of efforts. For example, multiple departments with similar requirements often examine and validate software against desired security requirements separately to match their definition of "security". Such challenges demand rational solutions, by way of unification of efforts and help in achieving objectives that are practical and affordable.

Enabling government to realize the expanding threat landscape, anticipate needs and opportunities, strategize and plan requirements, get secure software inducted, and deliver enduring results is the objective of this study.

SOFTWARE PROCUREMENT ECOSYSTEM IN INDIA – SECURITY PERSPECTIVE

Currently, government procurement in India is decentralized. Central government ministries, departments and public sector undertakings; 29 States, 7 UTs, have all established their own procurement processes; though some of the practices are shared. Though a framework that governs overall procurement of goods and services exists, there is no central legal framework giving explicit treatment to software procurement in India. There have been few policy initiatives that provide some guidance on the security considerations for software procurement. The below sections discuss the policy and legal framework that exists, standards and guidelines that have been issued, and existing procurement practices across government departments and how security fits into the overall scheme.

POLICY AND LEGAL FRAMEWORK

The National Cyber Security Policy released in July 2013 provides insight into the government's approach and strategy for the protection of cyberspace in the country, pointers to facilitate collaboration among key public and private sector players and develop a framework for specific actions and programmes key to facilitating a secure cyberspace. The policy "encourages government entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications." It also proposes "encouraging secure application/software development process (from design through retirement) based on global best practices."

Specific to securing e-Governance services, the policy contains the following points:

- To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all

Though a framework that governs overall procurement of goods and services exists, there is no central legal framework giving explicit treatment to software procurement in India

e–Governance initiatives in the country, to reduce the risk of disruption and improve the security posture

- To encourage wider usage of Public Key Infrastructure (PKI) within government for trusted communication and transactions
- To engage information security professionals/ organizations to assist e-Governance initiatives and ensure conformance to security best practices

These specific points with regard to e-Governance services talk about mandating implementation of global best practices to reduce risks, but no standards or guidelines have been established. Securing the software supply chain in e-Governance services and requiring security in software procurement or security inclusion in the software development lifecycle is not explicitly mentioned.

For Critical Information Infrastructure (CII), the policy "mandates secure application/software development process (from design through retirement) based on global best practices."

This mandate is limited only to CII, and this requirement does not apply to other government departments and agencies. Specific to reducing supply chain risks, the policy talks about aligning efforts to "create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT procurement." Thus, building resilience in procurement processes of the organization is emphasized and organizations are required to act accordingly.

Other important points in the policy with regard to software and strengthening of the ecosystem include:

- To promote a consortium of government and private sector to enhance the availability of tested and certified IT products based on open standards
- To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security

National Cyber Security Policy of India highlights creating an assurance framework to encourage secure application/ software development processes based on global practices

- To encourage and mandate as appropriate, the use of validated and certified IT products
- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices
- To build trusted relationships with product/ system vendors and service providers for improving end-to-end supply chain security visibility

The policy reflects the government's intent and desire to build a secure cyberspace. However, the policy is under implementation. Interaction with government agencies also revealed that their efforts to issue specific guidelines against few of the objective areas listed in the policy are underway. Whether measures with regard to software procurement policies and processes will be issued remains to be seen.

Information Technology Act 2000 and Information Technology (Amendment) Act 2008

The use of electronic records and digital signatures in government, its agencies, and private sector for various transactions across electronic records lifecycle, various sections on generation, authentication, its legal recognition, usage, storage and penalties, along with roles of stakeholders, have been mentioned in the IT Act.

Section 43A of IT (Amendment) Act 2008 requires that organizations have to maintain "reasonable security practices" to protect "Sensitive Personal Data or Information (SPDI)", as defined in Rule 3. If

the security requirements are covered as a part of a contract between the two parties, then it will prevail over the reasonable security practices requirement expected to be complied within Rule 8. Organizations can also demonstrate compliance to ISO 27001 ISMS to satisfy reasonable security practices conditions.

That essentially means that organizations necessarily need to take adequate steps, across their entire spectrum of operations, to protect SPDI. This would also subsume that adequate protection measures have to be built in the software that is being procured by the organization for ensuring that SPDI being processed is secure. However, Section 43A limits itself only to SPDI and is only applicable to "body corporates" and by definition of body corporates as defined in the Act, many of the government agencies would not qualify as body corporates. Hence, the section has limited relevance for government agencies in the context of security in software procurement.

Guidelines focused on use of keys (public and private) in government departments are also mentioned in the Act. Section 84A of IT (Amendment) Act 2008 provisions that for secure use of e-Governance and e-Commerce in the country, central government may prescribe modes or methods for encryption. But these methods are yet to be notified. Section 65 of the Act specially lists down source code tampering of software as criminal offence with fine and imprisonment liabilities.

Above listed are some of the major statements governing security aspects in the Act. We observe that there are neither specific sections nor rules or guidelines issued thereof that list requirements for secure development of software products or what practices need to be adhered to for ensuring security aspects are maintained during software procurement.

National IT Policy

The National IT Policy[6] was released in 2012, and its mission statement notes that it is intended "to ensure a secure cyberspace to facilitate trust and enable sustained growth of ICT". To make public procurement processes more efficient, it requires use of electronic mode, as well as transparency and competition.

With respect to security measures, one IT policy objective is to undertake policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology and people) and incentives for compliance. The policy also envisages "to create, establish and operate an Information Security Assurance Framework."

Subsequent to the policy, there have not been any guidelines with respect to security considerations or requirements or practices in IT procurement in government agencies.

A Joint Working Group (JWG)[7], set up under the leadership of Dy. National Security Advisor and including representatives of government and the private sector, fleshed out the details for Public Private Partnerships for enhancing cyber security in India and put forth recommendations in the report "Engagement with Private Sector on Cyber Security", which was released in October 2012. Several action items were suggested for enhancing the cyber preparedness of the country. Points such as mandatory software testing before procurement and deployment, the establishment of a certification ecosystem in India, and acceptance of software products tested through international standards and testing mechanisms such as the Common Criteria were emphasized; though there weren't specific guidelines on procurement. The JWG report also advocates setting up of CoEs to establish guidelines and processes on different cyber security components, such as issuing of best practices for different domains of operation in ICT.

State Government IT-Related Policies and Procurement Laws

Almost all states and UTs have government IT divisions and IT policies in place, though the level of maturity varies. Some policies address security requirements by using legal framework to strengthen security and privacy posture, implementation of appropriate security architecture involving the use of firewall, intrusion detection systems, access controls, business continuity and disaster recovery plans, promoting use of PKI, etc. A few states also promote creating a high-powered IT Security Task Force that can drive security initiative. While some policies are somewhat matured and provide quite granular security consideration, other policies do not ask for significant security considerations and mention of

[6]http://deity.gov.in/sites/upload_files/dit/files/National_20IT_20Policyt%20_20(1).pdf
[7]https://www.dsci.in/sites/default/files/Data%20Security%20Council%20of%20India%20(DSCI)%20-Recommendations%20of%20JWG.pdf

security only at a high level. Majorly, explicit mention of guidelines for security considerations in software procurement is missing. Few states have developed e-Governance policies. Some states give significant importance to information security and provide appropriate clauses to be incorporated during the procurement and deployment of software and hardware while rolling out the e-Governance projects. Security-specific conditions such as mandatory security certifications for applications, mandate of security audits of all the state government websites, security and privacy considerations of citizen data, provision for secure network for data or video transaction and provision for update and auditing of government website, portal, applications, etc. are the ones that are most frequent. Few states have enacted specific information security policies and/or guidelines that also include procurement of IT related goods and services.

In our analysis, in totality, we observe that at both the central and state level, there is not enough focus on security considerations that need to be taken into account during software procurement.

Procurement/Software Development-Specific Guidelines and Rules

Central and state governments of India derive their authority to contract for goods and services from Article 298 of the Constitution of India[8]. For the central government, Clause 4 (2) of Article 77 of the Indian Constitution, vests power of expenditure with the Finance Ministry. All financial transactions are governed by specific provisions and broad guidelines put forth in the General Financial Rules (GFR) 2005. High-level guidelines for works, goods and services procurement and contract management find mention in Chapters 5, 6 and 8 of GFR. The term "goods" includes all articles, material, commodities, livestock, furniture, fixtures, raw material, spares, instruments, machinery, equipment, industrial plant, etc. purchased or otherwise acquired for the use of government but excludes books, publications, periodicals, etc. for a library. Though not explicitly mentioned, by this definition, software procurement by government agencies can be considered to be covered. Similar steps are also applicable for state procurement. The finance departments of states

In 'The Public Procurement Bill 2012', the procurement of goods and services for national security purpose is given special treatment – whether software procurements, such as tools or solutions or applications for cyber security/ information security purpose, especially for critical information infrastructure, would also be exempted is to be seen

can formulate their own GFR, which are typically, as we observe, in line with GFR by the Ministry of Finance. The extant rules on GFR allow foreign bids when those goods are not available in the country. Delegation of Financial Powers Rules (DFPR), 1978 issued by the Department of Expenditure in the Ministry of Finance provides another set of guidelines where procurement-related rules have been suggested.

The procurement guidelines do not cover software procurement in detail as software is also considered a "good". Hence, there are no specific guidelines for security considerations that government agencies should incorporate during software procurements.

The **Public Procurement Bill 2012**, which is based on Vinod Dhall Committee report on procurement, aims at regulating government contracts valuing INR 50 lakh and above. It aims at ensuring transparency, accountability and probity in the whole process. The aim, according to the bill, is to ensure "fair and equitable treatment of bidders, promoting competition, enhancing efficiency and economy, and maintaining integrity and public confidence in the procurement process." This bill is not yet tabled in the Parliament.

As per the draft, procuring entities, including Central Public Sector Enterprises (CPSEs), would have to frame rules for public procurement of goods,

[8]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/186988/GovtProcurementinIndiaDomesticRegulations-1.pdf

work and services; thus replacing current model of GFR. It has a provision to debar bidders found engaged in corrupt and malpractices. In cases where procurement from a particular supplier is necessary to ensure standardization or compatibility with existing systems, and if it is adequately established, the bill does not require certification from a competent technical expert. Such a certification is required by existing regulations and model laws, such as UNCITRAL, on which the Information Technology Act 2000 is also based. It exempts procurements for disaster management, for security or strategic purposes, and those below INR 50 lakh. What appears is that the procurements of goods and services for national security purpose is given special treatment – whether software procurements, such as tools or solutions or applications for cyber security/information security purpose, especially for critical information infrastructure, would also be exempted is to be seen.

Similar to GFR, the Public Procurement Bill too doesn't list specific requirements for security considerations in the procurement lifecycle of goods, work and services. This indicates that at the policy level, security considerations to be taken into account during software procurement lifecycle aren't considered as important parameters that could elevate the requirement to combat supply chain risks.

Technology Advisory Group for Unique Projects (TAGUP) was set up by the Finance Ministry to look into various technological and systemic issues when it comes to software development for e-Governance projects with financial background such as Goods and Services Tax (GST), Tax Information Network (TIN), Expenditure Information Network (EIN), National Treasury Management Agency (NTMA), New Pension System (NPS). The framework put forth in this report is more generally applicable to the complex IT-intensive systems which are increasingly coming to prominence in the craft of Indian public administration. Certain points with regard to security in e-Governance projects that were highlighted are:

- Security is regarded as a hygiene factor
- Security should be given utmost importance in critical projects
- One time fund approval is not sufficient for security – it is an ongoing process that demands regular review and resource allocation

We observe that security as a subject has been sensitized in the report, and the report emphasizes importance of security in e-Governance projects. Though there weren't explicit pointers with regard to security considerations during procurement of software.

All the components of legal and policy framework mentioned above are indicative and might not be exhaustive. There might be additional rules, guidelines or legislations based on these rules. Broadly, government procurement is dealt through administrative rules and procedures. Presence of multiple procurement rules, guidelines, directives and procedures issued by multiple agencies, although incorporating some internationally accepted best practices, are not sufficient to cater to the growing needs of the domain that demands specific attention. To further complicate the matter, all these documents and guidelines aren't available at a single source for reference. Except for few state-specific laws, most of the instruments detailed above do not have force of law and some can only qualify to be subordinate legislation at best. Hence, there is a clear need for a well-defined structure that lays down a definitive framework for procurement of software that includes considerations for information security.

STAKEHOLDERS

There are multiple stakeholders that are concerned with the software procurement ecosystem – primary amongst them are DeitY and its agencies which are tasked to provide e-Governance services and build a conducive and secure environment for e-Services. Other major players have roles to play in the software procurement ecosystem. The below list was prepared with input from different departments on the role of the agencies, and not all may have been covered.

Department of Electronics and Information Technology (DeitY)

Primary objective of DeitY is to provide e-Infrastructure for delivery of e-Services by other government departments and agencies. They also work on policy matters – including framing laws, standards, frameworks, requirements, guidelines and rules – relating to information technology, electronics and the Internet. It also work towards promotion of standardization, testing and quality in IT and standardization of procedures for IT application tasks. It has several departments, committees, task forces, and commissions to help achieve these objectives.

Its mission is e-Development of India through multi-pronged strategy of e-Infrastructure creation to facilitate and promote e-Governance, promotion of Electronics & Information Technology – Information Technology-Enabled Services (IT-ITeS) industry, providing support for creation of Innovation/Research &Development(R&D), building knowledge network and securing India's cyberspace. The agencies under its purview include:

A. National Informatics Centre (NIC)

A "prime builder" of e-Government/e-Governance applications, NIC also is tasked to host, protect and ensure that government applications and portals run securely. NIC supports the ministries and departments of the central and state governments and union territories in setting up of ICT infrastructure, implementation of national and state level e-Governance projects, products and services, consultancy to the government departments, research and development, and capacity building. Over the years, with extensive work on software development, testing and maintenance, NIC has developed a comprehensive security document that lists security best practices and controls for every stage of the software lifecycle. It undertakes security testing of applications and portals, with help from industry experts, that it develops and hosts. For enhancing software testing capabilities, it has started empanelment of individual auditors from CERT-In empanelled organizations. It also works in capacity building by providing and organizing security courses in different streams. Security guidelines have been issued by NIC to various stakeholders on a regular basis. However, these guidelines do not comprehensively cover steps that are specific to reducing risk in software procurement lifecycle.

National Informatics Centre Services Inc. (NICSI) was set up in 1995 as a Section 25 company under NIC to provide total IT solutions to government organizations. It provides the following products and services to organizations in the central and state governments and PSUs:

- Hardware
- Systems software
- Application software
- Software development
- Intra-networking
- Wide area networking
- Videoconferencing
- Customized software, etc.

NICSI has drawn up a procurement plan compliant to GFR rules for the equipment required by various ministries and departments of government. A NICSI officer is also designated to be involved in the procurement process of government agencies; however, this wasn't reflected in government interaction. NICSI also negotiates with technically shortlisted vendors every three months, and the reduction in prices of items that follows on such negotiations is passed on to the government agencies.

B. Standardisation Testing and Quality Certification (STQC)

STQC maintains e-Governance standards. Based on this concept a Conformity Assessment Framework (CAF) for e-Governance projects has been developed and is in operation. STQC provides services including testing, calibration, IT and e-Governance, training and certification to public and private organizations. In IT and e-Governance, STQC provides assurance services through its IT centres for software quality testing, information security and IT service management by conducting testing, training, audits and certifications. STQC laboratories have national/international accreditation and recognitions in the area of testing and calibration, most noticeable being Common Criteria. It is also listed as one of the CERT-In empanelled agencies for conducting security testing of software and products.

C. Computer Emergency Response Team (CERT-In)

CERT-In is the national nodal agency for responding to computer security incidents. It works to build threat intelligence, forecast and provide alerts of cyber security incidents, and establish emergency measures for handling cyber security incidents. It also issues guidelines, advisories, vulnerability notes and whitepapers relating to information security practices and procedures.

It also provides expert input and consultancy on security to government agencies for procuring software.

CERT-In has created a panel of 'IT Security Auditors' for auditing, including vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations of the government, critical infrastructure organizations and those in other sectors of Indian economy. CERT-In has also issued guidelines for empanelled information security auditing organizations. These empanelled auditors are contracted by a customer directly to perform IT security audits.

D. National e-Governance Plan (NeGP)/ National e-Governance Division (NeGD)

It takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision. The existing or ongoing projects in the MMP category, being implemented by various central ministries, states, and state departments would be suitably augmented and enhanced to align with the objectives of NeGP.

NeGD was created as an autonomous business division under the Ministry of Communications and Information Technology for taking up the tasks being carried out by the Programme Management Unit of National e-Governance Plan (PMU-NeGP) at DeitY. Immediate tasks for NeGD include Programme Management of NeGP, inter-alia including facilitating and supporting DeitY in undertaking the various tasks such as facilitating implementation of NeGP, providing technical assistance to central ministries and state line departments, undertaking technical appraisal of all NeGP projects to examine issues such as overall technology architecture, framework, standards, security policy, service delivery mechanism, sharing of common infrastructure, etc.

The plan includes development of the National/ State Service Delivery Gateway (NSDG/ SSDG), State Wide Area Networks, State Data Centres (SDC), Common Services Centers (CSC) and development of e-Forms for service delivery. The infrastructure requirements of NeGP are broken down into core and support infrastructure requirements.

Based on the stakeholder description above, it is observed that there are multiple government agencies directly or indirectly involved in the IT

procurement but there is no nodal agency which is legally empowered to issue mandatory guidelines on software procurement that can ensure security aspects are adequately addressed in software procurement and development lifecycle. This leads to non-standardization of basic criteria in software procurement.

Other Important Stakeholders

Directorate General of Supplies and Disposal (DGS&D)

Certain procurement-related guidelines have also been issued by the Directorate General of Supplies and Disposal (DGS&D), the Central Purchase Organization. It concludes rate contracts with the registered suppliers, for goods and items of standard types, which are identified as common user items and are needed on recurring basis by various central government ministries or departments. To illustrate, if any central government department needs support in purchasing any COTS application or OS at standardized rates, it can be purchased through DGS&D. Its guidelines do not have any significant coverage on how government agencies should go about developing policies that enable them to augment robust procedures in procurement lifecycle. Software like any standardized item is in DGS&D's goods list. It has, however, some predefined criteria of security parameters that vendors need to fulfil before they can register their product with the department for bulk use. Most government departments have their own procurement cell, and very few depend on DGS&D for software procurement.

Though there is no designated nodal agency at the central or state level to monitor compliance against established rules, there are some standing committees that observe or act as procurements "watchdogs". Also, Comptroller and Auditor General (CAG) of India, is empowered to perform audits of procurement-related transactions. The findings are presented before legislature, and remedial actions are taken accordingly. The Indian Audit and Accounts Department of the CAG has also published an IT Audit manual[9]. It provides a comprehensive list of controls against which security audits can be conducted. However, audit of software security measures, and of security aspects during procurement is not covered in detail.

Central Vigilance Commission (CVC) is another agency that is conceived to be the apex vigilance institution, free of control from any executive authority, monitoring all vigilance activity under the central government and advising various authorities in planning, executing, reviewing and reforming their vigilance work. The CVC is entrusted with the responsibility of ensuring the compliance of procurement rules and practices of government department and agencies. Thus, through these mechanisms, certain checks and balances are introduced in the procurement system. CVC has also issued guidelines prescribing the procurement procedure to be followed by all central ministries. But similar to other procurement guidelines, this one too does not include detailed security components.

[9]http://www.icisa.cag.gov.in/background%20material-it%20environment/it-audit-manual/vol-1.pdf

POLICY ENABLERS

The government has issued policy enablers, including a security framework and model guidelines, to help government agencies strengthen security, including in software procurement.

E-Security Assurance Framework[10]

To address the need to develop standards and guidelines to strengthen information security in various e-Governance information systems, government came out with e-SAFE framework. The framework is split into various components, with each component focusing on one particular aspect, such as security controls, asset management, quality assurance etc. In the catalogue of security controls "e-SAFE GD 200", it focuses on security aspects in acquisition plans. Below listed are the components mentioned in the document:

- **System and Service Acquisition and Maintenance Policy**

  Controls: The policy on acquisition and maintenance of information system and its associated services shall be defined and established to ensure that the security requirements are identified and met during system development and maintenance lifecycle.

  Explanation: The security requirements of information system which includes business application, off-the-shelf software application, user developed application, operating system, infrastructure, etc. shall be identified prior to its development (may be during requirement phase) and these requirements and controls shall be implemented and maintained during its lifecycle.

- **Acquisition and Maintenance Process**

  Control: The acquisition and maintenance process shall define and establish (i) Security needs and relevant controls (ii) Design and development process (iii) Testing and evaluation methodology (iv) Documentation.

  Explanation: The detailing and granularity of the various phases of the acquisition and maintenance process depends on the classification of the system (based on Risk Assessment) to be acquired. The standard system development lifecycle as defined in International Standard may be adopted. These phases can be implemented either by those who makes acquisition or third party suppliers or outsourced partners.

- **Configuration Management of Information System**

  Control: The configuration management of the information system under development shall follow the configuration management policy and procedure defined in "Configuration Management."

  Explanation: During acquisition and maintenance of information system, either new information system can be developed or upgrading of existing system takes place. Configuration management process as defined in "Configuration Management" controls the changes to the system during development/upgrades, tracks the security flaws, integrate the authorization process and facilitate the relevant documentation.

- **Security Testing of Information System**

  Control: The information system under development shall be tested adequately to ensure the security requirements and controls identified during requirement analysis have been implemented and working without any problem.

  Explanation: The security testing of the information system under development should be carried out to verify the correct functioning of the security requirement and provides the confidence that the system will work satisfactorily during normal operation.

- **Technical Vulnerability of Information System**

  Control: The risk of exposure of information system (s) under operation to potential technical vulnerability shall be periodically evaluated and appropriate actions, as applicable, shall be taken timely to mitigate the risk.

  Explanation: Technical vulnerability testing and evaluation on the information system in use shall be periodically (at least once in year or as

[10] http://egovstandards.gov.in

and when new vulnerability is reported) done based on the published technical vulnerabilities and appropriate measures shall be taken if the risk resulting from exploitation of such vulnerabilities to the information system is considerably high.

- **Addressing Security in Third-Party Agreement**

  Control: Agreement with third-party and/or outsourced party involving accessing, processing, communicating or managing the information system (or a part of it and/or the associated components) or adding product or service to the information system, shall cover all security requirements.

  Explanation: Usually the operation of any information system is highly dependent on the service of the suppliers. Hence, it is necessary to identify through risk assessment the areas that require special attention through formal contract/agreement to ensure that the security of information system and information processing facilities is not reduced by the introduction of external party.

- **Management of Third-Party Security and Delivery Service**

  Control: The security controls, service definition and the delivery levels included in the third-party agreement shall be implemented.

  Explanation: The third-party agreement usually contains the security requirements (based on perceived risk from the third-party), the service definition (e.g. the various types of services provided by third-party) and the level of service (e.g. 99% availability of network service).

  The implementation as per the agreement by the third-party shall be monitored periodically and any decision on change in third-party services (service definition and its level) and security requirements and/or third-party, if required, is taken.

  Control Improvements

  - The service performances of the third-party shall be monitored regularly
  - The necessary changes, if required, in third-party services shall also be incorporated based on the monitoring results

Conformity Assessment Requirements (CARE), a separate standard, is intended to enforce implementation of standards and best practices in e-Governance solutions throughout the project lifecycle. The purpose of defining CARE is to enforce implementation of standards and best practices in e-Governance solutions. The Quality Assurance Framework (QAF) provides high-level guidance on security considerations during procurement.

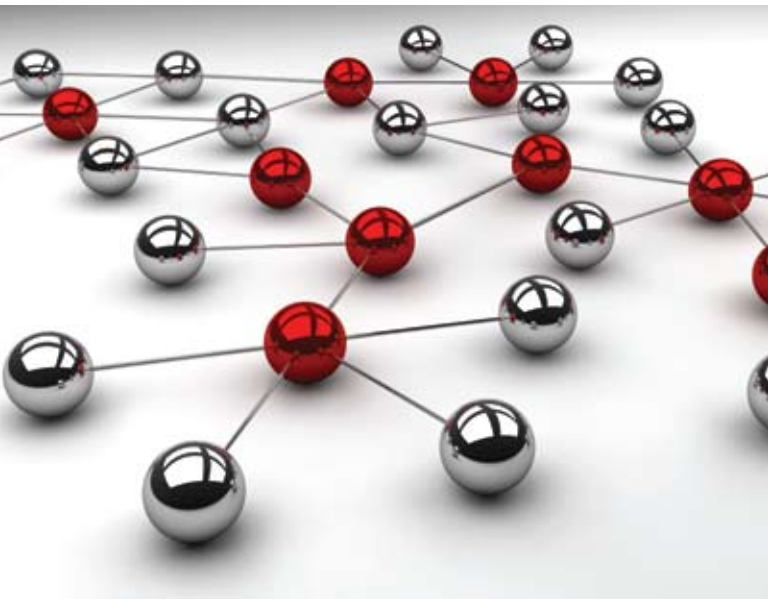
Through e-SAFE, DeitY has provided a framework that can be adopted by organizations to address security concerns throughout the lifecycle of the project. Although not comprehensive, the document provides a good starting point for the projects to consider security aspects and parameters during software acquisition (or procurement) and development lifecycle. There is a lack of awareness around the framework. It has not been widely adopted in the central government departments or across state governments. Many e-Governance projects have opted to devise their own framework suited to their project requirement than adopting e-SAFE.

Model RFP

DeitY has formulated the Model Request for Proposal (RFP), along with guidance notes and toolkits for preparing RFPs, to be used by line departments and state governments to procure goods, consultancy services, managed services for e-Governance projects. Use of model RFPs and various conditions and clauses listed under them are not mandatory, however, and its use has not yet picked up in e-governance projects. It is advisory in nature and aims at sensitizing the bid management teams on good practices and harmonizing/standardizing the RFP clauses and terms and conditions. Due to lack of awareness amongst stakeholders, few departments and state governments were not aware of its existence. Standardization in use of RFPs by various department and agencies can be achieved if model RFPs are used as the base criteria for developing customized RFPs. Model RFPs have been classified into two categories:

Category One

The category one RFP is for projects where there is high-level of clarity on the technology and the solutions. These would be typical implementation of COTS or ERP projects or any state MMPs. In e-Governance space, these projects would be applications with a simple citizen application workflow. In such projects, the risk of technology concerns is less. Selection in such cases typically is based on low-cost basis.



Category Two

The category two RFP is for projects with less clarity as to what is the solution that is expectsd. For example, these may be any large-scale implementation of any central MMP. These are risky projects and should follow Quality Cost-Based Selection (QCBS) evaluation. In such cases, the responsibility of technical feasibility of the proposed software solution would rest with the bidder. However the Proposal Evaluation Committee in this case should have expertise or should have access to expertise to objectively evaluate and compare the various solutions components proposed by the bidders.

In such projects the nodal agency should evaluate the critical parameters of the project covering system functionality, technology, current performance on key technologies proposed in isolation and together as a stack, details on implementation experience of the bidder, training methodology, performance in proof of concept (in case PoC is planned), certifications, past experience of the vendor in executing similar assignments, size of those assignments, profile of team members and project methodology. Here too, evaluation of security parameters is not a major component but listed as a component of technology. General belief is that the certifications may add value and are put as a pre-qualification criterion, provided they meet the condition specified above.

In the document, four kinds of model RFPs are provided:

- Model RFP Document for System Integrator/ Service Provider
- Model RFP Document for Procurement of Data Entry Services
- Model RFP Document for Hardware Procurement
- Model RFP Document for Software Application Development and Maintenance

In the Model RFP Document for Software Application Development and Maintenance, the following conditions are laid down that provide emphasis on security parameters.

- **Security Review**

  The software developed/customized shall be audited by the agency from a security and controls perspective. Such an audit 'may' also include the IT infrastructure deployed in connection with the software for the project. Following are the broad activities to be performed by the agency as a part of a security review:

  - Assessment of authentication mechanism provided in the application/components/modules
  - Assessment of data encryption mechanisms implemented for the solution
  - Assessment of data access privileges, retention periods and archival mechanisms
  - Server and application security features to be incorporated

- **Suggested Technical Evaluation**

  In the suggested technical evaluation method proposed in the document, security is taken as a parameter

The Model RFP provides some security clauses that can be used as a sample or template by organizations as they formulate their own RFP. However, these are high-level statements, and every project would be required to build more in their issued RFPs to give more importance and weight to security. The note below is also circulated as a part of the Model RFP providing guidance on what parameters should evaluations of RFPs be done.

Criteria	Basis for Evaluation	Max Marks
System Functionality	Meeting the requirements of <department> in terms of how close the proposal is to the functional requirements for the solution as have been proposed for <department> (In case it is COTS, it should be measured by degree of customization required)	20%
Technology	Demonstrated robustness of the technology deployed across other installations around the world, including: – Scalability – Security – Ease of implementation	20%
India-Specific Capabilities	Qualitative assessment based on the number of projects of similar nature in India and the size of those projects	7%
Industry-Specific Capabilities	Qualitative assessment based on the past experience of the bidder in executing similar assignments and the size of those assignments. [The definition of 'similar' should be such that it focuses on the areas which are 'innovative' or where the technical feasibility is a challenge in the context of the project]	7%

Training	Trainings proposed by the vendor and the amount of emphasis laid on training the employees schedule details, locations, sessions and their description	7%
Certifications and Credentials	Relevant certifications (SEI-CMMi, ISO, etc.)	7%
Profile of Proposed Team Members	Relevant assignment experience/years of experience/number of certifications in technology specific to the solution proposed	20%
Project Methodology, Support and Documentation	Qualitative assessment based on: – Understanding of the objectives of the assignment: The extent to which the systems implementer's approach and work plan respond to the objectives indicated in the statement/scope of work – Completeness and responsiveness: The extent to which the proposal responds exhaustively to all the requirements of all the terms of reference	7%
Inclusion of MSMEs in Project Delivery	As per requirement	7%

It is observed that security is listed as an evaluation parameter within the technology criteria. It can be said that it has still not emerged as a key parameter for evaluation. It does not get due prominence given its importance in today's operating environment. The guidance provided is only suggestive and departments can evolve their own evaluating parameters and assign weight according to their project requirements.

Model MSA/SLA

In the model Master Service Agreements (MSAs) and Service Level Agreements (SLAs) in the document titled 'Contract Agreement for Selection of System Integrators/Implementation Agencies', built alongside Model RFP documents, there are few security-specific clauses, security evaluation and testing that are given maximum coverage. In the section 'Obligations under the SLA', it is mentioned that the project shall be governed by the mechanism of final acceptance testing and certification is to be put into place by the nodal agency and implementation agency as under:

- Final testing and certification criteria will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of project development and implementation covering software, hardware and networking including the processes related to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service-oriented architecture, performance in relation to compliance with SLA metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and this agreement
- Final testing and certification criteria will be finalized in the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed

- Final testing and certification criteria will consider conducting specific tests on the software, hardware, networking, security and all other aspects
- Final testing and certification criteria will establish appropriate processes for notifying the implementation agency of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the implementation agency to take corrective action; etc.

MSA also has some specific clauses that emphasize building security requirements as per the legal norms. It says, "the implementation agency shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Act or Telegraph Act." In the management phase, specific consideration is given to security and safety

Security and Safety:

- The implementation agency shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Act or Telegraph Act, including the regulations issued by the department of Telecom (wherever applicable), IT Security Manual of the Nodal Agency as specifically stated in the RFP and follow the industry standards related to safety and security (including those as stated in the RFP), insofar as it applies to the provision of the services
- Each party to the SLA/agreement shall also comply with the Nodal Agency or the Government of India, and the respective state's security standards and policies in force from time-to-time, at each location, of which the Nodal Agency or its nominated agencies make the implementation agency aware in writing insofar as the same apply to the provision of the services
- The parties to the SLA/agreement shall use reasonable endeavours to report forthwith, in writing to each other, all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any party) either to gain access to or interfere with the Nodal Agency as the case may be or any of their nominees data, facilities or confidential information
- The implementation agency shall upon reasonable request by the Nodal Agency as the case may be or their nominee(s) participate in regular meetings when safety and information technology security matters are reviewed
- As per the provisions of the SLA or this agreement, the implementation agency shall promptly report in writing to the Nodal Agency or its nominated agencies, any act or omission which they are aware of, and could have an adverse effect on the proper conduct of safety and information technology security at the facilities of the Nodal Agency as the case may be

It is mentioned that any negligence in performance of services that directly cause any breach of security, like hacking, aren't forces of nature and hence, wouldn't qualify under the definition of 'Force Majeure.'

It reads: "In so far as applicable to the performance of services, service Provider will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes and technology to prevent any breach of security and any resulting liability therefrom (wherever applicable). Thus, the intent to have a secure software, and establishing accountability for the same, can be observed.

Audit rights are also a key element in the guiding document, and it highlights as a necessity the need to verify:

- The security, integrity and availability of all data processed, held or conveyed by the partner on behalf of the Nodal Agency and documentation related thereto
- Security audit and implementation audit of the system shall be done once each year, the cost of which shall be borne by the implementation agency

There is also lack of awareness around this document. Though few of the security-related clauses are covered, the coverage of security-related aspects can be increased to make this document a single reference point, for the security needs to be built into contracts, SoWs or SLAs.

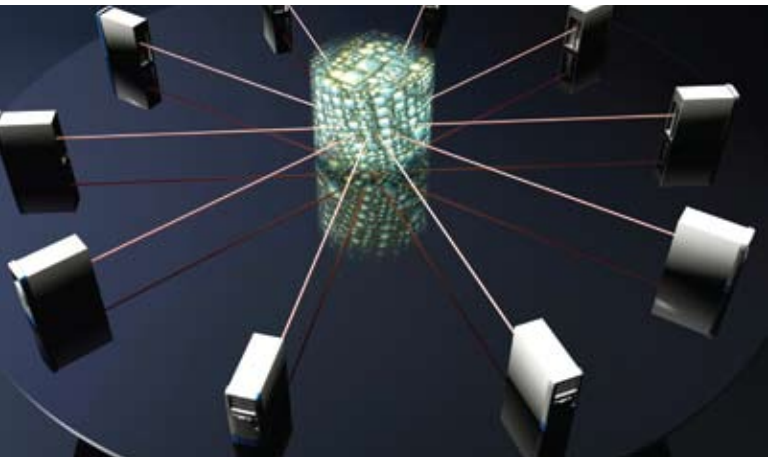
DeitY has also prepared a Project Lifecycle and Quality Assurance Framework (QAF) that is covered in Quality Assurance Framework (QAF) document, including the procurement phase[11]. QAF indicates the general operational principles and technical aspects that a quality assurance exercise should incorporate when customised to the requirements of a specific e-Governance project. This also includes security-related aspects at a high level.

DeitY also came out with a draft framework on Open Source Software Adoption in e-Governance Systems[12] in September 2013. It lays down the requirements to be considered, including security perspective, before and after a software is inducted. Specific to the procurement guidelines for OSS, security is listed as a factor for evaluation before induction, but details on what it would constitute are missing. It says specifics of security would be considered on a case-to-case basis.

The following procurement lifecycle map has been developed based on our interaction with government departments and entities, consultants, vendors, service providers and system integrators during the interview process and secondary research. This outlines a broad contour of the procurement lifecycle, for procurement of work, goods and services. Software procurement too, follows this lifecycle. All departments may not exactly follow these steps for procurement, as they may have evolved their own set of practices, but their practices and steps will map to the corresponding phases of the lifecycle.

1. **Requirement Identification and Definition:** A government department or agency that identifies the need for procurement of software for any project, including e-Governance projects, usually begins with a requirement identification exercise. For this, a background study is conducted by the project team, to list down the aim and objectives of the project and corresponding requirements, to fulfil these objectives. When adequate listing has been accomplished, after inputs from all of the relevant stakeholders, the requirements are put up in a prescribed format by the project team. Inputs from technical, legal and commercial aspects are built in this stage to ensure feasibility of the project

   In the absence of prescribed standards and guidelines, the requirement gathering process is not standardized across governments. At requirement identification and definition stage, inputs from different stakeholders are gathered. Usually, there is not much interaction with IT security team on issues outside the basic security deployment. Some of the government departments and few of the state governments make a point to include inputs from the security viewpoint, at least in key projects. Here, inputs from users of software also form an important component. External consultants are also engaged to ensure comprehensive requirement gathering. Involvement of experts from specialized government department such as NIC, CERT-In, or STQC is sought at this stage. From the sample lot interviewed, few of the major MMP projects consistently engage subject matter experts, usually from consulting firms and other security experts including those from the government, to clearly define the requirements.



2. **Financial Analysis and Feasibility:** The viability of the project, from a financial viewpoint is analyzed and a budget estimate is prepared. The finance team also takes inputs from various stakeholders to determine if any of the requirement definition is absolutely mandatory or just optional. This step could help neutralize a budget overshoot problem, in case any specific requirement is leading to a high cost estimate. The final budget is then sent to the project team for approval and budget is sanctioned. The budget sanctioning, again, is not consistent and depends on a case-to-case basis.

[11]https://egovstandards.gov.in/published_standards
[12]https://egovstandards.gov.in/system/files/PublicReviewDocument/Framework_on_OSS_Ver0.8.pdf

During interaction with different stakeholders, it was found that getting funds for security components is not a major challenge in a majority of the organizations. Organizations interviewed, have indicated that security requirements are usually not compromised for budget overshoot problems. But security requires consistent maintenance and update, given a dynamic and complex threat landscape, and organizations usually struggle to consistently allocate funds for security, in the later stages of software lifecycle management, if recurring allocation isn't identified and approved from the very starting.

3. **RFP Formulation:** A separate committee is set up to formulate an RFP for the project. Departments that procure more regularly and extensively have a dedicated procurement cell usually headed by an officer of senior rank in the department. The number of resources employed is typically proportional to the scope and size of the project. RFP for procurement of software usually has three different components which are technical, legal and commercial.

   For formulating an RFP, the requirement definition is converted into different components. Very few government departments and state governments refer to model RFPs issued by DeitY while formulating RFP for their projects; however, most stakeholders were found to be unaware of its existence. It is worth noting that the model RFP is only meant to provide guidance, and it is not mandatory to use model RFP components.

   For major MMP projects, at behest of the project team, the committee team consists of an expert from one of the DeitY departments – NIC or CERT-In or STQC. However, this is not witnessed across all the projects, but only a critical few. It is more of a best practice that is followed to ensure that requisite security functionalities are built as a part of RFP; and their inclusion is not mandatory. They also act as a checkpoint to ensure that desired security aspects become an integral part of the RFP – level of security depends on project-to-project basis. Requirements in RFP are built in a manner to avoid vendor lock-in of software, or service provider, or even the technology platform. Some departments and state governments also

engage external consultants for getting adequate inputs for RFP formation, given the importance of this stage.

In some RFPs, especially for critical projects at both central and state level, detailed security requirements were specified, while in others these were not very well-defined. Skill development training of software development teams on latest updates in application security and secure coding practices, is one of the requirements that is majorly put forth in quite a few of the RFPs involving development of software for major projects. Tested and certified software, usually on global standards, are given precedence in the RFP requirement. Common criteria certification requirements, such as attaining specific EAL levels for software products, are also listed in few of the RFPs. Although not found in many RFPs, some organizations specify the aspects such as source code ownership and other IPR-related pieces are covered.

After the review of a few RFP documents of key central and state government departments and some of the MMPs, non-standardization of clauses, specific to security requirements, strongly emerge. Even RFPs issued by the same department, but for different projects, sometimes do not have comparable security requirements. Some RFPs do not have security component at all, and project team expects the bidder to follow global best practices for security that they have adopted for the project, without necessitating security requirements

upfront. Contrastingly, in a few RFPs of critical and sensitive projects, the security requirements that are published have surpassed the level of security requirements mentioned in the Model RFPs, elevating the importance of security. This disparity arises because of how much weightage and importance that should security be given if the software being procured is essentially a product of department's vision and project team's understanding about security, in absence of any mandatory requirements for establishing security as an important component of RFPs in software procurement.

4. **Floating of RFP:** There are two ways of floating RFP – One is open, wherein the requirements are published, and there are some requisites that form pre-qualification criteria. Anyone who fulfils the qualification criteria and is willing to provide a software solution against the requirements that are submitted, can respond to RFP. Another is limited RFP, where pre-identified set of bidders, usually pre-registered bidders, are contacted to submit their response against the requirements.

5. **Pre-bid Meeting:** Some of the e-Governance projects that are highly complex in nature or have a massive scale, call for a pre-bid meeting of bidders to provide clarification, if any, over the requirements of the software solution they intend to procure. Clarification may also be sought on other aspects such as legal, commercial, architectural requirements. Usually a Q&A session between the bidders and project team would help clear doubts. Any special requirements that are not extensively explained in the RFP can be clarified.

   Security aspects usually form one of the most queried clarification items in such sessions. It is also a stage where providers of software showcase their limitations, if some aspects of the RFP and software requirement, including security features are not practical or difficult to build.

6. **RFP Response Gathering and Evaluation:** Detailed response to RFP, in prescribed format, is submitted by the bidders. There is a bid security fee, often called registration fee, which needs to be submitted as a part of the RFP procurement lifecycle process. Submission against technical and commercial aspects of the RFP, and also legal compliance details, have to be submitted separately by the bidders. Once all the responses are received and the bidding date is closed, they are evaluated based on the evaluation method prescribed in the procurement process. In processes where technical evaluation is required, parameters of evaluations are prescribed. Different evaluation methods are discussed in the section.

   The technical response from the bidders is evaluated before the commercial bids. At the evaluation stage too, experts from different departments of DeitY and/or industry experts and consultants are engaged for evaluation of technical bids. If need arises, the vendors who have submitted response against the RFP can be asked for clarifications sought by the technical evaluation committee. Interviews with stakeholders reveal that security features and related aspects are evaluated only against the requirements specified in the RFP, and extra features which vendors offer above and beyond software requirements aren't usually a factor in the selection, unless the features address other critical issues. In majority of the projects, we found that during the technical evaluation, scores are given against each of the parameter separately and that is used to derive an overall score for the technical aspects. Critical projects have additional weightage for security aspects. This step is important as it would clearly list down how the software would perform on

security parameters. Weightage is also given based on vendor's profile of executing projects of similar nature.

Evaluation of commercial bids is dealt with separately and then overall score is derived to finalize the bidder.

7. **Software Selection Process:** The selection is based on the factors initially identified in the process of procurement – whether the selection is on lowest cost or on the quality of software or a mix of both quality and cost or otherwise. If stated earlier as a part of the process, negotiations with the final selected vendor takes place, to arrive at a common ground with all the requirement expectations. At this stage, security aspects can also be negotiated, in terms of actual deliverables that would feature in the software.

Selection of software for procurement is mostly done by following one of the methods described below. The practices listed below are some of the methods of procurement that are prescribed and are in use by government departments and agencies. The process for selection usually depends on the size and scale of the project, risk associated, nature of software being procured, technical architecture of the organization, etc.

Cost Based Selection (CBS) or Least Cost Selection (LCS)	Used commonly, this method is suitable especially in cases where the requirement is basic in nature or is highly standardized, with limited requisite technical detailing and not much to differentiate the quality of competing developers. With bid applicants meeting the minimum technical requirement that is specified, the one with lowest cost wins after all the submissions against RFPs are opened. As security requirements are generic, or form a minor component, or are sometimes nil, lowest cost gets priority.
Quality cum Cost-Based Selection (QCBS)	In this method, evaluation is done based on the cost proposal submitted by the bidder and the technical specification and/or qualification of the bidder In such projects a due diligence is also done on the critical parameters of the project covering system functionality, technology, specific implementation experience, training methodology, performance in proof of concept (in case PoC is planned), certifications, past experience of the vendor in executing similar assignments, size of those assignments, profile of team members and project methodology. Usually the technical proposals will be allotted a weightage of 70% while the financial proposals will be allotted weightage of 30%, but it varies from department-to-department and project-to-project. Security aspect is an important component of technical aspects, but varies as per the requirement specification of the department procuring the software. This is one of the most widely used methods as technical requirements gain precedence over cost concerns. The weightings must be disclosed in the tender document. When the options are evaluated, scoring against each of the component is provided to arrive at an overall technical score rather than coming up with an overall score for the solution.

Fixed Budget Selection (FBS)	In this method, the RFP shall indicate the available budget and request the systems implementation agencies/system integrators to provide their best technical and financial proposals in separate envelopes, within the budget. The points as mentioned in QCBS, are applicable in this case also, with a difference, that here budget is pre-defined and bid entries should not exceed prescribed budget.
Quality Based Selection (QBS)	Under QBS method, the systems implementation agency/system integrator who has secured first rank in technical evaluation alone shall be called for further negotiation after opening and evaluation of its financial proposals. It is usually preferred before going for 'nomination' based procurement decision and vendor selection. The points as mentioned in QCBS above, are applicable in this case also.
Single Source Selection (SSS)	This method does not provide the benefits of competition in regard to quality and cost, lacks transparency in selection and could encourage unacceptable practices. Therefore, single source selection is used only in exceptional circumstances such as cases where selection of one vendor is necessary for operations of project or functionality of the project is impacted in some form by opting for other software solution, extension of existing contracts, standardization of software to be compatible with existing architecture and technology landscape, proprietary equipment obtainable only from one source, process design requires the purchase of critical software from a particular supplier as a condition of performance guarantee or in response to natural disasters.

The first two methods are the most popular methods for software procurement. The choice depends on the government agency's requirements and on the nature of the software being procured. Whereas QCBS is the most commonly recommended method, other methods such as LCS, QBS, selection under FBS or SSS may be adopted depending upon the nature and size of the assignment, continuation of the previous work, urgency of selection, and whether the number of qualified firms for the particular assignment is limited.

The importance assigned to security parameters during evaluation would determine how important is the issue being perceived by the organization procuring the software. Few organizations emphasize security when it comes to evaluation of software. It is not the most significant factor in deciding between competing software products. Some organizations, however, for critical projects, assign significant weight to security. Rising sensitization towards security issues and the perceived need to have reliable, secure and genuine software is steadily changing the landscape on the basis of the importance of security concerns.

8. **Contract signing and SoW Creation:** In this phase, a contract, usually the Master Service Agreement (MSA), is signed between the vendor and government department to lay down terms of engagement. In case the vendor is already registered; Statement of Work (SoW) is prepared that clearly pens down the exact requirement and deliverables expected as a part of the project. Here, detailing of the product specification and requirement is done.

   From most of the organizations interviewed, it was found that the process for development of software, for example secure coding or secure SDLC, is put up as a requirement. Generic security requirements such as, how the vendor will show evidence of software security testing processes and outcomes, the security acceptance criteria, how quickly and in what manner will the vendor communicate the discovery of vulnerabilities, the allowable time-to-fix for vulnerabilities, and the penalties for non-compliance or non-adherence to SLAs, etc. are considered in the contract more often than not. Very few of the projects that we came across go to an extent of stating conditions such as the right to audit

the development environment, source code ownership, defining exact security considerations and asking vendors to demonstrate compliance to standard or prevalent best practices. Along with Model RFP, DeitY also came out with Model MSA. None of the organization interviewed seem to have referred to it while drafting their own MSA or SoW. In absence of prescribed standards on general requirements, the level of detailing mostly depends on the procurement team's expertise and desire to put forth security requirements upfront, while all the important aspects may not be covered as a part of the agreement.

9. **Acceptance:** Once the software solution is ready to be procured, pilot testing is done to check functionality and feasibility of the software on all parameters. Security testing is one of the most important parameters for testing before software can be used in a live environment.

   Some stakeholders said that for Commercial Off-The-Shelf (COTS) products, this step is usually skipped – although third-party testing and certification framework such as Common criteria are well-recognized and accepted – as it also was evident from some RFPs. In case of website procurement, most of the government departments rely on global best practices such as OWASP for testing. Few departments recommend ISO 27001 as the baseline criteria against security requirements in the software. Departments such as NIC have prepared their own security testing manual and every website developed by NIC for any department is tested against these requirements. While automation is used to the extent possible in testing phase, manual testing is also emphasized by a few. Large number of departments also require third-party testing of website, usually by CERT-In empanelled auditors. Some critical projects have the requirement of obtaining certification from STQC, which is also a CERT-In empanelled agency, for testing of websites. Testing requirements and parameters vary from project-to-project. This step attains utmost importance in case the software being procured is an open source software. For other softwares, black box and white box testing and in some cases, grey box testing is also carried out to validate the security requirements. Some organizations demand full code review on security aspects. Assessment of authentication mechanism, access privileges provided in the application or components or modules is also undertaken for sensitive projects, dealing with personal information, and given sensitization towards privacy in the recent times. In addition, unit testing and integration testing are also carried out, either by vendor or by the procuring agency itself. However, modern practices such as fuzz testing, etc. aren't yet looked upon as a need to have the requirement amongst government agencies.

10. **Deployment and sign-off:** After software has been tested thoroughly and evaluation attains acceptance from respective stakeholders, it is deployed and sign-off is obtained. Some security problems will not show up until deployment into an organization's staging or production environment, so such testing is very desirable and is used as a tool by organizations, as a final check for the product.

    In some projects, only software development and deployment is a part of the scope. In other cases, however, deployment of software is only one of the phases and the entire lifecycle management of software is covered. This includes the maintenance and change management cycle, including management of software from all aspects. Since, software security requirements evolve over the life of the product, a patch management cycle generally is deployed. Patches are used to enhance software functionality, address vulnerability issues or fix bugs, and are deployed after a thorough testing

in test environment. Generally, vendors do not have direct access to modify or update the software in the live environment. Updates usually are approved by the project team before being deployed in the software. Some departments also require periodic audit and testing and, in certain cases, attaining certification. For the majority interviewed, secure software disposal did not appear as a part of the lifecycle. The issue of code ownership, on who owns the source code of the software, appeared in select interactions. Projects in the which IPR-related aspects aren't clarified in earlier phase of project lifecycle are settled at later stages, nearing closure.

Software Procurement Lifecycle Summary: Security Viewpoint

For the entire software procurement lifecycle in most projects, we have observed that security aspects are not given due emphasis at all stages. Lapses on security at any stage might result in a software product that is vulnerable from a security point of view. At a high level, it can be argued that central government projects are slightly better sensitized towards the security requirements than state government projects though there are quite a few projects at state level that have security high, on priority. How well security as a component is placed in the project and in the software, also largely depends on the expertise and sensitization of the individual or team spearheading the project.

Some of the issues that surfaced are attributed to lack of legal framework and in the absence of a legal framework, lack of mandatory guidelines by the government. The practices followed by different entities aren't standardized and vary in maturity across different areas. The lack of awareness among stakeholders, about Model RFPs being prescribed by DeitY for example, also leads to non-standardization. Unless governments elevate the role of security and establish practices that address security concerns throughout the procurement lifecycle, the security concerns in software and also in the supply chain, may largely remain unchanged.

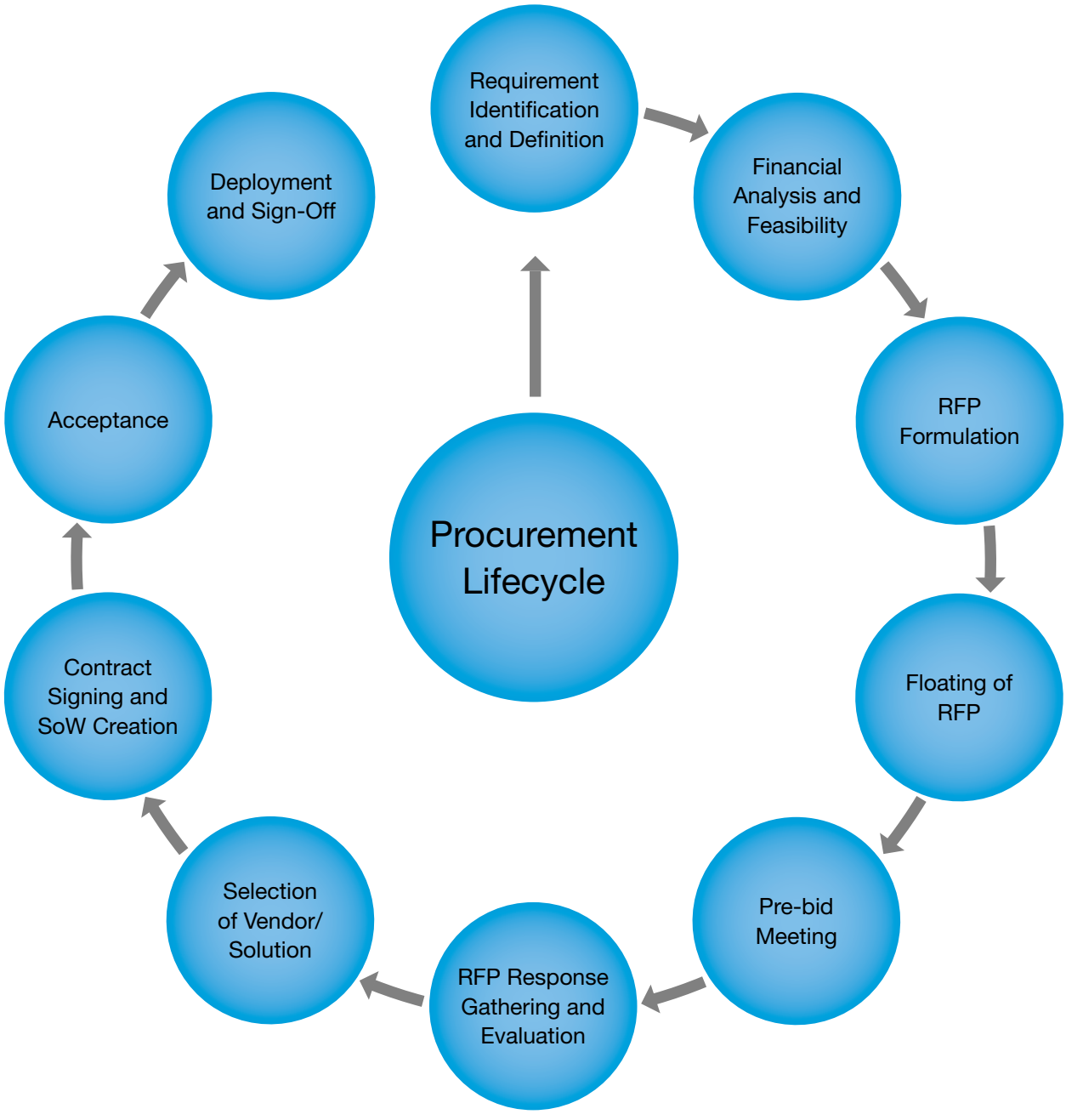


Figure 1: Software procurement lifecycle usually followed by government agencies in India

GLOBAL FINDINGS AND DEVELOPMENTS

A study of policies, laws and regulations of other countries including the United States, the United Kingdom, Japan, Australia and Singapore, among others, was conducted to determine best practices, contemporary developments and key learnings. Some of the below stated may not be attributable to all or most of the countries studied but may be specific to a particular country. For findings related to specific countries (the US, the UK and Japan) please refer to the Appendix.

Policy and Legal Framework

- A policy, law or regulation requires government agencies to develop and implement an information security program. Such a policy, law or regulation itself may not contain any specific provisions governing the security aspects of procurement of software in government agencies, though other policies or regulations may govern such aspects. However, it is implied that the information security program will have components that address security risks in the procurement of IT, including software
- The procurement-related policy, law or regulation will prescribe specific requirements to be considered by government agencies while procuring IT, including software. Such requirements can range from risk analysis to common security configurations to contract management

Rationale: *Given the responsibility of the government to protect citizens' and businesses' data and interests and unlike the private sector, lack of market drivers to address security risks, a mandatory policy or law or regulation is perhaps required.*

Implementation of Policy and Legal Framework

- A government agency is assigned responsibility to ensure that the policy and legal framework is implemented by the government agencies. This agency is authorized to solicit information from the government agencies, vis-à-vis compliance to the policy and legal requirements governing software procurement and evaluates their performance periodically. Additionally, the agency also provides advisories and guidance to the government agencies from time-to-time

Rationale: *For effective enforcement of the policy and legal framework within government. Also, helpful in establishing a single point of contact agency for all government agencies vis-à-vis policy or law-related advisories and guidance.*

Agency for Technical Assistance

- A dedicated agency provides technical guidance, through standards and guidelines, to government agencies to address the security risks when procuring software. Such an agency is empowered by the policy and legal framework to perform its functions. This agency develops and notifies standards, guidelines, best practices, checklists, etc. to help government agencies in addressing software security-related risks and comply with the policy or legal requirements

Rationale: *For addressing the issue of lack of technical competence and know-how within the government agencies vis-à-vis management of software related security risks. Also, helpful in harmonizing security requirements of government agencies and establishing standardized requirements and practices.*

Software Assurance Through Testing and Certification

- Governments and industry are making efforts to address governments' procurement-related security assurance requirements through ISO/IEC 15408 (Common Criteria) and the Common Criteria Recognition Arrangement (CCRA). It is being advocated that the requirements related to software assurance should be addressed by developing Collaborative Protection Profile (CPP) under CCRA, that is based on or aligned to the international standards. The software can be tested and verified against this protection profile

Rationale: *Government agencies often face similar security threats and hence, have similar security requirements. It will be beneficial for IT organizations as this would eliminate the need to test and certify same IT products across different countries.*

Authorization of Cloud Services for Government Usage

- Empanelment of cloud service providers including SaaS service providers is done by a government agency based on a well-defined authorization program that takes into account the common security requirements of all government agencies. The cloud service providers are required to implement the prescribed common security requirements and then get themselves evaluated by a government-approved third-party assessor. Based on the assessment findings, the responsible government agency authorizes the cloud service provider to provide cloud services to the interested government agencies

Rationale: *Provides a single window for security clearance through competent authority, giving boost to the adoption of cloud services within the government. Harmonizes the security requirements of government agencies and provides a cost-effective, predictable and standardized way of managing security risks. Beneficial for the private sector because of consolidated security requirements and access to government cloud market post one authorization.*

The above global findings have been taken into consideration while developing the recommendations, keeping in mind the Indian context.

RECOMMENDATIONS

POLICY AND LEGAL FRAMEWORK

The following recommendations have been developed taking into account: the views expressed by the government and industry experts in the interviews conducted, learning from the study of policy and legal framework in other countries and the Indian context.

1. Government should incorporate the information security requirements in the procurement of software by government agencies, both central and state agencies. This may be achieved either by (a) passing a new legislation or regulation, that may require government agencies to have a demonstrable information security program, which should also include components for addressing software risks, OR (b) revising existing procurement-related regulations or guidelines to include a requirement for the incorporation of security requirements by government agencies when procuring software. The policy and legal framework should recommend incorporation of security requirements that are based on international standards and best practices such as ISO/IEC 27034 and ISO/IEC 15048. The policy and legal framework should enable government agencies to take full benefits of the global software supply chain, that includes access to best-in-class software and expertise at competitive prices, and not create unreasonable restrictions on the procurement of software based on security considerations.

2. Through the policy and legal framework, the government should work towards eliminating counterfeit and unlicensed software from government software supply chains in order to reduce vulnerabilities and strengthen security.

3. To provide procedural and technical guidance to the government agencies vis-à-vis meeting the legal or regulatory requirements, the government should assign the responsibility to a dedicated agency to act as a Centre of Excellence (CoE). This agency also would develop and promote standards, guidelines, processes, tools, checklists or other instruments to assist government agencies in meeting the prescribed security requirements when procuring software. Such an agency may be established leveraging the public-private partnership models. Involvement of the private sector will help bring the required agility to devise solutions to address software security-related issues and risks, which are very dynamic in nature. The CoE should also act as a platform to share information, best practices and concerns between government agencies and software providers and facilitate problem solving. Specifically, the CoE could perform the following functions, among others:

I. Raise awareness about international standards and industry's best practices around secure software development and procurement. If required, develop and notify new standards and guidelines.

II. Establish collaboration mechanisms between government agencies for sharing information and best practices.

III. Conduct regular trainings of government officials responsible for software procurement, government chief information security officers, software developers, administrators, vendors, contractors, etc.

IV. Define government security requirements for software in consultation with government agencies and work towards including them as inputs in the development of collaborative protection profiles under the Common Criteria Recognition Arrangement (CCRA).

V. Define model provisions that may be incorporated in the government RFPs and contracts.

VI. Contribute in the development of international standards and guidelines vis-à-vis software security.

4. In cases where the software is required to be security tested before procurement, the testing should be done using international standards (such as the Common Criteria). The CoE can work toward defining the software security requirements in consultation with the government agencies (similar to collaborative protection profiles under CCRA), against which the lab can test and certify the software. The testing labs could be established in the private sector after proper accreditation by the responsible government agency. The staff of the testing labs should also be trained and certified in software testing through a training and certification scheme. The testing labs should implement appropriate safeguards to protect the intellectual property rights of the software providers and should not create any administrative hurdles for the providers. The government should also accept testing done in foreign labs, which is based on international standards such as Common Criteria under the CCRA. This will ensure use of standardizing testing methodologies and processes to bring predictability in testing.

5. For procurement of SaaS services by the government from the private sector, there should be an empanelment mechanism for authorizing SaaS service providers. This empanelment process should assess the security capabilities of the SaaS service providers and SaaS services, preferably through an independent third-party assessor. After authorization by the competent authority, the SaaS service providers should become eligible to supply SaaS services to all government departments.

6. The government, in partnership with industry, should create a national awareness campaign to educate different stakeholders including the IT, security and procurement leads of central and state government agencies on software security-related issues, policy and legal requirements, guidelines and best practices.

POLICY, PROCEDURAL, ADMINISTRATIVE AND TECHNICAL (ORGANIZATIONAL)

In the absence of legal or regulatory requirements and established standards and guidelines, the following practices may be followed by central and state government agencies. For specific guidance that may be required to implement the recommended practices, the agencies should work closely with the respective central and state expert agency or take help from expert bodies outside the government or organizations or academic institutions.

1. **Software Procurement Policy:** Includes security considerations in the software/ IT procurement policy of the agency. The policy should require integration of security requirements across the software procurement lifecycle including those related to eliminating counterfeit and unlicensed software.

2. **Roles and Responsibilities:** Define security-related roles and responsibilities of different stakeholders (security, procurement, legal, finance, etc.) involved in the procurement of software across the software procurement lifecycle.

3. **Risk Management:** Ensure that software-related security risks are assessed in the organizational risk assessment process and that appropriate and adequate risk mitigation measures are put in place to address the identified risks.

4. **Application Architecture:** The application architecture of the organization should take into account the software security related aspects, to ensure effective integration of security requirements.

5. **Classification of Software:** Classify software based on its criticality. This can be achieved by conducting a business impact analysis of the applications, which can take into account various parameters to determine criticality – sensitivity of government services provided, number of citizens accessing the application, nature of transactions performed, and processing of sensitive personal information, among others. The security requirements should be defined in accordance with the criticality of a particular application.

6. **Security Requirement Definition:** Define security requirements for the software to be procured after consulting all the relevant stakeholders within the organization. It is highly recommended that agencies also consult security experts outside the organization. To the extent possible, security requirements should be based on or aligned to international standards and best practices such as ISO 27034. In general, the following parameters can be considered for defining the security requirements, but not limited to:

- International standards and best practices
- Software procurement policy
- Information security policy
- Government guidelines or norms
- Security principles such as confidentiality, integrity, availability, authentication, authorization, auditing, configuration management, session management, exceptions, input and output validation, cryptography, among others
- Criticality of software
- Existing application/IT architecture

7. **RFI/RFP:** Includes the detailed security requirements identified above in the RFI/RFP and very importantly, enquire about the secure software development capabilities of the software provider.

8. **Security in Technical Evaluation:** Include security as one of the evaluation criteria for assessing software and/or a software provider. Set up a technical evaluation committee comprising relevant internal stakeholders and trusted security experts to assess the security capabilities of the software and software providers and evaluate whether they meet the security requirements.

9. **Industry Best Practices[13] for Secure SDLC:** Below are some of the secure SDLC best practices followed in the industry. **These may be used by the government agencies to evaluate software providers:**

   I. *Training* – Conducting regular trainings of project managers, architects, developers, testers, others on security

   II. *Requirement Definition* – Defining the security requirements across architecture and design, development and programming best practices and requirements for assurance, testing and serviceability, at the early stages

   III. *Design* – Following security engineering principles such as least privileges, separation of duties, etc.; analysing the attack surface

[13] http://www.safecode.org/publication/SAFECode_BestPractices0208.pdf

to reduce the opportunities for exploitation of potential vulnerabilities, performing threat modelling to find vulnerabilities and identify ways in which they may be exploited

IV. *Coding* – Incorporating necessary secure features in the development stage, using secure coding practices, conducting code review prior to compilation (static analysis)

V. *Code Handling* – Careful handling of source code, through change management and integrity checks so that only authorized persons are permitted to view or modify its contents

VI. T*esting* – Performing run-time verification through dynamic analysis to check software functionality, performing fuzz testing[14], conducting penetration testing

VII. *Documentation* – All the security-related processes followed and measures taken, including verification-related steps should be documented. The software documentation also includes guidance for customers on how to optimally configure security features and the risks of not doing the same

VIII. *Release* – Final verification is done to ensure that all of the security requirements have been met. This also entails that the provider also evaluates and documents risks posed by potential security gaps in the software

IX. *Integrity Verification* – Use of integrity verification techniques to provide assurance to the customers that the software provided is genuine

X. *Incident Response* – Identifying vulnerabilities through ongoing internal research and assessment, reporting mechanisms for external community, gathering intelligence through security solution providers, government bodies, customers, etc.; relaying the vulnerabilities to the development team for fixes and timely communicating to customers; communication with customers for resolving issues through fixes, workarounds, etc.; automation of security patch deployment

10. **Contract Management:** After selection of a software provider include agreed-upon detailed security provisions in the contract or Statement of Work (SoW). Suggestive provisions that may be included (but not limited to):

I. Secure SDLC processes to be followed by the software provider

II. Methods for verifying secure SDLC processes claimed to be followed by the software provider

III. Compliance to security requirements

IV. Integrity verification techniques – Maintenance of chain of custody

V. Configuration of software features for the purposes of security

VI. Right to audit the software provider and organizational premises especially the development environment

VII. Escrow arrangement

VIII. IPR ownership of source code

IX. Geographic locations where software development takes place

X. Right to conduct security testing of the software

XI. Vulnerability management and incident response – Liabilities, time frames for supplying fixes, workarounds, etc.

XII. Acceptance criteria for software releases, including patches

XIII. Support and servicing with regard to security – to ensure after sales technical support

XIV. Documentation related to secure SDLC processes, security features, customization of security features, etc.

XV. Plan for continuous monitoring of security risks and controls

11. Software Acceptance

I. *Compliance Demonstration:* Submission of evidence from the software provider that the agreed-upon security requirements have been met, secure SDLC has been followed and

[14] Fuzz testing is an effective testing technique because it uncovers weaknesses in the data-handling code, that may have been missed by code reviews or static analysis. It relies on building intentionally malformed data and then having the software under test, consume the malformed data to see how it responds – *Fundamental Practices for Secure Software Development, 2nd edition, SAFECode* http://www.safecode.org/publication/SAFECode_Dev_Practices0211.pdf

adequate testing has been done prior to the release of address against known and unknown vulnerabilities and the malicious code

II. *Integrity Verification:* Accept verified software/software components to reduce risk of counterfeiting. Techniques such as cryptographically signed software components, time stamping, among others may be used

III. *Configuration:* Ensure that security features and controls are properly configured in the production (live) environment. The software should be hardened as per the policy requirements

IV. *Testing:* Conduct comprehensive testing of the software, through internal or external experts, to validate that it meets security requirements – testing techniques could include – static analysis, dynamic analysis, white, grey and black box testing, fuzz testing and penetration testing

V. *Documentation:* Submission of documentation related to secure SDLC processes including architecture, design, requirements, programming, testing; security features and functionalities, customization of security features and functionalities

12. **Training:** Conduct training of relevant stakeholders, including government users who will use the software, IT administrators, etc. on the security aspects of running and administering the software.

13. **Software Updates and Patch Management:** Implement and enforce policies on software updates and patch management in consultation with the software provider. Regularly upgrade software versions and apply patches. However, do an impact analysis of the updates and patches from a security point of view for critical applications before deploying the patches in the production environment. Ensure that the updates and patches released by the software provider have been developed using secure SDLC processes and have not been tampered with during distribution.

14. **Change Management:** Enforce restrictions to the modification of software acquired and its features through formal change control procedures. Ensure that software undergoes a security review after any major technological or architectural changes within the organization.

15. **Threat and Vulnerability Management:** Keep track of the latest threats and vulnerabilities and if applicable, devise ways to address them. Subscribe to vulnerability advisories and databases and threat alerts. Conduct regular security reviews, audits/assessments, penetration testing, vulnerability scanning, etc. Report the identified vulnerabilities to the software provider for timely resolution.

16. **Software Asset Management:** Establish infrastructure, processes and roles necessary for the effective management, control and protection of software assets, throughout all stages of their lifecycle. Multi-part international standard ISO/IEC 19770 on software asset management could be used for this purpose.

17. **Security Policy Compliance:** The security controls as prescribed in the information security policy of the organization, should be applied to software/ applications – asset management, licensing requirements, access control, segregation of duties, protection of personal information and business continuity, among others.


STORAGE
DETECTION PROCESS
BIOMETRIC SCAN PROGRESS

APPENDIX 1 (COUNTRY-SPECIFIC ANALYSIS)

UNITED STATES

Policy and Legal Framework

There are laws, regulations and policies in the United States that govern the acquisition of information technologies, including software by federal agencies. Some of these are about information security in general, while others are specific to security considerations in the procurement of IT.

FISMA, 2002

The Federal Information Security Management Act of 2002 (FISMA) requires every federal agency to establish an information security program. The Act assigns responsibility to National Institute of Standards and Technology (NIST) to provide standards and guidelines to federal agencies on information security, including the minimum security requirements that need to be adhered to by the agencies. The Act also prescribes independent auditing of the security program and assigns Office of Management and Budget (OMB) the responsibility of overseeing the implementation of FISMA. The Act itself does not contain any specific provisions which govern the security aspects of procurement of software in federal agencies, though there are other important policies, circulars and guidelines that govern such aspects. From a technical viewpoint, the standards and guidelines developed by NIST have specific controls, regarding addressing risks in procurement of ICT products, including software.

The implementation of FISMA has been criticized for focusing on documentation to demonstrate compliance. To address such concerns, FISMA is being revised and in April 2013, the House of Representatives unanimously passed the Federal Information Security Amendments Act of 2013, though it is yet to become a law[15].

Comprehensive National Cyber Security Initiative (CNCI)

With the objective of enhancing federal government skills, policies and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk, an initiative to develop a multi-pronged approach for global supply chain risk management was listed under the Comprehensive National Cyber Security Initiative announced in 2008. Specifically, with regard to supply chain, the CNCI envisaged[16]:

- Creating greater awareness of the threats, vulnerabilities and consequences associated with acquisition decisions
- Developing and employing tools and resources to technically and operationally mitigate risk across the lifecycle of products
- Developing new acquisition policies and practices that reflect the complex global marketplace and

[15]http://beta.congress.gov/bill/113th/house-bill/1163
[16]NASSCOM-DSCI Report – Securing Our Cyber Frontiers, 2012

- Partnering with industry to develop and adopt supply chain and risk management standards and best practices

A Government Accountability Office (GAO) report of March 2012[17], mentions that certain challenges existed in meeting the objectives of CNCI, including defining roles and responsibilities, establishing measures of effectiveness and establishing an appropriate level of transparency (including for supply chain risk management activities) and that steps are being taken to address most of these challenges, including clarifying cyber security responsibilities and activities among federal entities.

OMB Circular A-130

The Office of Management and Budget (OMB) is the implementation and enforcement arm of the Presidential policy, government-wide. It reports directly to the President and helps a wide range of executive departments and agencies across the federal government to implement the commitments and priorities of the President. OMB issued Circular A-130[18] to establish a policy for the management of federal information resources. The circular includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices. From a security point of view, the circular prescribes incorporation of 'security into the architecture of information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into lifecycle budgets for information systems.' Specific to acquisition of IT, the circular states:

- Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information technology
- Structure major information systems into useful segments with a narrow scope and brief duration. This should reduce risk, promote flexibility and interoperability, increase accountability and better match mission need with current technology and market conditions
- Acquire off-the-shelf software from commercial sources, unless the cost-effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes

To achieve the stated security objectives, Appendix III of the circular – Security of Federal Automated Information Resources – provides further guidance and very importantly, assigns responsibilities of different federal agencies or departments including the Departments of Commerce, Defence, and Justice, and the General Services Administration (GSA), among others. While one of the important responsibilities of the Department of Commerce, through NIST, is to develop and issue security standards and guidance, GSA has been assigned the following responsibilities including those related to acquisition of IT:

- GSA should provide agencies, guidance for addressing security considerations when acquiring information technology products or services
- In addition, where cost-effective to do so, GSA should establish government-wide contract vehicles for agencies to use and acquire certain security services
- GSA should also provide appropriate security services to assist federal agencies to the extent, that provision of such services is cost-effective

Federal Acquisition Regulations (FAR)

The Part 39 of the FAR regulations prescribes the policies and procedures to be used in the acquisition

[17]GAO-12-361, IT Supply Chain: National Security Related Agencies Need to Better Address Risks
[18]http://www.whitehouse.gov/omb/circulars_a130_a130trans4#8

of information technology by or for the use of federal agencies pursuant to OMB Circular No. A-130. Following are the key provisions of Part 39:

- In acquiring IT, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from NIST
- Prior to entering into a contract for information technology, an agency should analyze risks, benefits and costs. Reasonable risk taking is appropriate as long as risks are controlled and mitigated
- Agencies shall ensure that the contracts for information technology, address protection of privacy in accordance with applicable laws and regulations
- The contracting officer shall insert a clause, in solicitations and contracts for information technology which require security of IT, and/or are for the design, development or operation of a system of records using commercial IT services or support services

GSA Acquisition Regulation

The GSA manages federal property, including operating and maintaining buildings, supplies and transportation acquisition and communication management[19]. The GSA clause GSAAR 552.239-71 'imposes significant obligations upon contractors by requiring contractors to afford the GSA access to the contractor's and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Such access is to be provided to the extent required in the judgement of the GSA in order to conduct an inspection, evaluation, investigation or audit (including vulnerability testing), to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data and to preserve evidence of computer crime.'[20]

There is also a requirement for government contractors to submit an IT security plan that complies with the FISMA and other federal laws and regulations.

President Obama's Executive Order for Improving Critical Infrastructure Cyber Security

In February 2013, President Obama issued an Executive Order (EO) for strengthening the cyber security of critical infrastructure in the United States. Though the EO does not specifically apply to government agencies, it would apply to those government agencies that own and operate critical infrastructure. With respect to IT procurement, the EO instructs the concerned authorities to make recommendations to the President on the 'feasibility, security benefits and relative merits of incorporating security standards into acquisition planning and contract administration. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cyber security.' These recommendations once finalized will likely result in changes to the existing IT acquisition practices, in the government agencies.

FedRAMP for Procurement of Cloud Services

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.[21] The mandatory scheme is operated by GSA. 'The FedRAMP assessment process is initiated by agencies or Cloud Service Provider (CSPs) beginning a security authorization using the FedRAMP requirements which are FISMA-compliant and based on the NIST 800-53 rev3 and initiating work with the FedRAMP PMO. CSPs must implement the FedRAMP security requirements on their environment and hire a FedRAMP approved third-party assessment organization (3PAO) to perform an independent assessment to audit the cloud system and provide a security assessment package for review. The FedRAMP Joint Authorization Board (JAB) will review the security assessment package based on a prioritized approach and may grant a provisional authorization. Federal agencies can leverage CSP authorization packages for review when granting an agency Authority to Operate (ATO), saving

[19]http://www.usa.gov/directory/federal/general-services-administration.shtml
[20]http://www.dlapiper.com/the-cybersecurity-framework-administration-congress-move-to-incentivize-private-sector-cooperation-strengthen-federal-acquisition-process/
[21]http://www.gsa.gov/portal/category/102371?utm_source=OCSIT&utm_medium=print-radio&utm_term=fedramp&utm_campaign=shortcuts

time and money.'[22] The scheme is operational and at the time of writing this report, 13 CSPs were declared FedRAMP-compliant for IaaS, SaaS and PaaS cloud services.

NIST Standards and Frameworks

The legal and policy framework in the United States, establishes the role of NIST to technically assist government agencies to comply with legal, regulatory and policy requirements. In executing its duties and otherwise, NIST has developed and published various standards and guidelines for the consumption of the community – specifically, government agencies. The important ones with respect to procurement of IT systems are briefly discussed below:

NIST Special Publication (SP) 800-53 rev4

FISMA directed NIST to develop (1) the security categorization of federal information and information systems based on the objective of providing appropriate levels of information security according to a range of risk levels and (2) minimum security requirements for information and information systems in each of such categories.[23] Subsequently, NIST published Federal Information Processing Standards (FIPS) – FIPS 199 for classification of information and information systems, into high, medium and low categories. The FIPS 200 requires federal agencies to meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53. After conducting the security categorization based on FIPS 199, organizations are required to select an appropriately tailored set of security controls in line with the minimum requirements in SP 800-53.

The SP 800-53 has been revised four times since the first publication and the latest version was published in April 2013. The SP 800-53 rev4 contains specific controls for the addressing of ICT supply chain risks including hardware and software. The System and Services Acquisition (SA) family of controls provide exhaustive controls, control enhancements, supplemental guidance and references:

Control No.	Controls
SA-1	System and services acquisition policy and procedures
SA-2	Allocation of resources
SA-3	System development lifecycle
SA-4	Acquisition process
SA-5	Information system documentation
SA-8*	Security engineering principles
SA-9	External information system services
SA-10	Developer configuration management
SA-11	Developer security testing and evaluation
SA-12	Supply chain protection
SA-13	Trustworthiness
SA-14	Criticality analysis
SA-15	Development process, standards and tools
SA-16	Developer-provided training
SA-17	Developer security architecture and design
SA-18	Tamper resistance and detection
SA-19	Component authenticity
SA-20	Customized development of critical components
SA-21	Developer screening
SA-22	Unsupported system components

*SA-6 and SA-7 have been withdrawn

[22]http://www.gsa.gov/portal/category/102375
[23]GAO-12-361, IT Supply Chain: National Security Related Agencies Need to Better Address Risks

In addition to System and Services Acquisition family of controls, there are other controls in SP800-53 that touch upon the supply chain aspects as well.

NIST SP 800-39 – Managing Information Security Risk Organization, Mission, and Information System View

Published in March 2011, NIST SP 800-39 is a part of the series of information security standards and guidelines developed by NIST in response to FISMA. This document also meets or exceeds the information security requirements established for executive agencies9 in OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources. The purpose of this document is, 'to provide guidance for an integrated, organization-wide program for managing information security risks to organizational operations, organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.' In line with its purpose, the document does not detail the practices, for managing IT supply chain-specific risks, but is more focused towards developing and implementing integrated risk management within government agencies wherein management of IT supply chain risks is just one part.

NISTIR 7622 – Notional Supply Chain Risk Management Practices for Federal Information Systems

In October 2012, NIST published the NISTIR 7622[24] – Notional Supply Chain Risk Management Practices for Federal Information Systems, which builds on the IT supply chain-related controls described in SP 800-53 and details the ICT Supply Chain Risk Management (SCRM) practices and defines the responsibilities of the acquirer, integrator and supplier for implementation of the practices.

NIST SP 800-161 – Supply Chain Risk Management Practices for Federal Information Systems and Organizations

An initial draft of SP 800-61 was released by NIST for public comments in August 2013. The purpose of this SP is 'to provide guidance to federal agencies on selecting and implementing mitigating processes and controls at all levels in their organizations, to help manage risks to or through ICT supply chains.' The document builds on concepts described in number of NIST publications including SP 800-53, SP 800-39, NISTIR 7622 among others from the supply chain point of view. 'It integrates ICT SCRM into federal agency enterprise risk management activities, by applying a multi-tiered SCRM-specific approach, including supply chain risk assessments and supply chain risk mitigation activities and guidance.'

NIST SP 800-64 rev2 – Security Considerations in the System Development LifeCycle (SDLC)

Published in October 2008, this document is to assist agencies in building security into their SDLC processes. It defines the different phases of SDLC and provides guidance for integrating security activities including roles and responsibilities of different stakeholders.

NIST SP 800-23 – Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products

Released in 2000, this document provides guidelines and recommendations to the federal agencies' acquisition and use of security-related IT products. This document was produced even before FISMA was enacted in 2002 and therefore, its usefulness needs to be established in the context of present usage in federal agencies. Having said that, it has been considered for the purpose of this study.

NIST Preliminary Cyber Security Framework

President Obama's Executive Order for Improving Critical Infrastructure Cyber Security directed NIST to develop a cyber security framework for strengthening security of critical infrastructure. NIST has come out with a preliminary cyber security framework which is structured around functions, categories, sub-categories and informative references. The five core functions are identify, protect, detect, respond and recover. Different security areas of domains of security have been mapped against these core functions. There is no focus on supply chain risks per se, though at many places SA family of controls have been referred to, against different functions and categories. The preliminary framework identifies Supply Chain Risk Management as one of the improvement areas of the framework.

[24]NIST Interagency or Internal Reports (NISTIRs) describe research of a technical nature of interest to a specialized audience. The series include interim or final reports on work performed by NIST for outside sponsors (both government and non-government). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in a more comprehensive form.

UNITED KINGDOM

- "An Introduction to Public Procurement" is a guidance document released by the Office of Government Commerce to set out the key concepts and principles of good procurement. It is intended for senior officials with limited experience of public procurement. It highlights the need of expertise in the procurement process. It also proposes need of specialist input in areas such as security, HR or risk management

- ***All about Open Source – An Introduction to Open Source Software for Government IT Version 2.0,*** document falsifies various myths about open source software. The objective of this document is to provide high level advice, on how to ensure open source software as it is fairly considered when procuring an ICT solution. As a key point of the policy, it highlights 'procurement decisions will be made on the basis on the best value for money solution to the business requirement, after ensuring that solutions fulfil minimum and essential capability, security, scalability, transferability, support and manageability requirements.' UK Government also promotes open standards and re-use, in the Government Action Plan[25], with prominence on security considerations during the procurement

- The ***UK Cyber Security Strategy 2011***[26] underlined the importance of security considerations in defence procurement. Through this, the UK government also intends to raise standards for public procurement and drive forward in the wider cybersecurity market

- In the ***e-Government Interoperability Framework***-Version 6.0[27], the significance of the security was highlighted. Government information systems will be designed to provide protection against the security risks of connection to the Internet, including the ability to protect against the vulnerability of downloading executable content code, that is not authenticated

- Communications-Electronics Security Group (CESG) develops HMG policy[28] for protecting data and advises on its implementation. The ***Security Policy Framework*** (SPF)[29] describes the standards, best practice guidelines and approaches that are required to protect UK Government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk managed approach to security, that enables government business to function effectively, safely and securely

The Legal Framework

All UK public procurement is governed by the ***European Union Treaty and the EU Procurement Directives and UK Procurement Regulations*** that implement the Directives. In line with the EU directives, the United Kingdom implemented The Public Contracts Regulations 2006[30], The Public Contracts (Scotland) Regulations 2006[31], Public Contracts Regulations 2006 (as amended by the Public Contracts and Utilities Contracts (Amendment) Regulations 2007 and the Public Procurement (Miscellaneous Amendments) Regulations 2011).

There are several international elements to the public procurement rules as they apply in the European Union. The World Trade Organization Agreement on Government Procurement[31] (GPA) covers the national security perspective during procurement.

- UK Government ICT Advice Note for Procurement of Open Source[33] lays down guidelines with regard to security considerations:

    - The security requirement for the ICT solution will need to be considered on a case-by-case basis and specified within the requirements for purchase. It takes the view that 'no one particular type of software is inherently more, or less, secure than the other' and does not favour one type over other. Each must be approached on a case-by-case basis

[25]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61962/open_source.pdf
[26]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[27]http://edina.ac.uk/projects/interoperability/e-gif-v6-0_.pdf
[28]http://www.cesg.gov.uk/policyguidance/Pages/index.aspx
[29]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200550/Understanding_the_SPF___FAQ_April-2013.pdf
[30]http://www.legislation.gov.uk/uksi/2006/5/pdfs/uksi_20060005_en.pdf
[31]http://www.legislation.gov.uk/ssi/2006/1/pdfs/ssi_20060001_en.pdf
[32]http://www.govopps.co.uk/guidance_db_files/guidances/guid_01.pdf
[33]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78962/ICT-Advice-Note-Procurement-of-Open-Source.pdf

- Before approving the use of software (including open source software), managers must ensure that the plan for software support and maintenance is adequate and that the support requirements are specified within the tender documentation. Security requirements are likely to be mandatory within an invitation to tender

JAPAN

With respect to Japan's Government procurement procedures, numerous domestic laws and ordinances have been enacted. These include the Accounts Law (Law No. 35 of 1947), Cabinet Order concerning the Budget, Auditing and Accounting (Imperial Ordinance No. 165 of 1947), and the Local Autonomy Law (Law No. 67 of 1947). As an international rule on procurement procedures, the Agreement on Government Procurement was concluded (effective January 1, 1996). The agreement falls under the framework of the World Trade Organization (WTO), with 42 countries and customs territories, including Japan, as signatory parties as of March 2013.

Each ministry[34] has defined its own procurement guidelines that drive procurement in the respective department. The central government's procurement policy is used as a baseline to derive these ministry-level procurement guidelines. To reinforce national procurement policy, management standards for information security measures for central government computer system were established by information security policy council. Following are the measures that have been put forth in the document.

Information Technology Promotion Agency (ITPA) became the certification body under the CCRA scheme to certify products based on Common Criteria standard, with an aim to 'ensure the security and reliability of information processing, evaluations from a technical perspective the information processing systems'. Japan Information Technology Security Evaluation and Certification Scheme (JISEC) is started by IPA in which Information Security Certification Office is set in JISEC

In the product category list, OS and Database, and explicit security requirements, are mentioned in the document. The evaluation standard is based on ISO/IEC 15408 Common Criteria standard. For procurement, EAL level 3 and above for OS and EAL level 2 and above for database is listed as a selection criteria. A list of security controls that can be used as evaluation parameter has also been defined. Procurement agencies can go above and beyond the prescribed list. These select security functions help in determining the security functionality of the product:

Security Audit, non-repudiation of origin-receipt, cryptographic functionality, access control, data authentication, export data protection, information flow control, input data protection, internal transfer data protection, residual information protection, roll-back, stored data integrity, transfer data confidentiality, transfer data integrity, identification and certification, security management, privacy control, security functionality protection, resource utilization management, TOE access control, trusted paths/channels

Japan's National IT Policy Supports Choice among Open International Standards

In 2007, Japan issued new guidelines for IT, which established that government contracting decisions should consider compliance with open international standards as one criterion among others. The agency drafting the rules publicly stated that the guidelines did not favor one standard over another.

Japan has also signed an agreement with the US Government that says Japanese Government procurement of competitive computer products and services from the United States and other foreign countries will be at par with indigenous production[35]. It covers the following provisions:

- Services covered by the measures related to Japanese public sector procurement of computer products and services:

[34]http://www.mofa.go.jp/policy/economy/procurement/q-a.pdf
[35]http://www.ipa.go.jp/security/jisec/jisec_e/

Security Requirements on IT Systems
(Baseline Requirement)

When purchasing component products for the information system, the Chief Information Security officer shall examine the necessity of selecting the certified products based on 'IT Security Evaluation and Certification Scheme'. If it is necessary and there are multiple candidate products which are equipped with required security functions, he/she shall select the certified product which also satisfies the required assurance level.

(Enhanced Requirement)

Chief information security officer shall request for ST evaluation and ST confirmation (ST: security target, i.e. the security functional design of the system) by the third party if he/she recognizes critical security requirements in the security system being implemented.

Procurement of Equipments
(Baseline Requirement)

Chief information security officer shall specify in the selection criteria that certification based on IT Security Evaluation and Certification Scheme shall be taken into consideration when there are security functional requirements and the procurement is made through the general assessment tendering system.

Software Development
(Baseline Requirement)

Chief Information Security Officer shall request for ST evaluation and ST confirmation (ST: security target, i.e. the security functional design of the software) by the third-party if he/she recognizes critical security requirements in the software being developed.

Operation and maintenance of computers; input of data into computers; development of computer systems, including development of software and systems integration; maintenance of computer software; and other related services

- Services covered by the measures related to Japanese public sector procurement of telecommunications products and services

This covers procurement of hardware and software including customized software.

It is observed that security has been given due prominence at policy level. Several initiatives that drive government procurement are in place. Specific to software procurement, detailed security requirements are built and derived from the government issued guidelines.

APPENDIX 2 (RELATED SECURITY STANDARDS)

International Standards Related to Software Security or Assurance or ICT Supply Chain

ISO Standards

- **ISO/IEC 27001 (Information security management systems – requirements) and ISO/IEC 27002 (Code of practice for information security controls):** These standards together provide specific controls and related implementation guidance for software security – A.14 System acquisition, development and maintenance and A.15 Supplier relationships

- **ISO/IEC 27034 (Application security):** This is a multi-part standard which provides a framework for an achievable and effective secure development process and policy. It does not prescribe a specific set of controls; rather ISO/IEC 27034 is intended to provide a framework to help organizations integrate security, within their existing software development lifecycle. It may be utilized for software applications developed internally, by external acquisition, outsourcing/offshoring or through hybrid approaches. The first part – ISO/IEC 27034-1 is published and focuses on secure software development. This part can also help an organization validate and identify gaps within its current application security program. Additionally, this part can help an organization implement aspects of ISO/IEC 27001 and ISO/IEC 27002 via the systematic approach to risk management. Other parts of the standard are under development

- **ISO/IEC 27036-3 (Information security for supplier relationships –** Guidelines for ICT supply chain security): This is the third part of the multi-part standard ISO/IEC 27036 on information security for supplier relationships and has been published. This part of the standard provides guidance to both suppliers and acquirers of ICT products and services on information security risk management with respect to the ICT supply chain risks, through the integration of risk management processes with system and software lifecycle processes, based on ISO/IEC 15288, 12207 and 27002

- **ISO/IEC 15408 (Evaluation criteria for IT security):** This is a multi-part standard which provides a framework for specifying security functional and assurance requirements of IT products, which can be evaluated by authorized testing labs under the CCRA international arrangement

Major Industry and Other Standards (Not exhaustive)

- **SAFECode**[36]

  The Software Assurance Forum for Excellence in Code (SAFECode) is a non-profit organization

[36] http://www.safecode.org

exclusively dedicated to increasing trust in information and communications technology products and services, through the advancement of proven software assurance methods. SAFECode works to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

Fundamental Practices for Secure Software Development, Software Assurance: An Overview of Current Industry Best Practices, Guidance on Software Integrity Controls, Framework for Software Supply Chain Integrity and Best Practices for Software Assurance are among few collaterals released by SAFECode.

OWASP[37]

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. Its mission is to make software security visible, so that organizations worldwide can make informed decisions about true software security risks.

There are numerous documents published by the OWASP on application security, such as Application Security Verification Standard, OWASP Top 10 – an Industry wide accepted report on 10 Most Critical Web Application Security Risks, OWASP Enterprise Security API (ESAPI) – a collection of security methods that a developer needs to build a secure web application, are few among the complete set.

The Open Group[38]

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. It leads the development of open, vendor-neutral IT standards and certifications.

The Open Group Trusted Technology Forum (OTTF) leads the development of a global supply chain integrity program and framework, in order to provide buyers of IT products with a choice of accredited technology partners and vendors.

[37]https://www.owasp.org/index.php/Main_Page
[38]http://www.opengroup.org/aboutus

APPENDIX 3

SECURITY CONSIDERATIONS IN A FEW PUBLICALLY AVAILABLE RFPs

RFP 1

1. **Software Applications Warranty and AMC of the Application Software**

- Patch management
- Assurance to comply with SLA and other requirements after patch implementation

2. **Evaluation of Technical Bids**

- Security Architecture: Methodologies and technologies for security
- Internationally accepted norms and standards for testing and certification
- Processes relating to the design of solution architecture
- Design of systems and sub-systems, coding, testing, business process description
- Documentation, version control, change control, security, service-oriented architecture, performance in relation to compliance with SLA, metrics, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP

3. **Engagement of professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects.**

RFP 2

1. Technical Advice

I. Security features

II. Well-documented change control procedure & proper integration with adequate security

III. Proper physical & logical controls i.e. IT security policy

IV. Security of the system at

- Software level for user management
- Data, privacy & confidentiality management
- Security policies and procedures

2. Technology Architecture

- Security standard: Data should be encrypted with standard encryption technologies during transmission

RFP 3

1. The software development agency shall prepare & submit System Design Document (SDD)/Process Design Report, which include Security Architecture

2. To maintain information security during transaction, the developed application should support both HTTP and HTTPS

3. The application must have integrated security/ monitoring features with the following:

- Definition of roles and users
- Define role-wise add/edit/view/delete rights for each entry form/report in all modules
- Digital time and user stamping of each transaction

Third-Party Audit (TPA)

The audit may cover one or more of the following aspects of the project:

- Functional requirement review
- Penetration testing of the systems and networks
- Application security assessment
- System performance testing/monitoring
- Review and assessment of security policies

RFP 4

Roles and Responsibilities of Service Provider

1. Security from Virus Threats and Data Maintenance:

- Protecting IT infrastructure and data from virus attack
- Unauthorized access/modification/deletion of data
- Any loss or damag suffered by ESD, departments or citizens due to such causes
- conformance to ISO 20000 27001 compliance
- Contracting certifying auditors and compensation to them for regular audit
- Security audit to be done for every 12 months
- Auditor selection to be approved by the authority

2. Functional requirements of business services

- Any B2C service can be added to the system only with the prior permission and with a view to ensure that the security of application is not compromised

3. Acceptance testing & certification

- Testing and certification by a third-party for software, hardware, networking and security
- A detailed Acceptance Test Plan (ATP) should be submitted by service provider to be reviewed by the authority

4. An exercise of acceptance testing of the systems by department itself and/or through a third-party

RFP 5

1. Security[1]

- The systems implemented should be highly secured
- Identification, authentication, access control, administration and audit and support for industry standard protocols to be provisioned
- Well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system
- Audit trails to be maintained
- ISO 27001 standards of security to be complied
- OWASP top 10 principles to be considered Proposed Application Architecture: Compliance with industry standards to all the aspects of solution, including but not limited to design, development, security, installation and testing

2. STQC Certification

- Functionality audit
- Nature and type of transactions being processed
- Systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc.

3. Review of Network and Website will Include

- Penetration and vulnerability testing
- Security exposures to internal and external stakeholders

4. Information security management

- Security of application and the data contained therein is paramount for the success of this project
- Adequate security measures to be undertaken to ensure confidentiality, integrity and availability of the information

5. Security requirements

- Ensure proper logical access security of all the information assets
- Classify information assets according to criticality
- Provide security including identification, authentication, authorization, access control, administration and audit and support for industry standard protocols

6. Proposed solutions to comply with the security standards and guidelines such as

- ISO 27001
- Information security standards framework and guidelines standards under e-Governance standards (http://egovstandards.gov.in)
- Information security guidelines as published by Data Security Council of India (DSCI)
- Guidelines for Web Server Security, Security IIS 6.00 Web-Server, Auditing and Logging as recommended by CERT-In (www.cert-in.org.in)
- System shall comply with IT (Amendment) Act 2008

7. Solution should support the below security standards

- Authentication, authorization, encryption, secure conversation, non-repudiation, XML firewalls, security standards support, WS-Security 1.0, WS-Trust 1.2, WS-secure conversations 1.2, WS-basic security profile
- A multi-layered detailed security system, covering the overall solution needs having the following features:
- Layers of firewall, network IPS, enterprise-wide antivirus solution, information and incident management solution, two factor authentication for all administrators i.e. system administrators, network administrators, database administrators, audit log analysis
- Database should have received the security certification of at least level 4 (EAL4) from the International Common Criteria for Information Technology Security Evaluation

8. Solution should be

- Able to monitor by periodic information security audits/assessments

  The scope of these audits/assessments may include, but are not limited to, a review of: access and authorization procedures, physical security controls, backup and recovery procedures, and program change controls
- Data in transaction as well as what is stored at various points, is appropriately secured as per minimum standard 128 Bit AES/3DES encryption
- Able to generate a report on all 'Authorization failure' messages per user ID
- Able to monitor security and intrusions into the system and take necessary preventive and corrective actions
- Option to be configured to generate audit-trails in and detailed auditing reports
- Well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system

9. Password Requirement

I. The minimum password policies to be defined
   - Minimum/Maximum password length, alpha-numeric combination of password, compulsory use of special characters minimum password age, password expiry period, repeat passwords, etc.
   - Enforce changing of the default password
   - Stored user IDs and passwords in an encrypted format
   - Passwords must be encrypted using MD5 hash algorithm or equivalent (selected bidder must provide details)

II. Ensure that the user web access shall be through SSL (https), only for all level of communication, for providing higher level of security.

ABOUT DSCI

DSCI is a not-for-profit organization and a focal body on data protection in India. It was set up as an independent Self-Regulatory Organization (SRO) by NASSCOM®, to promote data protection, develop security and privacy best practices & standards and encourage the Indian industries to implement the same.

DSCI is engaged with the Indian IT-BPM industry, their clients worldwide, Banking and Telecom sectors, industry associations, data protection authorities and other government agencies in different countries. It conducts industry wide surveys and publishes reports, organizes data protection awareness seminars, workshops, projects, interactions and other necessary initiatives for outreach and public advocacy. DSCI is focused on capacity building of Law Enforcement Agencies for combating cybercrimes in the country and towards this; it operates several cyber labs across India to train police officers, prosecutors and judicial officers in cyber forensics.

Public Advocacy, Thought Leadership, Awareness and Outreach and Capacity Building are the key words with which DSCI continues to promote and enhance trust in India as a secure global sourcing hub, and promotes data protection in the country.

www.dsci.in

DSCI Team

Rahul Jain, Principal Consultant

Rahul Sharma, Senior Consultant

Atul Kumar, Consultant

Designing & Branding

Priti Vandana, Manager-Marketing and Communications

ABOUT BSA

BSA | The Software Alliance (BSA) is a non-profit association and the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

ww2.bsa.org

BSA Team

Chris Hopfensperger, Director, Policy – APAC

David Ohrenstein, Director, Policy – America

Jared Ragland, Director, Policy – America

Yolynd Lobo, Director, Policy – India, APAC

Gouri Thounaojam, Sr. Manager, Compliance Programs & Policy, India, APAC

DATA SECURITY COUNCIL OF INDIA

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | **F:** +91-11-26155070 | **E:** info@dsci.in | **W:** www.dsci.in